Identifying and reducing technological contributions to end-user vulnerability

Lindsay J. Robertson
University of Wollongong

Follow this and additional works at: https://ro.uow.edu.au/theses1

University of Wollongong
Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au
Identifying and reducing technological contributions to end-user vulnerability

Lindsay J Robertson
MTech(Comp) BE(Mech) FIPENZ FIMechE CPEng CEng IntPE MIITP

This thesis is presented in fulfilment of the requirements for the award of the Degree of Doctor of Philosophy at the

University of Wollongong

11 Dec 2017
ABSTRACT

Essential life-needs are commonly supplied to end-users by complex and heterogeneous technological systems that have many potential failure-points and hence contribute vulnerability. The vulnerabilities under consideration in this study are those arising from the length and complexity of the technological system used to bring these life-needs to the end-user. Public awareness of dependence is evidenced at the corporate and national level by the expenditure of time and effort on infrastructure hardening, and at the individual level by a range of self-sufficiency and personal preparedness movements. Although the awareness of such dependence is commonly described using a term such as vulnerability, this term is imprecisely defined, and a lack of quantifiable measures hampers assessment of the absolute and relative value of methods that are designed to decrease vulnerability.

Published studies of infrastructure systems, supply chains, power distribution systems, communications and other networks have shown concern for system owners but little specific concern for the vulnerability of the end-user. Studies using network theory have considered homogeneous networks but these are not applicable to the heterogeneous technological systems that supply individuals. Risk analyses are highly dependent upon expert identifications of hazards and probabilities, and do not address situations in which there are intentional threats or long time-frames.

A review of published material indicated a need to consider the vulnerability of individual urban-dwelling end-users, and particularly apartment-dwellers, to the essential services that are available only via technological systems. The research question "For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used, and what reductions can be obtained by changes to the technological approach or configuration" was formulated to consider this need. A review of issues associated with the assessment of vulnerability also demonstrated the significance of the configuration of a technological system and a need to assess the contribution to vulnerability that is caused by heterogeneous technological systems. The number and the type of weaknesses in a technological system are shown to be a calculable property of the configuration of that technological system, and the metric of the number and type of weaknesses is well described by the term "exposure". The exposure metric is not dependent on the completeness of a brainstorming exercise to identify hazards, does not require any assessment of hazard probability and is
shown to be a valid measure of the contribution of the technological system to the end-user's vulnerability with respect to that specific system.

The research question is addressed by describing example cases in which services are delivered to a representative end-user. A number of possible examples were considered and six were chosen to represent a broad variety of goods and services, and a variety of technological systems used in the supply process. The exposure of the selected technological systems was examined. The investigations identified specific contributions to vulnerability and evaluated the effectiveness of possible approaches to reduce these vulnerabilities.

Measurement of the exposure of the examples and the hypothesised changes to the examples showed that this approach was capable of identifying contributors to vulnerability and of quantifying the reductions offered by hypothetical changes. Issues that were examined as hypothetical changes to the technological systems included the development of open-standards for the specification of intermediate products (allowing alternative providers), the introduction of highly decentralised options for services that are currently highly centralised and the application of re-purposable components. Analysis showed that application of the exposure metric generated insights and options that were not identified by risk analysis approaches; hence, this metric contributes to both practice and the academic field.

Hypothesised changes to the examples were assessed in terms of both effectiveness and nature. These changes were shown to offer significant reductions in vulnerability, achieved in some cases by reducing dependence on large and centralised systems and achieved in other cases by ensuring alternative sources for intermediate streams. Specific technological gaps, including the lack of power storage technology, were identified.

This study has demonstrated the contribution of technological systems to users' vulnerability. The study has also quantified this contribution to vulnerability for a range of cases and shown approaches for reduction of vulnerability.
ACKNOWLEDGEMENTS

My supervisors: Professor Katina Michael and Dr Albert Muñoz Aneiros.

Anne, my wife, and our kids, for their collective patience. My Mum and Dad – resting, but never forgotten.

Dr Tim Cousins (Director, Tim Cousins Australia Pty Ltd) for carrying out a thorough and independent review of the theoretical basis of the thesis.

Anonymous reviewers of journal and conference publications, for helpful comments.

Mr Brian Kouvalis BE F.IPENZ (Director, Sustainable Futures NZ Ltd) for an independent risk analysis of the exemplar sewage system.

Professor Pascal Perez and staff of SMART Infrastructure Facility for support and advice.

Dr M C Woodhall for expert proofreading.

Mr F Gleeson (yield engineer, data visualisation and training, Intel, Ireland) and Dr Grant Moule (Director, Moule Consulting) for valued comments.

Authors such as Isaac Asimov, whose inadequately appreciated imaginations catalyse ideas and inspire dreams!
PUBLICATIONS AND PRESENTATIONS


Research proposal presentation “Technological Contributions to End-user Vulnerability” to the School of Computing and Information Technology, Faculty of Engineering and Information Systems, July 2013.
# TABLE OF CONTENTS

1. Introduction ........................................................................................................... 1
   1.1 The research field ............................................................................................ 1
   1.2 The research topic ........................................................................................... 4
      1.2.1 Related research topics ............................................................................ 4
      1.2.2 Refinement of the research topic ............................................................ 7
      1.2.3 Research question ................................................................................... 9
   1.3 Illustration of the research field ..................................................................... 10
      1.3.1 Illustrative examples of the research field ............................................ 10
      1.3.2 Illustrative example of the research nature .......................................... 11
   1.4 Significance of the work .............................................................................. 12
      1.4.1 Significance of the research field ............................................................ 12
      1.4.2 Value of the research outcomes ............................................................. 12
      1.4.3 Application of the research results ....................................................... 13
      1.4.4 Original contribution of the work ......................................................... 13
   1.5 Scope of the work .......................................................................................... 13
   1.6 Conclusion ..................................................................................................... 14

2. Review of the literature ....................................................................................... 15
   2.1 Introduction .................................................................................................... 15
   2.2 Background to review of previous work ....................................................... 15
   2.3 Methodology for identification and review of the seminal literature .......... 17
   2.4 Definition of terms used in the literature ..................................................... 17
      2.4.1 Hazard .................................................................................................... 17
      2.4.2 Harm ..................................................................................................... 18
      2.4.3 Risk ....................................................................................................... 19
      2.4.4 Reliability-related terms ........................................................................ 24
      2.4.5 Vulnerability .......................................................................................... 25
      2.4.6 Exposure ............................................................................................... 33
      2.4.7 Resilience ............................................................................................. 33
      2.4.8 Robustness ............................................................................................ 36
      2.4.9 Survivability .......................................................................................... 36
      2.4.10 Critical reflections on published definitions ......................................... 38
   2.5 Application fields that are studied in the literature ................................... 39
      2.5.1 Society .................................................................................................. 40
      2.5.2 Ecosystems ............................................................................................ 40
      2.5.3 Infrastructure ......................................................................................... 41
      2.5.4 Supply chains ....................................................................................... 43
2.5.5 Computer and communication networks ........................................ 45
2.5.6 Power supply grids ........................................................................ 46
2.5.7 Water supply networks .................................................................. 47
2.5.8 Transport systems .......................................................................... 51
2.5.9 Analyses of interdisciplinary fields ................................................ 52

2.6 Published analytical techniques, related to technological vulnerability... 54
2.6.1 Analysis and classification of published techniques ...................... 54
2.6.2 Risk-based techniques .................................................................. 55
2.6.3 Accumulated scoring approaches ................................................. 56
2.6.4 FMEA and related approaches ...................................................... 58
2.6.5 Networks and graph theory ........................................................... 59
2.6.6 Hierarchical systems ..................................................................... 66
2.6.7 Cellular automata and agent-based systems................................. 66
2.6.8 Other approaches and theories ..................................................... 67

2.7 A taxonomy of published techniques ............................................... 69

2.8 Conclusions from review of published material ................................... 71
2.8.1 Summary of published material ..................................................... 71
2.8.2 Analysis of gaps in the literature.................................................... 72
2.8.3 Summary; development of research question ............................... 73
2.8.4 Research question ........................................................................ 73

3. Methodology ...................................................................................... 75
3.1 Introduction ....................................................................................... 75
3.2 Research phases ............................................................................... 75
3.3 Phase 1: development of theoretical basis ......................................... 76
  3.3.1 Theoretical basis ......................................................................... 76
  3.3.2 Criteria for theory ....................................................................... 77
  3.3.3 Validation of theoretical basis ....................................................... 79
  3.3.4 Implementation of analysis ........................................................ 79
3.4 Phase 2: development of initial data sets .......................................... 80
  3.4.1 Selection of examples for analysis .............................................. 80
  3.4.2 Definition of examples ................................................................. 84
3.5 Phase 3: analysis of examples ............................................................. 87
  3.5.1 Analysis outputs .......................................................................... 87
  3.5.2 Interpretation of analyses ............................................................... 88
3.6 Phase 4: hypothesising and testing changes to examples...................... 89
  3.6.1 Generating hypothetical changes ................................................ 89
  3.6.2 Analysis of effect of hypothesised changes ................................... 90
3.7 Phase 5: development of conclusions .......................................................... 91
  3.7.1 Answering the research question ......................................................... 91
  3.7.2 Development of general conclusions .................................................. 92
3.8 Conclusion of methodology description ................................................... 92
4. Development of a theoretical basis for measuring vulnerability ............... 93
  4.1 Introduction .............................................................................................. 93
  4.2 Context for a theoretical basis .................................................................. 93
    4.2.1 End-user services .............................................................................. 94
    4.2.2 End-user focus ................................................................................. 94
    4.2.3 Heterogeneous system description and representation ................. 94
    4.2.4 Static and dynamic contributions ................................................... 95
  4.3 Exposure as a theoretical measure of vulnerability ................................. 96
  4.4 Possible contributions to a measure from published techniques .......... 97
    4.4.1 Specific contributory aspects and gaps ......................................... 97
    4.4.2 Capabilities to be added to published approaches ......................... 98
  4.5 Development of proposed metric ............................................................ 98
    4.5.1 Measurement theory – the criteria for a metric ......................... 98
    4.5.2 Representation of a heterogeneous system .................................. 99
    4.5.3 Interpretation of data: defining and measuring the attribute ....... 101
    4.5.4 Clarifying the definition of the attribute ........................................ 103
    4.5.5 Interpretation of “exposure” values .............................................. 105
  4.6 Evaluation of proposed approach and metric ....................................... 106
    4.6.1 Representation ............................................................................. 106
    4.6.2 Completeness and uniqueness .................................................... 108
    4.6.3 Adequacy ..................................................................................... 108
    4.6.4 Precision ..................................................................................... 110
    4.6.5 Accuracy ..................................................................................... 111
  4.7 A consistent set of definitions and metrics .......................................... 111
  4.8 Conclusions ............................................................................................ 116
    4.8.1 A valid theoretical basis ............................................................... 116
    4.8.2 A theory of exposure ................................................................... 116
5. Definition of exemplar studies ................................................................... 118
  5.1 Introduction .............................................................................................. 118
  5.2 Description and verification of examples .............................................. 118
    5.2.1 Format of example descriptions .................................................. 118
    5.2.2 Granularity of example descriptions ......................................... 122
    5.2.3 Selection of analysis depth ......................................................... 123
5.3 Contribution of common subsystems

5.3.1 Internet communications system

5.3.2 Financial transaction

5.3.3 Road transport system

5.3.4 Other systems

5.4 Detailed description of examples

5.4.1 Example study #1: sewage system

5.4.2 Example study #2: collaboratively developed work information

5.4.3 Example study #3: local fuel supply

5.4.4 Example study #4: targeted first-aid

5.4.5 Example study #5: perishable food

5.4.6 Example study #6: essential specific medicine

5.4.7 Homogeneous system example

5.4.8 Dynamic system example: newspaper vendor example

5.5 Conclusion to the definition of examples

6. Calculation of exposure of examples

6.1 Introduction

6.2 Application of the analysis method to the examples

6.3 Analysis of examples

6.3.1 Analysis of contributory systems

6.3.2 Analysis of example study #1: sewage system

6.3.3 Independent risk analysis of sewage system

6.3.4 Analysis of example study #2: collaboratively developed work information

6.3.5 Analysis of example study #3: local fuel supply

6.3.6 Analysis of example study #4: targeted first-aid

6.3.7 Analysis of example study #5: perishable food

6.3.8 Analysis of example study #6: essential specific medicine

6.4 Application of theoretical basis to other examples

6.4.1 Application to homogeneous system examples

6.4.2 Analysis of the dynamic system (newspaper vendor)

6.5 Conclusions

6.5.1 Limitations

6.5.2 Specific conclusions for initial examples

6.5.3 Analysis of relative total exposure of actual examples
LIST OF FIGURES and TABLES

Figure 1: Development of research question .......................................................... 10
Figure 2: Research phases .................................................................................... 77
Figure 3 A representative complex technological system ..................................... 100
Figure 4 Rationalised representation of representative complex system .............. 101
Figure 5 Representation of system inputs and outputs ........................................ 101
Figure 6 Contributory system ............................................................................ 104
Figure 7 Generalised approach – contributory system .......................................... 104
Figure 8 Feedback loop representation ................................................................ 109
Figure 9 Illustration of selected terms ................................................................ 112
Figure 10 Example homogeneous system ............................................................ 145
Figure 11 Local storage effect ............................................................................. 175
Table 1: Published definitions of terms .............................................................. 32
Table 2: Application fields in the literature ......................................................... 39
Table 3: Classification of published techniques .................................................... 70
Table 4: Taxonomy of techniques related to risk and vulnerability ...................... 71
Table 5 Proposed definitions of key terms ........................................................... 78
Table 6: Identification and selection of examples for study ................................... 84
Table 7: Overview of examples for study ............................................................ 121
Table 8: Internet subsystems and exposure ....................................................... 152
Table 9: EFTPOS subsystems and exposure ....................................................... 153
Table 10: Sewage example subsystems and exposure .......................................... 154
Table 11: Work information example subsystems and exposure ........................ 156
Table 12: Local fuel supply example subsystems and exposure .......................... 158
Table 13: First-aid example subsystems and exposure ........................................ 159
Table 14: Fresh food example subsystems and exposure ..................................... 161
Table 15: Essential medicine example subsystems and exposure ...................... 163
Table 16: Effect of hypothesised changes to internet system ............................... 187
Table 17: Effect of hypothesised changes to EFTPOS system .............................. 191
Table 18: Effect of hypothesised changes to sewage system ............................... 195
Table 19: Effect of hypothesised changes to work information system ................ 199
Table 20: Effect of hypothesised changes to local fuel supply system ................. 202
Table 21: Effect of hypothesised changes to targeted first-aid system .............. 205
Table 22: Effect of hypothesised changes to perishable food system ................. 208
Table 23: Effect of hypothesised changes to essential specific medicine system .. 211
1. INTRODUCTION

1.1 The research field

Many life-needs that are essential to urban dwellers are supplied by complex technological systems. These systems have many weaknesses, which are potential failure-points and each of which is exposed to hazards. Risk management practitioners attempt to identify risks, but may fail either because a weakness is not identified or because a malicious and hence non-random hazard targets that weakness. The number of individual or combinatorial weaknesses in a technological system is shown to be a definable property of that technological system and a metric of the exposure, and thus a measure of the vulnerability contributed by that system. By studying both the number and the nature of individual or combinatorial weaknesses, for a number of real and modified technological systems, this study identified more secure approaches to supplying the representative end-users with goods and services that are essential to their lifestyle and livelihood.

The research must build upon a theoretical base and make a contribution to a theoretical field. A number of interdisciplinary theories address aspects of complex systems that assume multiple interacting and interrelated parts; these include general systems theory, sociotechnical theory, complexity theory, catastrophe theory and chaos theory. The scope of application of these theories will be examined, to determine the field to which this thesis contributes.

Sociotechnical theory is associated with organisational development and deals specifically with the interactions between employees and technology in their workplaces. It has origins in the Tavistock Institute in London, as reported by Long (2013). Sociotechnical theory emphasises the concept of "joint optimisation" as described by Cooper and Foster (1971) and proposes approaches to the design of task combinations and organisation structures in which the relationships between social, psychological and technical elements lead to both productivity and employee well-being. Task analysis, job rotation and process design are techniques that are commonly used, and typical results include increasing the responsible autonomy of teams, as proposed by Hackman and Oldham (1980), and the adoption of whole task concepts (i.e. job enlargement for employee groups, in order to generate a perception of the meaningfulness of tasks). Applications of sociotechnical theory assume that the
technology is capable of producing the goods or services for which it is designed, and consider people in their roles as operators of the technology. The current research considers people, who are the end-users, in their role as consumers rather than operators of technology, and considers the technology features that contribute to the secure operation of the technology, rather than assuming the capability of the technology. Hence, this research neither significantly derives from nor contributes to Sociotechnical Theory.

Chaos theory studies the dynamic response of systems in which the configuration and response functions are known and static, but are highly sensitive to the initial conditions as proposed by Alligood et al. (1997). Whereas chaos theory implicitly assumes that the outcome of a system is deterministic and continuous, catastrophe theory, e.g. as described by Igorevich (1992) and by Shil'nikov et al. (1999), applies mathematical analyses to systems in which the response functions to one or more variables are known, and thereby predicts the condition types and values at which the system dynamic response is unstable. The principles of catastrophe theory are used in some publications that are related to resilience, and authors such as Starossek and Haberland (2010) speak of "disproportionate collapse" in the context of civil engineering structures. Both chaos theory and catastrophe theory assume a known system configuration, with known response functions that are continuous within defined value ranges. It could be argued that representing a complex technological system with Boolean algebra is simply an example of a very specific and time-invariant response function and hence is an expression of catastrophe theory; however, both chaos theory and catastrophe theory are observed to be primarily concerned with dynamic responses and continuous response limits of a particular system rather than comparisons of the number and nature of technological weaknesses of a range of systems.

General systems theory was originally proposed by von Bertalanffy (1968, p. 32), who noted that "... there exist models, principles, and laws that apply to generalised systems or their subclasses, irrespective of their particular kind, the nature of their component elements, and the relationships … between them. It seems legitimate to ask for a theory, not of systems of a more or less special kind, but of universal principles applying to systems in general". Although end-user vulnerability to technological systems is within this definition, the general systems theory scope,
which is commonly categorised (Edson et al., 2016, p. 8) into three major domains, viz. philosophy, science and technology, is broader than necessary; for the purposes of the current research, it is necessary to consider only "systems engineering". Several definitions of "system" are found within the "systems engineering" field; the technological systems that supply goods and services to end-users are "systems" within the definitions presented by IEEE Std 1220-1998 "A set or arrangement of elements and processes that are related and whose behaviour satisfies customer/operational needs and provides for life cycle sustainment of the products." and ISO/IEC 15288:2008 Systems and Software Engineering – System Life Cycle Processes "A combination of interacting elements organised to achieve one or more stated purposes". NASA’s Systems Engineering Handbook (1995) states that "System engineering is a robust approach to the design, creation, and operation of systems … the approach consists of identification and quantification of system goals, creation of alternative system design concepts … selection and implementation of the best design". A similar definition is offered by Schlager (1956). Hitchins (2008) states that "Systems engineering (SE) is an interdisciplinary field of engineering, that focuses on the development and organization of complex systems. It is the art and science of creating whole solutions to complex problems".

In the context of the current research, the system goals are the delivery of defined services at defined service levels to an end-user; however, as the focus is on the vulnerability contributed by the complex technological systems to those system goals, the research can be considered to apply primarily to the development of engineering systems theory. The research develops approaches to the quantification and description of technological vulnerabilities, as these affect end-users; as such, it contributes to and extends a specific aspect of engineering systems theory and risk management practices.

The research has application to several related fields as follows. As the supply of goods and services that are essential to the selected group of end-users commonly involves critical infrastructure, the research contributes to the infrastructure research field, but is distinct because it is not focused on the security of the critical infrastructure per se. The supply of goods to the defined end-users generally also involves supply chains, however although this research has applications to theories of supply chain operation it is distinct because the focus is on end-user security as affected by the
complete technological system rather than the final supply chain security and profitability. A subset of the supply chain research field is the “network” field which includes computer networks and water supply networks. This research has applications to the network research field, but is distinct because it does not restrict consideration to networks that transmit only a single product.

1.2 The research topic

1.2.1 Related research topics

For the selected end-user group, i.e. high-density-housing urban dwellers, goods and services that are essential for their lives are delivered by complex technological systems. Researchers including Gheorghe and Vamanu (2004), Kumar et al. (2010), Khatri and Vairavamoorthy (2011) and Timashev and Tyrsin (2011), and publications such as AS/NZS ISO 31000:2009 and BS OHSAS 18001:2007, contribute to the large foundational base devoted to assessing the failure probabilities of specific technological systems, that are exposed to hazards for which historical measures of statistical probability exist or for which practitioners may assess probabilities based upon their experience. Authors including Chopade and Bikdash (2011), Gómez et al. (2011), Afgan and Veziroglu (2012) and publications including ISO GUIDE 73:2009 (Risk Management) propose definitions of “vulnerability” as a concept that correlates the state of a nominated technological system either statistically or in a "snapshot" with the probability of the occurrence of some hazard, to generate a more sophisticated assessment of the probability of failure. There is variation in the level of sophistication of the published approaches, from simple assessments of overall system loading by authors such as Günneç and Salman (2011) to more sophisticated correlations such as those proposed by Haimes (2006). Within this body of literature, the configuration and the components of the technological system are generally not described in detail, and are assumed to be static. The lack of definition of the system configuration and its correlation with outcomes makes it difficult to identify the major technological contributors to end-user insecurity, and makes it unlikely that these useful works will allow the effects of proposed improvements to be quantified and ranked.
The literature that includes significant comment on "resilience", e.g. by Nair et al. (2010), Shua et al. (2011) and Afgan and Vezioglu (2012), generally considers a nominated system’s time-domain response to a disturbance and implicitly assumes that the hazard level will not cause the system to fail. In the context of these publications, a disturbance is considered to be the occurrence of a hazard at a given level. A variation on this definition of “resilience” is provided by authors such as Strigini (2012), who seek to assess the hazard level or process state at which breakage occurs, and categorise that level as the “maximum tolerable disturbance”. Considerations of “resilience” under these definitions must assume a particular and complete technical system. The necessity of considering multiple components, each having complex response functions, can be expected to result in significant computational modelling. A further variation is proposed by Muñoz and Dunbar (2015), who consider the system properties linked to the capability of a supply chain to recover as an important contributor to its resilience.

The vulnerabilities of computer or communication networks have been studied by a large number of authors including Tu (2000), Doyle et al. (2005), Strigini et al. (2007), Misra et al. (2010), Liu and Zhang (2011), Idika and Bhargava (2012) and Lowis and Accorsi (2011), power distribution systems have been studied by Baldick et al. (2009), Buldyrev et al. (2010) and others, and water distribution networks have been studied by authors including Werbeloff and Brown (2011) and Yazdani and Jeffrey (2012). All these are examples of homogeneous systems that transmit a single product through a network. Such systems have been extensively studied using graph theory, which implicitly assumes that the same product or service is transmitted along all edges. This assumption is quite fundamental and is demonstrated by a simple illustration, as follows. Consider a graphical representation that shows node A linked to node B, which links to node C, and that also shows a link from node A to node C. An analysis that considers the effect of removing node B, or removing the link B–C, will be meaningless if A–C carries electrical power whereas A–B–C carries potable water. This limitation is particularly relevant for the current research because the systems under study are heterogeneous. As might be expected, some authors propose approaches that impinge upon broader topics: both Lewis et al. (2016) and Ray et al. (2016) and Ouффoué et al. (2017) consider systems that they characterise as “heterogeneous”, but in each case the description applies to the particular
characteristics of the nodes (equipment type and characteristics) rather than the
definition of what flows between the nodes. In each of the cases described by these
authors, that which flows between each node is essentially identical (digital
information).

Authors including Van Blaricum et al. (2005) and Chopade and Bikdash (2011)
recognise the significance, to the “vulnerability” of infrastructures, of interconnections
between different infrastructures, e.g. water and power; however, the analysis of real
infrastructural systems by modelling all interdependencies has generally been
considered to be impractical, although Haimes and Jiang (2001) have presented a
high level approach. Proposed simplification options have included overlaying
interacting homogeneous systems based on geography, such as the GIS database
approach proposed by Van Blaricum et al. (2005). The interactions of several overlaid
systems are assessed by modelling a geographically localised disaster, assumed to
cause failure of each homogeneous system node within range of the disaster. Other
options have included making various simplifications of the configuration and reliance
upon expert assessment of the probabilities of a hazard, as proposed by Yazdani et
al. (2011), and a coincidental weakness or the adoption of a system-of-systems
approach, as proposed by Gheorghe and Vamanu (2008). Although publications
dealing with “risk” and “vulnerability”, for example those by Gheorghe and Vamanu
(2004) and Khatri and Vairavamoorthy (2011), and publications including AS/NZS ISO
31000:2009, require assessments of the probability that a hazard will occur, they
seldom define a time-horizon during which the risk probability is assessed, and almost
always require expert assessment of probability.

Authors such as LePoire and Glenn (2007) show awareness of intelligently
misguided, intentional or directed hazards, and Wang et al (2015, p1674) note the
distinctive nature of intentional hazards and the "... significant uncertainties due to
behaviors of different rationality", but it is proposed that the distinction between
intentional hazards and random hazards has not been fully appreciated, and it has
not been appreciated that the consequence of this distinction is that a guided hazard
must be treated as having a probability of occurrence $p = 1.0$ in a consideration of
“risk”, because effort and intelligence will be used to target the hazard at an accessible
weakness. Intelligently misguided hazards can certainly not be assessed in the same
way as randomly occurring hazards with a statistical probability, but must be considered as “attacks”, as noted by Nair et al. (2010) and others.

1.2.2 Refinement of the research topic

“Vulnerability”, “risk” and “exposure” are key terms in this thesis; they occur throughout the reviewed literature and appear very commonly throughout this thesis. As a precursor to clarification of the research field, it is important to note that these terms are in common use, but with broad definitions such as those proposed in ISO GUIDE 73:2009. Furthermore, within specific fields, e.g. the definition of “risk” in the insurance field, some of these terms have acquired more tightly defined meanings. Some authors including Haimes (2006, 2011) have proposed somewhat tighter definitions but other authors, including Afgan and Veziroglu (2012) and Wang et al. (2012), have proposed variations or alternative definitions. A definition is essential if any measure of vulnerability is to be developed.

The clarification of the research opportunity noted that published material has not adequately considered how end-user supply security is affected by the configuration of the heterogeneous technological systems used. The clarification of the research opportunity also failed to reveal a metric that adequately quantifies the vulnerability of such technological systems. As every hazard must necessarily be linked to a weakness in a technological system, and because the probability of a hazard occurring must tend towards $p = 1.0$ with time, or be treated as having $p = 1.0$ in the case of directed hazards, the number of weaknesses in a technological system is a critical factor in determining the contribution of a particular technological system to the end-user’s vulnerability. This issue has been noted by Mishkovski et al. (2011) in the literature related to computer networks, but has not been explored for heterogeneous systems that are typical of those that deliver goods and services that are essential for the lifestyle of the identified group of end-users. Specifically, a more rigorous and quantitative approach to characterising the technological vulnerability of end-users makes it possible to quantitatively compare systems and to quantitatively compare alternative proposals for modifications to a system. The approach needs to be demonstrated by applying a range of examples of technological systems to the delivery of selected goods or services to an urban end-user, and quantifying those technological characteristics that specifically contribute to vulnerability at the end-user
level. Chapter 4 of this thesis progressively develops and justifies the concept of the vulnerability and exposure of a technological system, and defines this as the number of critical weaknesses in that technological system. A theoretical basis is developed, an approach for implementation is proposed and evidence to demonstrate that the proposed approach does offer answers to the research questions is presented.

Having developed a theoretical basis for evaluating the contribution of technological systems to end-user vulnerability, a methodology for selecting examples of technological systems that supply goods or services to end-users, and for applying this theoretical basis to these example studies, is developed. Each technological system that is studied is described in sufficient detail to demonstrate how the current system supplies a specific product or service to end-users.

A measure of the technological vulnerability is calculated for each of these examples, thus effectively modelling the working of the example system. This measure, which is labelled as the system “exposure”, measures the number of n-component/stream failures that will cause failure of the system’s designed output, and the $\{E_1, E_2, .. E_n\}$ exposure metric is shown to offer a valid measure of the vulnerability that the technological system imposes on the end-user. When operating within design parameters, technological systems produce outputs as long as inputs are available. For real systems, operation within design parameters cannot continue indefinitely and maintenance, i.e. replacement of generally pre-identified and commonly substitutable components, is required periodically. Over more extended timeframes, technological systems can also reach the point where they are inherently incapable of performing their function due to a need for maintenance, and eventually will also reach a point where redesign or replacement is required. These three time-frame scenarios are distinct and have separate implications for the end-user’s vulnerability. The relevant time-frame is defined for each example studied in this work.

The analysis then considers alternative technological scenarios, including alternative configurations and components, for each of the examples, and examines the effect of each change. Based on the hypotheses developed, several alternative technological configuration scenarios are examined within each study example, and allow testing of hypothetical approaches for exposure reduction. Each example study and each related scenario therefore generate a measure of the technological system’s exposure; this allows a quantitative comparison between the levels of exposure.
determined for each of the example studies, and conclusions on the relative vulnerability of end-users to the current technological systems. Each example study and each related scenario also allow an analysis of the specific processes and inputs that contribute to the exposure.

The technological configuration issues that have contributed to the calculated metrics of exposure are compared between each of the example study results, allowing the development of hypotheses for the general reduction of vulnerability. It is expected that the exposure of many technological systems could be significantly reduced by a small number of techniques, including open specification of intermediate products that would allow many alternative suppliers of these, decentralisation and localised generation of intermediate products, and some specific technologies that have inherently short supply chains. As several types of technological system are proposed as the basis of the example cases, the effect on the end-user "exposure" of generic approaches to reducing "exposure" can be tested.

1.2.3 Research question

The process of developing the research question is shown in Figure 1 and is presented in detail later in this thesis. As a result of the process illustrated in Figure 1, the research question of this thesis is:

For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used, and what reductions can be obtained by changes to the technological approach or configuration?
This research question can be broken down into two parts, identified as RQ(a) and RQ(b).

RQ(a): For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used?

RQ(b): For goods or services delivered to end-users, what reductions in vulnerability can be obtained by changes to the technological approach or configuration?

1.3 Illustration of the research field

Two examples are described simply to provide an introductory and high-level illustration of the field of interest of this thesis, and also an illustration of the types of conclusions that are expected. Aspects of these illustrative examples are examined in the thesis.

1.3.1 Illustrative examples of the research field

An initial review of the technological systems used to dispense petrol to an end-user at a petrol station, showed that simple financial transactions were required at several levels – purchase of delivered goods, purchase of power, payment of wages and the purchase of wholesale goods, and hence were a significant subsystem requiring consideration. At present, such transactions commonly require Electronic Funds Transfer at Point Of Sale (EFTPOS), which requires last-mile communications,
datagrams, local routers, interbank communications and centralised bank transaction verification. Alternative approaches, including the use of gold coins, “bitcoin”, e-wallet, cash or cheque media, would each involve significantly different technological systems for usage, and would have significantly different numbers of points of exposure.

The Longnow Foundation’s (02016¹) “Rosetta” project has created an extremely durable data-storage disk containing high-density information that can be read using a microscope. In contrast to this approach, media attention has been drawn to the real danger that long technology chains using proprietary specifications for intermediate products will result in information, which is the “service” provided by this example, becoming unavailable to the end-user. This phenomenon has been noted as a potential cause of a “digital dark-age”, in which much information becomes effectively unavailable.

For both the financial transaction, and the information retrieval examples, it is proposed that quantifying the number and the nature of the exposure points in the base case will reduce both user vulnerability and system exposure, and it will be very useful to consider alternative technological approaches for delivering the same goods and demonstrating the changes to the number and nature of the exposure points. The value of such review is dependent on a consistent approach, and on adequately addressing the practical difficulties: these issues are considered in section 4.5.4 of the thesis. Having taken a consistent approach, and addressed the practical difficulties as proposed, it is considered that a review of even two examples suggests that it may be possible to identify some generalised approaches to reducing technological contribution to end-user exposure.

1.3.2 Illustrative example of the research nature

In the course of refining the research scope, a pilot study was carried out. This study attempted to quantify a measure of exposure for a specific example case, viz. the supply of petrol to a patron of a petrol station in New Zealand. A simple approach was used to codify the processes and streams involved, and to identify and quantify

¹ For an organisation whose projects include the design of a “10,000 year-clock”, the date format “02016” is used instead of “2016”.
the level of exposure. Although a more detailed and rigorous approach is used in the analysis of the example cases, the pilot study indicated that the proposed approach is practical and can generate valid metrics. The research examines this and all other example studies in depth and proposes and examines variations on elements, to evaluate the effects of hypothesised changes; such variations were not proposed or examined in the course of the pilot study.

1.4 Significance of the work

1.4.1 Significance of the research field

Infrastructure exists in order to deliver goods and services; however, it is argued that the focus should be on end-user security rather than on critical infrastructural security per se. The level of research and expenditure aimed at improving the security of critical infrastructure is ample evidence of the importance of delivering goods and services to end-users. Many nations expend significant monies on infrastructural security; specific governmental functions are commonly dedicated to this. This is evidence of the significance attached to the functioning of critical infrastructure. Proceeding from this observation to establishing the significance of this research requires only the establishment of a distinction between the focus of critical infrastructure and the focus of this research. The observation that the critical infrastructure field does not specifically examine implications for end-users provides this proof. The special 2013 section of IEEE Technology in Society Magazine, devoted to risk, has highlighted the issue and, by acceptance of a guest editorial by Robertson and Michael (2013), has provided further indication of public interest in the research topic. It may be noted that major journals, including Elsevier’s Technology in Society, IEEE’s Technology and Society, the Journal of Science, Technology and Human Values” and others, are devoted to researching the influence of technology on society generally. It can reasonably be proposed that the existence of these journals indicates a level of interest in the research topic.

1.4.2 Value of the research outcomes

To establish the value of the research requires a confirmation that the research offers some incremental and definable value and hence contribution to the field. The research develops and demonstrates a reproducible metric of the exposure of a
specified technological system that is intended to deliver goods or services to a specific category of end-user. Such a reproducible metric allows the ranking of technological systems according to their level of exposure, and allows options for a reduction in exposure to be assessed. Both of these capabilities contribute to economic value. The research demonstrates utility that is not available from current techniques, and the experience gained identifies aspects for future refinement.

1.4.3 Application of the research results

The reduction of the vulnerability of an end-user by reducing the exposure of a technological system supplying essential goods or services is inherently valuable to each user. An approach that refines the sources of vulnerability and allows a public body (that is ultimately responsible to end-users for the efficient delivery of services) to assess the relative value that can be achieved by alternative approaches is valuable for prioritising financial and human resource usage.

1.4.4 Original contribution of the work

This thesis analyses material that is not adequately covered in the literature, and demonstrates two specific gaps:

(a) The existence of an approach for quantifying the technological vulnerability that a heterogeneous technological system incurs for users dependent on goods or services that the technological system produces.

(b) The need for an emphasis on end-user(s), rather than on either a corporate supply chain or a national infrastructure.

The development and application of an exposure metric for heterogeneous systems addresses these gaps and is a contribution to the systems engineering field. Specific and general conclusions regarding approaches to the reduction in vulnerability for end-users demonstrate a valuable application within the systems engineering field.

1.5 Scope of the work

Following development of the research questions, the research initially develops and validates a method for quantifying technological vulnerability. The work then proceeds by selecting several exemplars of technological systems by which
goods or services are delivered. These exemplar systems are described and are shown to be representative of common systems for the delivery of the selected services. The vulnerabilities presented by these exemplar systems are analysed, and hypothetical improvements are also analysed. From these analyses, detailed and also generalisable conclusions are derived.

The research seeks to identify the extent to which end-users’ security is “exposed” by current technologies for the delivery of goods and services; such weaknesses are defined as those that are inherent in the configuration and specification of the technological systems, and not those that are the dynamic response of those systems to random inputs, which relate to the modelling of dynamic responses. The research therefore does not propose to include dynamic modelling; the theoretical basis for the research includes a more detailed justification of this concept.

1.6 Conclusion

The Population Reference Bureau (2009) reports that about 50% of the world's population currently live in cities, compared with an estimated 14% in 1900 and a projected 75% by about 2050. Efficient technological systems for the production and distribution of goods and services have not only enabled city living, but have also created dependence upon those systems for the continued lifestyle of these city dwellers. This issue has been widely recognised, but significant aspects have not yet been fully studied. This work examines the extent of vulnerabilities that are incurred by typical urban dwellers by examining a range of typical technological systems. The research considers existing approaches and identifies a specific field requiring study. Following a study of typical examples, some general conclusions emerge and provide insight into approaches to reducing the vulnerability of individuals. Initial decisions to focus on individual urban-dwelling end-users, technological systems and static analyses were made and are justified.
2. REVIEW OF THE LITERATURE

2.1 Introduction

The literature review is designed to establish the published underpinning of the proposed field of study. As the field of study is initially broadly defined and interfaces with other fields of study, the literature review considers published material that is peripheral to as well as central to the field of study. The analysis of the literature allows clarification of the scope of the study and confirms its unique contribution. As developed in Chapter 1, the research field and the research topic emphasise technological vulnerability and the end-user.

The research topic and research field also propose to assess options for decreasing end-user vulnerability; to meet this criterion, the evaluation of vulnerability must be robust and defensible, and sufficiently precise to allow alternative technological paths to be evaluated. Specifically, the technological characteristics, configuration or other distinguishing features of any technological system must contribute to a measure of end-user vulnerability in such a way that changes to these inputs are reflected in the numerical value that is generated – and hence, assuming sufficient precision, allow the exposure of one technological system to be compared with that of another, or variants to be compared with the original. Guan et al. (2011, p. 151) note this issue, commenting that “... the ability to determine whether or not risk reduction is achieved when modifications are made is important”. Werbeloff and Brown (2011) speak of the Australian water system principle of “security through diversity”. The proposed research may conclude that a diversity of supply options is a key to decreased vulnerability – but the proposed research will come to this conclusion by a researched process, rather than adopting it as an initial philosophy.

2.2 Background to review of previous work

Four broad groupings of persons who experience some vulnerability to technological failures are identified: individual, community, nations and corporates. The significances of technological failures for each of these groupings are significantly different. At a national level, “developed countries” have interconnected networks for the delivery of power, communications, transport and also sewage and water supplies. The national functioning and economic well-being of such countries is
currently dependent on those technological functions. Media attention shows that nations are aware that breakdown of their major infrastructure would be harmful – and that this threat is perceived to increase as systems become larger and more interconnected. Corporates generate profit by using technological functions and existing services and supply chains. They are always aware of risks to their profit and revenue streams, and use their resources to maximise profit. In contrast, individuals and small communities have a wide range of needs. Currently, most individuals, particularly in developed countries, depend upon a range of long "supply chains" and many technological processes for their basic needs. Unlike corporates or nations, individuals and communities generally have limited deployable resources or alternative sources of supply. The regular emergence of "survivalist" movements, the commonly observed interest in cottage skills and the regular emergence of concerns (whether well founded or not) about the technological breakdown of "society", as noted by authors such as Tainter (2003), are all considered to be responses to a sense of personal insecurity arising from a dependence on matters beyond the individual’s abilities or resources to control.

The literature review establishes the existing foundational basis of published material on the topic and refines the scope of the proposed study. The literature review seeks to clarify an original and valuable contribution, and to establish the foundations upon which the contribution can build. In order to do this, both the underpinning and the new aspects of the proposed field of research must be described. The proposed field of study has several distinctive aspects, and the literature review establishes the underpinning for each. These aspects are as follows.

(a) The study explores the vulnerability of the end-user, rather than the profit of a corporate entity operating a supply chain or of an infrastructure owner.

(b) The study seeks to "quantify" its outcome; terms that are quantifiable and approaches to quantifying vulnerability are important.

(c) Many networks are homogeneous, e.g. a communications network comprises only optical fibres or coaxial cables, and transmits only a single service, such as data packets. In complete contrast, the goods and services upon which the end-user relies incorporate processes that take inputs and create new outputs, and hence are not homogeneous. Within this work, such networks are identified as inhomogeneous or heterogeneous.
(d) The requirement to evaluate the ways in which technology contributes to vulnerabilities implies the identification of generic features that contribute to the vulnerability of existing systems, and is not constrained to increasing the resilience of specific systems.

(e) Whereas natural disasters and major environmental failures may trigger technological failures, the identified field of study addresses “technological systems”, regardless of geographical proximity, in contrast to “disaster survival” or “disaster management”, which relate to multiple systems within a defined geography.

2.3 Methodology for identification and review of the seminal literature

A list of terms, and regular expressions derived from them, was derived from the description of the research field and formed the basis of a search strategy. The literature survey commenced with keyword searches of major academic databases, e.g. Scopus. Synonym searches were used because many variations of keyword definitions were found and, in many cases, terms were found to be poorly defined. The initial search produced a large number of papers and their value to the proposed field was assessed. From that group of publications, a more closely targeted group was identified; key authors were also identified. Finally, the papers were categorised and the references from seminal works were reviewed where relevant. The review was considered to be fit for purpose when key references from newly identified papers were primarily to publications already identified.

2.4 Definition of terms used in the literature

Terminology such as risk, hazard, vulnerability and resilience is in common use, but is linked to a range of definitions. As the clarification of terminology, for the purposes of this research, became a central topic of the thesis, understanding the published definitions was a significant aspect of the literature review. The relevant terms, and their published descriptions and definitions, are summarised as follows.

2.4.1 Hazard

The UN’s “Total Disaster Risk Management Approach” (Guzman (n.d.)) provides the following definition: “Hazard is a phenomenon, an event or occurrence
that has the potential for causing injury to life or damage to property or the environment”. Similar definitions are stated elsewhere by authors such as Scawthorn et al. (1999). In contrast, ISO GUIDE 73:2009 “Risk Management — Vocabulary” defines Hazard (3.5.1.4) as a "source of potential harm". The use of the word “potential” implies that there is not an unavoidable causality between “hazard” and “harm”. That definition implicitly allows the concept of either a de minimus for the level of hazard, or the existence of as-yet-undefined parameters that result in a “hazard” causing, or not-causing, a “harm”. If the published definitions of “hazard” do not establish an immediate and causal relationship between hazard and harm, then it is important, within this thesis, to determine why, and to define the logical “gap” – i.e. what aspect must be additionally defined to establish the immediate and causal relationship between hazard and harm. Researchers such as Wang et al. (2012) note that different “hazards” may fall within different time-frames, although their paper considers only “long term” and “focussed” categories.

A number of relationships between hazard and harm are presented in the literature; clearer definition of these relationships is central to the topic of this thesis and will be developed in following sections. Several published relationships can be listed.

- A statistical probability that a hazard causes a harm, e.g. Russian roulette.
- A dependence on the extent to which the hazard can be prevented or mitigated. It can be noted that acute appendicitis is very unlikely to be fatal if even basic medical or surgical facilities are available.
- A dependence on the level of the hazard – carries the implication that, below a given level of hazard, mitigation is guaranteed; otherwise mitigation is impossible.
- A case where a “hazard” will always and inevitably cause a harm, e.g. by the exploitation of a software flaw.

### 2.4.2 Harm

Haimes (2011) considers that “harm” is synonymous with damage and, by extension, hurt, disaster or loss. Haimes (2011) therefore considers that “harm” is the inevitable, actual result of a hazard that is outside a tolerable limit. Some publications such as AS/NZS ISO 31000:2009 effectively define “risk” as “potential harm”. Many
publications have considered harm in terms of networks such as water supply systems, electricity distribution systems or communications networks. Günneç and Salman (2011, p. 502) note that:

“Connectivity is defined as the probability that nodes of a network remain connected, whereas network performance targets the functionality of a network. Connectivity measures include (i) Two-terminal reliability (the probability of a path existing between two specific nodes), (ii) All-terminal reliability (the probability that every node is connected with every other node), and (iii) K-terminal reliability (the probability that every pair of nodes in a specified node subset K is connected), as described in Konak & Smith (2006)”.

These researchers effectively equate “harm” to the network with loss of connectivity, and hence these definitions of connectivity do serve to refine the concept of “harm” to a network. Yazdani and Jeffrey (2012) note, in the context of water distribution systems, that many real networks have few input nodes and many output nodes.

2.4.3 Risk

The published literature includes a variety of definitions of “risk”, and the variety is notable, considering the common usage of the term. Aven and Guikema (2015, p. 2162) state that risk is defined by considering a set of scenarios, and for each the probability of that scenario, and the consequences of that scenario. Similarly, BS OHSAS 18001:2007 states that "... risk is a combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury or ill health that can be caused by the event or exposure(s)”. These definitions are commonly used by risk practitioners, combining probability with the magnitude of the consequences.

AS/NZS ISO 31000:2009 “Risk Management – Principles and Guidelines”, defines risk as the “effect of uncertainty on objectives”. In this definition, uncertainties include events that may or may not occur, and uncertainties caused by ambiguity or a lack of information. “Objectives” is plural, and “uncertainty” encompasses all possible factors, across all possible circumstances, i.e. the definition is extremely broad. Similarly, ISO GUIDE 73:2009 “Risk Management — Vocabulary” defines risk as the “effect of uncertainty on objectives” and also (section 3.6.1.3) as a “structured statement of risk usually containing four elements: sources, events (section 3.5.1.3),
causes and consequences" A risk source (section 3.5.1.2) is an "element which alone or in combination has the intrinsic potential to give rise to risk". An event (section 3.5.1.3) is the "occurrence or change of a particular set of circumstances". A hazard (section 3.5.1.4) is a

"source of potential harm - NOTE Hazard can be a risk source (3.5.1.2). Likelihood (3.6.1.1) is defined as the "chance of something happening" - NOTE 1 In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability (3.6.1.4) or a frequency (3.6.1.5) over a given time period".

Exposure (section 3.6.1.2) is defined as the "extent to which an organization and/or stakeholder (3.2.1.1) is subject to an event" Consequence (section 3.6.1.3) is defined as the "outcome of an event (3.5.1.3) affecting objectives". Probability (section 3.6.1.4) is defined as the "measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty". For insight into the origins of the term, the Oxford English Dictionary cites the earliest use of the word in English (with the spelling as risque) as from 1621, and with the spelling as risk from 1655. It defines risk as: “(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility”. It is noted that this definition emphasises probability, rather than certainty of “harm”.

Khatri and Vairavamoorthy (2011) conclude that risk can be described in the form of Equation 1.

Risk is a function of \{\text{Likelihood}, \text{Severity}, \text{Vulnerability}\}

Equation 1

This definition is similar to the OHSAS definition, but adds the concept of "vulnerability". Kumar et al. (2010, p. 3717) study supply chains. They state that "[r]isk in supply chains can be defined as the potential deviations from the initial overall objective that, consequently, trigger the decrease of value-added activities at different levels". Gheorghe and Vamanu (2004, p. 614) state that
"the risk of a disruptive event equals the probability of the event's occurring, times the measure of event consequences powered to a subjective consequence perception exponent... Webster's Dictionary (e.g. the Landoll, Ashland, Ohio, USA edition, 1993) retains, in the entry for “risk”, the instrumental ingredients of the formula. Indeed, according to that source, there are: ’... Risk (noun) – A chance of suffering or encountering harm or loss”.

Timashev and Tyrsin (2011) develop the concept of system entropy as a more complete definition of the risk of failure. This definition is applied to a pipeline, with several known defects, any of which could cause failure within a given time interval if (over)pressure is known. This definition is useful and, in principle, could be extended to other systems, but the cases in which it is practical to gather such data are limited. Practitioners in the insurance industry identify an object that is the subject of potential harm as “the insured risk”; although this definition has very limited acceptance outside the insurance industry, it serves to illustrate the breadth of definition that exists.

There are two primary distinctions within the published definitions of risk. The first relates to the “vulnerability” aspect. Some researchers recognise three factors – the probability of a hazard, the vulnerability to that hazard and the magnitude of the consequence; other authors recognise only two factors, viz. the probability of a hazard and the magnitude of the consequence. This difference is simply a question of granularity of definition. The "two factor” group implicitly defines the "event" as one that exceeds the resilience of the system, and so inevitably results in the consequential harm. The second difference relates to the difference of focus between consequences and causes. The definition offered by Gheorghe and Vamanu (2004) considers the effect of one, well-defined event on the consequences; in contrast, definitions such as those in the Oxford English Dictionary and AS/NZS ISO 31000:2009 implicitly consider the cumulative probabilities of all of those hazards, which individually would be associated with the quoted consequence.

Based on the above definitions, four parameters are commonly assumed to contribute to “risk”: defined harm, defined hazard, time-frame (implicit) and “vulnerability”. It is useful to examine each of these parameters individually. Defined hazard must include a metric; most quantitatively defined “hazards” exist continuously at some nominal level, and their significance can be assessed only if a metric is quoted. However, qualitatively, defined hazards can be assigned a Boolean level (1 or 0) of existence. The "probability" of a defined hazard can be properly defined only
if a set of known environmental parameters is defined; it could then be proposed that, if a large number ('n') of parallel universes existed, each having precisely that same set of known parameters, and if a given hazard occurred in 'y' of them during an observation period of 'm', then the probability of that hazard is expressed in Equation 2.

\[
\text{Probability (Hazard, known parameters, m) = } \frac{y}{n}
\]

Equation 2

If the assumption is made that hazards occur randomly, then a treatment that models stochastic hazard events and corresponding mitigation measures could be applied as described by Dimitrova et al. (2015). Assumptions of randomness are problematic, however: If the probability of catastrophic failure of aircraft structures in the era when the British “Comet” went into service had been considered, a statistical measure might have been developed. Once the phenomenon of metal fatigue was clearly understood and the knowledge applied, a statistical probability of catastrophic failure remained, but the shape of the probability curve was changed. Effectively, one of the previously unknown factors had become known, and was hence removed from the definition of that “risk” – but, as many unknown factors remained, a “risk” could still be computed. The concept of “risk” actually sidesteps the issue of whether hazards are inherently deterministic, but with factors as-yet-undiscovered, or whether hazards are inherently probabilistic in the sense used in the quantum mechanics field. For the purposes of this work, “risk” can be defined adequately in terms of a probabilistic function of properties that are not defined. For that subset of cases in which simple parameters can be measured across a very large number of superficially identical objects, e.g. failure rates of light bulbs, it might be claimed that historical records can legitimately be used to predict the future probability profile – although, even for this stereotypical case, whether environmental variables such as global warming will affect the relationship between historical record and future risk might be questioned. For the vast majority of cases, this approach is at best impractical and, commonly, it is actually meaningless. After many space-shuttle launches, the Challenger was destroyed when a solid rocket casing joint failed. Computing the probability of failure, immediately after the loss of the Challenger, based on historical records would be useless because future launches did not proceed at the
temperatures that caused the failure of the solid rocket seals. After many more launches, another shuttle was lost because of a heat-shield breach; computing the failure probability after that event may have been slightly more accurate because no effective method for identifying or fixing future heat-shield breaches was found. The key issue is that, once known factors are eliminated, engineers very seldom have enough historical data to predict risk with other than a very wide margin. The difficulties of assigning probabilities to rate events is well-known, and in the first issue of the Risk Analysis journal, Weinberg (1981, p. 5) speaks of large and rare failures, and notes that "in neither instance is it practical to build enough nuclear reactors or DC-10's to observe the failure rate".

Vulnerability to a defined hazard effectively represents some assessment of the causality linking a defined hazard to a defined harm. Conceptually, this could be expressed as a probability, or as a trigger or maximum tolerable level for the hazard. The vulnerability to a defined hazard will also be dependent on the precise state and configuration of the current system. It must also be observed that the same defined harm may be linked to more than one defined hazard. This is a significant issue and one that must be addressed later. It may further be observed that a time-frame must be defined, in order to assess the probability of a given hazard occurring; with no time-frame, it can be assumed that every hazard will exceed the tolerance level at some time. This issue is particularly significant to the scope of this thesis. Finally, the initial system state would need to be defined since for a particular hazard, over the same time-frame, if the effect of a defined level of hazard is to be assessed. This can be illustrated by considering a power line that is operating at 99% of its rated capacity; a "hazard" comprising a 2% demand spike will cause a “trip” and hence a harm, whereas the same demand spike would cause no harm to the power line if it had been loaded at only 90% of capacity. Using the same example, it can be noted that other hazards may be unaffected by the loading of the power line, and hence would have different vulnerability levels.

Korombel and Tworek (2011) have researched (p 51) the "assessment of investment project risks in business practice" and conclude that risk management should combine qualitative and quantitative information, yet conclude by describing a classical risk assessment tool.
The extent and breadth of the risk assessment and analysis field make a simple summation difficult. It is reasonable to note that although techniques such as Dephi method (Hallowell 2010) can be used to improve qualitative assessments of risk, even seminal authors such as Aven (2012, p. 1655) note that the risk field lacks clarity on many concepts and principles. In a later paper, Hansson and Aven (2014) review the process of risk assessment and while noting the development of the field, continue to note the difficulties of both qualitative assessments and broad consensus.

2.4.4 Reliability-related terms

A number of commonly used terms measure system performance. These measures are commonly reported historically, e.g. a power station’s availability is commonly reported in an annual report. These are well-accepted terms, are often defined carefully and have contractual significance. Such terms include “Reliability”, “Mean time between failures (MTBF)”, “Mean time to failure (MTTF)” and “Mean time to repair (MTTR)”, generally as proposed by Wang and Doucette (2016). MTTR is commonly stated in simple terms of the time taken to repair the component or system, or to restore functionality following the observation of a failure. Predictions of future performance may be attempted on the basis of historical observations of availability and the MTBF, but are imprecise because the conditions under which the historical values were observed are unlikely to be repeated exactly. These are system performance metrics, and are included for completeness despite the limited applicability to end-user vulnerability.

Reliability: Yazdani et al. (2011, p. 1574) state “The reliability of a water distribution system is usually defined as the probability of non-failure over a given period of time”. This definition assumes some particular system, under some particular operating conditions. In engineering systems, reliability is often expressed as the MTBF or the Mean time to repair (MTTR), which is the average, over a large sample of an identical and defined component or system operating under similar conditions, time to failure. Not only are the definitions of probability different, but the assumptions are also distinct. The MTBF is the result of observing a population of identical systems under similar operating conditions, whereas Yazdani et al. (2011) implicitly define a period of time and a unique system and operating conditions.
**Design redundancy**: Yazdani and Jeffery (2012) propose a concept of design redundancy in terms of the presence of independent paths available in the case where main supply paths fail. For a single component, a second identical component installed in parallel offers a redundant capacity. There are some specific cases, e.g. pipeline isolation valves, where components installed in series are used sacrificially to provide redundancy.

Engineering systems are sometimes specified to contain “N–1” or “N–2” redundancy; these terms are commonly assumed to mean that there is no single failure (N–1) or no two individual failures (N–2) that can cause a system failure. It might also be observed that these criteria are almost impossible to achieve in practice; few power stations will have a second control room, a second cooling water outfall or a duplicate high voltage switchyard. Assessing the effectiveness of redundancy is also difficult; two valves installed in parallel may be exposed to overpressure or corrosion from the same source – and so the existence of a “redundant” valve does not guarantee that the failure rate is halved. External alternative sources represent a practical approach to decreasing the inevitability of a particular “harm”; as an example, if a process depends on hydrogen generated by an electrolysis plant, a connection enabling supply from compressed hydrogen bottles will clearly mean that a hydrolyser failure does not necessarily cause a system failure.

**Availability**: In the context of engineering systems, e.g. a power station, “availability” is often contractually guaranteed in terms of (MTBF – MTTR)/MTBF. Availability is generally considered to represent the proportion of time for which a system is available, assuming normal scheduled maintenance.

### 2.4.5 Vulnerability

Published definitions of “vulnerability” include that of Wang et al. (2012, p. 3328), who state that “vulnerability is seen as a global system property that expresses the extent of adverse effects caused by the occurrence of a specific hazardous event”. This definition defines vulnerability as a ratio of the harm to the hazard, and can therefore be distinguished from the maximum tolerable disturbance concept, which does not assess the significance of the “harm” arising when tolerable disturbance levels are exceeded. Afgan and Veziroglu (2012) define vulnerability, simply and without detailed justification, as the opposite of resilience. ISO GUIDE 73:2009 “Risk
Management — Vocabulary” defines vulnerability in Section 3.6.1.6 as "... intrinsic properties of something resulting in susceptibility to a risk source (3.5.1.2) that can lead to an event with a consequence”. Chopade and Bikdash (2011) describe the vulnerability of an infrastructural system in terms of the probability that a disturbance causes some stated minimum consequence within a defined interval of time. This is very close to the "maximum tolerable disturbance” definition of vulnerability, although with reference to probability. In this context, Chopade and Bikdash (2011) do note that, for a power system, the consequence would be described in terms of loss of capacity (MW) or of power delivered (MWh). This is very specifically a network-oriented approach; if the normal charge for 1 MWh of power was applied, a dollar value could be quantified. If the power outage caused death because an individual’s heart–lung machine failed, this would simply not be registered. These authors present consequences as an aggregation of the loss: probability product.

Gómez et al. (2011, p. 215) offer definitions for vulnerability, illustrating both the number of issues to be considered and the lack of a single accepted and clear definition. They suggest that "... vulnerability is a concept tightly related to a hazardous event (i.e. there is not vulnerability if there is not a threatening event)”. These authors consider that a complete approach to vulnerability will need to model all attack vectors and will generate attack graphs. These authors also discuss (p. 216) the possibility that Bayesian approaches, which use risk analysis and the concept of survivability, i.e. the system performs when the hazard is within a given level, may be useful. The third approach discussed by these authors uses graph theory metrics as measures of vulnerability. Adger (2006, p. 269) quotes "The central idea of the often-cited IPCC definition (McCarthy et al., 2001) is that vulnerability is degree to which a system is susceptible to and is unable to cope with adverse effects”. Papers related to computer systems, e.g. Lowis and Accorsi (2011), commonly equate “vulnerability” with the existence of a software design flaw that can be exploited by a malicious person. A subtle distinction should be drawn here: for a pipeline with various faults, and corrosion rates that have probabilistic functions – as noted by Timashev and Tyrsin (2011) – failure at a particular time has only a probabilistic function. In contrast, a software weakness, such as a stack overflow opportunity, will cause the “harm” every single time a malicious operator chooses to exploit this “vulnerability”. Khatri and
Vairavamoorthy (2011) represent an urban water system using a system-of-systems approach. They propose a relationship as expressed in Equation 3:

Risk is a function of \( (\text{Likelihood}), (\text{Severity}), (\text{Vulnerability}) \)

Equation 3

Using a relationship as expressed in Equation 3, they establish the "vulnerability" quantity by reference to the configuration established in the "system-of-systems representation". Actual values seem to be derived using a modified “Delphi approach” rather than as a quantitative value derived from the configuration and components of the system. According to Khatri and Vairavamoorthy (2011), resilience describes the ability of a system to recover from failure to some state that is acceptable (without specifically defining acceptable). These authors effectively propose an average-unplanned-outage duration as “gamma”. They also provide a formula for system vulnerability that closely equates to an "average availability" figure, and is of the form expressed in Equation 4:

\[
\text{Vulnerability} = \sum_{\text{Possible outages}} (\text{severity of outage} \times \text{outage type})
\]

Equation 4

Werbeloff and Brown (2011, p. 2362) state that:

“The concept of ‘vulnerability’ is a dynamic concept and as such is difficult to define … Underpinning these varied understandings of vulnerability, is recognition of the need to maximise resilience, and thereby decrease vulnerability, in the face of increasing variability in or disturbances to natural resources. For this research, vulnerability is understood to mean ‘the degree to which a system is susceptible to and is unable to adapt in advance and in response to shocks and adverse effects from social and environmental change’.

There is no attempt to quantify either the “degree” that is quoted or vulnerability per se; the definition equates vulnerability with the converse of resilience, introduces concepts of adaptability (as contributors to resilience) and uses the word “susceptible” in a sense that is almost synonymous with the definition offered for vulnerability. Akgun et al. (2010, p. 3561) state that

"... [v]ulnerability can be defined as a “weakness in the system defended” in a most common and simplest way. Indeed, more vulnerable means easier to be damaged or..."
harmed. Although a comprehensive list of vulnerability definitions can be found in Ezell (2007).

These authors also state (Section 2, p. 3562) "... vulnerability highlights the notion of susceptibility to a scenario, whereas risk focuses on the severity of consequences within the context of a scenario".

Starossek and Haberland (2010), in the context of engineering structures, suggest that vulnerability should be considered as the opposite (antonym) of robustness and should be linked to the concept of damage tolerance. They particularly examine the situation in which an initial event triggers a progressive and catastrophic failure. Gheorghe and Vamanu (2004, p. 614) quote a dictionary definition as "Vulnerable (adjective) – Open to physical injury or attack; (hence) vulnerability".

Baldick et al. (2009, p. 1) offer the following definition: a "... vulnerable system is defined ... as a system that operates with a reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances". These authors include reference to "N−1" and "N−2" redundancy approaches. They also state (p.1) that:

"At present, there is not a commonly accepted vulnerability index or assessment method for power systems. If a power system loses a significant portion of its ability to carry the power flows due to cascading line outages, it is considered a vulnerable configuration".

Piwowar et al. (2009, p. 1873) present a useful discussion and propose a very simple index of system vulnerability, as expressed in Equation 5:

\[ W(x) = \sum_i \text{weighting} \ast \text{vuln}(y) \]

Equation 5

They also take a "lookup table" approach to threat magnitude, noting (on p. 1877) that:

"Our methodology can be very useful to prevent or mitigate the effects of a potential attack. It has been created to answer the amazing increase of international threats. It takes into account several parameters to be as exhaustive and efficient as possible".

This paper presents a thorough approach for evaluating a specific system but it is neither generalised nor theoretically based. It is essentially an extension of simple risk analysis. According to Estrada (2007, p. 296):
“In a network representation of a food web, nodes represent species and links represent who eats whom in the ecosystem (Proulx et al., 2005). This kind of representation permits to analyse the similarities and differences between complex systems of very different nature, ranging from technological to biological and social systems (Strogatz, 2001; Albert and Barabasi, 2002) ... [m]ost food webs have less-skewed uniform or exponential DDs (Dunne et al., 2002a)². However, they also display high fragility to intentional removal of the most connected nodes”.

This paper illustrates an interesting distinction, stating on p. 297 that:

“We start by defining informally the concept of network expansibility. A food web having “good expansion” properties is the one that cannot be divided in at least two isolated “large” parts by disconnecting a “small” number of nodes or links (Sarnak, 2004; Gkantsidis et al., 2006). These nodes or links, which make the function of bridges between these parts, are known as bottlenecks. Consequently, a “Good Expansion Network” (GEN) is a network without bottlenecks”.

The paper includes a useful discussion of the correlation between degree distribution (DD) and bottlenecks, and Good Expansion Networks (GENs). Agarwal et al. (2001, p. 142) state that the objective of their paper is “... to present the basis of this new general theory of vulnerability which is applicable to all systems that can be represented as a graph e.g., traffic networks, pipe flows, electrical circuits etc.” The researchers also state that "A system is vulnerable if any damage from any action or source produces consequences that are disproportionately large in comparison with that damage". They quite reasonably note that a system may be vulnerable under one type of "attack" but not under another and continue (p. 150):

“Vulnerability is defined as the susceptibility of a system to disproportionate consequences in the event of damage or failure and is measured using a vulnerability index. This is the ratio of the consequences to the relative damage demand. Thus the higher the vulnerability index the more vulnerable a system. Because both consequences and relative damage demand are non-dimensional numbers the vulnerability index can be used to compare the quality of the form of two ... different systems”.

Not only is it difficult to quantify a ratio of damage to hazard but also, for the common case where a harm (inaccessibility of some goods or services) is nominated in advance, an index value based on the smallest disturbance that will cause failure

---

² Degree Distribution (DD).
is an inadequate description of the total vulnerability induced by the system. It is moot whether a system having hundreds of weaknesses that can fail with a moderate level of hazard causes more vulnerability than a system having a single weakness that would fail with a low level of hazard. Einarsson and Rausand (1998, p. 535) state that:

“The vulnerability concept has yet not been given a generally accepted definition for technological applications. In some of the references cited above, vulnerability is considered to be similar to the risk concept, although with a somewhat broader interpretation. The threats referred to are often external to the system, and may involve deliberate actions. In this paper, we will use the term vulnerability to describe the properties of an industrial system that may weaken its ability to survive and perform its mission in the presence of threats”.

Similarly, Baldick et al. (2009, p. 1) consider electrical power systems, and propose a definition in which a vulnerable system is defined as a system that operates with a “… reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances”. These researchers also note the possibility of “N−1 and N−2” design redundancy approaches.

Martin (1996, p. 2–3) takes a significantly different view from that of previously quoted researchers, stating that:

“... [t]he system’s vulnerability can be defined as the chance that a specified change in the environment leads to disruption of the usual purposes of the system ... A technological system can be said to be resilient in the face of a particular threat if it is capable of maintaining its purposes when the threat is realized... vulnerabilities are defined in relation to particular threats”.

The first part of Martin’s statement considers the probability that a hazard will cause some defined harm, while the second part of the statement appears to consider a maximum tolerable disturbance for a nominated threat.

Aven and Guikema (2015, p. 2169) state that “…vulnerability can be viewed as risk conditional on the threat or the attack, and various vulnerability metrics can be defined, such as the expected loss given a specific attack.”

A Complete Guide to the Common Vulnerability Scoring System (CVSS) as noted by Mell et al (2007 section 1.7), provides the following definitions.

“Vulnerability”: a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability. “Threat”: 
the likelihood or frequency of a harmful event occurring. “Risk”: the relative impact that an exploited vulnerability would have to a user’s environment”.

The authors of this document use the term vulnerability to mean design weakness and it can be reasonably assumed that, every single time the CVSS-defined vulnerability is exploited, the harm will result. With that observation, the term threat does not mean defined hazard, but rather hazard probability, and if, for example, a hacker were to exploit a vulnerability a hundred times per minute, presumably the frequency of a harmful event occurring would need to accommodate this situation.

Several categories of definition can be identified from these published extracts, and are presented in Table 1.

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harm to hazard ratio</td>
<td>The ratio of “harm” to “hazard” is a common definition, used by authors such as Agarwal et al. (2001. p. 142), Starossek and Haberland (2010) and Wang et al. (2012).</td>
</tr>
<tr>
<td>Resilience</td>
<td>Some authors (Starossek and Haberland, 2010; Werbeloff and Brown, 2011; Afgan and Veziroglu, 2012) define “vulnerability” very simply as the opposite of “resilience”. Specific metrics for resilience include (a) the time for a system to return to a “normal” state following a disturbance or (b) an integral of the “disturbance effect” with respect to time.</td>
</tr>
<tr>
<td>Maximum tolerable disturbance</td>
<td>Maximum tolerable disturbance is noted as a measure of vulnerability by authors such as Starossek and Haberland (2010) and Gómez et al. (2011). This definition relates to the capability of the “system” to adjust its performance to accommodate the “disturbance”, e.g. a chemical processing plant may change its operating conditions to accommodate changing properties of the feedstock. This definition also relates to the spare capacity of the system (an electric grid operating substantially below its rated capacity may be able to “absorb” the disturbance caused by a line failure – whereas a grid that is operating at rated capacity cannot).</td>
</tr>
<tr>
<td>System property</td>
<td>Vulnerability is considered as a system property, recognising multiple threats, by authors including Piwowar et al. (2009. p. 1873). These authors present a useful discussion and propose a very</td>
</tr>
</tbody>
</table>

31
simple index of system vulnerability: \( W = \sum \text{[weighting*vuln(y)]} \). Baldick et al. (2009, p. 1) offer the definition a "... vulnerable system is defined in [1] as a system that operates with a reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances".

| Susceptibility of consequence to risk | Susceptibility of consequence to risk is stated in ISO 73, Chopade and Bikdash (2011) and Martin (1996). Martin (1996, p. 2) states that a system’s vulnerability can be defined as "... the chance (probability) that a specified change in the environment leads to disruption of the usual purposes of the system". This category of definition assumes that there is a probability \( 0 \leq p \leq 1.0 \) that an event will cause a harm. This definition takes no account of the system’s capability to adjust to, or absorb, the “disturbance”. |
| A zero tolerance factor | A specific known weakness, for which a system has zero tolerance. If the probability that a particular event will cause a specific harm is 1.0 (i.e. is certain), then the system can be said to have zero tolerance to that event. Merriam Webster's Dictionary (n.d.) presents two definitions of "vulnerable": (a) "easily hurt or harmed physically, mentally, or emotionally" and (b) "open to attack, harm, or damage". In both cases, the adjective implies a normal application to a noun (person), and both definitions distinguish a person who has few or poor defences against harmful attack, or whose defences can be overcome without a requirement for a powerful attack. |

| Table 1: Published definitions of terms |

Adger (2006, p. 277) includes a significant comment in the paper’s conclusion, stating that "I have reviewed divergent methods and epistemologies in vulnerability research. The diversity and apparent lack of convergence over time are, in many ways, a reflection of the divergent objectives of the research and the phenomena being explained ... this diversity, I argue is a strength and sign of vitality, not a weakness, of vulnerability research."
Whether diversity can be equated with strength is moot, but Adger’s identification of diversity of terminology is considered a valid summation.

2.4.6 Exposure

The term “exposure” is used in ISO GUIDE 73:2009 “Risk Management — Vocabulary”, and is defined (3.6.1.2) as the "... extent to which an organization and/or stakeholder ... is subject to an event". This “definition” could more accurately be considered as a description, because no enumeration or quantification is associated with the term “extent”. The lack of any quantification or categorisation of “extent” leaves the opportunity for such a definition to be proposed.

2.4.7 Resilience

“Resilience” is yet another term that is commonly used, yet for which an adequate definition is non-trivial. It is also a term that, according to many authors, lacks a well-established definition. A number of definitions are offered by authors, including Yazdani and Jeffrey (2012) quoting Bruneau et al. (2003), who defined resilient systems as those with the properties of (1) reduced failure probabilities, (2) reduced failure consequences and (3) reduced time to recovery. Such systems are characterised by the four infrastructural qualities of robustness, redundancy, resourcefulness and rapidity and incorporate the notions of risk (probability of failure and its consequences), reliability, recovery, and system tolerance both pre- and post-failure. System vulnerability is consequently regarded as the antonym of resilience. The “resilience engineering” sub-discipline of engineering has attempted to capture a definition of “resilience”: Hollnagel (2011), quoted by Duffey (2012), defines resilience for an organisation in terms of the ability to respond to upsets by maintaining or regaining some nominal state. Khatri and Vairavamoorthy (2011) and Afgan and Veziroglu (2012) each describe resilience in a very similar way but without Hollnagel’s focus on organisations. These authors effectively propose an average-unplanned-outage duration as “gamma”, which is to be minimised. They also propose a formula for system vulnerability in the form of Equation 6 which equates to an "average availability" figure.
\[
\text{Vulnerability} = \sum_{\text{Outage possibilities}} \{\text{Severity_of_outage} \times \text{Outage_type}\}
\]

*Equation 6*

Shua et al. (2011, p. 264) state that:

“At present, researches on measuring method of supply chain resilience are limited, and quantitative studies are scarce, which is not enough to provide accurate theoretical basis for practical applications.” and (p. 265) that “From the definition, we noted that resilience could be measured in two ways: the time needed for achieving a normal state; the gap between the normal state and the original state ... Therefore, we define resilience as the rapidly recovery ability to an equilibrium after the supply chain is attacked by a disturbance and we use the recovery time to measure...this”.

These researchers propose modelling each element in a supply chain using a proportional-differential response sub-model. Each element would therefore have a time-dependent response and a rate-of-change-dependent response. This means that the response of the supply chain, in terms of return-to-equilibrium, can be calculated from the interconnected response of the elements. Their primary conclusion (p. 268) is that:

“The therefore, this model is useful for engineering management. It makes clear that increasing safety inventory, improving the efficiency of reserve capacity and strengthening the abilities of coordination within the cost margins could enhance supply chain elasticity”.

Nair et al. (2010, bottom of Col2, p. 54) state that no satisfactory definition of vulnerability has been established, and (p. 54, 55) that "... resilience has been defined in terms of the number of failures that a computer network can sustain while remaining connected". In this paper, the resilience measure (p. 55) is stated as "... the resilience definition adopted here for an IM component ... can be expressed as the post-disruption fraction of demand that can be satisfied using specific resources while maintaining a prescribed level of service". These authors use a graph theory notation, but define capacity and other constraints for each link (p. 56). The risks to each link are assumed to be known probabilistically. They consider four specific attack scenarios and a network consisting of five components each with less than five constraints. This allows a resilience index to be computed for each of several levels of budget-for-repair, allowing economic evaluations to be made. Afgan and Veziroglu (2012) make reference to the concept of “maximum tolerable disturbance”. This
definition implies that “resilience” is related to the scope or quantum of a "hazard" that does not result in “harm”, i.e. the hazard level is below some defined "maximum tolerable disturbance". They also propose that, if a system parameter is instantaneously “perturbed”, and a given time is required for the system parameter to return to “normal”, then the resilience of the system for that parameter can be defined in terms of the area under the “response–time” curve. The resilience of the system as a whole is established by a sum of normalised resiliencies to individual parameters. Despite most researchers’ assertions that a definition is not generally accepted, there is a general acceptance of one key point: resilience refers to the path by which a system returns to “normal” following the occurrence of a “hazard”. This distinguishes the definition of “resilience” by establishing that it refers to levels of hazard that do not exceed the capacity of a system to either absorb, or adjust to, the presented hazard.

The published definitions therefore fall into three broad categories.

(a) Definitions similar to that adopted by Nair et al. (2010, p. 55), i.e. “... the resilience definition adopted here for an IM component [alpha] can be expressed as the post-disruption fraction of demand that can be satisfied using specific resources while maintaining a prescribed level of service" or p. 54–55) "resilience has been defined in terms of the number of failures (or the level of disturbance) that a computer network can sustain while remaining connected", are unique to these researchers.

(b) Definitions similar to that adopted by Afgan and Veziroglu (2012), who propose that, if a system parameter is instantaneously “perturbed”, and a given time is required for the system parameter to return to “normal”, then the resilience of the system for that parameter can be defined in terms of the area under the parameter–time curve. The definition proposed by Shua et al. (2011, p. 264), i.e. "... [f]rom the definition, we noted that resilience could be measured… the time needed for achieving a normal state", is a less sophisticated approach.

(c) Definitions such as that developed by Strigini (2012), establish the concept of “maximum tolerable disturbance”. The concept asserts that, for a hazard below the “maximum tolerable disturbance”, the system will eventually return to its original state and hence only transient “harm” will be caused. In contrast, a hazard greater than the “maximum tolerable disturbance” will cause a long-lasting harm.
2.4.8 Robustness

Several types of definition of robustness have been proposed. Within the biological field, Kartascheff et al. (2009) equate community robustness with the fraction of species that survive after a defined event. This definition is oriented more closely towards the collective end-users, and hence has value. It is perhaps unfortunate that, in more technical fields, “robustness” is more commonly interpreted – e.g. by Derrible and Kennedy (2010) – as descriptive of a network that has a high “maximum tolerable disturbance” value. According to Chopade and Bikdash (2011, p. 1):

“Robustness signifies that the system will retain its function and resources largely unchanged or nearly unchanged when exposed to perturbations. Resilience implies that the system can adapt to regain a stable acceptable level of performance after perturbations but the new state may be significantly different [5]…”

Their reference in [5] is to Holmgren (2006). Starossek and Haberland (2010, p. 3) state that, in "... [s]umming up these definitions, robustness refers to the ability of a structure not to respond disproportionately to either abnormal events or initial damage”.

Leong and Doyle (2016) propose p1511 that "A robust system is equivalent to a setup where a person can balance a stick easily because uncertainties inherited in the human sensorimotor system affect the stick balancing task minimally. A fragile system implies otherwise. ". They offer a detailed mathematical treatment of stick-balancing problem, but the paper concludes by noting the trade-off between robustness and efficiency and that delays (mathematically) actually tend to increase robustness. These authors also refer to "heterogeneous" by which they infer the eyeball, brain, nerve system, musculature combination, i.e. a relatively narrow context.

2.4.9 Survivability

Published references include those by Einarsson and Rausand (1998, p. 535), who state "A system is said to survive an accident (or some other disturbance) if it is able to operate from a specified time after the accident, and to regain a similar market
position as it had prior to the accident”. Levitin and Lisnianski (2001) state (abstract) that

“... vulnerable systems, which can have difference states corresponding to different combinations of available elements composing the system... Both the impact of external factors (attack) and internal causes (failures) affect system survivability, which is determined as probability of meeting a given demand”.

A very similar approach is proposed by Korczak et al. (2005). Sajdak and Karni (2006) propose that it is necessary to define assailant capabilities for each type of threat. They state that to do this fully is infeasible, and therefore suggest that an integrated probabilistic approach is required. Sheldon et al. (2004, p. 293) state that "... [s]urvivability of a system can be expressed as a combination of reliability, availability, security, and human safety”. Other researchers have considered discuss anti-malware approaches to increasing the “survivability” of a wireless information network. Jiang and Xue (2011) address a similar issue, using similar terminology. Richards et al. (2008) define survivability in terms of the capability of a system to minimise (without quantification) the effect upon the delivery of some value of a defined disturbance. These authors propose a highly descriptive, framework approach, as opposed to an approach using and generating well-defined numerical values. Zhao and Xu (2009) consider the survivability of scale-free networks, and note the effectiveness of establishing new links between low-degree nodes in this regard. Gómez et al. (2011, p. 216) argue that Bayesian approaches use risk analysis and the concept of survivability – i.e. the system can be expected to perform at design level, while a hazard is within a given range of levels. Wang et al. (2011) state (in their abstract) that "... [n]etwork security assessment is critical to the survivability and reliability of distributed systems”. Finally, Li et al. (2012) state that network topology is a promising approach to improving network survivability.

Serageldin and Krings (2015) acknowledge the potential for malicious acts, and the potential for these to affect “survivability”. No definition of "resilience" is provided, but "resilient", "survivability" and "fault tolerant" terminology is used almost interchangeably.

These published definitions and descriptions fall into two categories, i.e. those in which a homogeneous system, such as a wireless network, may or may not continue to offer its service. These cases are only marginally distinguishable from the
discussions of “maximum tolerable disturbance” in the context of “vulnerability”, and it is therefore argued that the “vulnerability” definition could be used in these cases, and those in which there is a complex system, e.g. a warship, that is subject to multiple “hazards” and may have varying levels of serviceability. The concept of serviceability also needs careful definition: if a ship sinks, it has clearly not survived; if the ship’s guns and engines are functioning, but its radar is not operational, an enemy aircraft can approach with impunity, so that the medium-term survivability is problematic at best.

2.4.10 Critical reflections on published definitions

Several common themes have appeared in the reviewed works.

- For many of the terms, published definitions are not agreed upon.
- Many of the definitions offered lack precision. Specifically, it can be noted that the scope of the harm is not always identified – and failure to define the “harm” precisely leads to ambiguity when other risk, hazard and vulnerability issues are considered. In the context of this study, it is particularly important to distinguish whether a specified “harm” is to the profit of a network-owner, or to the end-user of network services.
- Many of the offered definitions are not precisely scoped. It is notable that time-frames are seldom defined, but these actually have a practical significance. Over a sufficiently long time-frame, the probability of almost any event tends towards 1.0.
- Many definitions note that, when high-level failures, i.e. harms, are considered, multiple hazards must be considered and each hazard will be associated with specific probabilities, maximum tolerable disturbance levels and other factors. Despite noting the need to consider these factors, there is both lack of precision and lack of agreement on the relationship of terms.
- Few authors quantify the definitions offered.
  The lack of precision of definitions, the lack of agreement on definitions and the lack of quantification of relationships between relevant factors present difficulties. This thesis must propose and justify a definition of vulnerability and approaches to quantification.

38
2.5 Application fields that are studied in the literature

Many related fields are very well covered in the literature: disaster preparedness, engineering risk and some aspects of infrastructure robustness are obvious examples. These fields overlap; however, each also has unique aspects. Several “dimensions” have therefore been distilled from the reviewed literature, and are summarised in the following table.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harm object</td>
<td>• Society, humanity or ethnic group</td>
</tr>
<tr>
<td></td>
<td>• Region or city, or small community</td>
</tr>
<tr>
<td></td>
<td>• Specific supply chain, commonly a commercial venture</td>
</tr>
<tr>
<td></td>
<td>• Homogeneous network, e.g. a computer, water or power supply network</td>
</tr>
<tr>
<td></td>
<td>• An individual</td>
</tr>
<tr>
<td>Danger (hazard)</td>
<td>• Natural disaster, e.g. volcanic eruption or an earthquake, characterised by localised multi-system failures</td>
</tr>
<tr>
<td></td>
<td>• General failure of a specific, homogeneous system, e.g. communications, internet or finance systems</td>
</tr>
<tr>
<td></td>
<td>• Specific hazard to a specific system, e.g. broken fibre-optic cable, malware on computer system, structural member or equipment item failure</td>
</tr>
<tr>
<td>Time-frame</td>
<td>• Immediate, i.e. typically immediate to a few hours; affects non-storable consumables, e.g. electricity</td>
</tr>
<tr>
<td></td>
<td>• Short term, typically a few days; a period during which stores can be consumed</td>
</tr>
<tr>
<td></td>
<td>• A “beyond-storage” time-frame in which reasonable storage is exhausted, and failure occurs unless there is a functional supply chain</td>
</tr>
<tr>
<td></td>
<td>• “Maintenance” time-frame, typically months or years; the time in which failure becomes common without maintenance</td>
</tr>
<tr>
<td></td>
<td>• “Replacement” time-frame, often years; after which the equipment has reached the end of its working life</td>
</tr>
</tbody>
</table>

Table 2: Application fields in the literature

The initial literature survey revealed that certain application fields have been the subject of significant study. These fields are described in the following sections.
2.5.1 Society

Distinguishing what issues and aspects genuinely have “societal” significance is no trivial exercise. Tainter (2003) has attempted to distil the issues that have truly been causal in historical collapses of particular societies: his conclusion, in essence, is that historical societies have collapsed when the burden of maintaining the society has exceeded the benefit to its members. Tainter also states that his analysis is not valid for current “society”, primarily because of the high level of interconnectedness and interdependence of our current society. Diamond (2005) concludes that societies fail when a critical component of their environment, e.g. forestation, soil or water source, is damaged beyond regeneration. Earlier authors such as Adam Smith (1723–1790), as explained by Hayek (1976) and Toynbee (1934) have pointed out that such ubiquitous concepts as perpetual growth are inherently impossible. Numerous publications, e.g. Carreño et al. (2007), consider the consequences of geographically localised natural disasters. Posner (2004) attempts to consider some of the society-wide catastrophe scenarios from a risk and cost-of-mitigation approach. The literature review revealed publications that analyse failures of historical societies; however, although these suggest “vulnerabilities”, the literature review did not reveal any publications that claim, with any adequately reasoned basis, to assess the requirements for the survival of today’s society.

2.5.2 Ecosystems

The vulnerability of ecosystems has been studied by several authors who generally consider a geographically defined area holding a variety of species, each of which has evolved to the point where its viable options for food and survival are limited. For example, Kartascheff et al. (2009) study ecosystem stability, but their paper is of limited applicability because it defines stability in terms of the number of species and their connectedness within an ecosystem. The paper does consider the adaptation of a web, in terms of foraging adaptation, and defines the robustness of entire communities (in terms of the fraction of species that survive after population dynamics). The paper also identifies four types of food web model, i.e. random, cascade, niche and nested hierarchy. Briske et al. (2010) study the vulnerability characteristics of ecosystems and, although offering few quantitative approaches, present some useful concepts, including (p. 37) the idea that “… [t]hresholds are
defined as boundaries in time and space in non-equilibrial systems that separate alternative stable states (i.e., dynamic regimes) organised around unique attractors or equilibrium points”.

2.5.3 Infrastructure

Researchers, including Gómez et al. (2011), assert the importance of current infrastructure to society. As national infrastructures are clearly associated with technological contributions to end-user vulnerability, these must receive careful consideration. However, it is significant that works previously cited do not specifically:

(a) justify the “essential” nature of the infrastructures identified;
(b) propose a clear definition that allows “infrastructure” to be identified and distinguished from systems that are “not infrastructure”;
(c) include, in considerations of vulnerability, the option of supplying end-user services in a different manner;
(d) consider the possibility of a disruptive technology, e.g. a major breakthrough in energy storage and solar cell technology, which would make power transmission grids irrelevant.

Published papers that examine infrastructural vulnerability include those by Li et al. (2012) who, in the context of homogeneous systems, consider that network functionality is commonly measured by average path length and connectivity. Chopade and Bikdash (2011) initially focus on the vulnerability of SCADA systems; however, their second major topic is the vulnerability of critical infrastructures, which they identify as including power supplies, communications, transportation, water supplies and buildings. Although this paper focuses on a somewhat narrow scope of interdependencies, it does attempt to analyse the techniques that might be applied to the modelling of interdependencies. Haimes and Jiang (2001) and Eusgeld et al. (2011) address the issue of infrastructural interdependence, Eusgeld et al specifically studying the interdependencies between the communications infrastructure of SCADA systems and the electrical power distribution infrastructure. Gómez et al. (2011) open their paper with the following statement:

“Socioeconomic development and sustainability highly depend on the construction and operation of infrastructure networks. Therefore, robustness, reliability, and
Resiliency of infrastructure networks are vital to the economy, security and wellbeing of any country.

Yazdani and Jeffrey (2011, p. 2) state that “Examples of infrastructure networks include urban roads, rail network, power grid, gas pipeline networks, water distribution networks, and supply chains”. Although not specifically quoted as examples of “infrastructure”, the authors note (p. 10–11) “western Australian gas pipelines and... the sewer system”. Akgun et al. (2010, p. 3561) add “airports” to the list of critical infrastructures, and describe infrastructures as “Critical facilities are the systems that have a high impact to the psychology, health and welfare of the population, and are essential to the operations of the economy and government such as airport, dam, governmental facility, harbor, nuclear power plant and oil plant”.

Oliva et al. (2010, p. 76) identify “Infrastructures such as energy grids, transportation networks and telecommunications systems are critical to the welfare, economy and security of every developed country”. Gheorghe and Vamanu (2008, p. 1) state that: “Infrastructures like energy and water supply networks, transportation systems, telecommunications and, more recently, the IT realm are so vital, ubiquitous and interlaced with the fabric of the societal dynamics and life that their sudden unavailability, denial of service, or impairment may severely affect the security, welfare and social health of an entire nation”.

Moore et al. (2007, abstract) state that: “The Department of Homeland Security (DHS), Directorate of Information Analysis & Infrastructure Protection (IAIP), Protective Services Division (PSD), contracted the American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME ITI, LLC) to develop guidance on Risk Analysis and Management for Critical Asset Protection (RAMCAP)” and “Underlying the need for a technical vulnerability process was the realization that the potential for infrastructure protection initiatives far exceeds the resources available”.

Nazarova (2006, p. 567) identifies the following: “Economic, social, ecological, transportation, and other complex systems cover practically all spheres of real life. Many of them, such as telephone, telegraph, Internet, water pipelines, and fuel and power complex are geographically distributed systems. The level of development of the country’s economy, and in extreme situations, the lives of people depend on their state and quality of functioning”.

42
Gheorghe and Vamanu (2004) note a list of infrastructures including transportation infrastructures, communication systems, electricity transmission systems, banking systems, water delivery infrastructure and process industries.

If it were possible to obtain power via solar cells, batteries and an inverter with reliability and costs lower than via power station and transmission lines, then individuals would do so. Similarly, if it were possible for individuals to safely treat sewage less expensively than via centralised treatment plants, then citizens would exert considerable pressure to gain permission to do so. Current infrastructural system design has evolved under the twin pressures of adequate performance and citizen pressure to minimise cost. Therefore, infrastructural systems do have several characteristics. Firstly, large infrastructures will inevitably resist change (possess inertia), and either actively or passively discourage alternative technical approaches to the supply of needs. Secondly, the studies of infrastructural vulnerability tend to emphasise the complete infrastructure as a unit – yet a power supply grid that splits temporarily into sections, each of which has one generator, or a water grid that splits into sections, each with one reservoir, causes little concern to the end-user. Some authors do acknowledge this issue; for example, Werbeloff and Brown (2011) speak of the “Security through Diversity” (STD) implementation strategy that is being adopted for water supply in parts of Australia. Finally, it may be noted that, as an infrastructure grows, so does the cost of both maintaining the infrastructure and protecting it against both intentional and unintentional attack. This is effectively the scenario examined by Tainter (2003) and, if unchecked, could lead to a service in which costs exceed value. The interdependence of infrastructures is widely acknowledged, e.g. by Haimes and Jiang (2001), but approaches for quantifying the interdependencies and adequately addressing them are not well developed.

2.5.4 Supply chains

Studies of supply chains are generally focused on the interests of a corporate owner, and hence extend neither to raw materials or processing steps nor to the end-user. Significant publications relating to supply chain robustness and/or vulnerability include Chen and Lin (2012) who consider (Section II(A)) that complex supply chain networks can be represented in graph theory notation, as a set of vertices representing enterprises and edges representing flows between enterprises. They
apply a simulation algorithm that systematically "breaks" nodes, starting with highest-degree nodes (p. 593), and recalculate

dominated graph properties after each iteration, equating these graph properties with supply chain vulnerability. Specifically, this paper asserts (p. 594) that

"... under the restriction of a certain connectivity, the biggest remove scale of nodes or edges which a complex supply chain network can bear is called the invulnerability degree or stability degree of the network".

Kumar et al. (2010, p. 3717) study supply chains and appear to equate risk with harm, stating that

"Risk in supply chains can be defined as the potential deviations from the initial overall objective that, consequently, trigger the decrease of value-added activities at different levels". They also state (p. 3719) that "This paper addresses such issues by identifying and measuring various risks present at every level in a supply chain and decides the optimal policy with minimum risk factors and overall cost".

They develop a generic mathematical model for a four-tiered supply chain approach, i.e. suppliers, plants, warehouses and markets, and notation to allow the identification of routes between one tier and the next below. Further, they note (p. 3727) that

"This hypothetical supply chain can be structured as a multiobjective mixed integer programming (MOMIP) model. In this paper, the objective is to minimise the total cost, TC, of the supply chain operation which includes supplier cost, production cost, warehouse associated cost and market cost".

Estrada (2007, p. 296) make a definitional simplification allowing a network analysis of a food web. They state:

"In a network representation of a food web, nodes represent species and links represent who eats whom in the ecosystem (Proulx et al., 2005). This kind of representation permits to analyse the similarities and differences between complex systems of very different nature, ranging from technological to biological and social systems (Strogatz, 2001; Albert and Barabasi, 2002 ... ".

Similarly, Ludema (2006) provides an overview of supply chain terminology, quotes graph theory and also identifies supply chains as "nearly decomposable systems".

The scope of the supply chain literature varies considerably: Kumar et al. (2010) consider a generic manufacturing, warehousing and transport operation. As previously noted, the defining quotation within their paper (p. 3727) is:

"This hypothetical supply chain can be structured as a multiobjective mixed integer programming (MOMIP) model. In this paper, the objective is to minimise the total cost,
TC, of the supply chain operation which includes supplier cost, production cost, warehouse associated cost and market cost”.

In other words, for a closely defined subset of possible “supply chains”, they demonstrate an analytical approach to maximising profit to the chain-owner, for operations between some defined raw materials supplied to their warehouses and some product available in a retail outlet. In contrast, Chen and Lin (2012) use a graph theory approach similar to that used for homogeneous networks such as computer communication networks. Their paper does not draw upon any actual measured data or representations of real supply chains; it is effectively a theoretical exercise in the application of graph theory.

2.5.5 Computer and communication networks

As Forester and Morrison (1990, p. 462) state “As society becomes more dependent on computer and communications technologies, we also become more vulnerable to computer and communications breakdowns”. Authors who have published significant works in the field of computer and communications networks include Idika and Bhargava (2012, p. 75), who state that

“… a security metric (or a combination of security metrics) is a quantitative measure of how much of an identifiable security-relevant attribute an entity (e.g., a network) possesses. In this work, we focus on improving three previously proposed attack graph-based security metrics: the Shortest Path metric, the Number of Paths metric, and the Mean of Path Lengths metric”.

Liu and Zhang (2011) examine a range of vulnerability reporting approaches, and propose a composite scoring system to address perceived weaknesses of these approaches. Tu (2000) has a single aim: to establish that the internet is, in fact, a "scale-free" network, using the definitions of Barabási and Bonabeau (2003). Strigini et al. (2007) comment extensively on the vulnerability and resilience of computer networks, but without advocating specific approaches. In a seminal work, Doyle et al. (2005) note the well-reported characteristics of scale-free (SF) networks, and conclude disappointingly (p. 6) that

“It is certainly appealing that SF network models can avoid all Internet-specific structures, such as protocol stacks, technological or economic constraints, and user heterogeneity, yet make interesting and testable predictions. Unfortunately, this fact
yields results that collapse when tested with real data or when examined by domain experts”.

These analyses of “computer networks” have several characteristics. Firstly, homogeneous networks are assumed, i.e. only one commodity flows through every connection of the network, and there is basically one type of “node”. Secondly, there is implicitly an ability to re-route traffic on an ad-hoc basis. It is noted that, whereas these characteristics allow interesting options for academic study, they are limited to narrow and tightly defined fields.

2.5.6 Power supply grids

As with computer networks, power supply grids offer scope for analysis, and for optimisation as well as the examination of vulnerabilities. Although few authors make note of the fact, they are actually not homogeneous because a grid would commonly include more than one voltage level. Power grids are also distinct in their operational characteristics: whereas a water supply is still “useful” if the flow is minimal and a computer network is still “usable” if the dataflow reduces to a very slow baud-rate, neither the power users nor the grid operators or the grid protection systems will tolerate frequency excursions of more than about 1 Hz or voltage excursions of more than a few percent from nominal values.

Researchers who have published significant analyses of the vulnerabilities, risks and resilience issues of power supply grids include Buldyrev et al. (2010, p. 1025), who start by noting the problem of cascading failure across networks. They state that

“We present exact analytical solutions for the critical fraction of nodes that, on removal, will lead to a failure cascade and to a complete fragmentation of two interdependent networks. Surprisingly, a broader degree distribution increases the vulnerability of interdependent networks to random failure, which is opposite to how a single network behaves”.

This paper cites a real-world situation “... power network and an Internet network (a supervisory control and data acquisition system) that were implicated in the blackout that affected much of Italy on 28 September 2003”. The approach taken in this paper (p. 1025) is

“To model interdependent networks, we consider for simplicity, and without loss of generality, two networks, A and B, with the same number of nodes, N. The functioning
of node $A_i$ ($i = 1, 2, \ldots, N$), in network $A$, depends on the ability of node $B_i$, in network $B$, to supply a critical resource, and vice versa".

Baldick et al. (2009, p. 1) state that a "... vulnerable system is defined in [1] as a system that operates with a ‘reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances’. The paper also makes reference to "$N-1$ and $N-2$" design redundancy approaches. They also state (Col2, p. 1) that:

"At present, there is not a commonly accepted vulnerability index or assessment method for power systems. If a power system loses a significant portion of its ability to carry the power flows due to cascading line outages, it is considered a vulnerable configuration".

These researchers state (p. 2) that the "... TRELSS (Transmission Reliability Evaluation of Large-Scale Systems) ... is an industrial tool used to identify cascading failure problems", and state (p. 4) that "... [t]he combinatorial growth in the number of ways cascading failures can occur make them very difficult to analyze, and ... develop a continuous-time Markov chain model of a dependability system that explicitly tackles this problem". A graph theory approach to modelling a power grid system is proposed, and these authors note the difficulties of this approach, stating (p. 5) that:

"A cascading failure model based on small-world networks was proposed in ... and can be used to identify the vulnerable lines. The model assumes that a node will fail if a given fraction $\gamma$ of its neighbors have failed. Starting with initial failures on a few isolated nodes, the process will become cascading when these initial failures lead to subsequent failures due to exceeding of the fraction $\gamma$".

The assumption of adjacent node failure is valuable, reflecting real world experience. The researchers however conclude (p. 7) that a clear solution has not been found, and state that:

"Since power system cascading is diverse, complicated, and computationally intractable, there is no single model, tool or approach that can address all aspects of cascading or answer all the questions about managing the risk of cascading failures".

The

2.5.7 Water supply networks

Water supply networks are functionally different in several respects from power supply grids: end-users commonly have at least a nominal amount of storage,
and the supply network may still be considered to be “functional” even if the quality of supply decreases and the flow is reduced to a tiny fraction of the design flow; the “design specifications” for the system are much less stringent. As with power supply grids, water distribution “networks” tend to have few supply points and many smaller off-take points. Water supply systems have been studied by many researchers, including Yazdani and Jeffrey (2012), who model water distribution systems as weighted, directed graphs, concluding that

"... the demand adjusted entropic degree provides a measurement of node centrality refined and suited to the analysis of spatially organized infrastructure networks with limited connectivity. In the absence of hubs and highly connected nodes, which are responsible for a great percentage of network connectivity and regarded as the points of vulnerability to targeted attacks in scale-free networks".

This paper considers two well-documented real water distribution systems, and concludes that critical nodes can, at least theoretically, be identified, commenting that less sophisticated graph analysis techniques did not succeed in identifying more critical nodes because they lacked the more sophisticated approach to edge weighting and the weighting of the significance of specific nodes. Werbeloff and Brown (2011) comment specifically on the cities of Melbourne and Perth, in the light of severe stresses on water supplies, and Australia’s national decision to adopt a “security through diversity” policy for increasing the security of urban water supplies. According to these researchers (p. 2362):

"It is increasingly recognised that traditional urban water systems are ill-equipped to effectively address these complex and interrelated challenges (Vlachos & Braga 2001; Brown et al. 2009), leaving cities vulnerable to the effects of variable water conditions".

This is a discussion paper, presenting a broad range of options under headings of "threshold capacity", "coping capacity (damage restriction during an emergency)", "recovery capacity" (damage reaction after an emergency) and "adaptive capacity" (envisioning proactive planning). Yazdani and Jeffrey (2011) note that there are fundamental differences between infrastructure networks, stating that geographical constraints on systems such as water distribution networks impose severe restrictions on network layouts, and require different analyses from systems without geographical constraints. They also note (p. 4) that a proper representation of a water distribution network would need to include pipe loss factors, pump capacities etc., but this is too hard; they therefore adopt a simplified approach, treating networks as undirected
graphs and "... statistical properties of network topology and applications of graph theory to identify the structural patterns and building blocks of the networks". Four real-world water distribution systems are studied; the authors note the usefulness of the graph metric, stating (p. 6) that

"... central-point dominance ... which, in the analysis of flow networks, may be used to indicate how network flow is controlled by centrally located point(s), or to quantify the degree of concentration of the network layout around a center. Central-point dominance is calculated by taking the mean over the betweenness centrality values of all nodes indexed by the maximum value of betweenness (achieved at the most central-point)."

These researchers describe "link-per-node ratio", "central-point-dominance" and "clustering coefficient" values, which they claim is an indicator of path redundancy, but later say (p. 7) that it is not a good measure. They also propose (p. 7) the use of a "meshedness coefficient" as a better measure of redundancy. They additionally state (p. 10) that

"One of the most important objectives in the operation of WDNs is to maintain the path connectivity between the source(s) and the consumers (network nodes) and make such path connectivity as short and efficient as possible. Therefore, instead of assessing the efficiency based on the connectivity between all pairs of nodes, it is more appropriate to measure the efficiency based on the connectivity between a root node such as a reservoir and other nodes in the network".

One such measurement is reported as the network's route factor and is proposed as the average of the individual route factors for each water source (to a defined point). This is a remarkably simplistic approach to the issue. The paper comments on the value of graph theory metrics, noting that it is possible to establish a threshold for the random removal of nodes, for a specified degree distribution, and is related to the loss of a network's large-scale connectivity. They recognise (p. 12) that the actual functional requirement of the network is the provision of water, and that supply nodes, i.e. reservoirs, are most important even if these do not appear as highly connected. They state (p. 12) that

"To this end, the structural vulnerability and robustness of a WDN may be investigated by quantifying the level of optimal-connectivity of network design, by identifying critical locations and the most influential components followed by studying their failure consequences on network performance... one way to identify the critical locations in
WDNs is by detecting the cut-sets, i.e., the sets of components whose removal results in disconnection”. However, they also note that, for sparse networks such as most water distribution networks, the measurements (route factors) generally equate to “1” and there is a need for some other (undefined) measurement to apply to structural vulnerability and fault tolerance. The paper’s conclusion states that

“Network robustness and structural vulnerability were investigated by using techniques to identify the influential components and critical locations (e.g., articulation points and bridges) and quantifying the network’s well-connectedness with respect to the existence of such locations, in the absence of degree-based hubs and given the sparse structure of networks. Descriptive measurements, including those derived from the spectral analysis of network connectivity and Laplacian matrices, quantified the level of structural network tolerance against failures and removal of components and enabled a basic comparison between different network designs”.

The scope of the study by Yazdani et al. (2011, p. 1577) is Kumasi, in Ghana, which has a population of over 1.5 million people with rapidly growing water consumption industries. Specifically, these authors state the scope of their work as

“We created four hypothetical network expansion options, starting from a tree-like expansion with no loops, gradually moving toward more looped structures which are deemed better-conceived networks with greater redundancy. Subsequently, we performed the calculations for various resilience metrics and compared the results with those from the unexpanded network to assess how robust the expansion options are and how they contribute to enhancing or degrading the overall system robustness and its ability to deliver service”.

These researchers note the effects of oversimplification in their concluding statements (Col 2, p. 1577) that

“The proposed methodology may therefore be regarded as a relatively quick-to-implement precursor to more detailed trade-off analyses... However, it should be borne in mind that purely topological measurements may only partially describe the network structure and fail to entirely characterize its properties... This shows that oversimplification of water distribution systems into abstract graph models is extremely useful but far from sufficient for a comprehensive assessment of system resilience and its robustness against perturbations and hazards…”

It is significant that water supply and power supply systems are both recognised as homogeneous, and that in both cases researchers who have applied graph theory
approaches conclude their research with warnings of the limitations of that approach and the dangers of oversimplification.

2.5.8 Transport systems

Transport systems have much in common with water distribution systems; both are geographically constrained and are considered to be “functional” even if capacity is severely reduced. However, they have a key difference, which also distinguishes them from computer systems: the transport medium is capable of re-routing – this is a function not of the “nodes” but uniquely of the actual medium (vehicles) using the network. Derrible and Kennedy (2010, p. 3679) study transport systems, emphasising

“In this paper, robustness deals more specifically with alternative paths offered to transit users and likelihood of accidents/failures. Performing such an analysis is all the more important considering it fits in the broader context of resilience (i.e. how cities can respond to major disruptions)... On a larger scale, by looking at 22 transit systems (bus and tramway) in Poland, Sienkiewicz and Holyst [41] found that some systems appeared to show a scale-free behaviour, with scaling factors ranging from 2.4 to 4.1; most systems also appeared to be small-worlds”.

The paper also notes (p. 3683) that “As a result, we prefer to use another indicator... degree of connectivity... Mathematically, it is essentially identical to the clustering coefficient defined above". They continue on to define a robustness metric (p. 3684), noting that a "... particularly adequate robustness indicator is the concept of associativity that was introduced by Newman". This paper is significant because it studies a large number of real transport networks, but its only contribution is to illustrate how these real-world networks correlate with theoretical scale-free/small world networks. Nair et al. (2010) consider a large “InterModal” transport system, i.e. a large port complex, which is categorised as a “transport system”, but is actually a diverse production system in the port of Swinoujscie in Poland. These researchers comment (bottom of Col2, p. 54) that no satisfactory definition of vulnerability has been established. The paper references many other authors’ attempts to measure resilience and suggests (p. 55) that

"... the resilience definition adopted here for an IM component [alpha] can be expressed as the post-disruption fraction of demand that can be satisfied using specific resources while maintaining a prescribed level of service".
The same paper uses a graph theory notation, but defines (p. 56) capacity and other constraints for each link. The risks to each link are assumed to be known probabilistically. The paper proposes the calculation of a resilience index for each of several levels of budget-for-repair, allowing economic decision making.

2.5.9 Analyses of interdisciplinary fields

Several papers address a number of fields. These papers include Werbeloff and Brown (2011, p. 2362), who comment that

"It is increasingly recognised that traditional urban water systems are ill-equipped to effectively address these complex and interrelated challenges (Vlachos & Braga 2001; Brown et al. 2009), leaving cities vulnerable to the effects of variable water conditions". Akgun et al. (2010) propose a “…fuzzy integrated vulnerability assessment model (FIVAM)” that is based on fuzzy set theory and a multiple attribute rating technique. They also propose “…fuzzy cognitive maps (FCM) methodology…” and the use of group decision making. They propose that these can be applied to any major infrastructure. Robertson (2010) starts by noting the hierarchy of needs as proposed by Maslow (1943) and correlating these with the current technological approaches used for their supply. Crutchfield (2009) discusses the issues of technological fragility without addressing specific details – and certainly without offering any metrics or approaches for improvement. Gheorghe and Vamanu (2008) present a very broad-scoped paper, which treats the whole world as "system of systems" and adopts the approach of identifying a large number of "indicators", for which public data are available, and using an algorithmic approach to combining these to show "surfaces", whose shape can be interpreted to indicate vulnerability. LePoire and Glenn (2007) present a qualitative analysis of the effects of technological advances both to aid and to counter the threat of terrorism. Svendsen and Wolthusen (2007) use a modelling approach built on graph-theory principles and present a more sophisticated model of interdependent infrastructures, including the representation of flows and the storage of components at nodes. However, their conclusion includes the statement that they

“... have presented an abstract model of critical infrastructures which aims to capture essential properties of different infrastructure types while retaining an overall computational complexity which makes it amenable for large-scale analyses. This necessarily is less accurate than domain-specific models, but it does allow for the
modeling of interactions and interdependencies which such domain models cannot capture”.

Homer-Dixon (2006) notes that his three examples illustrate that society’s fate is always uncertain, and that devastation can happen at any time (regardless of the strength of the society), caused by a variety of complex factors. Van Blaricum et al. (2005, p. 226) state that

“One promising tool for conducting the analyses described above is being developed by the U. S. Army Engineer Research and Development Center (ERDC). “Fort Future” is an integrated suite of planning and simulation tools. One part of Fort Future is called the Virtual Installation, or "VI". The VI is a GIS-based computable model of a community. It includes buildings, utilities, and the transportation network and it can be overlaid onto aerial photos for context”.

Three aspects of this paper are of particular interest: (1) it acknowledges the interconnectedness of the utilities; (2) it is built around the use of a single (opaque) computer simulation package; (3) despite reliance on that package, it does recognise that running simulations with different types of redundancy and backup etc. will allow the user to investigate the effect on multiple interconnected utilities. The main assumption by Gheorghe and Vamanu (2004, p. 616) is that

“... operational definition of vulnerability adopts the emergent, consensual understanding of vulnerability as a system’s virtual openness to lose its design functions, and/or structural integrity, and/or identity under the combined interplay of two sets of factors: U. Risk-featuring factors; and V. Management response-featuring factors”.

In this paper, U and V are identified as membership functions of fuzzy sets and the authors go on to note (p. 616) that "... an operable system may thereby appear as: • Stable, and thereby featuring a low vulnerability; • Critically unstable/vulnerable; or • Unstable, and thereby featuring a high vulnerability”. This is effectively a representation of a complex system by using a large set of "indicators", each of which is represented in fuzzy set notation. They conclude (p. 626) that

“Generic QVA models may be developed that, however, may not be universally applicable ... That implies, inter alia, a sound choice of the U- and V-type physical indicators, supported by a clear identification of the chief underlying concerns about the targeted system’s safety. • It is submitted that, from the safety standpoint, resilience may be less relevant than vulnerability. Resilience may come into play if,
and when, the issue of making the vulnerability countermeasures cost-effective would
come into consideration."

Rinaldi et al. (2001, p. 11) discuss a useful case study, and while they quote
interdependency, the description is arguable more closely related to the issue of
single points of failure for multiple systems. The case study is described as

"In the case of the Galaxy 4 failure, the loss of a single telecommunications satellite
led to an outage of nearly 90% of all pagers nationwide … From an interdependency
perspective, it also disrupted a variety of banking and financial services, such as credit
card purchases and automated teller machine transactions, and threatened key
segments of the vital human services network by disrupting communications with
doctors and emergency workers”.

Their definition (p. 3) is noteworthy: "This additional complexity exhibited by a system
as a whole, beyond the simple sum of its parts, is called emergent behaviour and is a
hallmark of...” complex systems. The paper defines several types of interdependence
between infrastructural systems, which need to be acknowledged. The paper also
notes (p. 19) the concept of coupling order – of interdependence. The authors of the
paper propose viewing connected infrastructures using an “agent” approach (p. 20)
and they suggest (p. 16) that "... a comprehensive analysis of interdependencies is a
daunting challenge. Today’s modelling and simulation tools are only beginning to
address many of the issues outlined above: the “science” of infrastructure
interdependencies is relatively immature”. The paper also presents several
conclusions, including the six dimensions of interdependency, i.e. type of failure,
infrastructural characteristics, state of operation, types of interdependencies,
environment and coupling and responsive behaviour.

2.6 Published analytical techniques, related to technological vulnerability

2.6.1 Analysis and classification of published techniques

Amongst the literature relevant to the thesis topic, several analytical
techniques were identified. This section describes these techniques. This section
attempts to use a terminology that is uniform across the various named techniques. It
also attempts to define the techniques in terms of the inputs that are used in principle
or in practice, the outputs generated and the potential applicability to the field of study.
The boundaries of these analytical techniques are not clearly defined: some authors
attempt to optimise resources expended against additional reliability to obtain reduced vulnerability of systems such as supply chains, power distribution networks and water distribution systems. These analyses also overlap with the operational analysis field and related optimisation techniques.

2.6.2 Risk-based techniques

Risk-based techniques are characterised by the use of probability factors, sometimes by a combination of a hazard-probability factor, a vulnerability-probability factors and a potential harm. Classical risk analysis has been useful to the engineering community, although it could be argued that this is due more to the enforced discipline of completing a risk-register than to the rigour of the analytical approach. In the context of computer networks, Idika and Bhargava (2012, p. 75) state that "... a security metric (or a combination of security metrics) is a quantitative measure of how much of an identifiable security-relevant attribute an entity e.g., a network possesses". Moore et al. (2007, abstract) state that:

"The Department of Homeland Security (DHS), contracted the American Society of Mechanical Engineers Innovative Technologies Institute, LLC (ASME ITI, LLC) to develop guidance on Risk Analysis and Management for Critical Asset Protection (RAMCAP) … a process is needed to identify the priorities for allocating these limited resources. This process should be based on guidance that defines consistent, objective, and integrated application of risk analysis methods".

Einarsson and Rausand (1998, p. 535-536) state that "... risk is the “opposite” of safety”. Some approaches to improving the estimation of probability have been proposed. Timashev and Tyrsin (2011) develop the concept of system entropy, as a more complete definition of the risk of failure: this definition is applied to a pipeline, with several known defects, any of which could cause failure within a given time interval if overpressure is known. The definition is useful and, in principle, could be extended to other systems, but the cases for which it is practical to gather such data are limited. Taking a quite different approach, Khatri and Vairavamoorthy (2011) quote “Dempster–Shafer theory”, which is a qualitative research technique that is also intended to improve the assessment of probability. Newton et al. (2006) consider Bayesian belief networks, for a similar purpose.

In summary, risk analysis is a topic upon which a huge amount has been written: the papers described above are a small portion of the body of literature, yet
are considered to span the seminal literature and be generally representative. The specific issues that limit the applicability of risk analysis to the research topic can be enumerated as follows.

(a) The term “risk” is generally used in the sense of a “defined harm”. This is distinctly different from the colloquial use of the term, which is more commonly associated with simple probability, e.g. “a high risk activity”.

(b) Various approaches, e.g. Dempster–Shafer belief systems and Bayesian probability calculations have been proposed to improve the consensus of expert opinions of probability.

(c) Approaches such as “system entropy” can, assuming the availability of very detailed data, improve assessments of risk probability.

(d) Definitions show a curious lack of precision in the degree to which they link defined harm, strictly and only, to a defined hazard. Most risk definitions in principle relate a “harm” only to a single specified hazard – yet “risk matrices” commonly list major “harms” and a limited set of hazards that cannot even remotely encompass the range of hazards that link to the defined risk.

(e) Time-frames are seldom if ever defined, making the assessment of hazard probability somewhat subjective.

(f) Although a “scoring matrix” rather than a numerical multiplication is used, the approach does tend to obscure the difference between large-harm events with low probability and low-harm events with comparatively high probability.

(g) Although the use of the term “vulnerability” acknowledges, semantically, that, in many practical cases, the existence of a hazard does not inevitably lead to the defined harm, the term generally is poorly defined and obscures a large and very complex topic.

2.6.3 Accumulated scoring approaches

A number of authors have noted that, for many practical “harm” events, there is a large range of types or categories of “hazard”; lacking any uniformity, these authors have attempted to consider each disparate type of hazard separately, and then to merge or separately represent the resulting metrics. Similarly for “vulnerability”, some authors have developed metrics for “vulnerability” using various
definitions of the term and various levels of precision of the terminology, and have
developed a metric of the general form of Equation 7.

\[ V = fn \{ S_1, S_2, S_3, \ldots \} \]

Equation 7

where each "S" score is obtained from a lookup table that uses textual definitions of
various degrees of some attribute and assigns a numerical score to each – or group-
consensus approach. As an example, Liu and Zhang (2011) analyse several
computer-vulnerability reporting systems and propose a composite scoring system.
The “scoring” approach is very common and coarse definitions (e.g. “High” “Medium”
and “Low”) are used in matrix representations of risk and consequence, in many risk
types of indices, including numerical, colour-codes and letters, and recommends that
risk indices should be numerical and mapped from specific risk values. The
researcher also proposes that decisionmakers should consider developing measures
that are derived from several such values.

Several researchers have recognised the difficulties of quantifying networks
that are heterogeneous and that have factors that are not readily codified with graph
theory notations, and have attempted to address these issues by developing numbers
of separate indices and then combining these indices into a single value. Examples
of this approach are included in the work of Zhang et al. (2009), who propose
integrating the use of several types of index, including the capability of supplying
power safely, static voltage security, topological vulnerability, transient security and
risk indices. Afgan and Veziroglu (2012) envisage a set of "quality indicators". A
"disturbance" moves one of these from its static value and the system recovers, i.e.
returns to the static value over a time interval. The authors integrate the disturbances
over time, then apply a weighting factor to each of these integrals using a separate
weighting factor for each integral and then add the sum of the (weighting*integral)
values to derive a "resilience index" for the system. Wang et al. (2012) assert that no
single approach to the vulnerability of interdependent infrastructures, and hence a
framework of analysis, is required. They consider several graph-theory-base network
metrics as possible design criteria, consider long-term vulnerability and specific
vulnerabilities separately and attempt to rank the significance of critical components.
Khatri and Vairavamoorthy (2011) offer what is effectively an accumulated scoring approach, because they use a consensus approach to developing vulnerability indices, and values for fuzzy set inputs. Gheorghe and Vamanu (2008, p. 3) state that “A virtual example of vulnerability analysis, using an indicator-based diagnosis, for the case of New Zealand is being presented, by way of an illustration” and “… whereas for risk one does have a formula, that says that, the risk of a disruptive event equals the probability of the event’s occurring, times the measure of event consequences powered to a subjective consequence perception exponent”. In contrast, there is no similar formulation for vulnerability. These researchers conclude (p. 8) that

“The exercise reported in this paper should be considered an investigation window into the complex topics of vulnerability assessment... model adopted to understand and quantitatively estimate the vulnerability of complex interdependent ‘system of systems’”.

Moore et al. (2007) and Gheorghe and Vamanu (2004) also describe accumulated scoring approaches. Accumulated scoring approaches have a common defining characteristic: they identify a set of factors, then develop, by consensus or lookup table or other approach, numerical values that may be precise or fuzzy for each of these factors and then arithmetically manipulate the numerical values to develop a single indicator value. The strength of this approach is that almost any list of “factors” can be addressed and the weakness is that each of the “factors” actually has dimensions, but the factors are treated as dimensionless when they are combined. Two specific problems can arise from this weakness: firstly, the factors may be interdependent; secondly, the numerical treatment can obscure underlying issues; for example, one system may score high on one factor and low on another factor whereas another system may have opposite scores for the same factors, generating the same combined index.

2.6.4 FMEA and related approaches

“Failure modes and effects analysis” (FMEA), USDoD (1980) considers a well-defined and generally simple engineering system, tabulating for each individual component the consequences of failure (categorised as “fail open”, “fail closed” or “fail fixed”). The FMEA approach will generally show just how many “hazards” can contribute to a single defined “harm”.

58
2.6.5 Networks and graph theory

A significant number of publications, e.g. Chopade and Bikdash (2011) and Yazdani and Jeffrey (2012), apply the basic notations of graph theory in their analyses; this approach therefore warrants a close examination. A network is represented as a collection of nodes that are connected by “edges”. These can be represented as a two-dimensional matrix of nodes, with the matrix values representing the connections between each node. It is also quite possible to represent a graph as a simple table in which each tuple corresponds to a “connection” or “edge”, and records the start and end vertex and the edge details. Having represented a network either as a table or as a matrix, various analyses can be applied. Scale-free or “small world” networks can be distinguished, as explained by Barabási and Bonabeau (2003) and others. “Connectedness” or various other metrics such as spectral gap, algebraic connectivity, clustering coefficient, meshedness coefficient and degree distribution can be calculated, as described by Yazdani and Jeffrey (2012). Those researchers use these approaches to describe the topological characteristics of a network and propose that the meshedness coefficient and the algebraic connectivity coefficient are particularly significant. The effect on the path between two vertices can be calculated, if a specific vertex or a set of vertices is removed. The effect on the path between two specified vertices can also be assessed, if one or more nodes are removed. Many analyses of this type have referenced the seminal work of Barabási and Bonabeau (2003), who showed that a “scale-free” network is robust against random node attacks but is vulnerable, in terms of network performance, to attacks on specific, highly connected nodes. A network, as considered in this paper, is always homogeneous. Although this conclusion has not been disputed, other authors such as Yazdani and Jeffrey (2012, p. 3) state that “The algebraic connectivity of a graph is a non-negative number whose magnitude represents structural robustness against efforts to decouple parts of the network”. These authors then move from an examination of the difficulty of assigning adequately representative values to edge weights, to the use of the “entropic degree... a quantitative measure of node importance by which network nodes may be ranked according to their centrality and failure induced impact on network performance”. These authors consider that their key finding is that the “demand-adjusted entropic degree” provides a measurement of node centrality and is useful for the analysis of
infrastructure networks that are geographically constrained. Yazdani and Jeffrey (2012a) also develop several mathematical descriptors of water supply networks, and attempt to correlate these with measures of “robustness”. Graphical representations allow these researchers to do several things, i.e. to apply rules and algorithms to adjacent vertices or nodes, to model the concept that proximity increases the probability of consequent failure, to statically or dynamically reassign either signed or unsigned weightings to the edges, modelling their “capacity”, and to analyse the number and location of vertices that must be removed before specified sections of the network become isolated. Graphical representation also allows the number and location of “edges” that must be removed before specified sections of the network become isolated – or before the path capacity between them degrades to some nominated level. By hypothesising changes to the network, it is possible to investigate the effect, on any of the above assessments, of adding redundant edges at various points of the network. Li et al. (2012), for example, focus completely on the efficiency of methods for adding various targeted links to a “network” in order to achieve specified “network parameters” or to develop metrics of how heavily loaded a network or network segment is, compared with its rated maximum load. This offers a proxy for “vulnerability”, if that definition of “vulnerability” is adopted, and is the same concept as that mentioned by Günneç and Salman (2011), although primarily by quoting Jenelius et al. (2006), who argue that “… vulnerability appears when the network is under pressure with full capacity, and a small amount of further stress may cause a major damage that may cascade through the system”.

Papers of particular note in this field include Shen et al. (2011), who present one of the most comprehensive theoretical analyses of the “vulnerability” of power law graphs: they do not attempt to use real-world examples, but their use of pairwise connectivity does perhaps make the otherwise very abstract paper valuable to this analysis. Yazdani and Jeffrey (2011, p. 4), commenting on urban water systems, note that, to properly represent a water distribution network, it would be necessary to include pipe loss factors, pump capacities etc., and, as the authors consider that this is too hard, they propose a simplified approach, treating networks as undirected graphs and using statistical properties of network topology and graph theory to identify the structural properties of the networks. Yazdani et al. (2011) use a graph theory approach to study the vulnerability of a specific water distribution system. Their paper
includes (p. 1577) a table of the graph properties that are commonly used in this and other works. As well as presenting results, this paper notes the limitations of the graph theory approach, commenting (p. 1574) that

"A comprehensive assessment of WDN resilience would entail an analysis and modeling of system performance or failure data ... the data needed to support such an analysis are typically non-existent ... proposed methodology may therefore be regarded as a relatively quick-to-implement precursor to more detailed trade-off analyses."

Buldyrev et al. (2010) apply graphical representations to two interlinked networks (a power grid and a SCADA system). These researchers start by stating the problem of cascading failure across networks, and state (p. 1025) that

"We present exact analytical solutions for the critical fraction of nodes that, on removal, will lead to a failure cascade and to a complete fragmentation of two interdependent networks. Surprisingly, a broader degree distribution increases the vulnerability of interdependent networks to random failure, which is opposite to how a single network behaves."

These authors use real-world data from a power network and an internet network. Their approach (p. 1025) is

"To model interdependent networks, we consider for simplicity, and without loss of generality, two networks, A and B, with the same number of nodes, N. The functioning of node Ai (i = 1, 2, ..., N), in network A, depends on the ability of node Bi, in network B, to supply a critical resource, and vice versa."

This is somewhat interesting, because the authors start by removing a set of nodes from one network, then effectively use the 1:1 correspondence between the nodes of one network and those of the other to derive a set of nodes to be removed from the connected network. They state (p. 1028) that "After this work was completed, we learned of the independent work of E. Leicht and R. de Souza, also addressing the challenges of interacting networks". Derrible and Kennedy (2010) consider transport networks, and specifically an examination of actual rail networks, and state (p. 3679) that "On a larger scale, by looking at 22 transit systems (bus and tramway) in Poland, Sienkiewicz and Holyst [41] found that some systems appeared to show a scale-free behavior, with scaling factors ranging from 2.4 to 4.1; most systems also appeared to be small-worlds". They note (p. 3683) that
"As a result, we prefer to use another indicator, which is common in the graph theory literature and was first introduced to transportation by Garrison and Marble [20]. It is referred to as degree of connectivity and is extensively used in network research by the transportation community. Mathematically, it is essentially identical to the clustering coefficient defined above…"

Baldick et al. (2009, p. 4) consider electrical power systems. They state that

"The combinatorial growth in the number of ways cascading failures can occur make them very difficult to analyze, and [37] develop a continuous-time Markov chain model of a dependability system that explicitly tackles this problem".

A graph theory approach to modelling a power grid system is proposed, and the authors state (p. 5) that

"A cascading failure model based on small-world networks was proposed … and can be used to identify the vulnerable lines. The model assumes that a node will fail if a given fraction γ of its neighbours have failed … the process will become cascading when these initial failures lead to subsequent failures due to exceeding of the fraction γ”

The authors conclude (p. 7) that “Since power system cascading is diverse, complicated, and computationally intractable, there is no single model, tool or approach that can address all aspects of cascading or answer all the questions about managing the risk of cascading failures”. Estrada (2007, p. 296) states that

"In a network representation of a food web, nodes represent species and links represent who eats whom in the ecosystem … This kind of representation permits to analyse the similarities and differences between complex systems of very different nature … food webs have less-skewed uniform or exponential DDs (Dunne et al., 2002a). However, they also display high fragility to intentional removal of the most connected nodes."

This paper proposes (p. 297) an interesting distinction between a network that can be readily split and one that cannot. The concept of a good expansion network is described as

"We start by defining informally the concept of network expansibility. A food web having “good expansion” properties is the one that cannot be divided in at least two isolated “large” parts by disconnecting a “small” number of nodes or links (Sarnak, 2004; Gkantsidis et al., 2006). These nodes or links, which make the function of bridges between these parts, are known as bottlenecks. Consequently, a “Good Expansion Network” (GEN) is a network without bottlenecks".
Wu et al. (2007, p. 2665) state their scope as "... the World Wide Web [2], metabolic networks [3], electric power grids [4] and many others". This paper quotes (p. 2665) Albert et al. (2000) as the seminal work on network classification, and the paper is built around the issue of whether the "attacker" has enough information to "target" the most vulnerable nodes and hence the issue of whether, when progressively removing nodes and observing network performance the least, most or intermediate important nodes are removed first. Dekker and Colbert (2004) note, as have other researchers that scale-free networks are resistant to random attacks, but not to targeted attacks, and that some infrastructure networks, e.g. telecom networks, are not "scale-free". Gheorghe and Vamanu (2004) state in the abstract of their paper that:

"Quantitative Vulnerability Assessment (QVA) oriented standpoint. Complexity induced vulnerability continues a line of work initiated under the joint Alliance for Global Sustainability (AGS)-ETHZ project VAMCIS (Vulnerability Assessment and Management of Critical Infrastructures)".

This work is aimed at critical infrastructures, and these researchers equate complex systems with graphical representations in which nodes (knots) represent components or people etc. and links (edges) represent interactions. The researchers describe (p. 78) "Connectivity as penetrability" and state (p. 79) "... higher connectivity rhymes with a higher vulnerability". The paper states (p. 79) that "... the higher the vulnerability relevance of the knots involved in the exchange path of any knot of origin, including the relevance of the knot of origin itself, the higher the vulnerability induced in the overall system by the respective knot of origin. Assumption 3: the higher the cumulated vulnerability relevance of the system’s knots, the higher the system vulnerability itself". The paper places a large reliance on DOMINO (decision support system software). The conclusions are not supported by any data, and this paper seems to primarily demonstrate the capabilities of the decision support software. No specific infrastructure is examined, and no specific conclusions are proposed or supported. Holme et al. (2002) present a purely theoretical approach, similar to many others, considering graph theory properties and effects upon vulnerability. Edge and node attacks are investigated, and the paper states (p. 056109-12) that

"None of the network models shows a behavior very similar to the real-world networks: Even the clustered scale-free network model with both high clustering and the scale-
free degree distribution...fails to describe successfully the scientific collaboration network”.

Agarwal et al. (2001, p. 142) state that “The objective of this paper is to present the basis of this new general theory of vulnerability which is applicable to all systems that can be represented as a graph e.g., traffic networks, pipe flows, electrical circuits etc.”

They develop (p. 147-148) an approach that they term "clustering", which they claim to be a process by which the structural vulnerability concepts can be embodied into a graphical representation. Albert et al. (2000) have published a seminal work on scale-free networks, concluding that "... we demonstrate that error tolerance is not shared by all redundant systems: it is displayed only by a class of inhomogeneously wired networks, called scale-free networks". Tu (2000) has one single aim, i.e. establishing that the internet is, in fact, a “scale-free” network. Misra et al. (2010, p. 560) state that “When high dimensional systems perform critical tasks, the task is shared by and dynamically allocated among the components. The ability to distribute function dynamically enables robust and self-stabilizing function in a highly variable environment, but breaks down when collective loads are excessive”.

These researchers’ conclusion (p. 560) is that "We have developed a neuromorphic information processing pipeline that can characterize the vulnerability of complex systems. The process consists of extracting a dynamic measure of network activity and ... succeeded in identifying extreme events that are distinct from high demand but otherwise effective system activity".

This conclusion uses the term vulnerability, but the approach and measure is more closely related to other authors’ description of resilience.

The specific aspects of graph theory that affect its potential applicability to this research can be enumerated as follows.

(a) The “nature” of the edges is assumed to be identical – hence a graphical representation of a transport system assumes that all edges are “roads” and the representation of a water supply system assumes that all edges are pipes carrying water. It is proposed that such systems be characterised as “homogeneous”.

(b) Many authors note that, for large networks, complete solutions are computationally impractical in most cases. Some authors, particularly Gómez
et al. (2011), not only acknowledge this issue but also propose approaches to make the problems more computationally tractable. These particular authors map a real network on to a “fictitious” network with hierarchical clusters – but they retain the same simplistic definitions of the underlying network, which is a road network, in which the probability of link failure is linearly proportional to the length of the road.

(c) “Nodes” or vertices are likewise assumed to have no function other than to aggregate, accept, redistribute or dispense whatever flows along the edges.

(d) The topology of the network is considered to be fixed; this presupposes that it is not possible for an operator to re-route edges in response to a “harm”.

(e) Whereas significant numbers of publications, such as Gómez et al. (2011), use real-world network data as test data, many authors acknowledge that the accuracy of the representation is problematic – specifically that there are factors affecting actual network performance that are not captured by the graph theory representation. Yazdani et al. (2011, p. 1581) state that

“However, it should be borne in mind that purely topological measurements may only partially describe the network structure and fail to entirely characterize its properties … oversimplification of water distribution systems into abstract graph models is extremely useful but far from sufficient”.

(f) Chopade and Bikdash (2011) consider the use of graph theory metrics for SCADA systems. The paper does not actually produce an approach or a metric that addresses interconnectedness – it basically applies graph theory to each of two networks individually, and generates graph theory results for each. The conclusion states:

“In this paper we used graph-theoretic vulnerability analysis to study the performance of networks … affected by the removal of vertices and edges … analyzed the effects of vulnerability on the structure of the networks. The major drawback with the generic graph analysis is that the performance measures are not related to the practical decision-situation … careful to note that the analysis of error and attack tolerance is perhaps too imprecise to enable a realistic study”.

(g) The definitions of nodes and edges are not necessarily simple: Guan et al. (2011) note an approach for SCADA systems using a directed graphical representation, where the nodes represent stages of a potential attack and the
edges represent expected time-to-compromise for different attacker skill levels. These authors also develop (using a set theory approach) a “reachability set”. Mishkovski et al. (2011) make a very important distinction within the application of graph theory to networks by distinguishing between an approach that considers the capability of individual paths, and thus distinguishes between a case where an edge failure causes flow to be redistributed, and an approach where a failure actually causes a cascading failure because of a sequential overload of paths.

2.6.6 Hierarchical systems

Several authors consider treating systems as fundamentally hierarchical (tree) structures. In particular, Eusgeld et al. (2011) state that there is no universally accepted definition of the term “system-of-systems” but consider that this phrase should be applied to distributed and possibly independently operating systems that evolve with time. These authors consider the topic of interdependencies between critical infrastructures and reference the work of Rinaldi et al. (2001). These researchers assert that the high level architecture (HLA) approach with an underlying agent based modelling (ABM) approach is the best approach for modelling the interactions between the SCADA system and the power generation system under consideration. The model allows them to evaluate a small number of specific types of “hazard”, and to detect some unrecognised vulnerabilities. This paper presents preliminary conclusions: the researchers acknowledge that their model is still under development, that their results are preliminary and that their model is highly targeted at a specific case. The paper demonstrates that detailed modelling of a specific system can uncover vulnerabilities, but the authors acknowledge that such a detailed modelling approach cannot necessarily be extended to every case in which systems interact.

2.6.7 Cellular automata and agent-based systems

Zio et al. (2007, p. 196) note that “The network security with respect to the hazard is evaluated by combining the modeling and computational powers of Cellular Automata (CA) [2] and Monte Carlo (MC) simulation [3]”. The authors identify (p. 197) the basis of cellular automata (CA) computing as
"CA are mathematical models of dynamic systems. The dynamics of CA unfolds at discrete time steps on a discrete lattice of cells \( L \), typically assumed homogeneous (all cells bear the same properties) [2].

This appears to be useful for the specific cases investigated – which are limited to homogeneous networks, in which finite delays to "infection" are caused by the network "edges". However, the usefulness is limited by the inherent "OR" assumption, i.e. that a node passes "infection" to all connected nodes, as soon as it is "infected" by any one of its connected nodes.

Oliva et al. (2010, p. 76) state that

"Infrastructures such as energy grids, transportation networks and telecommunications systems are critical to the welfare, economy and security of every developed country ..." The paper acknowledges the difficulty of adequate modelling. The paper quotes Agent Based Modelling and Simulation (ABMS). In the discussion, (p. 80), the authors state that "Although the IIM framework is compact, elegant and capable of modeling cascading effects, the high level of abstraction does not support accurate analyses of the real nature of dependencies".

2.6.8 Other approaches and theories

A number of other theories and approaches are reported. The following approaches have been applied to fields similar to that of this thesis, and so are examined.

Normal accident theory: Perrow (1984) has proposed the phrase "normal accidents", and has asserted that it is only necessary for a system to be complex, tightly coupled and capable of generating a large harm in order for such a harm to become inevitable. He proposes that individual errors and faults are inevitable and that, sooner or later, a particular error will cascade within a tightly coupled system to generate a catastrophe. Perrow (1984) basically asserts the initial premise for this thesis but, where he simply asserts inevitability, this thesis characterises and quantifies the exposure of a technological system and thereby illustrates how the imputed vulnerability can be effectively reduced.

Chaos theory: “Chaos theory” considers systems in which minor variations to input conditions may cause very large changes to outputs. Examples include weather patterns and vertical pendulums. The theory is commonly associated with the “butterfly wing” effect, an apocryphal scenario in which the beat of a butterfly’s wing
triggers a cascade of effects leading to the downfall of a remote kingdom. The original work in this field was by Lorenz (1963). Catastrophe theory has similarities to chaos theory, dealing with the behaviour of systems that exhibit sudden changes in behaviour, e.g. because of structural failure. As the current work concentrates on characterising the relative vulnerability of technological systems to well-defined changes of behaviour, these fields appear to have limited application to this work.

Complexity theory: Complexity theory has similarities to chaos theory, and was historically derived from systems theory thinking, is primarily applied to organisations and deals with systems of highly adaptive components. As such, it is of limited application to the topic of this work. Exemplar publications include that by Manfred (2010).

“Truck hit factor”: This measure, which has been given a number of names, including “bus/truck factor” and “bus factor”, has been used in the software development field to measure the number of software development team members who could become unexpectedly unavailable, without jeopardising a project. Although the context is a homogeneous system comprising only individual team members, the metric assumes that any team member can take the role of any other team member and so the factor is slightly different from the graph theory factor, which established that a number of broken links were required to isolate system input from system output.

Cognitive mapping: Murungweni et al. (2011) propose the use of “fuzzy cognitive mapping” and apply it to the rural livelihoods and work in the Great Limpopo Transfrontier Conservation area, which is in South Africa. Their objective is to assess the vulnerability of the population to the various hazards faced. This is a qualitative approach, in which stakeholders and focus groups define a set of state variables and then the interactions, represented by directed and weighted arrows, between these state variables. The effects of a small number of scenarios, e.g. drought, are also represented by weighted directed arrows that are linked to relevant state variables. The authors effectively consider that, if an arrow carries a heavy weighting (focus group derived), then the target is highly vulnerable to the “source” of the arrow, which they assume is the hazard. Akgun et al. (2010, p. 3561) state that “Vulnerability can be defined as a “weakness in the system defended” in a most common and simplest way”. This paper states (p. 3562) that:
"Vulnerability assessment problem can be recognized as a group decision-making (GDM) problem under multiple criteria. Therefore, there is a value in considering fuzzy set theory and GDM methods for critical facility vulnerability assessment …"

This is an example of an accumulated scoring approach, in which a single assessment is achieved by using a scoring system for disparate elements, and then the “scores” (initial vulnerability values) are aggregated numerically. Newton et al. (2006) use a Bayesian belief network to predict the impacts of commercialising non-timber forest products on livelihoods. Murungweni et al. (2011) state that “… BBNs and FCMs have the ability to combine quantitative and qualitative information and have some similarity in the way they use a transparent, graphical representation of the functioning of the system, which can supplement existing, less transparent frameworks that analyse vulnerability (e.g., Fraser 2007, Ericksen 2008)".

2.7 A taxonomy of published techniques

Several orthogonal dimensions can be identified within these analysis approaches, and will help the classification of the techniques described above. These are proposed as follows.

<table>
<thead>
<tr>
<th>Title</th>
<th>Classification feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time-frame</td>
<td>It is possible to consider techniques whose applicability is limited to the short term, e.g. supply chain disruptions, to the medium term, e.g. natural disasters, or to longer term issues, e.g. societal breakdown.</td>
</tr>
<tr>
<td>Geographical constraint</td>
<td>Techniques can be classified according to whether they are relevant to a localised geographical area (managing the effects of natural disasters is a large field of study), or whether they have wider geographical significance.</td>
</tr>
<tr>
<td>Homogeneity of technology system</td>
<td>Techniques can be classified according to whether they deal with a single, homogeneous “service” flowing in a network or diverse “services” or “flows”, or whether the technique envisages the creation of intermediate product streams. A system that considers a single product or service can be characterised as “homogeneous” and, in contrast, a technological system that involves a range of goods and services can be characterised as “heterogeneous” or “inhomogeneous”.</td>
</tr>
<tr>
<td>Accuracy of definition</td>
<td>A technique can be characterised by the accuracy of the definition of the technological configuration to which it is applied.</td>
</tr>
</tbody>
</table>
A technique can be classified by the approach used for the identification and classification of harms and hazards, and specifically by noting whether hazards are identified by brainstorming approaches, or by some analytical approach.

A technique can be characterised according to whether it develops quantitative, semi-quantitative or qualitative results – and whether the results can be used to test whether a proposed change offers any, or a defined level of, improvement in vulnerability.

A technique can be characterised according to whether the analysis is based on real data or on an expert opinion of probabilities.

Table 3: Classification of published techniques

<table>
<thead>
<tr>
<th>Name</th>
<th>System type</th>
<th>System configuration</th>
<th>System state defined</th>
<th>Time-frame identified</th>
<th>Harm identification method</th>
<th>Hazard identification method</th>
<th>Hazard characterisation</th>
<th>Exposure quantification</th>
<th>Quantitative or characterised</th>
<th>Dynamic or static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk analysis</td>
<td>I</td>
<td>N</td>
<td>N</td>
<td>I</td>
<td>B</td>
<td>B</td>
<td>EC</td>
<td>N</td>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>Risk + Vulnerability</td>
<td>I</td>
<td>N</td>
<td>N</td>
<td>I</td>
<td>B</td>
<td>B</td>
<td>EC</td>
<td>N</td>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>System vulnerability</td>
<td>I</td>
<td>N</td>
<td>??</td>
<td>I</td>
<td>D</td>
<td>B</td>
<td>EC</td>
<td>N</td>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>Resilience</td>
<td>I</td>
<td>N</td>
<td>Y</td>
<td>D</td>
<td>D</td>
<td>B</td>
<td>D</td>
<td>N</td>
<td>Q</td>
<td>D</td>
</tr>
<tr>
<td>Accumulated scoring vulnerability</td>
<td>I</td>
<td>N</td>
<td>N</td>
<td>I</td>
<td>B</td>
<td>B</td>
<td>EC</td>
<td>N</td>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>Network model</td>
<td>H</td>
<td>Y</td>
<td>N</td>
<td>S</td>
<td>D</td>
<td>B</td>
<td>B</td>
<td>Y</td>
<td>Q</td>
<td>S</td>
</tr>
<tr>
<td>AB modelling</td>
<td>I</td>
<td>Y</td>
<td>Y</td>
<td>S</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>N</td>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>FMEA or FTA</td>
<td>I</td>
<td>Y</td>
<td>Y</td>
<td>I</td>
<td>D</td>
<td>D</td>
<td>B</td>
<td>N</td>
<td>C</td>
<td>S</td>
</tr>
<tr>
<td>PROPOSAL</td>
<td>I</td>
<td>Y</td>
<td>N</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>B</td>
<td>Y</td>
<td>Q</td>
<td>S</td>
</tr>
<tr>
<td>Criteria</td>
<td>Values</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System type</td>
<td>I for heterogeneous system, H for homogeneous system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System configuration</td>
<td>N for not explicitly defined, D for defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System state defined</td>
<td>N for not defined, D for defined in detail, B for general system state (e.g. bulk loading) defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time-frame identified</td>
<td>N for not defined, I for implicitly identified as &quot;life of project&quot;, D for defined, S for snapshot (i.e. instantaneous)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harm identification method</td>
<td>B for brainstormed value, D for derived value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazard identification method</td>
<td>B for brainstormed, D for derived from configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazard characterisation</td>
<td>B for Boolean, with assumption that it is above tolerable limit, D for defined quantitatively, EC for expert classification, P for predefined, D for derived</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output type</td>
<td>Q for quantitative, C for categorised</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation of system response</td>
<td>S for static, D for dynamic (time-domain response)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Taxonomy of techniques related to risk and vulnerability

2.8 Conclusions from review of published material

2.8.1 Summary of published material

Several key points, relevant to the clarification of the field of research, can then be distilled from the survey of publications.

(a) The resilience-related techniques generate time-domain responses from a specific system rather than considering what “breaks” the system.

(b) The risk and accumulated scoring-related techniques do not explicitly characterise the underlying technological system.

(c) There is widespread recognition that complex and interconnected systems tend to generate vulnerabilities.

(d) The literature also clearly, and perhaps obviously, identifies that a hazard exists only if it is linked to a “weakness”.

(e) The graph theory approaches are relevant to homogeneous systems only.

(f) The FMEA and similar approaches are relevant but need adaptation to characterise the underlying system.

(g) No quantitative measure of exposure (which is colloquially associated with vulnerability) that can be applied to a heterogeneous system has been identified.
2.8.2 Analysis of gaps in the literature

Published studies have considered a number of systems, including water distribution systems, power distribution systems, communications systems and a range of supply chains. The effects of a failure upon an individual end-user are considered to be significantly different from the effects of a failure upon a system operator and there is a need for an examination that focuses on an individual end-user. Published studies that develop quantitative measures other than expert-assigned scores have related to homogeneous systems, i.e. systems in which a single type of goods or services is transported. The definition of scope established in the introduction has been clarified to focus upon the end-user’s dependence on complex heterogeneous technological systems. The literature includes many approaches to the assessment of vulnerability. Most published assessments relate to systems, and it can be noted that the focus on individual end-users allows a clearer definition of the fail criteria for the technological system to be evaluated. Published studies have revealed techniques that provide quantitative analyses of homogeneous systems but not practical quantitative measures that can be applied to heterogeneous systems, despite the observation that most technological systems supplying goods or services to individuals are in fact heterogeneous. Analyses of heterogeneous systems have generally not considered the specific configuration and the numbers of weaknesses in a system, despite a widespread awareness that systems with more weaknesses result in a user who is more vulnerable to that system. Many reviewed publications have relied on expert opinions of the level of risk, yet have not addressed the case where hazards are intelligently guided and whose occurrence is not random. Dynamic studies of complex heterogeneous systems could be made for defined initial states, if complete response functions for all components were available. Although certainly of interest, published material has concluded that techniques to allow adequately complete studies of this type are impractical because of the lack of availability of input information and computational effort. Whereas high levels of vulnerability are intuitively and generally attributed to long supply chains and complex systems with “many things that can go wrong”, there is a need for an approach that quantifies this attribute.
2.8.3 Summary; development of research question

In summary, an opportunity has been identified for the development of an approach that will evaluate the vulnerability, incurred by a typical end-user, to a heterogeneous technological system that supplies goods or services. The research question originates from the observation that the identified group of end-users is dependent for its continued mode of life upon the supply of goods and services that are in turn dependent upon long chains of processes and intermediate products. These long chains will probably expose the end-users to a deficit of security in the continuation of their lifestyle. The configuration of these chains, and their length, clearly contribute to the end-user's vulnerability, yet the effect of the length and the configuration of these technological chains has not been adequately explored. The research question proposes to explore this issue and to derive conclusions regarding the exposure of present technological systems, and conclusions regarding means of decreasing end-user vulnerability.

Chapters 1 and 2 have, by an iterative process, clarified the field of research and reviewed the current state of knowledge in that field. These chapters have also clarified a specific topic that is not adequately addressed in the literature, and have demonstrated that a contribution to this topic would be of significant interest.

2.8.4 Research question

Deriving from this process, the research question is established as:

For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used, and what reductions can be obtained by changes to the technological approach or configuration?

This research question can be considered in two parts, identified as RQ(a) and RQ(b).

RQ(a): For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used?

RQ(b): For goods or services delivered to end-users, what reductions of vulnerability can be obtained by changes to the technological approach or configuration?
3. METHODOLOGY

3.1 Introduction

This chapter develops a methodology for answering the research questions, and for generating the contribution to the topic. The requirement for a quantitative assessment of the vulnerability presented by a technological system makes it essential to specify a method that has an established theoretical basis, to generate a measure of vulnerability. The investigation of contributions of technological systems to end-user vulnerability requires applied research in order to carry out an exploratory, formulative and descriptive analysis of the topic. By applying a quantitative measure of vulnerability, the research will gain familiarity with the extent of current vulnerabilities and will develop new insights into approaches for reducing these vulnerabilities.

3.2 Research phases

The methodology establishes five phases for the research. These are described below.

**Phase 1** develops and justifies a theoretical basis for the analysis of the exposure of an arbitrary technological system; a method of application of the theoretical basis is also generated. The development of this theoretical basis is a contribution to the research field.

**Phase 2** describes how the selected goods or services, which are to be the subject of the initial analysis, are selected. Phase 2 also describes how data required to analyse these technological systems is to be obtained, validated and described.

**Phase 3** describes the analysis (using the method established in phase 1) of the data obtained as a result of phase 2. Numerically, this analysis demonstrates the relative vulnerability of the end-user to the technological systems used to supply each of the selected goods or services. The outcomes of this phase provide the answer to Research Question (a) (RQ(a)). The outcomes from this analysis form the basic data required as input to the next phase of the research, and are likely to be as significant as the numerical analysis of exposure.
Phase 4 uses the outputs of phase 3 and the data generated within phase 2. From these two inputs, this phase of the research generates a set of hypotheses changes, each representing a specific change to the technological system identified and described in phase 2 of the research. These allow the hypothetical approaches to a reduction in end-user vulnerability to be tested.

Phase 5 of the research again applies the methods generated in phase 1 to the hypothesised modifications to original technological systems, developed in phase 4 of the research. The outcomes of this analysis test the hypotheses developed in phase 3 of the research, and allow answers to Research Question (b) (RQ(b)) to be developed. These research phases are illustrated in Figure 2.

3.3 Phase 1: development of theoretical basis

A metric is required to answer the research question, and a theoretical basis for such a metric must be developed and justified. This section builds upon existing techniques and theoretical bases, and on an analysis of issues not covered in the literature, to develop a metric, and a theoretical basis for that metric, that can answer the research question.

3.3.1 Theoretical basis

This section covers the definitions needed as the basis of any formulation of a theoretical basis, and the criteria for a theoretical basis in terms of both defensible theory and capability to answer the research question. In order to develop a theoretical basis for "exposure", which measures the technological contribution to vulnerability, several definitions are required, and are proposed in table 5.
3.3.2 Criteria for theory

The research field, as defined by the research question, specifies the evaluation of the technological contribution to end-user vulnerability. The research question implicitly includes several criteria for an acceptable theoretical basis.

(a) As the "technological system" (as distinct from the final-goods-distribution system) must create and supply goods to the end-user, a heterogeneous system is described, i.e. a system having processing steps and intermediate goods or service streams. A theoretical basis for assessing the contribution of the technological system to end-user vulnerability must allow evaluation of the contribution of heterogeneous systems.

(b) The study must be indexed to the security of the end-user, as opposed to either infrastructure or supply chain security per se.
A nominated service level must be specified, to describe and quantify the specified goods or services to be delivered to the end-user.

A quantifiable metric must be generated, and this metric must be demonstrated to provide a measure of the contribution of the technological system to the user’s “vulnerability”.

Since the research questions seeks to “measure of vulnerability can be attributed to the technological systems”, the quantifiable measure must be based upon, i.e. derived from, the configuration and components of the technological system alone, with no necessity for direct consideration of the probabilities of hazard occurrence or the instantaneous states of the technological system, or the correlations between hazard frequency and component state.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-user</td>
<td>The proposed approach is defined in terms of a single, representative urban-dwelling end-user. It is proposed to simply note the number of end-users likely to be represented for each example study.</td>
</tr>
<tr>
<td>Service level to end-user</td>
<td>For any case, it is necessary to define a service level for the goods or services supplied to an end-user. This will allow a Boolean evaluation of whether the service level is, or is not, available. Separate analyses can be considered for differing service levels if required.</td>
</tr>
<tr>
<td>Technological system</td>
<td>Defined as a heterogeneous system involving creation and transmission of intermediate products and delivers goods or services to the end-user.</td>
</tr>
<tr>
<td>Functioning of technological system</td>
<td>A technological system has been defined to include processes and intermediate streams that may include partially complete goods or services, essential information etc. As a service level for the delivery of the final goods or services is defined, the delivery of these can be defined using a Boolean value (True/False). The level of intermediate services can then also be defined, as Boolean variables, according to its effect on the service-level delivery of the final goods or services.</td>
</tr>
<tr>
<td>processes and intermediate streams</td>
<td></td>
</tr>
<tr>
<td>Time-frame for consideration</td>
<td>Timeframes for consideration are:</td>
</tr>
<tr>
<td></td>
<td>• Operational time-frame, in which the technological system is dependent only upon inputs in order to function.</td>
</tr>
<tr>
<td></td>
<td>• Maintenance time-frame, in which minor spare parts and additional skills are required in order to return the system to operational mode.</td>
</tr>
<tr>
<td></td>
<td>• Replacement time-frame, in which major sections of the technological system must be replaced.</td>
</tr>
<tr>
<td></td>
<td>These are proposed because they have well-defined differences in technological requirement and hence significant differences in the exposures calculated for each. Maintenance and replacement scenarios include durations in which equipment can be acquired or (re)created.</td>
</tr>
</tbody>
</table>

Table 5 Proposed definitions of key terms
3.3.3 Validation of theoretical basis

The theoretical basis proposed for the calculation of exposure is presented, and, provided that the inputs are adequately defined as Boolean values, the proposed theoretical basis allows calculation of exposure in terms of a Boolean algebra that is provable in terms of formal logic. As proposed by Davis et al. (2007), the question of whether the proposed approach will generate novel or more useful insights into a phenomenon can be tested. Two complementary approaches are proposed. Firstly, classical risk analysis can be applied to one of the examples selected for analysis as part of this research; the comparison of outputs will illustrate whether additional insights are generated by the proposed approach. Secondly, in the development of the theoretical basis for the "exposure" concept, it was noted that homogeneous systems can be considered as a subset of all possible heterogeneous technological systems. It is therefore possible in principle to either take a homogeneous system that has been analysed in a publication related to homogeneous systems, or to generate an exemplar homogeneous system and analyse this using both the exposure approach and one or more of the graph theory metrics that are commonly applied to homogeneous systems. It would also be possible to use a process of formal logic to show that the proposed exposure metric would generate outputs of equal significance to the homogeneous system analysis approaches noted in the literature.

3.3.4 Implementation of analysis

The approach used to answer the research question represents each technological system using a Boolean algebraic expression, and evaluates that expression in a truth table, for combinations of inputs. Evaluation of that expression requires that the inputs to each truth table line item be represented, and that the Boolean expression generating the output from each table be calculated. Almost all computer languages contain provision for Boolean operations and for the construction of complex expressions by nesting these. It can be noted that software Expert system shells are effectively no more than constructs of interlinked IF–THEN–ELSE rules applied to named variables. As spreadsheets, and indeed almost all computer languages, include the capability to represent Boolean expressions, the criterion for the selection of an implementation approach gives prominence to the simplicity and transparency of the representation of data and outputs. It is proposed to use a
spreadsheet approach to the construction of truth tables for each example studied, and it is noted that other approaches could generate identical outputs.

3.4 Phase 2: development of initial data sets

The research question relates to technological systems that deliver selected goods and services to end-users. Phase 2 of the research has generate the data relating to technological systems for delivering selected goods or services to end-users. The task has two distinct sub-tasks: making the selection of the goods or services to be analysed, and acquiring and verifying the data for initial analysis.

3.4.1 Selection of examples for analysis

The research question indicates that the required data for analysis will relate to selected goods or services without further definition, and to end-users – also without further definition. The analysis then requires the selection of goods or services, and a definition of the end-user. Earlier sections of the thesis have included background and scoping statements that provide context for this work, and hence can guide the definitions and selections made within this task. Specifically, an earlier section of the thesis has noted that urban-dwelling individuals requiring essential goods and services are increasingly vulnerable to failures of complex, interlinked and heterogeneous technological systems. Current risk analysis techniques do not quantify the impact of existing configurations, or proposed reconfigurations, of a technological system from an end-user perspective. There is a need for a means of comparing the vulnerabilities imposed on such end-users by technological systems, and of evaluating the changes proposed to reduce end-user vulnerability. As analysis is to be applied to a selection of goods or services, example studies involving selected goods or services are implied. Under the heading of "When to Use a Case Study Approach", Baxter and Jack (2008) consider that a case study approach should be used when the objective is to answer questions of how and why observed outcomes occur and when it is important to consider the contextual conditions of the studied case.

End-user. In selecting case studies, Eisenhardt (1989) notes that the essential first step is defining the "population" from which the case studies will be selected. Eisenhardt (1989, p. 536–537) proceeds to note that for the "selection of
cases... the concept of a population is crucial, because the population defines the set of entities from which the research sample is to be drawn". For this study, the "population" is the complete set of end-user needs. The research question neither refines the population by stipulating typical nor refines any other particular descriptor for the end-user; however, the introduction to this thesis references urban individuals and cites apartment dwellers as an example. This effectively narrows the scope of the "population". Although the research question does not include any finer definition, considerations include the scope of persons who could possibly fit within the definition, the homogeneity or otherwise of the group and various practical issues.

Practical considerations would suggest that data would be indexed against users in significant Australian or New Zealand cities. This practical consideration would need to be challenged if it were considered that such cities were sufficiently atypical, in terms of the technological systems used to supply similar end-user needs, as to negate their use as an indexation basis. Australian and New Zealand cities are considered to be reasonably typical of cities of similar size in the developed world, in terms of technological approaches to supplying end-user needs, and hence are used as a basis for the indexation of data. It is therefore proposed to define the "end-user" as an individual who fulfils the following criteria.

(a) Lives in an apartment, and hence has limited practical capability for farming or for large-area solar collectors.
(b) Lives close to the centre of a city of more than about 200,000 individuals.
(c) Lives in Australia or New Zealand.
(d) Is employed, i.e. is assumed not to be severely financially constrained.
(e) Commutes more than 10 km to work, which is considered to be beyond the range of cycling or walking, for the majority of persons.

The selected group may be assumed to have built their lifestyle around a set of assumptions regarding the availability of certain goods and services; other groups have found alternative approaches to the disposal of sewage, the acquisition of fresh foods etc. However, for the selected group, it is not practical to transition to such alternative approaches in the time-frame that would be required, and hence the continued supply of services in substantially the current manner can be claimed to be "essential" to this common lifestyle.
**Selected goods or services.** The research question identifies supplied goods or services. A large range of goods and services exists. Several approaches could be proposed for the selection. It would be possible to use a hierarchy of needs, e.g. that proposed by Maslow (1943), and to make an arbitrary selection from each of the tiers of needs identified. It would also be possible to use a hierarchy of needs, e.g. that proposed by Maslow (1943), and to select, from one tier, all or most of the items that apply to the defined end-user. For example, if criteria for physical survival were selected, food, water and warmth needs would be identified. Yet another option would be to identify needs that are typical of some broad categories of indicative technological system that are involved in their production and delivery.

The analysis of the research opportunity has not specifically hypothesised that the current technological systems used to supply needs that are more essential to the target group were exposed to greater vulnerability than the current technological systems used to supply less essential needs; the analysis also has not hypothesised that the exposure of the technological systems and the resultant user vulnerability were correlated with the level of need. For this reason, approaches (a) and (b) are not proposed. The analysis of the research opportunity developed a hypothesis that some types of goods or services were currently more vulnerable than others, and additionally hypothesised that there were features of many current technological systems that represented particularly high vulnerability. Provision for testing these hypotheses suggests the need to identify broad categories of goods or services having somewhat similar technological approaches within categories, but the greatest breadth across categories. This reasoning suggests that a theoretical approach rather than a random sampling approach should be adopted for the selection of the goods or services to be studied. Eisenhardt (1989, p. 537) explains that, in such an approach, cases "... chosen to fill theoretical categories and provide examples of polar types... random selection is neither necessary nor even preferable".

Table 6 sets out several categories of goods or services from which case studies could be selected. A larger “population” of candidate goods and services could be developed, but the items listed in Table 6 are considered to be both significant and representative of a range of technological sophistication levels and end-user need-levels. Each item is described, and a very coarse-grained categorisation is made of
the level of need of the service, and the technological level of the current means of providing the service.

<table>
<thead>
<tr>
<th>I</th>
<th>Need</th>
<th>Need level</th>
<th>Tech. level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Water</td>
<td>High</td>
<td>Low</td>
<td>Potable water supply</td>
</tr>
<tr>
<td>2</td>
<td>Sewage</td>
<td>High</td>
<td>Med</td>
<td>Sewage disposal for apartment dweller</td>
</tr>
<tr>
<td>3</td>
<td>Power</td>
<td>High</td>
<td>High</td>
<td>Assume mains voltage (i.e. within acceptable voltage range)</td>
</tr>
<tr>
<td>4</td>
<td>Petrol</td>
<td>High</td>
<td>Med</td>
<td>Petrol delivered at local petrol station</td>
</tr>
<tr>
<td>5</td>
<td>Personal travel (few tens of km)</td>
<td>Med</td>
<td>High</td>
<td>Implying petrol or diesel, and road and car</td>
</tr>
<tr>
<td>6</td>
<td>Long-distance transport</td>
<td>Low</td>
<td>High</td>
<td>Generally implying air travel</td>
</tr>
<tr>
<td>7</td>
<td>Simple message</td>
<td>Med</td>
<td>High</td>
<td>A message to another individual</td>
</tr>
<tr>
<td>8</td>
<td>Personal or work information</td>
<td>Low</td>
<td>High</td>
<td>Capability to store and retrieve, view, edit and share personal information – family records, important writings, music, business and design information</td>
</tr>
<tr>
<td>9</td>
<td>Targeted first-aid</td>
<td>High</td>
<td>High</td>
<td>Case where required response to a medical situation is simple, but diagnosis and communication of correct action is essential. Choking, childbirth, fish-hook removal</td>
</tr>
<tr>
<td>1</td>
<td>Perishable food, local supply</td>
<td>High</td>
<td>Med</td>
<td>Implying short-shelf-life food requiring limited cold chain needed for distribution and chilling at end-user dwelling</td>
</tr>
<tr>
<td>1</td>
<td>Perishable food, remote supply</td>
<td>High</td>
<td>High</td>
<td>Implying short-shelf-life food requiring sophisticated cold chain distribution system and post-harvest treatment needed for distribution and chilling at end-user dwelling</td>
</tr>
<tr>
<td>1</td>
<td>Long-life foodstuff, local manufacture</td>
<td>High</td>
<td>Med</td>
<td>No cold chain required. Limited packaging required for transport. Limited stocks normally held</td>
</tr>
<tr>
<td>1</td>
<td>Long-life foodstuff, remote manufacture</td>
<td>High</td>
<td>High</td>
<td>Sophisticated packaging and distribution chain required, possibly with bulk and retail packaging separated and storage of seasonal produce. No cold chain required</td>
</tr>
<tr>
<td>1</td>
<td>Essential ongoing Medicine</td>
<td>High</td>
<td>High</td>
<td>Insulin? Clotting factor? Ventolin™, anti-coagulant, anti-depressants</td>
</tr>
</tbody>
</table>
Table 6: Identification and selection of examples for study

In order to generate the most broadly applicable answers to the research question, the examples selected should be representative of a range of products or services and typical of some broad categories of technological system required. These need to be representative and unbiased. The highlighted items from the above table represent both systems that are primarily long-life infrastructural systems (sewage), systems involving primarily the exchange of information, systems requiring planned and ad-hoc specialised production and delivery systems, and systems requiring essential commodities (e.g. fuel) and are therefore selected for study. As there is a need for comparison between systems and as it is not practically possible to select more than a moderate number for study, the above is considered to be a “fit-for-purpose” approach to the selection of examples for analysis.

3.4.2 Definition of examples

A methodology for defining the scope of the selected initial example studies, and for obtaining the raw data for each, is required. This requires a decision on the type of study to be undertaken.

Type of data required. Having selected examples of goods or services for study, a methodology for acquiring the data for initial analysis is required. It would be possible to identify a particular end-user, i.e. a specific individual, and a small number of clearly identified goods or services acquired on specific dates. The technological system that supplied those defined items could then be identified and would comprise experimental data. This would fall within Andrade’s (2009, p. 20) definition.
"The case study is “an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident”.

Yin (1984) develops a similar definition, i.e. that case studies are rich, empirical descriptions of particular instances of a phenomenon. A diametrically opposite approach would be to simply hypothesise example cases for the purpose of testing a proposed analysis method. Approaches similar to this are taken by some authors, e.g. Shen et al. (2011) in the investigation of theoretical aspects of networks. In considering the approach to be used, it is useful to review the process leading to the definition of the research topic. It was hypothesised that there were common factors spanning technological systems, which contributed to the vulnerability of a wide spectrum of end-users; this hypothesis needs to be tested. The research question additionally proposes a requirement to explore, quantitatively, the effects of hypothetical changes to technological systems. The "case study" approach, requiring a detailed description of a very specific example, therefore seems likely to fail to draw out the generality of conclusions indicated as required by the research question, and "constructed" examples will not offer the level of credibility required in order to answer the research question.

It is therefore proposed that, instead of analysing case studies, experimental data from a range of primary and secondary sources will be used to develop typical data that are demonstrably representative of the technological systems delivering the selected goods or services. For example, rather than examining the specific steps that conclude with a specific cabbage arriving on a particular individual’s dinner plate, the steps relevant to a small range of fresh green vegetables, to a person assumed to live in a representative inner city area, will be examined and a dataset that is representative of the technological system currently used to deliver perishable, locally produced foodstuffs to an end-user in an apartment building will be assembled. This approach effectively defines “simulation modelling”, generally following the description used by Davis et al. (2007), who defined simulation as “… a method for using computer software to model the operation of real-world processes, systems, or events (Law & Kelton, 1991)”.

Format of data required. The data for evaluation will then consist of descriptions of technological processes, intermediate streams and transport and
communication paths, raw materials and finished goods or services of the complete technological system required to deliver specified goods or services to end-users. These descriptions must be such that input parameters to the quantitative analysis method can be generated from the descriptions.

Methodology for acquisition of data. A definition of a representative "end-user" has previously been developed, and a small number of goods or services have been selected for evaluation. A description of the technological system, demonstrated to be representative of real-world cases, is required for each example studied. This section considers methodological options for acquiring the required data for each goods or service example to be analysed. The methodological options for acquiring the required data, for each example of goods or services to be analysed, include a survey approach, a multi-case study approach and a hybrid of these approaches. It is quite possible to use either informal case study data or indeed surveyed data as a means of ensuring that a simulation is an adequate representation of the "real world". Each of the candidate methodologies for data acquisition has specific characteristics; the positive and negative contributions towards answering the research question must be considered in selecting the methodology to be applied.

A hybrid approach is proposed, in which a "construct" dataset is developed for each selected goods or service example using background knowledge and publicly available information, and specific items of each such dataset are tested by limited survey of actual examples of the technological systems used for the particular goods or services. This approach is practical, and since the data is representative of real systems, its analysis can reasonably be claimed to generate useful and demonstrably valid answers to the research question. The proposed approach can be illustrated with an example: if "petrol supply at a local station" is the example of goods or services, background knowledge would be quite sufficient to establish that bulk supplies arrive via diesel-fuelled tanker and that electric pumps are used to meter and dispense the petrol. A relatively simple survey of retailers would confirm the approximate number and location of bulk supplies and the number of refineries. The use of selected sources of information to confirm specific aspects of example datasets is well known in case study literature; for example, Baxter and Jack (2008, p. 554) state
“A hallmark of case study research is the use of multiple data sources, a strategy which also enhances data credibility ... Potential data sources may include, but are not limited to: documentation, archival records, interviews, physical artefacts, direct observations, and participant-observation... In case study, data from these multiple sources are then converged in the analysis process rather than handled individually”.

In summary, datasets for the technological systems representative of those used for the delivery of each of the selected goods or services, to a representative end-user, will be developed from background knowledge plus publicly available information, and selected aspects will be clarified and validated by enquiry and by survey of actual systems. In validation of simulation data under the heading of "Strategies for Achieving Trustworthiness in Case Study Research", Baxter and Jack (2008) consider the importance for qualitative research of providing enough detail to allow the reader to assess the trustworthiness of the data and hence the credibility of the analysis. They note that such credibility will require careful formulation of the question, appropriate selection of case studies and sampling methods, plus systematic and detailed handling of information.

Adopting these strategies, this research will ensure that enough detail is provided to allow readers to assess the validity of the work, ensure that the research question is clearly written and use sampling strategies that will ensure that the simulation case studies are indeed representative of actual data and that the basis for this assertion is documented.

3.5 Phase 3: analysis of examples

3.5.1 Analysis outputs

The analysis of the initial examples will generate measures of the absolute and relative "exposure" of the technological systems that are studied. The theoretical basis of the proposed metric is developed within Chapter 4, where the validity of the Boolean algebraic representation of the technological system is argued, and where the exposure metric is justified as a valid measure of the contribution to the end-user's vulnerability. The exposure metric is established as the primary, but not the only, analysis approach for individual example studies. Beyond the metric of exposure, the examples will be treated in a similar way to case studies, and the processes of theory building from case studies, as described by Alaranta (2006), will be used. The process
of defining the components and boundaries of each exemplar technological system, and identifying each point of exposure, whether to single or multiple failures, is also an output of the investigation and allows an analysis of the specific contributors of various subsystems to the exposure metric.

This quantitative plus qualitative approach will analyse the hypothesis that some common technological systems are more exposed than others – and provide insights into the specific subsystems whose exposure values contribute most to the vulnerability of the end-user. In addition to the analytical method developed in Chapter 4 of this thesis, classical risk analysis of one of the examples will be carried out; this will demonstrate whether additional insights are generated by the evaluation of exposure for that example.

3.5.2 Interpretation of analyses

The dataset used as the basis for analysis, plus the information resulting from the analysis of the dataset, effectively form a "case study", in the terms used by (e.g.) Eisenhardt (1989) and also Yin (1984), who describe case studies as detailed descriptions of particular instances of a phenomenon.

In case study literature, the process of deriving theory and/or hypotheses from case studies is described by authors such as Eisenhardt and Graebner (2007), who note the research strategy of building theoretical constructs or propositions from empirical evidence described in case studies. Eisenhardt and Graebner (2007) also note that the process of building theories from case studies is a process that is poorly codified. An exposure metric, as developed in this thesis, is a single compound integer; it is useful for ranking the relative vulnerability of technological systems and for quantitatively assessing alternative proposals for changes to a particular technological system. The research question, "For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used, and what reductions can be obtained by changes to the technological approach or configuration?", implies a process of review and a process for the development and testing of theories and/or hypotheses. The analysis of the initial examples will allow the identification of the specific processes and streams (components of the technological systems) that contribute to the exposure of each studied system, and will allow descriptors of these to be categorised, with a view to
developing propositions that show generalisable principles that, in ranges of technological systems, cause increases in exposure, and hence in vulnerability of the end-user who depends upon the system. These identifications will also provide the foundation for the formulation of hypotheses (hypothetical theories) for a reduction in vulnerability.

3.6 Phase 4: hypothesising and testing changes to examples

3.6.1 Generating hypothetical changes

As the generation of alternatives is dependent on the outcomes of the initial analysis, this is the aspect that can be least well defined in advance of the initial analysis work. This exploratory research process of examining the results of the initial dataset analyses, proposing technological alternatives and examining the effects of proposed changes is considered to be one of the most potentially valuable aspects of the research. Davis et al. (2007) note that

“Although scholars writing about theory development (e.g., Dubin, 1976; Pfeffer, 1982; Priem & Butler, 2001; Sutton & Staw, 1995; Whetten, 1989) may have different emphases, most agree that theory has four elements: constructs, propositions that link those constructs together, logical arguments that explain the underlying theoretical rationale for the propositions, and assumptions that define the scope or boundary conditions of the theory. Consistent with these views, we define theory as consisting of constructs linked together by propositions that have an underlying, coherent logic and related assumptions”.

The research question proposes examining the effect of changes to the initial datasets (current representative technological systems). The basis for these changes will be developed as an outcome of the analysis of the initial datasets, i.e. if a particular item is found to contribute significantly to vulnerability in more than one of the initial datasets, then it would seem to be reasonable to define the characteristics of the item, seeking common factors. The identification of common contributors to user vulnerability will also allow the generalisation of the approaches to a reduction in user vulnerability.

This is considered to be a valid approach for answering RQ(b). Eisenhardt (1989) provides a tabular breakdown of the steps required to generate theories and/or hypotheses from case studies; in part, this process includes (Table 1) the "Interactive
tabulation of evidence for each construct" and "search evidence for "why" behind relationships…" Eisenhardt (1989, p. 539) also notes that this analysis of "within case" data is the "least codified part of the process". The inputs to the theory and hypothesis development task are the outputs of the analysis task. It must be noted that the analysis task is a simulation, rather than a case study, under the definitions used by Yin (1984) or Andrade (2009).

Having observed common characteristics of the processes and streams, which would be considered to be "constructs" in the term used by Davis et al. (2007) that contribute to the vulnerability of the end-user across multiple examples, propositions for the underlying causes can be assembled and categorised. From these propositions, hypothetical changes can be identified for testing.

3.6.2 Analysis of effect of hypothesised changes

RQ(b) is a "hypothesis-testing research" type of question, requiring approaches appropriate for this type of question. Within this task, technological changes that hypothetically reduce end-user vulnerability associated with the delivery of a particular type of goods or service that were developed in phase 4 will be tested. The test approach will be identical to that used in phase 3 of the research. Effectively, this task will be close in nature to an "instrumental" type of case study, as defined by Baxter and Jack (2008), i.e. accomplishes more than just understanding a situation, and additionally helps to refine theory and assists in our understanding of other matters. Eisenhardt (1989, p. 546) states in her conclusion that "... one strength of theory building from cases is its likelihood of generating novel theory", which is considered as justification for the approach. Hypotheses will have been formed by detailed observation of the specific processes, streams and subsystems that contribute to the exposure value, by deducing common characterisations of these, and then formulating exposure-reducing hypotheses based on those characterisations. The hypotheses will be tested firstly by simply observing decreases in exposure values for the delivery of the same service and service level, to the end-user, and by critically assessing whether the characterisations of exposure causes are either valid or optimal.
3.7 Phase 5: development of conclusions

3.7.1 Answering the research question

RQ(a) asks “For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used?” RQ(b) asks "For goods or services delivered to end-users, what reductions of vulnerability can be obtained by changes to the technological approach or configuration?" The "what reductions" phrase in RQ(b) indicates a need for a quantitative and qualitative evaluation of the effect of each hypothesised change.

Having tested the propositions (that are embodied in hypothetical changes), Chapter 8 not only will report the outcomes in terms of contributions to the vulnerability of the end-user, and thus supply direct answers RQ(b), but also will test the categorisations used to develop hypotheses and will synthesise the tested propositions into a small set of principles that could be described as "coherent logic", in the terms used by Davis et al. (2007). These, demonstrably generalisable principles will supply the most important contribution of the study.

The description and the definition of technological system “exposure” are considered to represent a contribution to the body of knowledge. The contribution can be described as follows:

(a) They expand both the concept of risk analysis, which is generally applied to a whole system without detailed indexation to system configuration, to take account of the configuration of the technological system in question. By insisting on a tighter definition of the system and the time-frame in question, more rigorous outcomes can be expected from the application of the risk analysis approach.

(b) They specifically identify the importance of identifying loci of weakness in a technological system, without consideration of the probability of hazard.

(c) They identify and describe the concept that, for a technological system supplying goods or services to an end-user, a (mis)guided hazard has a qualitatively different effect from a probabilistic hazard.

(d) They allow the consideration of heterogeneous systems, which is not possible using the graph theory analyses applied to homogeneous systems.
They allow demonstration, by reference to measurement theory, that they are a valid measure of the contribution of the defined technological system to an end-user’s vulnerability.

They allow the hypothesising of principles based on an analysis of initial examples.

They allow testing of these principles by analysing hypothetical changes to initial examples, showing that the principles are generalisable.

Chapter 1 has described the significance of the field of research. Answers and conclusions generated in this field can therefore be assumed not only to represent a significant contribution to the field of study but also to offer valuable application to society.

3.7.2 Development of general conclusions

The results from the analysis of hypothesised changes to the examples will themselves be reviewed. From the conclusions related to the example studies, more general conclusions regarding the value of the approach, and the applicability of the generalised conclusions, as well as the conclusions related to the specific examples will be presented.

3.8 Conclusion of methodology description

The methodology includes the development of a metric to measure end-user vulnerability. The methodology has proposed and justified the use of exemplar studies, analysed quantitatively, as a means of answering the research question. From initial analyses, hypothesised changes and re-analysis, the methodology has proposed the development of generalisable conclusions.
4. DEVELOPMENT OF A THEORETICAL BASIS FOR MEASURING VULNERABILITY

4.1 Introduction

Previous chapters have established both a gap in the awareness of the contribution of technological systems to end-user vulnerability and a gap in the theoretical basis for measuring this contribution. The first phase of the research, defined in Section 3.3, requires the development of and justifies a theoretical basis for the analysis of the exposure of an arbitrary technological system and a method of application of the theoretical basis.

This chapter commences by establishing the context of the measurement and the theoretical approach. A theoretical basis for representing an arbitrary technological system, and for demonstrating that the representation is a valid mapping from the real system, is developed and refined. Starting with the representation of an arbitrary technological system, a proposal is made for generating a measure of the contribution to vulnerability, which is the phenomenon of interest. That attribute is then shown to be a valid measure of the phenomenon of interest, described as the contribution of a technological system to end-user vulnerability. The accuracy, precision and scaling of the proposed measure are examined.

4.2 Context for a theoretical basis

The research question therefore requires the implementation and operation of an approach that meets the requirements for a contribution to the body of knowledge in the form of a valid measurement, as described by Hand (2004) and by Suppes (2009). In order to meet these requirements, it is necessary to represent a complex technological system, strictly within the identified context, which might involve a large number of operations and intermediate steps and partial design redundancies and possibly also single points-of-failure. The representation must at least be homomorphic in terms of the operations and streams, and preferably should be isomorphic in order to give assurance that the representation does not omit significant features of the real system. It is further necessary to identify, from that representation, an attribute that can be demonstrated to be a valid measure of the phenomenon of interest and to confirm that the metric is invariant with respect to irrelevant factors, that it incorporates all relevant factors and thus is complete, that there are no
correlated variables and that it has definable levels of both precision, such that independent researchers can obtain outputs that are numerically similar, and acceptable accuracy. It is also necessary to evaluate the scale factors of the metric, i.e. the rate of change and scope of values of the metric, and to evaluate how the values derived for the metric will correlate with the conclusions to be reached.

4.2.1 End-user services

The research question focuses on the delivery of goods or services to the end-user, and hence a proposed metric must relate to this. Adequate definitions of a service level and of the specific goods or services allow a Boolean variable to define this delivery or non-delivery. The descriptions of goods or services and a service level therefore allow a clear definition of “delivery” for a particular case, but do not preclude a separate examination of technological vulnerability associated with various different service levels.

4.2.2 End-user focus

The contribution of the technological system to the end-user's vulnerability, in regard to selected goods or services, is the context of the research. The emphasis is on the contribution of the technological system rather than the significance of the particular goods or services under consideration. However, the example studies will be selected with a view to examining goods or services that have a range of effects upon, and hence significance to, end-users.

4.2.3 Heterogeneous system description and representation

The contribution of the technological system to vulnerability cannot be constrained to consideration of that portion of the technological system that is responsible for the final distribution of completed goods or services. It must be assumed that the “contribution” arises from the whole technological system, which includes the incremental addition of value to the goods or services, which is distinguished from the simple distribution of goods that is implicit in the analysis of supply chains and in the analyses applied to computer communication systems and power or water distribution systems. The analysis of the contribution of the technological system to vulnerability therefore requires the characterisation of a
technological system that is heterogeneous and must therefore consider processes, intermediate streams and sources of inputs.

Researchers such as Pacheco et al. (2016) use the term heterogeneous, but without any definition. These researchers note (p1) that "...Protecting and securing the resources and services of smart cities become critically important due to the disruptive or even potentially life-threatening nature of a failure or attack on smart cities' infrastructures...." and propose an approach to protection based upon Moving Target Defense (MTD) techniques for communications and data infrastructures; they therefore propose a much narrower interpretation of “heterogeneous” than is used in this work.

4.2.4 Static and dynamic contributions

Published definitions of “vulnerability” have been extensively examined in Chapter 2 of this work. Significant divergence and lack of clarity among published definitions have been noted. The proposed approach to improving the precision of these varied definitions is to use the phrase "dynamic vulnerability" to describe the dynamic response of a functioning system to a specified perturbation. Dynamic vulnerability measures, which are not analysed in this thesis, would take account of the instantaneous state of all system components and the magnitude of nominated perturbation(s), and would assume that the system will not actually fail. Metrics of dynamic vulnerability would measure the response of a system, starting at a defined status, to a defined perturbation. Dynamic vulnerability is then the inverse of resilience, as defined in this section.

Once a defined level of service from a technological system is defined, a recursive application of that service level output will also define the nominal state of all streams and processes "upstream" of the final delivery of goods or services. This set of states, which represent nominal operating conditions for the defined service level, also allows a clear definition of a maximum tolerable disturbance for each stream and process variable, as the perturbation from the nominal state that will cause failure to achieve the service level output. The definition distinguishes the dynamic vulnerability situation from a static vulnerability measure.

Having assigned the term “dynamic vulnerability" to describe dynamic and continuous responses and having defined the scope of that phrase, "vulnerability" is
will be used to describe the contribution of vulnerability that is made to the user by the technological system components and configuration alone. The work of Chapter 4 has been to show that the proposed "exposure" metric is a valid measure of this vulnerability. The research questions upon which this thesis is based relate to static vulnerability. It is proposed that static vulnerability should be considered as a precise antonym of robustness, noting that robustness is commonly associated with the design and configuration of a technological system, rather than the margin between design and overload performance.

4.3 Exposure as a theoretical measure of vulnerability

The end-user focus and the definition of service level generate a very clear target for the consideration of vulnerability. The variations of the definition of vulnerability have been stated previously, and commonly include the concept of susceptible to attack, which requires a clear definition of the term "attack" and a definition of "susceptible". The research question seeks to quantify the contribution made to vulnerability by a technological system. The process of formulating this question specifically excludes consideration of the external events that could contribute to failure and also excludes consideration of the probability of any of those events occurring. This approach pre-supposes that, if a weakness existed, it could cause failure either because of random events over a long time-frame or because of malicious activity within a short time-frame. As the probability of external hazards does not affect the specific contribution to end-user vulnerability of the technological system, any aspect of the technological system that is capable of causing failure makes the same contribution to vulnerability as any other aspect of the technological system that is capable of causing failure. Assuming either long time-frames or the presence of malicious activity, the contribution to vulnerability of the technological system can be associated with the number of modes of failure that are possible, and can be associated with the configuration of the technological system.
4.4 Possible contributions to a measure from published techniques

4.4.1 Specific contributory aspects and gaps

Risk analysis approaches do not prescribe a description of the target technological system at all, and hence do not necessarily derive any measure that relates specifically to the technological system. The limited applicability of homogeneous systems has been described previously. Both resilience analysis and FMEA offer foundational concepts that can contribute to a metric that meets the requirements of this research, because both require a clear definition of the target technological system. An FMEA analysis commences by establishing a very clear definition of a technological system, which is commonly an interconnected system of valves, pipework, pumps and control systems, and then examines the effect of the failure of each component within that system. FMEA commonly assumes a Boolean (fail or operate) status of each input although, in some cases, fail-open, fail-closed and fail-fixed modes may be considered. The analysis normally examines the effect on the system output. FMEA analysis commonly results in a tabular representation of the effect of each selected component failure. FMEA is commonly carried out to establish whether a defined level of design redundancy (N-1 etc.) has been achieved. For example, if an N-1 design redundancy (system failure cannot be caused by the failure of any one component) is specified, FMEA would examine the effect of each individual component failure upon system output. If an N-2 design redundancy was specified, i.e. system failure cannot be caused by the failure of any two components, then FMEA would examine the effect of each possible combination of two component failures upon system output.

The research question requires assessment of the complete contribution of the technological system to end-user vulnerability. The FMEA analysis approach, which examines fail or no-fail conditions of each component without design review to achieve a specified design redundancy, can generate a tabulated representation of the single input fail criteria that cause a failure to meet the service delivery criteria. Therefore, if each possible failure mechanism could be evaluated as either operational or non-operational, and the delivery or non-delivery to the end-user is the final output, then both the resilience analysis and the FMEA analysis would yield
similar outputs that could be represented in a tabular format showing single failure causes.

4.4.2 Capabilities to be added to published approaches

Resilience analysis generates output responses to single inputs, and so does not completely characterise a system whose failure may arise from combinations of failures. Similarly, FMEA provides a simple tabular representation of the effects of each component’s failure and is generally used only to demonstrate that a design redundancy requirement of a tightly defined system is met. The development of an adequate theoretical basis requires that all of the potential failure modes of a technological system are defined and characterised, as well as being shown to provide a valid measure of the attribute of interest. This is the capability to be contributed by the enumeration of a technological system’s exposure as a measure of its contribution to the end user’s vulnerability.

4.5 Development of proposed metric

The aspects of published techniques that can be built upon to generate a theoretical basis that meets the requirements of the research question have been identified. The limitations of published techniques have been identified, and the capabilities that must be added have also been identified. The criteria to be met by a theoretical basis, in order to address the research question, have been established.

4.5.1 Measurement theory – the criteria for a metric

"Measurement" is itself a concept requiring careful application to any new analysis approach, in order to ensure the relevance of the proposed approach. Suppes (2009, p. 825) states that

"A conceptual analysis of measurement can properly begin by formulating the two fundamental problems of any measurement procedure. The first problem is that of representation ... we must show is that the structure of a set of phenomena under certain empirical operations and relations is the same as the structure of some set of numbers under corresponding arithmetical operations and relations. Solution of the representation problem for a theory of measurement does not completely lay bare the structure of the theory, for there is often a formal difference between the kind of assignment of numbers arising from different procedures of measurement. This is the
second fundamental problem, determining the scale type … based on the proof of an invariance theorem for the representation”.

Similarly, Hand (2004, p. 3) offers an initial definition — "...quantification: the assignment of numbers to represent the magnitude of attributes of a system we are studying or which we wish to describe." This definition is operationalised initially by noting the previously established context for the measurement and a "phenomenon of interest", by representing the heterogeneous system in some way, and establishing a mapping from the real system to a system that corresponds to, and behaves in the same way as the real system, within which a measure can be developed. Finally, the definitions are operationalised by defining an attribute to represent the phenomenon of interest, and confirming the validity of the measure.

4.5.2 Representation of a heterogeneous system

Heterogeneous technological systems can be described as progressively adding value to raw inputs, and ultimately generating a specified output. These systems could also be described in terms of applying processes to input and intermediate streams, generating further intermediate streams until the final output is created. It should be noted that a homogeneous system is a specific case of a heterogeneous system, in which the process types are limited to aggregation and distribution, with no transformations. The definition of a service level of output allows representation of the output using a Boolean variable. Consider the final delivery of the goods or services; this can be assumed to be feasible if a set of conditions is fulfilled, e.g. a road exists, an operational truck is available and fuel and a driver are available. This could be represented as a Boolean AND function with four inputs. If each of those inputs is considered in turn, it is proposed that their availability can also be represented as a Boolean variable, which is the output of a Boolean function of several inputs. Extending this principle allows a complete technological system to be represented as a complex Boolean algebraic expression, which considers the specific processes, the intermediate streams and the input streams, and results in a Boolean representation of the service level delivery conditions for defined goods or services to an end-user. Figure 3, using standard symbols for AND and OR gates, illustrates a simple example of this approach.
Figure 3 A representative complex technological system.

Figure 4 provides a more realistic example of a heterogeneous technological system, including cases in which some streams have alternative sources, and including processes that have some common requirements and some unique requirements. Real technological systems may also include operations that are mutually exclusive, indicating a need for a functionality representing the case where IF (a) then NOT (b). Such a “NOT” construct can be used in conjunction with the definition of stream availability level, e.g. to describe a situation in which the sufficient level of stream capacity to ensure the functioning of (a) will preclude the sufficient level of stream capacity to ensure the functioning of (b).

A computationally complete Boolean algebra requires only the “AND”, “OR” and “NOT” constructs, and these have been shown to be sufficient to represent an arbitrary heterogeneous technological system for delivering goods or services to an end-user. The final service delivery can be represented by a Boolean variable and, by applying the definition recursively, intermediate streams can be considered to have Boolean values according to whether they do, or do not, cause failure of the final service level delivery. This allows the representation of streams and process availabilities as Boolean variables. The “NOT” function can be used, although its value in the field of this thesis is problematic, but, as there is no function that allows “distribution”, a stream availability cannot be simply assigned to the input of more than one gate. The system needs to be re-drawn as demonstrated in Figure 4. This re-drawing illustrates the correct treatment of the case where an input stream affects more than one process.
4.5.3 Interpretation of data: defining and measuring the attribute

A truth table, as illustrated in Figure 5, based on Boolean algebra, and including all valid inputs, can be used to represent the possible outputs of the technological system for each possible combination of input availability or non-availability.

```

Figure 5 Representation of system inputs and outputs

```
Considering a system, of which representative parts are illustrated in Figure 5 above, it can be seen that there are a number of points for which a single failure will cause the system output to fail. These are added to generate the $E_1$ value, representing the highest level of vulnerability. There are also cases where a combination of two or more failures will need to occur simultaneously in order to cause the system output to fail. These generally arise from duplicated systems, are represented using “OR” gates and are added to give the $E_2$ value. Continuing this approach, it is possible to construct a composite metric of the form \{$E_1$, $E_2$, $E_3$... $E_n$\}, where $E_1$ is the number of single points of failure and $E_2$ is the number of cases where two independent failures must occur in order for the system to fail. The $E_2$ value must exclude cases where either one of the inputs would alone have caused output failure – otherwise the values would be over-represented. Similarly, the $E_3$ value must exclude cases where a combination of two of the failing inputs would have caused output failure. This representation and concept expands upon the “N–1”, “N–2” design redundancy concept, arguably adds rigour to that definition and is proposed to provide a measure of the relevant attribute.

It has previously been argued that probabilities of a particular process or stream failure, i.e. the probability that a hazard aligned to that process or stream is of sufficient magnitude to cause the operation of the process or stream to fall below a level that would cause failure of the technological system output, should be excluded from consideration for two reasons: firstly, because these will tend towards a probability of 1.0 over a sufficiently long time-frame or under the assumption of directed attack; secondly, because they are characteristic of external hazards rather than the intrinsic components and the configuration of the technological system that are the topic of the research question. It has also been established that (a) arbitrary heterogeneous technological systems supplying to a single point with a defined service level can be represented as a Boolean algebraic expression, and (b) the response of the system to permutations and combinations of failures can be represented in the form \{$E_1$, $E_2$, ... $E_n$\}. It is therefore argued that the number of vulnerability points, i.e. possible points of failure, of the technological system is a valid mapping of the “vulnerability that can be attributed to the technological system” on to an attribute. Within AS/NZS ISO 31000:2009, as the definition assigned to the term “exposure” is closely related to the concepts described above, for the purpose of this
work, the quantitative evaluation \( \{E_1, E_2, \ldots, E_n\} \) will be referred to as the “exposure” of the technological system.

### 4.5.4 Clarifying the definition of the attribute

**Granularity.** Generating an accurate exposure value requires a careful consideration of the assessment process and, specifically, the granularity of the representation. To illustrate using an example, if every transistor in a memory chip were considered to be a potential cause of failure, the “exposure” value calculated for the computer would be exceedingly high. In contrast, if the computer were considered to be a complete, replaceable unit, then it would be assigned an exposure value of 1. A pragmatic definition will address this issue: if some subsystem is potentially replaceable as a unit, and can be attacked separately from other subsystems, then it should be considered to be a potential source of failure. This definition is proposed to allow an adequate level of precision – i.e. reproducibility by different practitioners.

**System boundaries.** One system boundary must be at the end user: definition of the other system boundaries is essential for an analysis and will be set pragmatically at the points where a sufficiently large number of sources of the input stream are available, and hence can be considered to be unconditionally available.

**Contributory systems.** It can be expected that there will be cases where a stream that is an input to one technological system is itself the product of another technological system, i.e. a contributing system. The technological system that generates the input will itself have some degree of “exposure”, and it is important to have a valid basis for calculating the contribution that is made to the exposure of the end-user. This issue is illustrated in Figure 6.
A more generalised approach is required. The problem can, in fact, be generalised by considering that each input to a gate (Boolean AND or OR operation) has an exposure vector, and developing the principles by which the gate output can be calculated from these inputs. This is illustrated in Figure 7.

**Figure 7 Generalised approach – contributory system**

For the AND gate, the contributory exposure vectors are simply added component-wise; hence the output metric is

\[
\{(A_1 + B_1 + C_1), (A_2 + B_2 + C_2), (A_3 + B_3 + C_3) \ldots (A_n + B_n + C_n)\}.
\]

For the OR gate, the issue is more complex. For the case where there are three inputs to the OR gate, the calculation is as shown in Equation 8.

\[
E_1 = 0
\]
\[
E_2 = 0
\]
\[
E_3 = 2^{(A_1 \cdot 1 + B_1 \cdot 1 + C_1 \cdot 1) + (A_2 \cdot 1 + B_2 \cdot 1 + C_2 \cdot 1) + (A_3 \cdot 1 + B_3 \cdot 1 + C_3 \cdot 1) + (A_4 \cdot 1 + B_4 \cdot 1 + C_4 \cdot 1) + (A_5 \cdot 1 + B_5 \cdot 1 + C_5 \cdot 1)}
\]

**Equation 8**
It should be noted that, when calculating the $E_3$ value, one fail from each input MUST occur for the output to fail; however, each remaining combination of fails contributes to the $E_3$ value. The $E_4$ and subsequent values are calculated in exactly the same way as the $E_3$ value. It can be noted that, because the contributory system has effectively added streams and processes, the length of the output exposure vector is increased when the contributory system is considered. In principle, an exposure vector of very great length could be postulated.

The fact that contributory $E_1$ values are added to the total exposure of a parent system is significant: a single point of failure is not lost when the contributory system is added to the parent system. As a practical example, if the “O” ring seal failure had been identified as a contributor to the $E_1$ exposure of the Thiokol Solid Booster Rocket, then the elimination of all $E_1$ values for the parent system, which was the Challenger space shuttle, could not have been achieved unless the “O” ring weakness was addressed. The use of an exposure metric potentially addresses the colloquial saying “it’s always the smallest things that get you”.

Pragmatic limits on depth of analysis. Some pragmatic observations can be made. As, for example, $E_3$ combinations cannot by definition include any $E_2$ or $E_1$ combinations, and $E_4$ combinations cannot include any $E_3$, $E_2$ or $E_1$ combinations, there will be a tendency for the values of these quantities to decrease. Upper bounds can be set: for a system with $N$ inputs and, if $E_1 = n$, then $E_2 \leq (2^{(N-E_1)})$ etc. and it can be observed that, if a system with $N$ inputs has an $E_n$ value of 1, then this system can be only a single “OR” with $N$ inputs and all higher E values ($E_1...E_{(n-1)}$) must be zero. The proposed approach is therefore to nominate a level to which exposure values will be evaluated. If, for example, this level is set at 3, then the representation would be considered to be complete when it could be shown that no contributory systems added to the $E_3$ values of the system as represented.

4.5.5 Interpretation of “exposure” values

A significant purpose of this investigation is to allow the evaluation of proposed changes and the comparison of technological systems. The effectiveness of proposed changes can be assessed by considering the composite metric. For example, it might be considered to be valuable if the $E_1$ value were reduced by a given percentage. Comparison of technological systems is difficult unless the defined attribute can be
validly assigned a single value that can be proven to be mapped from the actual “exposure”. A rational means for converting an exposure represented in the form \( \{E_1, E_2, E_3, \ldots, E_n\} \) into a single attribute value is useful though not essential. The mapping from the exposure expressed as \( \{E_1, E_2, E_3, \ldots, E_n\} \) on to a single attribute value can be made by considering that there is likely to be an average cost of protecting each point of exposure and hence that simply adding the unique \( E_1, E_2, E_3 \) values provides a single value for the attribute, which offers a valid means of comparing technological systems. It is also noted that a qualitative interpretation of the distribution of \( E_1, E_2 \) etc. values will provide additional insight and would also allow the assessment of progress towards, for example, a target of \( E_1 = 0 \). This conclusion assumes that the \( E_1 \) and \( E_2 \) etc. combinations are exclusive, as previously defined.

4.6 Evaluation of proposed approach and metric

Recognition of the concept that long supply lines and systems with large numbers of potentially fatal flaws and with no alternative sources are "exposed" can be found in documents as historical as "Sun Tsu, The Art of War" (Griffith 1963), in the concern expressed by Senator John Glenn regarding the Mercury spaceflights (Glenn, 1997) and in very many other publications. Although the term published definitions of “vulnerability” and the phrase “contribution to vulnerability” may not be precisely defined, these observations indicate that the “exposure” attribute is a valid representation of the phenomenon of interest. In addition to providing a valid representation, it must be demonstrated that the proposed assessment of "exposure" represents a reproducible and accurate measure that actually represents the contribution of the technological system to vulnerability.

4.6.1 Representation

Suppes (2009, p. 825) notes that

"A conceptual analysis of measurement can properly begin by formulating the two fundamental problems of any measurement procedure. The first problem is that of representation, justifying the assignment of numbers to objects or phenomena. What we must show is that the structure of a set of phenomena under certain empirical operations and relations is the same as the structure of some set of numbers under corresponding arithmetical operations and relations".
Similarly, Hand (2004, p. 3) proposes an initial definition as "quantification: the assignment of numbers to represent the magnitude of attributes of a system we are studying or which we wish to describe". Hand (2004, p. 132f) presents detailed descriptions of the "validity" of a representation, and describes several distinct types of validity, which are effectively descriptions of alternative approaches to establishing validity.

In the context of this work, an evaluation is needed of whether the proposed theoretical basis (the numerical evaluation of "exposure") actually represents the performance indicator described in the research question, by considering the validity criteria proposed in works such as Hand (2004). Hand's concepts of "criterion validity" and "content validity" seem to be of lesser relevance, because they are related to other comparative measures, whereas the proposed measure has been developed in response to an identified "gap" and therefore does not align clearly with other measures. Hand's (2004, p. 133) description of "construct validity", in contrast, is described as "... involves the internal structure of the measure and also its expected relationship with other, external measures. Construct validity thus refers to the theoretical construction of the test: it very clearly mixes the measurement procedure with the concept definition".

The term vulnerability generally has two elements: firstly, the knowledge that possible failure modes exist; secondly, the knowledge of practical inability to adequately prevent those modes. The lack of ability to prevent failure modes is likely to include practical issues of physical access to particular loci of potential failure, but is also likely to include an awareness that the multiplicity of such loci and the lack of adequate alternatives present a major practical problem. It is proposed that these somewhat intuitive concepts are actually described in quite rigorous logical terms by the Boolean representation of the technological system involved and, because the exposure metric \( \{E_1, E_2, E_3 \ldots E_n\} \) is constructed directly from the representation of the technological system, this has a construct validity in the terms proposed by Hand (2004).

The extent to which the proposed theoretical basis represents the issues in the research question is effectively an examination of the scope and validity of the framework of assumptions and boundaries within which the representation is claimed. In the examination of risk issues, the rationale for assuming all hazards to have a
probability expressed as $p = 1.0$ was established. The definition of service level does, certainly, allow a Boolean evaluation of the provision of a stated service. It might be argued that an infinite number of service levels is theoretically needed to characterise the supply of goods or services, but this is unlikely to be a practical issue: a water supply that is adequate for two criteria, e.g. “drinking only” and a “normal bathroom and clothes or dish washing and food preparation”, is likely to achieve the goals of the measurement, i.e. informing decision and allowing comparison of alternative technological systems. The exposure metric does depend critically on the system boundaries selected. These boundaries effectively represent inputs that are considered to have an exposure of \{1,0,0\} and, for a valid calculation, the system boundaries need to be defined precisely.

### 4.6.2 Completeness and uniqueness

As the Boolean algebraic representation of the real system will generate the same results, in terms of Boolean delivery or non-delivery of service levels, as the real system under the same combinations of input failures, the Boolean representation can be said to be homomorphic. The real system and the Boolean algebraic representation can be said to be homomorphic in terms of the processes and streams. Assuming adequate descriptions of the processes and streams and relationships, it is actually possible to re-draw an actual system from the Boolean algebraic representation. This proves that the representation is not only homomorphic but also isomorphic, allowing an inverse mapping.

### 4.6.3 Adequacy

It must be established that it is possible to represent all practical technological systems unambiguously by Boolean algebraic expressions. Several authors have drawn attention to the complex interactions and possibly feedback loops between subsystems. It is important to establish with confidence that an arbitrary technological system can be represented unambiguously with a Boolean expression. A particular consideration is whether technological systems in fact include feedback loops, and if so whether the proposed approach can represent these.
Figure 8 Feedback loop representation

Figure 8 demonstrates a progressive re-drawing of a system initially considered to include a “feedback loop”. For a system, e.g. an electronic system, where initial conditions are not pre-determined, the output of this system as shown in the first representation, is indeterminate when S05, S06 and S10 are true. As the evaluation of exposure considers the number of points that will cause the failure of an operational system, initial conditions are always determined. The system can then be simplified as shown in subsequent parts of Figure 8. For systems with input conditions that are not indeterminate, representations of configurations involving feedback can be decomposed to simple Boolean representations and therefore the exposure values can be determined.

Haimes and Jiang (2001) consider fractional values of interaction between infrastructural systems, using these fractional values to assess the decrease in functionality of one system resulting from the decreased functionality of another.
These concepts have at least superficial similarity to the colloquial concepts of inter-system feedback. Although valuable, Haimes and Jiang’s approach to a description of interdependence does not quantify exposure as a metric of vulnerability and relies on problematic processes for calculating the levels of interaction.

Feedback must be considered in its broader context. Diamond (2005) and others have noted that, within a geographically and economically constrained civilisation, a full positive feedback of failures, caused by a single essential resource failure, can cause societal collapse. Geographical regions, e.g. those affected by natural catastrophe, are now not tightly constrained in terms of trade, geography or information; therefore, disaster relief is possible. However, our highly inter-connected world is certainly still exposed to global environmental failures such as major climate change, and Diamond’s scenarios emphasise the exposure concept because there are effectively exposure values associated with all major environmental resources, including fresh water, clean air and a viable temperature range. These are not discounted, but the topic of this thesis is technological contributions and it is the technological contributions to which attention is drawn.

4.6.4 Precision

Precision is achieved when different practitioners apply the same concepts and techniques to a problem, and all generate metrics that are close in value to those generated by others. The Bureau Internationale des Poids et Mesures (2008) provides a well-accepted distinction between the term “precision” and the term “accuracy”. It defines (p22) precision as “closeness of agreement between indications or measured quantity values obtained by replicate measurements on the same or similar objects under specified conditions”. This is similar to the concept of reproducibility. Achieving an adequate level of precision is closely linked to the definition of system granularity, and indeed to the definitions of what constitutes a “process” and an “intermediate stream”. Consider an example: at a macro level, a cell phone needs power only. A main processor unit may contain more than a billion transistors and, if any should fail, the unit will not operate, and a decision is therefore required on whether to assign an exposure value of 1 billion or an exposure value of 1. Two somewhat pragmatic tests can be applied. If a subsystem can be replaced as a unit, then it should be considered to be a “process” and, if it is practically feasible
for an attack to be directed at a subsystem without affecting its neighbours, then it should be considered to be a “process”. There is no real mechanism for an attacker to target a single transistor of a chipset; neither is it possible to replace even a processor alone – which would suggest the personal computer (PC) motherboard as the appropriate level of granularity for a “process”. It would be possible in future to build up a library of exposure vectors for larger components, e.g. the PC, to be incorporated into analyses using the principles developed for contributory systems.

4.6.5 Accuracy

When considering representation, evidence has been presented that the metric does relate to the attribute of interest – the question of accuracy remains, i.e. whether the measure offers a moderately linear representation of the quantity of interest. The Bureau Internationale des Poids et Mesures (2008) provides a well-accepted distinction between the term “precision” and the term “accuracy”. It defines (p21) accuracy as “closeness of agreement between a measured quantity value and a true quantity value of a measurand”. Real examples of the importance of this issue can readily be envisaged. If alternative changes to the technological system have, for example, a cost ratio of 2:1, and the alternatives have exposure values that also have a 2:1 ratio, then the quality of the decision will depend critically upon the accuracy of the exposure measure. The adequacy of the accuracy of the proposed measure is justified by a simplifying assumption. To adequately mitigate each exposure value will require some effort and expenditure and, whereas costs might vary significantly between cases, it is reasonable to assume that, when a large number of exposure “points” (single or combination failure points) is under consideration, the expenditure for mitigation will bear at least a moderately linear relationship to the number of such points. This principle will apply whether the designer’s target is to bring $E_1$ to 0 or $E_1$ and $E_2$ to zero.

4.7 A consistent set of definitions and metrics

An internally consistent and defensible set of definitions is needed to avoid confusion in the remainder of the thesis. Figure 9, below, illustrates many of the concepts. The following definitions are proposed, and correlations with published definitions are noted.
Figure 9 Illustration of selected terms

(a) Risk

Definition. The probability that a given hazard will occur (at a level above the maximum tolerable level) during a nominated time-frame.

Explanation. Risk must be applied to a hazard that, in turn, is always related to a specific weakness: a hazard is irrelevant unless it is associated with a weakness.

It has already been argued that, when either long time-frames or (mis)guided hazards are considered, the risk probability approaches 1.0. If a specific risk has a known probability function, i.e. it will exceed a nominated value for a known percentage of time, it would be possible to calculate a Bayesian probability that there will be an instant when the loading of a particular weakness plus the hazard value will exceed the maximum tolerable value of that weakness. Although this is computationally possible, both the "guided hazard" and the long time-frame arguments depreciate the value of this approach. The practicality of the approach is also hindered by noting that every weakness may have an unlimited number of
hazards linked to it, and that every potential hazard for every weakness must therefore be considered to be a component of a Bayesian probability calculation.

Alignment. This definition aligns with many published definitions, but differs from many non-academic definitions, e.g. the insurance industry's usage that considers an "insured risk" to be the asset that might suffer damage. This aligns with common definitions: risk is quoted as "high", when a hazard is likely to occur, through to "low", when it is assessed that a hazard is unlikely to occur.

(b) Hazard

Definition. Something that causes a perturbation in the performance or availability of a process or stream that is part of the technological system – e.g. a severe weather effect, e.g. “more than xx mm rain” is a hazard.

Alignment. Consistent with AS/NZS ISO GUIDE 73:2009, which defines Hazard (3.5.1.4) as a "source of potential harm".

(c) Service_level

Definition. Rate of delivery of specified goods or services, to a single point.

Explanation. Definition of a service level allows a Boolean representation of “harm”, i.e. the non-supply of goods or services.

(d) Harm

Definition. The failure to deliver some specified level of service or goods.

Explanation. This definition applies equally to the output of a technological system and to the end-user failure-to-receive.

Alignment. This definition does not consider the consequence of failure-to-deliver, e.g. if a technological system delivers toothpaste, then this definition of "harm" refers to the failure to deliver toothpaste, rather than caries or halitosis.

(e) Technological system

Definition. Scope is defined by that needed to produce the service level of specified goods and where failure will cause specified harm, i.e. a failure to supply.

(f) Weakness

Definition. When applied to a technological system, “weakness” is proposed to be defined as a stream, process or other facility whose function is a part of the technological system in question, and whose absence or inoperability contributes to the possibility of harm.
**Explanation.** Weakness is directly associated with the potential for harm, i.e. the potential that, if the locus of weakness fails, then "harm" (a failure to deliver service) may result. The uncertainty in the "may" is due to two factors: if the attack on the weakness is below the maximum tolerable limit, or the configuration of the system provides redundancy for the function of the weak point.

**(g) Exposure**

**Definition.** A metric derived from the number and the configuration of the weaknesses of a technological system.

**Explanation.** Exposure is qualitatively related to the difficulty or cost of preventing harm. A high level of exposure means that protection is difficult and expensive as many weaknesses must be protected.

**Alignment.** This definition clarifies the ISO definition.

**(h) Vulnerability**

**Definition.** A summation, for each combination of weaknesses that can cause the defined harm, of the risks that hazards associated with those weaknesses will cause the harm. If the risk for every hazard is considered to be \( p = 1.0 \), vulnerability is synonymous with exposure.

**Explanation.** The entity that is proposed to be "vulnerable" must be identified and could be a person, or a technological system, associated with a specified harm. The definition considers both exposure and total hazard probabilities, indexed to a specific HARM. The concept of how close an operational system is to failure is captured by the concepts of resilience and maximum tolerable disturbance, and should not be associated with the term vulnerability.

**Alignment.** Aligns moderately with the definition stated by Akgun et al. (2010, p. 3561), who propose that "... [v]ulnerability can be defined as a "weakness in the system defended".

**(i) Robustness**

**Definition.** Opposite of exposure.

**Explanation.** Robustness can therefore also be mapped directly to the exposure metric. A system whose \( E_1 \) and \( E_2 \) exposure values are zero could be asserted to be robust, because these values show that there are no single or dual process or stream failures that will cause the system to fail. In contrast, a system whose \( E_1 \) exposure value is high could be asserted to lack robustness, i.e. be
vulnerable, because a failure of any of the contributors to the $E_1$ value will cause failure. The proposed definition is NOT the opposite of vulnerability, because risk is not involved. The proposed definition relates only to the system configuration and components.

Alignment. Published definitions are similar but opposite to the definitions of resilience.

(j) **System state**

**Definition.** The instantaneous load level of each process and stream of a technological system.

(k) **Resilience**

**Definition.** Dynamic output response of a system, to a perturbation whose level is below the maximum tolerable disturbance for the weakness with which the perturbation is aligned. This is the “dynamic vulnerability” of the system.

**Explanation.** A system is only “resilient” as long as the output function is continuous with respect to input perturbations, i.e. “harm” (system failure to meet the service level) has not occurred. Any measure of resilience must specify the initial system state, the perturbation level and the perturbation target, i.e. the weakness. It is argued that, whereas the resilience metric is applicable to systems that have not failed, the exposure metric measures possible modes of failure. This division of applicability scopes is valid for common cases such as the supply of 230 VAC electrical power, which is generally either available or not available, and a system that is dependent on an electric motor that either operates or does not, according to the availability of the power supply.

Alignment. Published definitions of resilience, as noted in Chapter 2 of this thesis, commonly consider system performance responses to perturbations of inputs, and specifically the time taken to return to some defined state or an integration of the deviation of system response against time. These definitions implicitly assume a response function without discontinuities, i.e. that the system does not actually fail, a knowledge of the instantaneous state of the system and a means of calculating a dynamic response to a specified perturbation.

(l) **Maximum tolerable disturbance**
**Definition.** The level of perturbation for each stream or process, over and above the system state loading that is normal, for the system service delivery level to the design number of users that will cause stream or process failure.

**Alignment.** Simply refines the descriptions used by Starossek and Haberland (2010) and Gómez et al. (2011) by establishing the clear boundary between an operational system responding to a perturbation and a system that causes harm, i.e. fails.

(m) **Resilience limit**

**Explanation.** Hollnagel et al. (2006) consider how close a system’s normal usage is to the failure level; this term is proposed to capture this concept. A simple measure might be the ratio of maximum tolerable disturbance to normal state.

### 4.8 Conclusions

#### 4.8.1 A valid theoretical basis

This chapter has developed the theoretical basis of the analysis, by starting with a review of the context for an acceptable theoretical basis for a solution to the research question, and then demonstrating how valid constraints on two existing techniques lead to the same conceptual framework for a solution. It has then been demonstrated that an arbitrary heterogeneous system can be mapped on to a Boolean expression and that the evaluation of the Boolean expression for all combinations of process or stream failure generates a metric that is a valid representation of the number of weaknesses (or the number of points requiring protection effort) of a technological system. Finally, it has been demonstrated that this attribute’s metric is a valid representation of the phenomenon of interest (the system property described in the research question), the metric is invariant with respect to factors specifically outside the defined context, the metric does adequately consider all factors that are valid within the defined context and the accuracy and the precision of the proposed measure are fit for purpose.

#### 4.8.2 A theory of exposure

This thesis is concerned with the contribution of technological systems to end user’s vulnerability, and a theoretical basis for measuring this by an evaluation of systems’ exposure. Crittenden and Peterson (2011) what a theory is, and note many
definitions of theory, including "A supposition or a system of ideas intended to explain something, especially one based on general principles independent of the thing to be explained" and "A scientific theory is an explanation or model used to account for observations". Wacker (1998) proposes that conceptual definitions, domain limitations, relationship building and predictions are the essential elements of a valid “theory”. This thesis provides a system of ideas intended to explain something and additionally provides conceptual definitions, a domain limitation (introduction), relationship building as a result of validating the metric and a predictive capability because the proposed metric can be used to evaluate potential changes. On this basis, a "theory of exposure" could be considered to meet the definitions of a valid theory, when formulated as “An end-user’s vulnerability to a technological system supplying specific goods/services is measured by the number and the nature of points-of-failure which are expressed as the “exposure” of that technological system". 
5. DEFINITION OF EXEMPLAR STUDIES

5.1 Introduction

This chapter defines the initial exemplar technological systems to be studied. The technological descriptions assume that the individual user lives in a city with a population of about 200,000–500,000. This size is selected because it encompasses a significant number of cities, particularly within Australia and New Zealand. While this population range is noted, it is not intended to be a rigorous definition, but rather a range that allows representative exemplar studies to be described. Mega cities (perhaps of many millions) might, for example, have dedicated power stations that are not envisaged within the exemplar studies, and villages of tiny population might (for example) lack an internet Point of Presence. An operational time-frame is assumed, i.e. it is assumed that no maintenance or replacement of equipment is needed but operational supplies are required. Section 3.3 of this thesis notes that “maintenance” and “replacement” time-frames are longer and hence in practice allow specialised equipment to be acquired or (re)created. The end-user is not a named individual, but must be demonstrated to be representative. It seems to be reasonable to consider that a "representative person" will be neither blind nor deaf, and will be capable of operating household or personal equipment. On the basis of smartphone and laptop ownership statistics, the physical and intellectual ability to operate a smartphone can reasonably be assumed. It also seems to be reasonable to assume that a "representative person" will have the financial means to live in an apartment, with power, water and communications facilities connected, and will have the financial capacity, independent of technological capacity, to purchase common goods or services. The examples are chosen to demonstrate goods or services whose absence would effectively force significant lifestyle change upon the representative persons.

5.2 Description and verification of examples

5.2.1 Format of example descriptions

A consistent format, as described in Table 7, is used across all examples, using the following headings.

- Title, and version control information.
- Initial description, and key features.
• Confirmation of analysis time-frame.
• Justification for inclusion of the example – in terms of significant effect upon the end-user if the goods or services are not available.
• Clarification of the end-user service level and goods or services description.
• Text description of the example. Clarification of boundaries, i.e. inclusions and exclusions, and justification in terms of selected level.
• Confirmation that the example description is representative of real implementations of the service: this is likely to involve include research of actual systems implemented in a small number of cities and/or referenced within public sources.
• Representation of process, stream and configuration descriptions in terms to be used in the analysis, including discussion of granularity.
<table>
<thead>
<tr>
<th>1 Sewage</th>
<th>2 Work information</th>
<th>3 Local fuel supply</th>
<th>4 Targeted first-aid</th>
<th>5 Perishable food</th>
<th>6 Medicine</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial description</strong></td>
<td>The sanitary removal of human waste, on an “as-required basis”, and resulting in the discharge of environmentally acceptable waste.</td>
<td>The capability to store and retrieve, view, edit and share work information.</td>
<td>The service, in this case, is the supply of petrol at a local petrol station.</td>
<td>The service, in this case, is the correct application of a first-aid measure.</td>
<td>The supply of a perishable food. Fresh whole milk is selected because it is a staple food and requires a technological system that is similar to that required by other fresh food.</td>
</tr>
<tr>
<td><strong>Time-frame</strong></td>
<td>An “operational” time-frame has been selected for study, i.e. it is assumed that no maintenance or replacement of equipment is needed.</td>
<td>An “operational” time-frame has been selected for study, and so no maintenance or replacement issues are considered.</td>
<td>An “operational” time-frame has been selected for study; hence maintenance and replacement of components are not envisaged.</td>
<td>Only an “operational” time-frame has been selected for study.</td>
<td>An operational time-frame has been selected for study; hence no significant maintenance or replacement of equipment or processes will be required.</td>
</tr>
<tr>
<td><strong>Justification</strong></td>
<td>Public transport services (trains, buses) in New Zealand are generally considered to require on-board toilet facilities if the journey is longer than 2 hours; although this is clearly only a guideline, it does demonstrate that the facilities are considered to be essential for even relatively short occupancy intervals.</td>
<td>The storage and transmission of information is foundational. A consulting engineer without access to functional email, or file server facilities, is likely to be unable to carry out expected tasks. Similarly, the apartment dweller is unlikely to have the storage space to hold significant tomes of family history or reference material.</td>
<td>For the size of city considered, public transport (coverage and frequency) commonly makes such activities as grocery shopping and commuting to work only marginally practical for many, and the distances are arguably too long for many to reasonably walk.</td>
<td>Life-threatening medical emergencies can certainly occur for the apartment dweller; for many, the time until death is shorter than the time for a paramedic to arrive. Life or death will depend upon the ability of a co-dweller to diagnose the problem, and apply the correct measure.</td>
<td>It is common for apartment dwellers to purchase, store and use fresh food – and deprivation of this capability would constitute a “significant change to lifestyle”. This justifies the consideration of a fresh food example. Fresh milk is a very common food.</td>
</tr>
<tr>
<td>Service level</td>
<td>Description and definition of boundaries</td>
<td>Representative example?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------</td>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The sanitary removal of human waste, as required, via the lavatory and resulting in the discharge of environmentally acceptable water to waterways, sea or landfill.</td>
<td>Water-flushed lavatory, flushing water, gravity-fed systems, pumping stations, coarse screen sedimentation, trickle-filter aerobic digester clarifier, oxygenation ponds, dewatered biosolids, transport to landfill.</td>
<td>A survey of sewage systems used by cities within this size range reveals a level of uniformity.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The definition of service delivery implies that the complex information is able to be read, seen and updated by more than one party, before being read by the intended “recipient”.</td>
<td>Laptop hardware and software, packet exchanges with router, ISP exchange packets with local router if local table (updated by BGP and similar protocols), allows it to use T3 and/or T1 links to high speed routers and local ISP has links to DNS servers, exchange packets if T1 links to undersea cables).</td>
<td>Statistics show that a large proportion of the population have either laptops or “smart phones” and rely on these for work as well as essential personal information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The service is achieved when pre- or post-purchased petrol, whose quality is within the fuel specification limits, is supplied at a normal flow-rate, to a vehicle parked in the forecourt of the petrol station.</td>
<td>Petrol pumps, purchase transaction and transaction completion, local control and data collection system, operator, external communications system, fuel metering.</td>
<td>For the type of petrol station described, the processes and equipment are observably very similar across a wide range of locations internationally.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The delivery of the description of the manoeuvre, to the first-aider, in a form that can be appreciated, and within minutes.</td>
<td>Differential diagnosis between choking and heart-attack, access a source of information, identify the condition and receive detailed instruction on the treatment.</td>
<td>Much “first-aid” literature strongly suggests that the field is considered to be significant.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The availability, to a consumer, on demand, of whole milk with acceptable bacteriological, nutritional and taste properties (and Codex standard protein, fat etc. levels).</td>
<td>Working refrigerator, transport from the retail outlet, retail outlet, communications and stocktaking system and financial transaction capability. Transport to the retail outlet, bulk transport of consumer packages, processing and packaging system, pasteurisation equipment.</td>
<td>The processes generating pasteurised and chilled milk are defined by regulatory bodies such as the IDF and Codex formulations.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service level criteria are defined in terms of delivery of the medication (of adequate purity and known strength to the end-user, in a form that the end-user can use).</td>
<td>Raw feedstock materials, synthesis of active compound, packaging, ordering and payment system, distribution chain, manufacture of (empty) metered-dose inhaler units, filling, shipping and distribution chain, pharmaceutical dispensing and financial transactions.</td>
<td>Medical statistics identify asthma as a common condition. Ventolin™ is commonly prescribed for the relief of even severe asthma.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Overview of examples for study
5.2.2 Granularity of example descriptions

Analysis requires the definition of streams, which may be streams of liquid, transported streams of items, streams of electrical power, streams of information or other intermediate or final products, and also definitions of “processes”, which transform streams. Practical definition requires a consideration of the granularity of the representation; for example, it would be possible to define a “power station” as a process that takes fuel and produces electricity, but it would also be possible to consider a power station boiler that takes fuel and produces steam, a power station steam turbine that takes steam and produces shaft power and a power station generator that takes shaft power and produces electricity. It would also be possible to consider finer levels of granularity; for example, it would be possible to describe the components of the steam turbine, e.g. main valves and their actuators, drain systems and lubrication systems.

The “exposure” metric generated by the analysis will depend on the degree of granularity described, and therefore a valid level of granularity. Considerations of granularity must be defined rigorously; the definition is proposed to include the following.

(a) A process should not be subdivided beyond the point where an attack would inevitably affect an adjacent sub-process. If any attack would inevitably affect an adjacent sub-process, it is not valid to consider the exposure of the two sub-processes separately. Two examples will illustrate this principle. A computer CPU chip may contain a billion transistors; however, as these are not practically accessible individually, they should be considered as a single point of failure (actually, this numeration will extend to the motherboard including all SMDs, but excluding RAM contents, because these can be accessed separately and represent an additional source of failure). In contrast, consider a long above-ground pipeline comprising many flanged pipe spools (possibly identified on an engineering bill of materials (BoM) as spool 123AA_001, spool 123AA_002 … spool_123AA_020). As such spools can potentially be attacked individually, a higher $E_1$ value could be assigned. For an underground pipe, it might be more likely that a pipe might be replaced on a city-block-by-city-block basis, allowing this to be used as the unit length. For
an undersea fibre-optic cable carrying internet data, the cable can be “hooked” and brought to the surface for repair, although this is a major operation. For the undersea cable, the number of repeaters can also be assessed, and an $E_2$ value based on the assumption that two adjacent repeaters need to fail, in order to make the complete cable inoperable, can be built.

(b) A process should not be subdivided beyond the point where a component or process would normally be replaced as a unit. For example, a computer printer has paper transport, electronics and similar subsystems, but it would normally be considered to be a disposable unit for which significant repair costs would exceed the new purchase cost. The proposed analysis is of the number of weaknesses, not of the number of possible attacks; although it is possible that some printer subsystems could be attacked without necessarily affecting the others, a significant failure would be considered simply as “printer failure”, and would result in the installation of a new printer.

(c) As the granularity should be consistent within each example, if an internet router within an apartment is considered, so should a router operated by the ISP through which the household’s internet connection is made.

(d) The level of granularity should be consistent across examples. This issue is assisted by the use of standardised contributory subsystems, applied to more than one example study.

(e) The granularity should allow meaningful assessments across all possible time-frames – hence, items that can be individually replaced should be identified so that a “replacement” time-frame can be assessed.

### 5.2.3 Selection of analysis depth

Within Chapter 4, it was proposed that the treatment of contributory systems should be addressed by setting a level to which the exposure values should be calculated, e.g. whether analysis should stop at $E_2$, $E_3$ or further. Rarely, engineering systems will include main, backup and emergency systems ($N$–3 design redundancy): examples include the provisions for lowering landing gear on fighter aircraft or lubrication oil systems on the main turbo-generators of a power station; however, even in cases where system level $N$–2 design redundancy has been specified, this is commonly not achieved because some common systems are impractically expensive.
to duplicate. For this thesis, it is not proposed to consider exposure modes and values below $E_3$. This level is considered to be more stringent than good engineering practice for most fields.

5.3 Contribution of common subsystems

The example studies are representative of many particular examples used for the delivery of the nominated goods or services. The analyses of the common contributory subsystems are similarly representative of many actual examples, and are defined so as to align in scope with the example studies. Several of the example systems include elements of communications, a need for financial transactions and/or a need for various commercial road transport. Where these subsystems are essentially identical across the examples, it is reasonable to treat them separately, and to improve the consistency of the examples by referencing the same common subsystem analysis. It is therefore important to ensure that the same subsystem scope is included in each relevant example, and that the individual example analyses include all exposures that are not in the common subsystem’s scope.

5.3.1 Internet communications system

Initial description. Whether a “smart phone” or a laptop or tablet is used, a user application such as browser software or an email client serves as a user input/output device and, with the operating system and software drivers, converts data to and from packets that are exchanges with a domestic router. From the point where packets of data leave the household router, an “internet communication system” conveys these packets to the input of another household router. There is significant variation in the input/output systems; however, for very many examples, the system between the exit from the user’s router and the entry to the remote user’s router is essentially identical. This internet communication system includes the telephony copper wire from the household router to the suburb’s digital subscriber line access multiplexer (DSLAM) cable termination point, the fibre-optic cable from the suburban DSLAM to the ISPs and Point-Of-Presence at the city’s “peering point”, i.e. the point where the city-wide internet connections are multiplexed on to a national peering network of fibre-optic links. From one of a small subset of these peering points, packets are routed to the connection point to a separate provider’s undersea fibre-
optic cable system. The routing in each case is directed by a border gateway protocol (BGP) that ensures that all routers can recognise the destination of packets and send these to the next appropriate router. Undersea fibre-optic cables use a very heavily protected set of optical fibres, with repeaters about every 400 km, to transmit packets to a remote termination point. The process is then reversed, leading ultimately to the presentation of packets to the input of a household router at the designated destination.

**Justification for presentation of example.** From the point where packets leave the domestic router, an almost identical system provides a foundational service for many others, and for several examples studied in this work.

**Service and service level.** The exchange of packets of information between the household router and the systems outside the household is proposed as the service level.

**Example description and definition of boundaries.** As the TCP/IP software within users’ systems is capable of error detection and for requesting the resend of packets, there is no need to specify “error-free reception of a file” as the service level. Furthermore, as household systems (smart phone, browser application etc.) vary considerably, these are not defined as within the common internet subsystem. The systems outside the household, from the telephone line leaving the router onwards, are defined as within the boundaries of the internet contributory system. For the exemplar system, the local household router exchanges packets via the simple telephone system’s copper wires to the roadside DSLAM system that commonly serves a city suburb. The roadside DSLAM facility multiplexes the packets exchanged with the complete suburb’s internet connections, and exchanges these with the ISP’s point-of-presence, which is commonly located in a telephone exchange building serving a city. The ISP’s point-of-presence is also a "peering point", connecting to other national "peering points". The ISP’s point-of-presence exchanges packets with other national peering points, allowing full internet connections. For offshore connections, ISPs purchase bandwidth from organisations that provide and service undersea cables, and packets are forwarded from peering points, via undersea cable, to offshore equivalents of peering points. At the distant end, a mirror image process leads to the exchange of packets to the distant router’s termination point.
Confirmation that example description is representative. Discussion with local ISPs has indicated that the system as described is representative; however, it is noted that many variations are possible, including the increasing availability of fibre to the home.

Definition of processes, streams and configurations. Packets are exchanged with the local DSLAM system IF local copper-pair cables are intact. The DSLAM multiplexes these packets to its fibre-optic cable IF it has power, AND the termination system is operational AND the multiplexer is operational. Packets are exchanged between the DSLAM and the ISP point-of-presence IF the fibre-optic system from the DSLAM to the city telephone exchange is intact. Packets are exchanged within the national peering points IF the national fibre-optic cables are intact, AND the ISP’s routers AND router tables AND power supplies are operational. Packets are exchanged with the undersea cable service provider IF the fibre-optic cable to the undersea cable termination point is operational. Packets are exchanged from end to end of the undersea fibre-optic cable IF the cable is intact AND power for repeaters is available.

5.3.2 Financial transaction

Initial description. Many, although not all, of the exemplar systems include a requirement for a financial transaction with the end-user. As this is common, and as the EFTPOS system for such transactions is very common, this is selected as a common subsystem. The “financial subsystem” will be referenced as such within each example, but will itself include the “internet system” as a contributory system. The scope that is uniquely within the “financial system” therefore excludes the scope defined for the internet communications common subsystem.

Justification for presentation of example. As the use of debit cards for even very minor transactions is common, it is useful to consider the exposure of the simple financial transaction system.

Service and service level. The service level will be deemed to be the display of a “transaction-accepted” message at the merchant’s EFTPOS terminal. This message will normally be sufficient assurance for the merchant to release the purchased goods or services and to complete the transaction with the consumer.
Example description and definition of boundaries. The financial transaction system uses the internet communications system several times; however, as the communications system is considered to be elsewhere, the subsystems required are as follows. The “acquirer bank” system that the EFTPOS terminal connects to, and which manages further transactions, is required. The merchant needs a service agreement with the acquirer bank and hence the acceptance of the acquirer bank’s terms and conditions. In order to use the EFTPOS system, the end-user also requires an account and hence acceptance of the user bank’s terms and conditions. Having received a request from an EFTPOS terminal, the acquirer bank requests information on credit availability from the user bank and makes the financial transfer to its account. The acquirer bank then makes the transfer of credit, possibly overnight in a batch mode, to the merchant’s bank.

Confirmation that example description is representative. The EFTPOS payment system is now almost ubiquitous in New Zealand; amounts of less than $10 are commonly transacted.

Definition of processes, streams and configurations. Noting that the communications systems are addressed elsewhere, the processes and hardware required for financial transactions are the EFTPOS terminal, which fulfils a similar function to a domestic router, and the computers, applications and storage systems at the acquirer bank, the user’s bank and the merchant’s bank. The accept message to the EFTPOS terminal will originate from the acquirer bank. The acquirer bank will issue the accept message once the user’s bank has accepted the transfer of funds to the acquirer bank and it has queued the transfer of funds to the merchant’s bank. The user’s bank will confirm the transfer of funds to the acquirer bank once it has confirmed that the EFTPOS transfer request refers to an account whose user has accepted the bank conditions, i.e. is valid, and has sufficient credit. The acquirer bank will confirm the queuing of the transfer of funds to the merchant’s bank once it has a confirmation from the merchant’s bank that the merchant has accepted the bank terms and has a valid account.

5.3.3 Road transport system

Some example cases, including those concerned with the transport of raw milk, sewage treatment bio-solids and medical items, require the transport of goods
by road. Although all these cases do require a road system and fuel, there are few other similarities, because, in some cases, vehicles such as milk tankers are required whereas, in other cases, general-purpose vehicles such as passenger cars or light trucks are adequate. As an identically scoped road transport system cannot readily be applied across multiple examples, road transport is treated separately within each example. Chapter 7 of this thesis identifies several general approaches to decreasing exposure, one of which is the use of re-purposable components. The adoption of standardised shipping containers is an excellent example of that principle.

5.3.4 Other systems

Electrical power is used by many examples, but the circumstances of the power delivery vary (three-phase high-voltage supplies to factories, single-phase low-voltage supplies to houses and supplies to different countries are some examples). For these reasons, electrical power will not be treated as a common subsystem, and electrical power supplies will be treated separately for each example. Urban-supply potable water is used in several examples, and the means of supplying it is identical in each case but, as the means of supplying it is somewhat trivial, an exposure of $E_1 = 1$ is simply added to each relevant example.

5.4 Detailed description of examples

5.4.1 Example study #1: sewage system

Initial description. The service, in this case, is described briefly as the sanitary removal of human waste, on an “as-required basis”, via the lavatory installed in a multi-storied apartment and resulting in the discharge of environmentally acceptable water to waterways or sea, and the dumping of solid waste of environmentally acceptable specifications to landfill. This example therefore includes the plumbing within the apartment, the pumps and pipework for aggregating and moving the sewage and the sewage treatment plant.

Time-frame for analysis. An “operational” time-frame is assumed, i.e. it is assumed that no maintenance or replacement of equipment is needed but that operational supplies are required. Practical issues for this example will include the assumption that landfill capacity is available for dewatered sludge and that any flocculent chemicals are available.
**Justification for presentation of example.** Public transport services (trains and buses) in New Zealand are generally considered to require onboard toilet facilities if the journey is longer than 2 hours. Although this is clearly only a guideline, it does demonstrate that the facilities are considered to be essential for even relatively short occupancy intervals. Historically, the provision of sanitary means of sewage disposal has been considered to be a primary contributor to population health, and to be essential if major disease outbreaks (either as a result of direct contamination, facilitation of breeding of flies, rats or other disease vectors, or indirectly by contamination of drinking water supplies) are to be avoided in any population concentration. Natural disasters and major equipment malfunctions have occasionally caused treatment facilities to be unworkable. The resultant discharge of raw sewage into municipal waterways constitutes a significant hazard, requires significant remediation and is certainly not acceptable over even a medium term. For the apartment dweller, the lack of a workable method of the sanitary disposal of sewage will effectively reduce the apartment to the status of emergency accommodation, and the lack of this service will certainly involve significant and unwanted changes to the lifestyle of the apartment dweller. Without a functional sewage disposal system at the end-user level, apartment dwellers would be obliged to make very significant changes to their lives – perhaps by using portable sewage collection systems at street level, as was done in Christchurch following the 2011 earthquakes.

**Service and service level.** The service, in this case, is the sanitary removal of human waste, as required, via the lavatory installed in a multi-storied apartment and resulting in the discharge of environmentally acceptable water to waterways or sea, and the final disposal of solid waste of environmentally acceptable specifications to landfill. In practice, many sewage treatment station processes will include bypasses, allowing untreated sewage to be dumped to waterways or sea in case of equipment failure or overload – however, such operations would not be within the service level definition.

**Example description and definition of boundaries.**

(a) The service commences with a water-flushed lavatory in an apartment. This initial operation also requires the availability of flushing water, which would generally require the use of a booster pump to supply water to a high-level
header tank in the apartment block, and would require the power supply to the
apartment building plus a level control system for the header tank.

(b) Almost all city-scale sewage systems currently use gravity-fed systems, which
are commonly clay or ceramic pipe systems or concrete and brick-lined
tunnels in larger cities, to link dwellings to major pumping stations.

(c) Pumping stations are commonly located in deep pits accessible from ground
level, and incorporate large-capacity, low-head pumps that are commonly
duplicated with changeover valve systems to allow maintenance. The
pumping station pumps would commonly require three-phase 415 V power
supplies, and a motor-start system operated by a control signal generated
either locally or remotely. Multiple pumping stations between any one
apartment and the local sewage treatment station may be required.

(d) Sewage treatment commences with an initial coarse screen with a motor-
powered system for extracting large pieces. Screened waste goes to a
sedimentation process with a powered scraper chain system for removing
initial settled sludge and a pump to transfer this to the sludge treatment
system. Waste from the initial sedimentation process is pumped to a trickle
filter to remove finer particles and allow decomposition. An aerobic digester
takes the trickle filter outlet and aerates this thoroughly using a powered air
blower and a sparged air-contact system (deodorisation). A final clarifier
allows spent digestate to settle and to be pumped to the sludge treatment
system, and allows clarified and treated water to be discharged to oxygenation
ponds. Oxygenation ponds allow natural oxidation processes to eliminate
bacteria.

(e) Treated water is discharged to waterways.

(f) Treatment plant sludge is commonly digested anaerobically to generate
methane and bio-solids.

(g) Bio-solids are mechanically dewatered and conveyed into trucks.

(h) Trucks convey the dewatered bio-solids to landfill.

Explanation. As electrical power supplies to sewage pumping stations and to
local flushing water supply pumps are unlikely to have multiple feeders, these must
be considered in the exemplar system, upstream to the nearest substation. The
substation can be expected to have multiple feeders and therefore it is not considered
to be necessary for the exemplar systems to consider the electrical power supply further upstream. Significant pumping stations would commonly have a "local/manual" capability, in which a remote control is normal, but allowing an operator to select "manual" at the pumping station and thereafter to operate the pumps and valves locally. As the dewatered and treated solid waste is disposed to landfill, the example must include the road transport aspects, the landfill capacity and the waterway discharge and testing. Some treatment plants include embedded cogeneration using the anaerobic digester gas; others do not. As the embedded cogeneration is not in any way necessary to the operation of the sewage treatment station, it is not considered here.

As electrical power supplies to sewage pumping stations and to local flushing water supply pumps are unlikely to have multiple feeders, these must be considered as contributing to $E_1$ values downstream from the nearest substation. Although substation configurations vary, these commonly have multiple in-feeds; thus, it is not reasonable to assume that a representative substation has exposure at the $E_3$ level. Significant pumping stations would commonly have a "local/manual" capability, in which a remote control is normal, but allowing an operator to select "manual" at the pumping station and thereafter to operate the pumps and valves locally. As the dewatered and treated solid waste is disposed to landfill, the example must include the road transport aspects, the landfill capacity and the waterway discharge and testing. Some treatment plants include embedded cogeneration using the anaerobic digester gas; others do not. As the embedded cogeneration is not in any way necessary to the operation of the sewage treatment station, it is not considered here.

**Confirmation that example description is representative.** An informal survey of the configuration of sewage systems used by cities within this size range, specifically Auckland, Melbourne, Sydney and also Wellington, reveals a level of uniformity, and hence the configuration in the example is considered to be "representative". There are still some smaller cities that rely on the discharge of sewage to the sea; however, this is neither common nor desirable practice. Some treatment plants include embedded cogeneration using the anaerobic digester gas; others do not. A representative cogeneration system is described, but no contribution to the exposure is assessed.
5.4.2 Example study #2: collaboratively developed work information

**Initial description.** The service, in this case, is the capability to store and retrieve, view, edit and share information; although the title specifies work information that could include client lists, design information, accounting records, reference information, academic papers and contractual agreements, other vital information such as family records, important writings, ethical, political and regulatory information and music will be very similar. The "information" addressed by this example should be considered to be complex, because the definition could be expected to include text, music, images, design information and databases and should be considered to have at least potential longer term significance. The definition also specifies storage (although the storage term is not defined). The definition specifies sharing (hence transmission to a defined recipient and an integrity check). The definition includes "edit", implying that the information can be updated in some way that is intelligible to self and others. The example assumes that the end-user has normal eyesight, that material is in a mutually understandable language and that the user has the financial resources to obtain communication services.

Very little editable information is truly analogue; almost all reference information is in, or can readily be represented in, a digital form. Issues relevant to the selection of "example information" include: is the format specified and whether this is or is not publicly available; to a lesser extent, is the format commonly used, versatile and capable of including complex information in an editable and storable form? Options for "example information" would include a photograph, spreadsheet, word document, engineering drawing or pdf file. The example that is selected is the exchange and updating of a simple spreadsheet. The technological aspects of this example will therefore be much broader and more complex than ephemeral messages such as an SMS message or a shout of warning, and will include the consumer electronics (end-user equipment – hardware and software), the communications network and the remote end-user equipment. The significant issues to be addressed in the development of this example are defining the granularity of the processes and streams and determining which processes and streams do not actually contribute to the boundary level of exposure (E₃), i.e. are massively duplicated.

**Time-frame for analysis.** As an “operational” time-frame is assumed, no maintenance or replacement issues are considered. The operational time-frame
means that there is no need to consider such issues or those of outdated and unsupported software or of hardware, such as a digital video disk (DVD) reader, maintenance or replacement. Although it does not impinge on the definition of the current example, it is noted that much concern has been raised over the longevity of current information storage approaches; this specific issue will be addressed when hypothetical changes to the example study are considered – and is particularly relevant for compressed and “lossy” representations such as JPG and MP3, which are dependent on complex algorithms to restore information to a presentable form, and for “closed” representational formats such as those used on current DVDs.

**Justification for presentation of example.** It can be observed that the storage and transmission of information is foundational to civilisation – the recording of medical, veterinary and agricultural knowledge, the teaching of engineering, the recording of contracts and commitments, and the recording of family history information, cartography and chemical information are essential. A consulting engineer without access to functional email, or file server facilities, is likely to be unable to carry out expected tasks. Similarly, apartment dwellers are unlikely to have the storage space to hold significant tomes of family history or reference material but their lifestyles will be significantly impaired if that type of material is inaccessible and future generations are impoverished if recent learnings cannot be incorporated into the body of knowledge. The apartment dweller is also likely to be geographically remote from a “tribal village” and hence is dependent on records rather than oral history and local knowledge for life-context. For at least a significant portion of apartment dwellers, employment requires immediate access to both means of communication and stored and editable data. The inability to receive, store, update, edit and pass on information, such as that defined in the example scope, would effectively isolate a significant portion of the representative population from employment in their selected fields of expertise; as such, the lack of this service would effectively force significant lifestyle change upon the representative users.

**Service and service level.** The definition of service delivery implies that the complex information can be read, seen and updated by more than one party, before being read by the intended recipient. The service will be deemed to be delivered when a representative user can read, at a convenient time, information created and updated recently by a third party. “At a convenient time” implies some storage. “Created … by
a third party" implies that at least recent edits are reasonably possible. Note that the identification of a destination individual "alone" does not imply encryption, but that "read" does imply that the recipient can comprehend the information in the same way as it was sent, edited, sent and stored. The service definition can then be refined to mean that a representative user can read, at a convenient time, a simple analysis spreadsheet that has been transmitted to the representative user alone, and can in turn edit the document and dispatch it to another party.

**Example description and definition of boundaries.** This example describes a PC being used to view and edit a spreadsheet that has been developed by a remote colleague and emailed.

(a) User’s PC, with power supply, operating system and software.

(b) Data communications, which has a local component, an internet transmission path (which is considered to be a common subsystem by this thesis) and a remote component to the remote user’s PC.

(c) The remote colleague’s PC with power supply, operating system and software.

**Confirmation that example description is representative.** Statistics for Australia and New Zealand show that a large proportion of the population have either laptops or "smart phones", and hence are assumed to also have the financial means to connect to the internet, and the intellectual capability to operate the devices. Allowing for the percentage of population who are either too young or incapacitated, this indicates that the exemplar end-user is representative of a large proportion of the population. Not only are the example details considered to be representative of the specific service that is considered, but also the example is considered to be essentially identical to the case of an electronic (EFTPOS) financial transaction; in that case, an EFTPOS terminal is used instead of a laptop and a piece of bank-owned software is used instead of the second end-user.

### 5.4.3 Example study #3: local fuel supply

**Initial description.** The service, in this case, is the supply of petrol at a local petrol station. The scope must consider the operation of the dispensing pumps, the local fuel storage tanks, the metering and transactional services, the refilling of the underground tanks from fuel stored in national reserves and the creation, from crude sources, of national reserves. The bulk fuel is assumed to be available from only one
source. New Zealand currently has only one refinery. As the station is unlikely to have duplicated power feeders from the nearest substation, this supply must be considered. The local substation will probably have at least dual in-feeds from the national grid; thus, there is no need to consider power supply security further back than it. The financial transaction subsystem (EFTPOS) is covered elsewhere. A staffed station is assumed and hence staff facilities including sewage and water supply are required.

**Time-frame for analysis.** An “operational” time-frame is assumed; hence maintenance and replacement of components are not envisaged. Although petrol stations have some storage, the refilling of the underground tanks from fuel stored in national reserves can be accomplished by only a limited number of approaches, which must occur frequently, and therefore will be considered to be an operational issue.

**Justification for presentation of example.** Within very large cities, the population density generally makes good public transport economic and allows a citizen to carry out normal functions, such as grocery shopping and commuting to work, using public transport. For the size of city considered (of a population between about 200,000 and 500,000), public transport coverage and frequency commonly make such activities as grocery shopping and commuting to work only marginally practical for many, and the distances are arguably too long for many to reasonably walk. For such representative persons, the lack of an operational private vehicle will certainly cause significant disruption to lifestyle.

**Service and service level.** The service is achieved when pre- or post-purchased petrol, whose quality is within the standard fuel specification limits, is supplied at a normal flow-rate, to a vehicle parked in the forecourt of the petrol station.

**Example detailed description and definition of boundaries.**

(a) Petrol pumps are operable if both fuel and electrical power to operate the pumps are available.

(b) The pumps can be operated if the fuel can be metered, a local control and data collection system, to transmit the amount pumped to the cashier, is functional and a capable operator is available. The fuel metering will be possible if the meter is functional and power is available.
(c) As the station is not automated, the availability of a capable operator is practical only if an operational water supply, an operational sewage disposal system and power for lighting and security are available.

(d) A customer financial transaction is required, and is proposed to be EFTPOS.

(e) As the station storage is limited, the supply of the bulk fuel must be considered.

(f) The production of bulk motor specification fuel from crude oil must be considered, noting that New Zealand has a single refinery.

Confirmation that example description is representative. For the type of petrol station described, the processes and equipment are observably very similar across a wide range of locations internationally.

5.4.4 Example study #4: targeted first-aid

Initial description. The service, in this case, is the correct application of a first-aid measure. A significant number of unpredictable medical events could possibly affect an apartment dweller. In many cases, these can be life threatening; in a significant proportion of examples, the correct application of first-aid can markedly improve the probability of avoiding injury or death. Illustratively, these could include electrocution, poisoning, acute allergic reactions, cardiac arrest, acute asthma attack and arterial bleeding from an accidental cut. The accepted approach for treating acute choking, i.e. a foreign body blockage of the airway, is known as the “Heimlich manoeuvre” and is selected for this example. An acute airway blockage can present itself unpredictably, quickly and without warning. In the context of a representative apartment dweller, in a situation where a person’s airway has become blocked, the person’s life is under threat within a matter of minutes. The remedy for this particular situation is simple provided that the diagnosis is made quickly and accurately, and that the procedure is described.

Making the assumption that the end-user does not have significant first-aid training, they are reliant on a specific technological approach to get the “service”, i.e. the diagnosis and the treatment information that is required. This example will consider the contribution of the technological system to their vulnerability. The example has similarities to the work information example and the financial transaction subsystem – however, it differs because this system requires only one-way information from a static source.
**Time-frame for analysis.** Only an “operational” time-frame can be considered. The essence of the issue is very short term access to critical diagnostic and treatment information – the process is either successful or disastrous within a few minutes, i.e. it has a defined time interval. There is no option for repairs or maintenance to technological systems or components during the defined time interval.

**Justification for presentation of example.** Life-threatening medical emergencies can certainly occur for the apartment dweller. For emergencies that involve loss of airway, acute loss of blood or electrocution (to name a few), the time interval between instantiation and death is an order of magnitude shorter than the time for even a quickly dispatched paramedic to arrive. For such situations, life or death will depend upon the ability of a co-dweller to diagnose the problem, identify the appropriate life-saving measure and apply that measure. A targeted first-aid example represents a case where the life and well-being of the apartment dweller is critically affected and is therefore justifiably included. The diagnosis of choking is not difficult but it may also not be trivial. The Heimlich manoeuvre is not difficult to perform; however, it is not intuitively obvious – it needs a detailed explanation to be made quite quickly available to the first-aider. The example illustrates a case in which some trivial assistance may be required to fully understand a situation and, having achieved that, where some very specific and detailed information must be transferred to a person within a short period of time. As the apartment dweller has no real knowledge of geographically close experts, and is dependent on technological approaches for diagnosis and treatment method, the current technological means of providing the “service” does contribute to the end-user’s current vulnerability.

**Service and service level.** The service is defined by the delivery of the detailed description of the manoeuvre, to the first-aider, in a form that can be appreciated. The service level is defined by time. If complete airway obstruction has occurred, the choked person could suffer permanent brain damage within 4–6 minutes and death within 10–15 minutes.

**Example description and definition of boundaries.**  
(a) The first-aider communicates symptoms and understands the required action, which is described by a remote expert.  
(b) The communication system is needed to identify and contact the remote medic; this implies related topics of search, and confirmation that the person
is qualified. Assuming that a qualified person or other knowledge source is identified and contacted, he, she or it will probably have no problem in diagnosing the problem or recommending the solution.

(c) The provision of the first-aid advice depends critically on the availability of a knowledge base that has the capability to understand symptoms, to allow confirmation and refinement of these symptoms and to identify and describe recommended actions in a form and timeliness to allow remedy.

**Explanation.** The example description is adequately covered in the initial description. It might be significant to make a differential diagnosis between choking and heart-attack, but this is unlikely – circumstances and history are likely to make the diagnosis of choking clear. Therefore, the necessity is for the co-dweller (strictly speaking, the Heimlich manoeuvre can be performed by the choking victim alone) to access a source of information, identify the condition and receive detailed instruction on the treatment – within the time-frame that will preserve life. The person making the diagnosis and applying the treatment is likely to use a “smart phone” to access an internet-based medical self-diagnosis service, and follow the treatment. The example definition of service does not consider outcomes; simply, the information that is necessary to enable an effective remedy to the medical condition is conveyed, in a manner that can reasonably be expected to be comprehensible, to the co-inhabitant.

**Confirmation that example description is representative.** There are large bodies of literature and institutions devoted to the named topic of “first-aid”, strongly suggesting that the field is considered to be significant and there is the real possibility of improving a medical outcome using minimal, i.e. non-specialised and non-professional, procedures. The general field is therefore considered to be representative of a broad spectrum of “first-aid” procedures. As most first-aid procedures require minimal equipment and rely primarily on diagnosis and simple actions applied quickly, the Heimlich manoeuvre can be considered to be representative of a first-aid procedure, because it requires no equipment, requires immediate action and primarily requires diagnosis and knowledge. Although many local or national medical services do offer “helpline” types of access to human experts, and emergency calls to ambulance services are available to bring paramedics to a location, recourse to online medical help is increasingly common (e.g. the WebMD
service and the St Johns organisation’s first-aid advice (n.d.); therefore, the technological approach presumed for the example is considered to be representative.

5.4.5 Example study #5: perishable food

Initial description. The service, in this case, is the supply of a perishable food. Vegetables, fruit, dairy products, meat and fish and bakery products could be considered. Fresh whole milk is selected because it is a staple food and requires a technological system that is similar to that required by other nominally processed fresh food. Nevertheless, the technological system is not trivial – the pasteurisation step requires close control if bacteriological safety is to be obtained without deterioration of the nutritional and taste qualities. The example will therefore consider the aggregation, processing, transport and retailing of milk. As a large number of cows, located in a wide area, produce the raw material and a large number of tankers are capable of farm collection, it is reasonable to consider that scope beyond the processing plant's reception area is adequately duplicated. The example considers that the availability of a consumer pack of acceptable quality whole milk, in the refrigerator of the user’s apartment, is the correct end-point of the example.

Time-frame for analysis. An operational time-frame will be considered. This implies that neither equipment maintenance nor equipment replacement is required. Consumables such as “cleaning-in-place” (CIP) chemicals and fuel need to be considered. Financial services are necessary for retail transactions and fuel, drivers, vehicles and roads are necessary for transport, but maintenance is not considered to be necessary within the operational time-frame.

Justification for presentation of example. The apartment dweller obviously needs food, although it could be argued that it is possible to survive without any fresh food and/or by eating out as an alternative to purchasing, storing and cooking food. It would be very common for apartment dwellers to purchase, store for the short term and use fresh food – and deprivation of this capability would constitute a “significant change to lifestyle”. This justifies the consideration of a fresh food example. Fresh milk is a very common food – alone or as an ingredient. Usage is common across age groups, cultures and socio-economic classes. It can be considered to be a representative fresh food. As moderately similar systems would be required for the delivery of many short-shelf-life foods, it is argued that this example is representative.
of a category of goods or services whose non-availability would cause significant lifestyle change.

**Service and service level.** The service and the service level are defined by the availability, to a representative individual consumer, on demand, of whole milk with acceptable bacteriological, nutritional and taste properties (and Codex standard protein, fat etc. levels) at the point of use, which is the apartment refrigerator.

**Example description and definition of boundaries.**

(a) At the delivery point (where the service and the service level are supplied), a working refrigerator and electrical power are required. Transit to the apartment requires electrical power to operate the elevator.

(b) Transport from the retail outlet to the consumer location requires fuel, a driver, an operational vehicle and roads.

(c) The purchase requires availability of the product, a retail outlet and a transaction system.

(d) The retail outlet requires staff, electrical power, functional lighting, communications and a stocktaking system.

(e) The retail outlet requires a functional sewage system and a functional water supply.

(f) The retail outlet requires the bulk transport of consumer packages.

(g) The processing and packaging system, pasteurisation equipment, control system, CIP system, CIP chemical supply, pipework and valve changeover system for CIP, electrically powered pumps, electrically operated air compressors, fuel and fired hot water heaters, packaging equipment, packaging material supplies, water supply, waste water disposal, sewage system and skilled operators. As limited numbers of processing plants are practically accessible for the retail outlet, these must be considered. Although there will be variation in packaging equipment types, each of these can be considered to be a single process and a single "weakness". Processing plants are staffed and therefore require an operational sewage disposal system. Processing plants require a substantial water supply for processing, CIP and staff facilities.

(h) On-farm processing is not considered; the scope boundary is at the outlet of the farm milk vat.
Explanation. Power is required for the processing facility, for the retail outlet and for the end-user’s refrigerator. These power supplies can be considered to be separate. As neither the processing facilities, nor the retail outlet, nor the apartment would commonly have duplicated electrical power feeders, these and associated protection systems must be considered back to the nearest substation. The substation can be assumed to have multiple input feeders; thus, the electrical power system need not be considered any further "upstream" than the substation. The hot water boiler and hot water circulation system for the pasteuriser would commonly be fired with fuel oil, but including enough storage that it would commonly be supplied directly from a fuel wholesaler, hence applying a portion of the processes noted in relation to the fuel supply example.

Confirmation that example description is representative. The processes leading from raw milk collection, up to the point where pasteurised and chilled milk is packaged, are defined in considerable detail by regulatory bodies such as the International Dairy Federation and Codex milk formulations – and can therefore be considered to be representative. Distribution to supermarkets, retail sales and distribution to individual dwellings are similar across most of the western world and are considered to be adequately representative as are the processes from retail outlet to end-user availability.

5.4.6 Example study #6: essential specific medicine

Initial description. The service, in this case, is the supply of an essential medicine that enables an apartment dweller to continue to function at a normal level. This example could consider either a new vaccine that is researched, developed and distributed in response to a new disease or a well-known medicine that is required on an ongoing basis for a chronic condition (e.g. insulin, Ventolin™) or a well-known medication that is needed for a not-infrequent acute condition (e.g. penicillin). The new vaccine example is not selected as an example to be studied because, although there are standard processes for attempting to find or develop a vaccine, it is not certain that these are sufficiently standardised that a described system will be able to be confirmed to be representative.

The “vulnerability” criterion suggests the selection of a medicine that is needed on a long-term basis by a significant section of the population, and whose non-
availability would result in significant lifestyle change for those requiring the medicine. For useful analysis, a medicine should have a well-known composition and synthesis. For regularly used medicines, the World Health Organisation (WHO) publishes a model list of essential medicines. The medicine selected from this list for study is salbutamol sulphate, commonly marketed as “Ventolin™”, which has been used widely for the relief of acute bronchospasm (asthma). Without this common medicine, many persons’ ability to function adequately will be affected. This example will illustrate the synthesis, and delivery models, without the ill-defined discovery aspect that is associated with developing a vaccine for a new epidemic. The service will be considered to have been delivered when a fully charged metered-dose Ventolin™ inhaler is handed over to a user. It is useful to note that, although Ventolin™ is commonly administered by metered-dose inhaler (MDI), it is actually quite possible (although less convenient) to administer the salbutamol sulphate orally, intravenously or using a hand-pumped nebuliser (atomiser) to provide fine droplets of dissolved substance. The dose tolerance is high, allowing many alternative delivery options to be considered to be feasible.

**Time-frame for analysis.** As an operational time-frame is to be analysed, no significant maintenance or replacement of equipment or processes will be required. Because MDIs are not refillable, they will be treated as consumable items. As relatively large supplies of salbutamol can be produced with a fixed set of reaction glassware, an operational time-frame clearly need not take account of the maintenance or replacement of this equipment. As relatively large numbers of MDI devices can be filled and sealed by a production line, an “operational” time-frame clearly need not take account of the maintenance or replacement of the filling and packaging equipment.

**Justification for presentation of example.** There are a number of medical conditions that allow a person to live a reasonably normal life with treatment, but would severely reduce their capabilities without treatment. Asthma affects a significant portion of the western world’s population, and specifically about 800,000 New Zealanders are affected by asthma, chronic obstructive pulmonary disorder and other respiratory conditions; if not controlled, they can lead to significantly decreased ability of the individual to function. Certainly, for many people, the lifestyle that is possible with the help of well-known medications would not be possible without them.
Within a longer time-frame, although asthma is defined as a reversible bronchospasm, repeated episodes, i.e. as would occur without adequate medical control, lead to progressively irreversible damage to the lungs and to longer term impairment. The simple “Ventolin”™ bronchodilator, using the salbutamol sulphate active ingredient, is very widely used and is generally effective in controlling bronchospasm. The effects upon lifestyle and the significance of the proportion of the population affected justify the inclusion of an example of this type, and the effectiveness of Ventolin™ justifies its specific example.

**Service and service level.** The service level criteria are defined in terms of delivery of the medication, of adequate purity and known strength, to the end-user, in a form that the end-user can use. As the medication is normally self-administered, the criterion is the availability of the active ingredient, in a form that allows self-administration, using available equipment, as required. Because the medication is normally administered via an MDI, this will be assumed to be the basis of the example. It is noted that, although the active ingredient, salbutamol sulphate, is normally administered using an MDI, it can be taken orally or given intravenously, and, because the effects of exceeding the recommended dose are generally not severe, the dosage is not particularly critical.

**Example description and definition of boundaries.**

(a) User acquisition of MDI: financial transaction. Pharmaceutical dispensing systems including financial transactions, as most countries have at least part charges.

(b) User acquisition of MDI: prescribing permission. Medical diagnostic and prescribing systems, which include regulatory issues, financial transaction systems and availability of skilled staff.

(c) MDI filling, packaging and distribution. The filling of MDIs requires loading with the active ingredient formulation, pressurisation with propellant, assembly of metering valve and sealing and swaging of the completed unit (under clean-room conditions). Assembly of the consumer package requires attaching the printed label to the MDI, folding and gluing the printed box, packing of the inhaler and information sheet and the distribution of filled MDIs. Shipping and distribution chain for filled MDIs available from multiple providers.
Manufacture of MDI container and distribution. Manufacture and filling of MDI containers. Components are container, propellants, formulation, metering valve and actuator (plastic mouthpiece/holder). The container is manufactured by a deep-drawing operation, taking an aluminium sheet as the raw material and using an electrohydraulic deep-drawing press to create the container. The metering valve is created using two pieces of equipment. The perforated actuation tube that releases the dose when depressed, and allows the loading of another dose of propellant plus active ingredient, when released from depression, would normally be formed using an electrically operated CNC lathe, from an aluminium or plastic tube stock. The metered-dose chamber is formed by a deep-drawing operation that is similar to that used to form the container (the chamber must hold a metered dose, at a pressure similar to that in the main container but of smaller volume) and minor components such as spring, tube seals etc. The container and cap are each formed by a common electrically operated pressure-injection process using a thermoplastic. The metering valve is assembled using common semi-automated processes.

MDI active ingredient distribution. Distribution via a traceable distribution chain.

MDI active ingredient – synthesis, testing and dilution. Creation of the active ingredient. Assembly of raw feedstock materials, which are available from a large number of sources, for the synthesis of salbutamol. Synthesis of the active compound, confirmation of purity and analysis. This process has been optimised to a six-stage chemical process as described by Imperial College (2016) "ChemWiki" ‘Synthesis of Salbutamol’. It is assumed that the active compound is made in only one location. Steps include the creation of a formulation, including dilution with an acceptable substrate, of the active compound, packaging and cold storage of the active ingredient, ordering and payment system and related communication systems to allow wholesale distribution of the active ingredient, and the distribution chain for the active ingredient to national level factories that are responsible for the manufacture and filling of MDIs.

Explanation. As MDIs are normally carried on the person, and do not require refrigeration, no final transport step for the MDIs is included in this example. Because
multiple options for the pickup of MDIs by end-users are available, these are also not considered to contribute to the defined exposure.

**Confirmation that the example description is representative.** The "end-user" is not a named individual, but must be demonstrated to be "representative". The criteria for "representative" are set out earlier and, as current medical statistics identify asthma as a very common condition, it is considered that an asthma sufferer can reasonably be identified to be representative of a portion of the target population. Ventolin™ is very commonly prescribed for the relief of even acute and severe asthma, and can thus be considered to be a representative treatment.

### 5.4.7 Homogeneous system example

This section will describe the development of a representation of a homogeneous system. This will be a completely hypothetical example, and will not be verified by interviews etc. Its only purpose is to demonstrate that an exposure metric can be developed for a homogeneous system example and to assess the insights available from the analysis of exposure.

*Figure 10 Example homogeneous system*
Considering the system shown in Figure 10, the individual streams and dependencies can be represented as follows (using the notation “Pa” to represent process node or vertex A, and “LM” to represent the edge from vertex L to vertex M).

\[
\begin{align*}
\text{Out} & \quad \text{IF} \quad (Pm \text{ AND (LM OR KM)}) \\
\text{KM} & \quad \text{IF} \quad (Pk \text{ AND (JK OR IK)}) \\
\text{JK} & \quad \text{IF} \quad (Pj \text{ AND CJ}) \\
\text{CJ} & \quad \text{IF} \quad (Pc \text{ AND AC}) \\
\text{AC} & \quad \text{IF} \quad (Pa \text{ AND Input}) \\
\text{IK} & \quad \text{IF} \quad (Pi \text{ AND DI}) \\
\text{DI} & \quad \text{IF} \quad (Pd \text{ AND AD}) \\
\text{AD} & \quad \text{IF} \quad (Pa \text{ AND Input}) \\
\text{LM} & \quad \text{IF} \quad (Pl \text{ AND HL}) \\
\text{HL} & \quad \text{IF} \quad (Ph \text{ AND (EH OR GH)}) \\
\text{EH} & \quad \text{IF} \quad (Pe \text{ AND BE}) \\
\text{GH} & \quad \text{IF} \quad (Pg \text{ AND FG}) \\
\text{BE} & \quad \text{IF} \quad (Pb \text{ AND DB}) \\
\text{DB} & \quad \text{IF} \quad (Pd \text{ AND AD}) \\
\text{FG} & \quad \text{IF} \quad (Pf \text{ AND BF}) \\
\text{BF} & \quad \text{IF} \quad (Pb \text{ and DB})
\end{align*}
\]

Substituting the input conditions for intermediate streams, the complete system can be represented by Equation 9:

\[
Out = \text{IF} \quad (Pm \text{ AND (PI AND (Ph AND ((Pe AND (Pb AND (Pd AND (Pa AND Input)))) OR (Pg AND (Pf AND Pb AND (Pd AND (Pa AND Input)))))) OR (Pk AND (Pj AND (Pc AND (Pa AND Input))))))})
\]

*Equation 9*

It is to be expected that, as this is a homogeneous system, the resulting Boolean expression is shown to be dependent only on the processes and the single input stream. The total exposure of the system can be shown to be \(\{2, 2, 4\}\), and the analysis of exposure is shown to illustrate the actual vulnerability of the system. Although this example does show that it is possible to represent a homogeneous system as a Boolean expression and to calculate the associated exposure, it can be noted that few, if any, systems are truly homogeneous; for example, a computer communications network will require processors, power and memory at each node, as well as connections to the other nodes.

### 5.4.8 Dynamic system example: newspaper vendor example

Many aspects of supply chains have been studied extensively, and the field of study of this thesis has been carefully distinguished from those. It is however valuable to apply the theoretical basis of this thesis to a classical problem in order to illustrate the contribution offered.
The “newspaper vendor problem” is a classical problem in the field of operations research and supply chain theory. This example problem is described by Khouja (1999), although many other authors have proposed variations to consider risk aversion, resale discounting and limited stock exchange. In Khouja’s explanation of this model, a newspaper seller purchases a stock of newspapers from a wholesaler and sells them one by one to purchasers over the course of a day. The model’s premises are: (a) the newspaper stock must be purchased once, at the start of each day; (b) the demand for purchased papers is variable; (c) unsold papers have zero value at the end of the day; (d) the vendor wishes to maximise profit.

This thesis investigates the technological barriers to the availability of the nominated services, and how the technological aspects contribute to the vulnerability of the end-user of the services. This example will be studied on that basis. An “operational” time-frame for analysis is assumed, i.e. it is assumed that the newspaper vendor’s shoulder bag, the roads and the newspaper production facilities remain operational for the time-frame of the analysis and require neither repair nor replacement. In this case, the service for the end-user is the acquisition of a newspaper. In other examples studied in this thesis, the process for transporting goods or services to the place of use has been considered; however, for this case, it is equally likely that the purchased newspaper will be read on the train or bus, and the final transport step is not normally considered in the models that are published in the context of operational research. The classical “newspaper vendor” study does not consider the capacity of the newspaper production plant, or its continued operation; these are assumed.

Assumptions made in the current thesis study of this classical problem are as follows.

- There is no technological reason but only a profit maximisation reason why the newspaper vendor cannot order sufficient papers. It is assumed that the printer’s capacity is not limited.
- There is no interchange of stock amongst vendors during the day – if that were possible, the process description would include a range of “OR” gates to illustrate the fact that a vendor could have multiple potential suppliers of stock, and, assuming good communication and logistics, there would effectively be only a trivial problem remaining.
• The vendor's ability to purchase "sufficient" papers is not constrained by the vendor's financial capability.
• Each purchaser has the financial means to purchase a newspaper.

The model for analysis within this thesis then reduces to the following.

(a) The purchaser is assumed to be at a location used for retail sales by the vendor.
(b) The purchaser (end-user) carries out a minor financial transaction to purchase the newspaper.
(c) The vendor has transported himself or herself to the normal sales location, carrying the stock of papers.
(d) The vendor has completed a financial transaction with the newspaper supplier, for the purchase of stock.

5.5 Conclusion to the definition of examples

The process for assembling the initial datasets must provide data that can be analysed in following tasks, but must also be demonstrably valid and representative, as set out in the project methodology. The assembly of data has been documented sufficiently well to allow replication of the results by a competent researcher or independent validation of the results by a review of the input data. This chapter supplies all the material needed for the analysis to be documented in the following chapter, and has carefully considered the granularity of the representations and the configurations of the system, including the design redundancies. The subsystem definitions align with the Chapter 6 tables that analyse the contribution of each subsystem to the total user vulnerability.
6. **CALCULATION OF EXPOSURE OF EXAMPLES**

6.1 **Introduction**

Having developed a theoretical basis for the evaluation, and having selected and described a suite of examples, this section implements the analysis and presents the results. Several approaches to the calculation of exposure values are considered in this section and, after examination, an approach that is appropriate for the examples is selected and refined. The refinement includes the establishment of reasonable limits of calculation. The implementation of the analysis method is described. For the analysis of the examples, analyses at subsystem level are presented – the subsystems are those described in Chapter 5. The full analysis that considers all processes and streams, and all relationships, is presented in Appendix B to this thesis. This section describes the steps taken to validate the analysis method, and to verify the results. Chapter 5 included validation that the example descriptions and scopes were valid for the purposes of analysis.

In addition to analysing the examples that have been specifically selected for study, this chapter also applies the analytical method to an illustrative homogeneous system and to a dynamic system (newspaper vendor) problem. The analysis of the homogeneous system demonstrates that such a system can indeed be shown to be a special case of the category of heterogeneous systems, and that the exposure of such a system can be calculated and shown to offer useful insights. The application to the dynamic system is presented simply to demonstrate application to a classical supply chain optimisation problem – and, in this case, also shows valid conclusions. The exposure metrics obtained for each of the example studies are discussed, in terms of absolute values, significant characteristics and relative magnitude.

6.2 **Application of the analysis method to the examples**

6.2.1 **Implementation of the analysis method**

This section will refine the proposed analysis method. The process for implementation of the analysis approach will also be developed as will the process for the setting-up of inputs. This task and section will include the enumeration and description of failure combinations that imply one, two, three or more weakness points simultaneously, and will also address the question of the representation of
intermediate streams that are required for multiple dependent streams – this may result in weighting according to the exposure reduction offered. Generating the qualitative analysis outcomes will be by inspection, reasoning and deduction. Three approaches to the generation of the quantitative outputs are considered.

(a) Algorithmic approach. It is possible to construct an algorithm that will systematically test each possible combination of inputs to the Boolean expression representing the technological system. For a system with $n$ inputs (processes and input streams), this equates to $(2^n - 1)$ combinations. It is possible to design more computationally efficient algorithms that initially establish, by testing, all of the $(n)$ $E_1$ values, then establish, by further testing, all of the $(2^{(n-E_1)} - 1)$ combinations, counting the $E_2$ values (i.e. testing all two-input combinations, and only counting those that did not trigger the $E_1$ criteria) and then establish, by further testing, all possible $E_3$ values and only counting those that did not trigger either the $E_2$ criteria or the $E_1$ criteria.

(b) The progressively contributory approach. Noting the generalised calculation approach presented in Section 4.5, it would be possible to develop a methodology that started with the processes and streams that are most distant from the end-user, to calculate their contribution to exposure and to apply this approach recursively to processes and streams next closer to the end-user until the exposure value applicable to the end-user is derived.

(c) Inspection. The exposure metric can be derived by simple inspection of the well-defined Boolean expression and the well-defined process definitions. The selection of the process for the generation of quantitative results is on the basis of "simplest approach, achieving fit-for-purpose". Initial estimates of the numbers of processes and streams involved, and the complexity of the configurations, suggest that the (c) approach is practical and can be shown to yield correct results.

6.2.2 Representation and verification of analysis results

Different descriptions of the exemplar systems appear in three places: Chapter 5 establishes that the exemplar process is representative of processes used in typical cities of the 200,000–500,000 population range selected, and identifies major subsystems, dependencies, design redundancies used in actual systems and example boundaries. Chapter 6 describes the subsystems carefully. In the results
appendix (Appendix B), each process and each stream associated with each subsystem are identified, and the logical relationships (logical gates) that describe the system configuration are defined. The exposure values derived in the spreadsheet are then presented in Chapter 6. The use of a consistent set of subsystems between Chapter 5, Chapter 6 and Appendix B make it less likely that key items are omitted or incorrectly accounted for. The process therefore gives a good level of assurance that the final derived values do represent the described and verified example.

6.3 Analysis of examples

Having described the example systems and confirmed that they are representative of real systems and established example boundaries, the exemplar systems and common subsystems are defined in Appendix B. The analyses of the common subsystems and the exemplar systems are reported in this section.

6.3.1 Analysis of contributory systems

This analysis is of the exemplar common subsystems, as described in Section 5.3 of this thesis that contribute to various combinations of example studies. The analysis is undertaken separately to ensure the consistency of treatment across examples. The subsystems to be evaluated are internet communications and financial transactions. Power supply, road transport and potable water supply are treated separately within each example.

**Internet communications.** The basic systems of the internet are responsible for an increasing proportion of total data transmission; this includes not only www page requests and email but also much of the traffic associated with phone calls and financial transactions; these include the software TCP/IP protocols that are used to disassemble and reassemble files from the local and T1 packet routing protocols, and the less visible but equally essential systems associated with domain name servers and border gateway protocols.

Although the internet is designed to be able to survive multiple link failures, several factors have resulted in a situation where a relatively small number of very-high-capacity transmission media actually carry a huge proportion of the total data traffic, and a relatively small number of high-capacity routers, with associated routetable updating mechanisms, are responsible for a very large proportion of the total
internet traffic. What was a highly distributed network of connections, each having approximately equal capacity, has been refined by market pressures into a system in which a very few linkages actually have the capacity for the imposed traffic — although other paths for data may exist, they may be totally incapable of handling the traffic if the main linkage became unavailable.

<table>
<thead>
<tr>
<th>Technological contributor</th>
<th>Exposure contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legend:</strong> E₁ is the number of single proc/stream failure exposure. E₂ is the duel proc/stream exposure (excluding E₁’s), E₃ is the triple proc/stream exposure (excluding E₁’s and E₂’s).</td>
<td></td>
</tr>
<tr>
<td>Household router exchanges packets via the simple telephone system's copper wires to the roadside DSLAM system that commonly serves a city suburb.</td>
<td>2 0 0</td>
</tr>
<tr>
<td>The roadside DSLAM facility multiplexes the packets exchanged with the complete suburb's internet connections, and exchanges these with the ISP's point of presence, which is commonly located in a telephone exchange building serving a city.</td>
<td>2 1 0</td>
</tr>
<tr>
<td>The ISP’s point of presence is also a &quot;peering point&quot;, connecting to other national &quot;peering points&quot;. The ISP’s point of presence exchanges packets with other national peering points, allowing full internet connections.</td>
<td>5 3 0</td>
</tr>
<tr>
<td>File transferred from network access point to peering point.</td>
<td>3 2 0</td>
</tr>
<tr>
<td>Data transfer via undersea cable. For offshore connections, ISP’s purchase bandwidth from organisations that provide and service undersea cables, and packets are forwarded from the peering point, via undersea cable, to the offshore equivalent of the peering point.</td>
<td>1 7 0</td>
</tr>
<tr>
<td>At the distant end, a mirror image process leads to the exchange of packets to the distant router’s termination point.</td>
<td>12 6 0</td>
</tr>
<tr>
<td><strong>TOTALS (not summed, because various examples use different sections of this standardised system)</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Table 8: Internet subsystems and exposure*
Financial transactions. EFTPOS transaction systems are ubiquitous in New Zealand; few people carry cash and there are cases, such as the Huntly library in the Waikato (2016), where cash is no longer accepted (this issue is in dispute).

<table>
<thead>
<tr>
<th>Technological contributor</th>
<th>Exposure contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legend: $E_1$ is the number of single proc/stream failure exposure. $E_2$ is the duel proc/stream exposure (excluding $E_1$’s), $E_3$ is the triple proc/stream exposure (excluding $E_1$’s and $E_2$’s).</td>
<td>$E_1$ $E_2$ $E_3$</td>
</tr>
<tr>
<td>The EFTPOS terminal, which fulfils a similar function to a domestic router, obtains a merchant-to-user transaction request and ensures the security protocols for the communication of packets.</td>
<td>3 0 0</td>
</tr>
<tr>
<td>Communications from EFTPOS terminal to acquirer bank.</td>
<td>12 6 0</td>
</tr>
<tr>
<td>The accept message to the EFTPOS terminal will originate from the acquirer bank. The acquirer bank will issue the accept message once the user’s bank has accepted the transfer of funds to the acquirer’s bank and it has queued the transfer of funds to the merchant’s bank.</td>
<td>8 0 1</td>
</tr>
<tr>
<td>Communications acquirer bank to user’s bank.</td>
<td>12 6 0</td>
</tr>
<tr>
<td>The user’s bank will confirm the transfer of funds to the acquirer’s bank once it has confirmed that the EFTPOS transfer request refers to an account whose user has accepted the bank conditions, i.e. is valid, and has sufficient credit.</td>
<td>7 0 0</td>
</tr>
<tr>
<td>Communications acquirer bank to merchant bank.</td>
<td>0 0 0</td>
</tr>
<tr>
<td>The acquirer bank will confirm the queuing of the transfer of funds to the merchant’s bank once it has confirmation from the merchant’s bank that the merchant has accepted the bank terms and has a valid account.</td>
<td>7 0 0</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td><strong>49 12 1</strong></td>
</tr>
</tbody>
</table>

Table 9: EFTPOS subsystems and exposure

6.3.2 Analysis of example study #1: sewage system

The definition and analysis of the sewage system supplied to the apartment user shows that the system can be considered in three sections: those closely associated with the user and the apartment, the sewage pipework system and the treatment plant.
**Technological contributor**

Legend: $E_1$ is the number of single proc/stream failure exposure. $E_2$ is the duel proc/stream exposure (excluding $E_1$'s), $E_3$ is the triple proc/stream exposure (excluding $E_1$'s and $E_2$'s).

<table>
<thead>
<tr>
<th>Exposure contribution</th>
<th>$E_1$</th>
<th>$E_2$</th>
<th>$E_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apartment systems</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>The sewage pipework and pumping system</td>
<td>6</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>The sewage treatment plant</td>
<td>18</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Cogeneration system</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Final disposal</td>
<td>6</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td><strong>34</strong></td>
<td><strong>4</strong></td>
<td><strong>6</strong></td>
</tr>
</tbody>
</table>

*Table 10: Sewage example subsystems and exposure*

Whether the definition of the service includes a requirement for environmentally acceptable discharge will have a major effect on the exposure values. If the definition of service allows the dumping of untreated sewage into waterways, then the defined service is not affected by the availability of the sewage treatment system. As skilled operators are required for sewage treatment plants, they contribute to the exposure of these systems. Multiple vehicles and personnel are considered to be capable of the transport of bio-solids; thus, this is assessed to contribute only to exposures of higher order than $E_3$. The local road system is required for the disposal of dewatered solids; however, as it is reasonable to assume that multiple routes are
available to trucks, this is considered to be a contribution to an “E” value higher than $E_3$.

The combined metric is analysed as $\{34, 4, 6\}$. The largest numerical contributor to the evaluated “E” value is actually from the multi-stage process required by the sewage treatment plant; this contribution is very closely associated with the definition of the “service”, which stipulates “environmentally acceptable discharge”. The pipework system from the user to the treatment plant makes a significant contribution to the total exposure, because there is a need to account for the length of the pipe sections. The significance of this issue has been demonstrated by the experiences of Christchurch, following the 2011 earthquakes. Sewage disposal is dependent on a power supply, which is local to the user, for a booster pump and on a power supply for the treatment plant. The treatment plant power supply is more significant and hence more difficult to substitute, but the necessity is linked to the requirement for an environmentally acceptable discharge quality. As the end-user payment for sewage removal services is via quarterly municipal “rates” bills, an electronic financial transaction system is not a contributor to the end-user’s exposure in this case. Road system and power supply requirements are in common with other examples; however, the absence of an immediate need for a financial transaction service is noteworthy.

**Summary.** This analysis of the exposure of the technology chain evaluates the vulnerability that it imposes on the end-use. Specifically, this analysis shows that, as for many services, the contribution of services close to the end-user is noteworthy. In this case, the gravity-fed pipework system from the user to the pumping station represents a significant vulnerability for the end-user, a conclusion that is validated by the experience of Christchurch citizens after the 2011 earthquake. The major contributor to the numerical exposure is the multiple sequential stages of treatment that are needed to transform the sewage into streams that can be discharged without environmental damage.

### 6.3.3 Independent risk analysis of sewage system

An independent consultant was tasked with carrying out a risk analysis of a sewage system. The scoping of the study was aligned with the example study, and the results are included in Appendix A. The risk analysis failed to identify significant
points of exposure that are identified as a result of the analysis in Section 6.3.2. It is possible that these unidentified exposure points were considered by the consultant to have a low risk of hazard; however, the value of that assumption is shown to be limited.

6.3.4 Analysis of example study #2: collaboratively developed work information

This example study can be considered to be two local operations and an internet connection. The operations local to both of the end-users contribute, as might be expected, significantly to the $E_1$ value. Contributors include the power supply to two computers and routers, data wiring via the telephone system, normally referred to as the “plain old telephone system” (POTS), and to the two local internet points of presence and the power supply wiring to the local substation. The internet system is considered separately, as a standard subsystem.

<table>
<thead>
<tr>
<th>Technological contributor</th>
<th>Exposure contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$E_1$</td>
</tr>
<tr>
<td><strong>Local end-user functions</strong></td>
<td></td>
</tr>
<tr>
<td>The local end-user components and inputs include a functional local PC (considered to be a single hardware unit), a local PC power supply (which includes local and household wiring as contributors to the $E_1$ value), a local substation transformer that contributes 1 to an $E_2$ exposure and an assessed contributor to the $E_3$ value from the national grid power supply. In addition to the PC hardware, the local PC operating system, email client software and file display software (spreadsheet) are considered to contribute separately to the $E_1$ value, because each can be targeted independently of each other and independently of the PC hardware.</td>
<td>6</td>
</tr>
<tr>
<td><strong>Data communications</strong></td>
<td></td>
</tr>
<tr>
<td>This is the internet communication subsystem – from local router to remote personal router.</td>
<td>25</td>
</tr>
<tr>
<td><strong>Remote user systems</strong></td>
<td></td>
</tr>
<tr>
<td>The remote user components and inputs are essentially identical (in terms of their contributions to exposure) to those of the end-user.</td>
<td>7</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td>38</td>
</tr>
</tbody>
</table>

*Table 11: Work information example subsystems and exposure*
In considering the granularity of the analysis, it is noted that, for most current PCs, as both the operating system and the applications are in volatile storage and can be “attacked” separately, both contribute to the $E_1$ value. The internet connection that is sandwiched between the two users generates a significant contribution to the higher $E$ values, arising from the multiple parallel transmission paths of T3 and T1 carriers. This is true for the representative example; however, there are certainly real cases where the level of redundancy is nil. In 2011, an old lady cut off Albania’s internet connection with her shovel, while scavenging for copper. Local routers are powered from the household 230 VAC power supplies and, as representative examples do not have uninterruptible power supplies (UPS), the household power supply contributes to system exposure even when the PC has a significant battery life. The ubiquity of the internet system for data transfer needs to be noted; also, although a representative configuration (i.e. an exposure value) can be defended, actual situations can differ. At a public meeting to discuss disaster preparedness in a small New Zealand town, locals expressed confidence that they had cell phones, landline phones and internet communications – and then found that all of these services were carried on a single fibre-optic cable.

In another age, the person generating the data (the topic of this example) would have posted a hard copy to a colleague. That approach actually incorporated many $E_1$ values, and generates interesting comparisons with the internet. A letter that has been destroyed cannot be recreated, whereas a corrupted data packet can be resent until an ACK advises that the received message checksums are valid, and hence error-free transmission has occurred.

### 6.3.5 Analysis of example study #3: local fuel supply

For the common case of an individual motorist seeking to refuel a vehicle, a local distribution centre, i.e. a petrol station, retails a bulk commodity. The commodity (petrol) is created in a centralised facility (refinery) and is distributed via a nationwide supply chain.
**Technological contributor**

Legend: $E_1$ is the number of single proc/stream failure exposure. $E_2$ is the duel proc/stream exposure (excluding $E_1$’s). $E_3$ is the triple proc/stream exposure (excluding $E_1$’s and $E_2$’s).

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Exposure contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$E_1$</td>
</tr>
<tr>
<td><strong>Petrol station pumping system</strong></td>
<td></td>
</tr>
<tr>
<td>The system that pumps petrol from the</td>
<td></td>
</tr>
<tr>
<td>underground storage tanks to the client’s vehicle.</td>
<td>5</td>
</tr>
<tr>
<td>For the defined example, a skilled</td>
<td></td>
</tr>
<tr>
<td>operator is required.</td>
<td></td>
</tr>
<tr>
<td><strong>Pump control and metering system</strong></td>
<td></td>
</tr>
<tr>
<td>A control signal is required to operate</td>
<td></td>
</tr>
<tr>
<td>the pumps (on/off) and a metering</td>
<td></td>
</tr>
<tr>
<td>system is required to tally the</td>
<td></td>
</tr>
<tr>
<td>quantity of fuel dispensed.</td>
<td>7</td>
</tr>
<tr>
<td><strong>Petrol station staff facilities</strong></td>
<td></td>
</tr>
<tr>
<td>A staffed station requires water,</td>
<td></td>
</tr>
<tr>
<td>sewage and power (required also for</td>
<td></td>
</tr>
<tr>
<td>other systems).</td>
<td>36</td>
</tr>
<tr>
<td><strong>Petrol station transactions</strong></td>
<td></td>
</tr>
<tr>
<td>EFTPOS financial transaction required.</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>12</td>
</tr>
<tr>
<td><strong>National bulk supply chain</strong></td>
<td></td>
</tr>
<tr>
<td>Fuel is distributed nationally using</td>
<td></td>
</tr>
<tr>
<td>road tankers; these require vehicles,</td>
<td></td>
</tr>
<tr>
<td>fuel, drivers and roadways, all of</td>
<td></td>
</tr>
<tr>
<td>which contribute.</td>
<td>1</td>
</tr>
<tr>
<td><strong>Production of fuel</strong></td>
<td></td>
</tr>
<tr>
<td>In New Zealand, there is a single</td>
<td></td>
</tr>
<tr>
<td>refinery, which accepts crude oil and</td>
<td></td>
</tr>
<tr>
<td>distills ISO standard petrol. There are</td>
<td></td>
</tr>
<tr>
<td>also multiple points at which refined</td>
<td></td>
</tr>
<tr>
<td>petrol can be imported, and cross-</td>
<td></td>
</tr>
<tr>
<td>availability agreements between</td>
<td></td>
</tr>
<tr>
<td>companies who retain stocks.</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td>98</td>
</tr>
</tbody>
</table>

*Table 12: Local fuel supply example subsystems and exposure*

The systems at the forecourt make a significant contribution to the total exposure; it is useful to note that metering and control systems for pumps contribute as well as the actual pumps. The financial transaction (EFTPOS and banking) system actually affects all examples that rely on a retailer-to-consumer transaction, and is a major contributor to $E$ values. Road transport uses vehicles that are commonly available, and hence actually contributes little to the higher exposure values. A manned petrol station has been selected for the example; the station cannot be operated without staff present, and this incurs the vulnerability to the end-user of a petrol station that is inoperable because staff facilities (sewage disposal, provision of water and light) are unavailable. These facilities make a major contribution to the exposure that the complete system incurs for the end-user.

**Summary.** This analysis of the exposure of the technology chain evaluates the vulnerability that it imposes on the end-use. Specifically, this analysis shows that,
despite the statistical reliability of the internet, the end-user is vulnerable to the non-availability of internet services, which includes not only the common subsystem that has been defined but also the domestic router, the power supply and the PC operating system and drivers. Non-availability is noted as involving not only technological failures but also technological effects such as surveillance, which may make the internet effectively unavailable to some users. This example considers the user’s capability to view a file, and this incurs a vulnerability associated with file format capability.

6.3.6 Analysis of example study #4: targeted first-aid

The technological system associated with this end-user need is actually very similar to the “work information” example. In both cases, basic PC and internet access technologies that are used directly by the end-user, who in this case is the first-aider, contribute to the \( E_1 \) values. The internet communications system itself is a significant contributor to both the \( E_1 \) values and the higher \( E \) values; this topic has been covered in detail elsewhere.

<table>
<thead>
<tr>
<th>Technology contributor</th>
<th>Exposure contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legend:</strong> ( E_1 ) is the number of single proc/stream failure exposure. ( E_2 ) is the duel proc/stream exposure (excluding ( E_1 )'s), ( E_3 ) is the triple proc/stream exposure (excluding ( E_1 )'s and ( E_2 )'s).</td>
<td>( E_1 )</td>
</tr>
<tr>
<td><strong>Local end-user functions</strong></td>
<td></td>
</tr>
<tr>
<td>The local end-user components and inputs include a local PC and power supply, which includes local and household wiring as contributors to the ( E_1 ) value, a local substation that contributes to ( E_2 ) and ( E_3 ) values. The local PC operating system and the software contribute separately to the ( E_1 ) value, because each can be targeted independently.</td>
<td>5</td>
</tr>
<tr>
<td><strong>Internet communications</strong></td>
<td></td>
</tr>
<tr>
<td>In the way that the example is constructed, this requires the use of a complete internet communications system.</td>
<td>13</td>
</tr>
<tr>
<td><strong>Selected static response</strong></td>
<td></td>
</tr>
<tr>
<td>At the remote “end”, this application reaches a different situation from the “work” example: the input can, is simply a case of identifying the correct diagnosis and presenting the response.</td>
<td>5</td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>23</td>
</tr>
</tbody>
</table>

Table 13: First-aid example subsystems and exposure

A significant difference between this example and the work information example is that the information required by the end-user in this case is relatively static.
If the “Heimlich manoeuvre” can be identified as the information required, then a static information source is quite adequate – nothing needs to be generated in real time at the “end” of the technology chain that is furthest from the end-user.

As with the “work information” example, the exposure generated by the internet data transmission hardware and protocols is a major contributor to this example. The home PC “subsystem” is also a subsystem that contributes, but to a lesser extent.

At the “far end”, i.e. the end furthest from the user, more than one option for the identification of a diagnosis and for the provision of the first-aid information could have been assumed with approximately equal validity. A human physician, for example, and an emergency department specialist, could interact with the end-user, or an expert system shell could be used to refine the diagnosis and provide advice.

Summary. This analysis of the exposure of the technology chain evaluates the vulnerability that it imposes on the end-use. Because the example proposes an internet-mediated communication, the analysis shows that the end-user is vulnerable to non-availability of the internet. The user, i.e. the first-aider, is also vulnerable to a failure of the consultant system, whether human or artificial, that generates the diagnosis and recommends treatment.

6.3.7 Analysis of example study #5: perishable food

This is an example where exposure is spread throughout a technological system, with major local contributions from only the financial transaction system and local power supplies. As the “service” is defined in terms of the product in the end-user’s refrigerator, contributors to exposure include the apartment power supply and access to the apartment.
<table>
<thead>
<tr>
<th>Technological contributor</th>
<th>Exposure contribution</th>
<th>E1</th>
<th>E2</th>
<th>E3</th>
</tr>
</thead>
<tbody>
<tr>
<td>User storage</td>
<td></td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>The example also assumes that the user can store the milk in a refrigerator that requires power.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User transport</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Processes associated with transport of consumer quantities of fresh milk to individual user’s premises make a limited contribution to the end-user’s exposure as the example assumes use of the user’s own transport.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retail transaction</td>
<td></td>
<td>49</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>The purchase of the fresh milk in consumer quantities from the retailer requires the full EFTPOS system, which is treated as a subsystem and contributes to the exposure of the end-user.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retailer system</td>
<td></td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>The retailer requires power, stock checking and refrigeration systems, which contribute.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retailer staff facilities</td>
<td></td>
<td>35</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>The retail outlet, described in the example, is unworkable without staff, and is therefore unworkable without staff facilities. Potable water has been assessed to have only a low exposure (E₁ = 1); however, the sewage system, as previously analysed, makes a very significant contribution to the total exposure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk transport to local retail facility</td>
<td></td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>The transport to the retailer contributes little to the exposure down to E₃ levels because there are very many transport alternatives.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raw milk processing</td>
<td></td>
<td>22</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Processing phase – from reception of the raw milk to the generation of the processed, quality-controlled and packaged milk product in a form that can achieve a stated shelf life requires testing to confirm quality and payment basis, pasteurisation and standardisation. The example shows that a representative processing plant packages the standardised and pasteurised milk into consumer packs for dispatch to retailer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raw milk collection system</td>
<td></td>
<td>13</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>The supply of raw milk to the processing centre involves a very large number of farms and a significant number of bulk transport options. None contribute to exposure levels in the E₁, E₂ or E₃ levels, these are not considered in this analysis. The metering testing and billing systems do contribute.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTALS</td>
<td></td>
<td>128</td>
<td>22</td>
<td>12</td>
</tr>
</tbody>
</table>

*Table 14: Fresh food example subsystems and exposure*
As there are very many farms, the supply of raw milk contributes to an “E” value higher than 3. Similarly, there are enough alternative road routes, tankers and drivers to ensure that no contribution to “E” values below $E_3$ are made by these processes and streams. For the representative example, it is assumed that, although there may be more than three processing facilities in a country, as supply chains are assumed to be regional, these facilities are deemed to contribute to $E_2$ values. As one of the essential input streams, for which not adequate storage technology exists, electrical power remains a contributor to the exposure of this technological system, and, although the national grid is likely to have many generators and significant transmission line redundancy, local power supply options commonly do not include those levels of design redundancy. Power is used at more than one point, even though distinctly different power sources and distribution systems are involved, and therefore these add separately to the exposure. As with all systems involving end-user purchase, the financial transaction system (EFTPOS) contributes a large exposure to the end-user. As with other examples, staff with particular skills are essential; if unskilled staff can carry out tasks with the help of instructional material, this significantly decreases the exposure to a lack of skilled staff; a fully automated retail facility or delivery system would also reduce the exposure offered by the retail facility. Staff facilities, and particularly sewage disposal systems, contribute significantly.

**Summary.** This analysis of the exposure of the technology chain evaluates the vulnerability that it imposes on the end-use. Specifically, this analysis shows that the end-user is vulnerable to the failure of the financial transaction system (EFTPOS) that has been used for the example, and this system, in turn, is vulnerable to failures of the internet communications system. As noted previously, non-availability can result either from a direct technological failure or from a technologically incurred feature such as surveillance capability, which renders the system effectively unavailable to the user. For a short-shelf-life product, dependence on a single centralised processing facility incurs vulnerability for the end-user. Transport systems have high levels of design redundancy and therefore incur minimal vulnerability. In addition to the vulnerabilities associated with the transactional facility, the retail facility’s dependence on staff, and hence staff facilities, incurs significant vulnerabilities for the end-user.
6.3.8 Analysis of example study #6: essential specific medicine

The supply of an essential specific medicine is a complex process. The technological system that places an MDI in a user's hands involves a local retail and regulatory system, a distribution supply chain and a multi-component manufacture and packaging system.

<table>
<thead>
<tr>
<th>Technological contributor</th>
<th>Exposure contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User acquisition of MDI: financial transaction</strong></td>
<td>49 12 5</td>
</tr>
<tr>
<td>The delivery, into the user’s hands, of a filled and functional Ventolin™ MDI is the end-point of this subsystem and the service level assigned for this example. For Australia and New Zealand, as part charges on medication such as Ventolin™ MDIs are levied, a financial transaction is required.</td>
<td></td>
</tr>
<tr>
<td><strong>User acquisition of MDI: prescribing permission</strong></td>
<td>0 0 1</td>
</tr>
<tr>
<td>MDIs are acquired from pharmacies, which acquire wholesale stock and require a prescription from a medical practitioner as a prerequisite for dispensing.</td>
<td></td>
</tr>
<tr>
<td><strong>MDI filling, packaging and distribution</strong></td>
<td>4 1 1</td>
</tr>
<tr>
<td>Following manufacture and distribution of MDI parts, the canisters are filled with the propellant and the active ingredient, and the metering chamber with metering valve is assembled and sealed to the canister. The completed unit is labelled and packaged, and the individually packaged MDIs are distributed in bulk packs.</td>
<td></td>
</tr>
<tr>
<td><strong>MDI: manufacture of container and distribution</strong></td>
<td>1 2 2</td>
</tr>
<tr>
<td>The design of MDIs has become reasonably standardised, and manufacture requires deep drawing of the canister and the metering chamber and the retaining cap from aluminium strip-stock, and the CNC machining of the hollow metering valve system. Near-identical MDI designs and a moderate number of manufacturing plants exist.</td>
<td></td>
</tr>
<tr>
<td><strong>MDI active ingredient – distribution</strong></td>
<td>0 0 0</td>
</tr>
<tr>
<td>Trackable distribution chain for sterile, diluted active ingredient.</td>
<td></td>
</tr>
<tr>
<td><strong>MDI active ingredient – synthesis, testing and dilution</strong></td>
<td>4 0 1</td>
</tr>
<tr>
<td>A &quot;six-step&quot; salbutamol synthesis process has become common. This uses commonly available chemical feedstocks and has a good yield. The purified salbutamol is distributed in standardised concentrations for packaging.</td>
<td></td>
</tr>
<tr>
<td><strong>TOTALS</strong></td>
<td>58 15 10</td>
</tr>
</tbody>
</table>

Table 15: Essential medicine example subsystems and exposure
The aluminium strip, from which the MDI bodies are formed, is considered to be available from very many sources, and to contribute to “E” values higher than $E_3$. Although there are alternative suppliers for the completed inhalers, in practice only a single branded type is available in most pharmacies; therefore, it seems to be reasonable to consider the production process. As with many other examples, the processes closest to the end-user contribute significantly to the end-user’s exposure.

It is noteworthy that, although the MDI has become the most common method of administration, salbutamol can be effectively administered either via nebuliser or by intravenous injection: The vast majority of the contribution to the exposure value is associated with the manufacture, filling and distribution of the MDI, rather than the creation of the active ingredient or the dilution of the active ingredient into a form that can potentially be administered. If the active ingredient were available to the user, there is little technological reason why the basic user requirement could not be met with a much lower level of exposure. Some countries do have completely free health services, but most, including New Zealand, require a contribution from the end-user which, as a reasonable representation of reality, requires the involvement of the EFTPOS financial system; this system, plus the associated internet data transfer mechanism, is a significant contributor to the end-user’s total exposure.

**Summary.** This analysis of the exposure of the technology chain evaluates the vulnerability that it imposes on the end-use. For this example, analysis shows that the end-user is vulnerable to the availability of the financial transaction system, which in turn is vulnerable to the availability of the internet system. As noted previously, the transport system has high levels of design redundancy and therefore incurs little vulnerability. The manufacture of the MDI canister also incurs limited vulnerability, but the local filling operations do incur notable vulnerability and the centralised synthesis of the active ingredient also incurs significant vulnerability.

### 6.4 Application of theoretical basis to other examples

#### 6.4.1 Application to homogeneous system examples

A single, completely hypothetical example of a homogenous system will be analysed for weaknesses (exposure points). This analysis would be expected only to confirm that the analysis of exposure points replicates similar analyses made using
graph theory approaches. This analysis would also serve to demonstrate how the proposed analysis of the exposure level can contribute insights in addition to those available from graph theory approaches.

6.4.2 Analysis of the dynamic system (newspaper vendor)

Assumptions made in the study are as follows. (a) There is no technological reason, only a profit maximisation reason, why the newspaper vendor cannot order sufficient papers; there is assumed to be no limit to either the printery capacity or the vendor’s purchasing capacity. (b) There is no interchange of stock amongst vendors during the day – if that were possible, the process description would include a range of "OR" gates to illustrate the fact that a vendor could have multiple potential suppliers of stock, and, assuming good communication and logistics, there would effectively be only a trivial problem remaining. (c) The vendor’s ability to purchase "sufficient" papers is not constrained by the vendor’s financial capability. (d) Each purchaser has the financial means to purchase a newspaper.

The model for analysis, then reduces to:

(a) The purchaser is assumed to be at a location used for retail sales by the vendor.
(b) The purchaser carries out a minor financial transaction to purchase the newspaper.
(c) The vendor has transported himself or herself to the normal sales location, carrying stock
(d) The vendor has completed a financial transaction with the newspaper supplier for the purchase of stock.

The exposure metric is shown to be \(4, 0, 0\). The \(E_1\) value (4) reflects the possible failure of the input stream, i.e. papers from the newspaper producer, failure of fuel or road to allow transport from the point of bulk supply purchase to the point of sale and non-availability of the newspaper vendor. As the model relates to a single vendor, selling a single product that is sourced from a single point, there are no contributors to \(E_2\) or \(E_3\) values, i.e. there are no combinations of two or three failures, where neither failure alone would cause output failure that would cause a service failure.
The whole newspaper vendor “problem” is an operational research problem of optimising a variable (profit) under conditions of uncertain demand and fixed supply cost – a semi-dynamic effect. If the vendor could download an electronic copy of the paper, a local printer could generate papers as required, paying the printery only the royalty for each copy sold. Such a change would eliminate the problem of predicting demand but this technological change would introduce the technological vulnerabilities of the printing process, including the availability of power, paper and communications to the newspaper file supplier. It is unclear whether the change would actually decrease the exposure of the end-user.

Assuming that only cash transactions are possible, the newspaper vendor is one of the examples that has the lowest technological exposure of all of the example studies, and it is difficult to develop a technological solution that has lower exposure. The example almost epitomises a case where the end-user is minimally vulnerable to technological failures.

6.5 Conclusions

This chapter has summarised and interpreted the findings from the analysis and review of the initial examples. This chapter has also summarised and interpreted the findings from the analysis of the homogeneous system example and from the “risk analysis” of the selected example studies. The detailed analysis has revealed subsystems that contribute to more than one example, but are not common across all examples. The examples have identified themes and issues that are common across all examples, to various extents, allowing both generalised conclusions and a claim that the conclusions can reasonably be further generalised.

The examples, as initially defined, have included a range of measures that have already reduced exposure. The use of shipping containers has allowed standardised handling equipment and the use of protection equipment has allowed effective design redundancy in national power supply grids. The use of standardised motor fuel specifications and standardised container road transport has allowed large levels of effective transport redundancy to be achieved. Although the examples are historical, it should be noted that almost all basic engineering standards, e.g. TEFC motors, metric-standard nuts and bolts, fuel specifications, materials specifications,
ISO OSI data specifications and open document format specifications, contribute significantly to the reduction in vulnerability of engineering equipment.

This analysis and the summary have answered RQ(a): “For goods or services delivered to end-users, what measure of vulnerability can be attributed to the technological systems that are currently used?”

6.5.1 Limitations

The analyses have illuminated several difficulties with the actual determination of exposure; these issues are worthy of comment. In particular, it has been found that it is important to establish a reasonable granularity for systems such as a long sewage pipe. Simplistically, such a pipe would contribute a "1" the end-user's $E_1$ value. Such a conclusion fails to recognise that sections of the pipe can fail independently of other sections, and thus can be considered to be separate weaknesses. A reasonable assessment of granularity has therefore been applied, assigning cumulative $E_1$ contributions to defined lengths of collection pipework. Similarly, it is important to establish a reasonable granularity for such items as a PC, which may contain billions of transistors, yet only a few simple and easily replaceable major components, and simple but large industrial equipment such as a trickle filter for sewage. The criteria proposed in Section 5.2.2 have been adopted.

The analysis has asserted that some streams, including power from the national grid, international shipping and the road network, commonly have more than three independent sources and hence can be considered to be unconditionally available. These assertions are justified, in detail, within the analysis of the specific examples, although exceptions occur in real systems where, for example, a community is served by a single road and a single power feeder.

The analyses have identified that issues of practical availability frequently exist; these commonly involve situations in which a user can access a service only by agreeing to specific contractual conditions. These situations need to be correctly identified as contributors to the $E_1$ exposure value.

6.5.2 Specific conclusions for initial examples

This section summarises the analyses of each of the examples studied, drawing attention to significant issues arising from the analysis.
**Sewage system.** Although the major contributor to exposure is the sewage treatment plant, it is notable that this exposure is predicated on the definition of the service, viz. the environmentally acceptable treatment of sewage. Had the service been defined as "the removal of sewage from the apartment", then the existence of bypasses for various stages of sewage treatment would have indicated a much lower total exposure. The treatment actually applied to the sewage is not complex, but economies of scale have led to the use of a single, centralised treatment plant.

The second largest contributor to end-user exposure is the pipework leading from the apartment to the treatment plant and particularly the gravity-fed pipework leading to the first pumping station. Following the 2011 Christchurch earthquakes, multiple disruptions of sewage pipework were a source of considerable difficulty, and cost estimates for repair were enormous. Sewage holding tanks for individual dwellings are used in semi-rural locations, but are not commonly used for urban locations or apartments; hence, the sewage collection pipework is a single point of exposure. Similarly, there is some degree of holding capacity in the settlement ponds and trickle filter tanks of the sewage treatment plant, perhaps sufficient to allow the replacement of small motors, but the holding capacity is not large. Power supply is essential to both the pumping stations and the operation of the sewage treatment plant; some plants use methane from anaerobic digestion of sewage to operate a cogeneration plant and provide power locally — although common, this was not considered to be sufficiently representative as to be included in the example definition. Loss of power supplied from the grid is therefore still considered to contribute to the exposure of the complete system. Although both are ultimately supplied from the national grid, the geographical separation makes it reasonable to expect that the pumping station supply and the sewage treatment plant supply will be sourced from separate substations and will certainly use separate low voltage feeders.

**Work information.** As would be expected, the internet communications system is the largest contributor to the system’s exposure, and it should be noted that, although the internet was originally proposed to have large design redundancy, the pressures to achieve economies of scale have resulted in increased dependence on fewer and faster communications links; this dependence has increased the levels of exposure. For individuals, access to the internet is via a commercial agreement with an ISP, raising the possibility that access will be practically unavailable if commercial
terms, e.g. re privacy of communications, are unacceptable to the user. This issue is also relevant for ISPs seeking access to international carriers. The user’s PC, operating system, applications and power supply also contribute to the user’s vulnerability and these contributors can be reduced, as indicated in Chapter 7 of this thesis.

**Fuel.** As most petrol stations have more than four pumps, the petrol station pumping equipment is massively duplicated and therefore does not actually contribute to the end-user’s vulnerability at the $E_3$ level. The largest contribution in this example is from the EFTPOS transaction requirement and the second largest is from the services required to allow staff to operate the petrol station. In defining the example, it was recognised that automated stations exist and require no staff, and that limited facilities for automated cash payments exist; however, it was argued that the staffed station using EFTPOS was representative of very many actual stations. The exposure contributed by the EFTPOS system arises not only from the communications requirements but also from an acknowledgement that such a transaction requires several parties to enter commercial agreements that potentially are unacceptable to them, and are therefore potential sources of practical unavailability. The staff facilities, and particularly the provision of sewage disposal and power, are sources of exposure and hence end-user vulnerability, but there is no real need to consider these as a source of a “feedback loop”.

**First-aid.** The details of the proposed system have been justified as representative; however, other possible approaches to providing this particular service could be considered to be equally representative. Under the described system, the contributors to exposure are moderately similar to those for the work information example, except for two important distinctions: (a) an automated search facility rather than another user are at the remote end of the communications system; (b) as the information supplied is static, i.e. generally will not change over a reasonable period of time, only a lookup system rather than an interactive system, as for the work information example, is required. This example requires care to describe the "user" as the person seeking the diagnosis and remedy, and to distinguish this person from the victim of the choking.

**Perishable food.** The fresh food example is distinguished by the need to centrally process a short-shelf-life material (fresh milk), and to then package,
distribute and retail the treated product. As the raw material is accumulated from a large number of farms, the actual raw material supply does not contribute significantly to exposure at the $E_3$ level, but the impracticality of long-distance transport and storage means that the processing plant does contribute to exposure, and the legal necessities of pasteurisation do not allow the processing plant to be bypassed. Pasteurisation, standardisation of protein and fat levels, and testing require close process control, which increase the economies of scale available from a centralised plant. The retail (EFTPOS) financial transaction necessities, and the retail staff facility necessities are similar to those for the petrol station example and contribute significantly to the end-user's exposure. As there are many transport options for raw material supply and for the distribution of wholesale products, these do not contribute significantly to the end-user's vulnerability.

**Essential medicine.** Although, the chemical nature of the salbutamol molecule and the preferred method of synthesis are public knowledge, production of the purified and tested salbutamol is typically highly centralised. This centralisation is driven partly by economics of scale and partly by quality assurance requirements. The design of the MDI canisters is patented and thus public knowledge – and the processes are standard metal production processes (deep-drawing, machining and crimping). Both the active ingredients (salbutamol, dilutant and propellant) and the MDI canister are high-value, long-life and low-volume items, and hence are readily amenable to stockpiling. Perhaps surprisingly, therefore, the major contribution to the end-user vulnerability is that associated with the final EFTPOS purchase transaction. Although it is recognised that cash transactions are possible, the EFTPOS transaction was justified as being representative in the example definitions. For a typical user, the medical practitioner permission, i.e. the legal requirements for access to prescription medicines, also contributes to the user's exposure.

### 6.5.3 Analysis of relative total exposure of actual examples

The total exposure of the analysed examples has been shown to be heavily influenced by the precise nature of the scope boundaries and the assumptions incorporated into the design of the examples. An objective of the thesis was to allow effort between infrastructures to be prioritised. An outcome that has perhaps been unexpected has been the highlighting of the need to prioritise effort on some common
subsystems because their effect has tended to overshadow the exposure metrics associated with the more central and obvious aspects of the examples.

6.5.4 Analysis of aspects that recur across examples

A small number of common subsystems have been identified. The exposure contribution of each has been estimated and the values have been added consistently to the examples using these standard subsystems. Some subsystems, notably road transport and power supply, were not included as standard subsystems in the analyses presented in Chapter 5 and the initial sections of Chapter 6. The decision to treat these separately within examples, as opposed to treating them as standard subsystems, was made because, although the subsystem services were common, their delivery varied significantly between examples. Cross-checking between examples has been used to ensure a consistent treatment of subsystems such as road transport and power supply.

6.5.5 Analysis of generalisable features of each example

The examples that have been studied were chosen to illustrate a wide variety of technological systems and were chosen specifically to cover high- and lower-tech subsystems, and situations with offshore and onshore components. Each exemplar system does include aspects that can be generalised, and their identification is valuable. In particular, it can be noted that many of the studies show examples of cases where economic considerations (economies of scale) have progressively led to highly centralised production systems, whose final designs make large contributions to the end-user’s exposure.

**Sewage system.** The treatment of sewage is an example of a collection system, with a single point of processing, with limited options for storage at large scale (as for the fuel example) and with limited options for storage at the user end. The system is distinctive because there are practical, although highly undesirable, options for bypassing the treatment system.

**Work information.** The analysis of the work information example illustrates the need for data formats that are mutually comprehensible by persons at distant ends of a communications system. This example is obviously highly dependent on the
communications system used. The example is generalisable to any field in which two individuals exchange and mutually contribute to some dataset, e.g. a document.

**Fuel.** The fuel supply example is characteristic of a system in which goods are created at a single point and are distributed via a supply chain, with retail facilities for the end-user. Fuel could be considered to be a moderate value item, making significant storage impractical at user premises. As fuel is considered to have strategic value, there is large-scale storage at a national scale. There are standard specifications for fuel, facilitating at least options for local production.

**First-aid.** The "first-aid" example is characterised by the need to access essentially static information (diagnostic and treatment advice) quickly. In the example, the data are held remotely and are accessed via a communications system and a remote data-search facility. In the example, both the communications system and the remote search facility contribute significant exposure. For any case in which static information is needed locally, there is no need for the information to be held remotely; it is entirely possible for reference information to be held locally. This conclusion can be generalised and shown to be applicable to fields including engineering and physics information, agricultural information, food processing information, animal husbandry and more general human and animal diagnostic and treatment information.

**Perishable food.** The fresh milk example is characteristic of many short-shelf-life products, featuring progressive creation and limited options for storage because of the characteristically rapid onset of spoilage combined with a low-value and high-volume, high-throughput product. Short-shelf-life products will generally require frequent retail activity, and hence both transport and the use of cash or EFTPOS systems.

**Essential medicine.** The essential medical supply example, examining the salbutamol MDI supply, is an example of a case in which components, whose makeup is public knowledge and that have a long shelf life, are progressively assembled into a final consumer device. This example can be generalised to cases where long-shelf-life streams are assembled. Stockpiling of intermediate and indeed final products can be designed to exceed maximum expected times to recreate processes. Ventolin™—progressive creation, more than one distribution system and good potential for storage.
7. EFFECT OF HYPOTHETICAL CHANGES TO EXAMPLES

7.1 Introduction

Two approaches will be used in the process of hypothesising changes to the selected examples: (1) each example will be scrutinised for features that are specific to that example and that could be changed; (2) a set of standardised approaches will be considered. The examples that have been studied have been shown to be representative, but have necessarily assumed defined service levels as a requirement for the analysis. The exposure has not been re-estimated for different service levels but, for some examples, such variations are expected to have significant effects on the calculated exposure. As a notable example, if sewage can be discharged without environmental consideration, all of the treatment plant processes can be bypassed and the exposure of the user can be reduced. The examples as described have necessarily included some specific choices and design features. Approaches to decreasing the exposure for some of these features will be described in this section; it could be argued that the analysis process has contributed to highlighting these options. For each example, the hypothetical changes are described and their effects on exposure and hence on the user’s vulnerability are assessed. A summary of changes is provided, noting the type of each hypothesised change and an assessment of the economic and technical effort required and of the magnitude of the effect.

7.2 Common features likely to offer significant reduction of exposure

It is possible to identify several categories of hypothetical change. Examining each such category helps to identify valuable hypothetical changes within the examples.

7.2.1 Local storage

A static analysis of technological systems has been presented, because the weaknesses of technological systems are static. Nevertheless, it is useful to consider the possibility that a local store of some intermediate stream can, within certain criteria, have a similar effect to a configurational change. Two scenarios are examined. Firstly, a cache of an intermediate product can continue to supply that stream to an upstream process until the downstream process is repaired or re-
established. Secondly, a cache of an intermediate product can continue to supply that stream to an upstream process until an alternative source is found, if the normal source fails.

Robertson (2010) considered the relationship between time-to-disaster and time-to-replace or time-to-repair. Figure 11 illustrates the effect of a cache on a system and shows that, if a cache, i.e. a local store of an intermediate stream, is sufficient to allow the repair of a supplying process before the cache is exhausted at the normal usage rate, then the local cache can be considered in the same way as an alternative process, with $E_2$ being equal to 1. If a local stockpile of an intermediate stream is sufficient to allow the implementation of an alternative supplier of the intermediate stream before the store is exhausted at the normal usage rate, then the local cache can be considered in the same way as an externally available stream, with no contribution to $E_1$. This criterion also implies that the supplying system has sufficient over-capacity with which to build up the cache. For cases where local storage cannot practically cover the time required to institute an alternative supply, it may still be valid to mention some qualitative decrease in vulnerability. The household storage of food supplies, water and fuel is highly significant for disaster situations, noting that disaster preparedness plans generally assume a relatively short period until normal supply modes are restored.

Figure 11 Local storage effect
7.2.2 Technological substitution

In many cases, alternative technologies may be substituted for existing technologies; such alternatives may allow significant reductions in exposure. This option is distinguished from the next by referencing only extant technologies. This category is particularly relevant to cases in which a current allocation of costs has resulted in one technology being preferred but not superior in any other way. In the context of this type of technological change, it must be noted that the existence of a durable and public specification for an intermediate stream will significantly promote alternative options for the stream’s supply. As practical availability contributes to exposure, a technological substitution that does not affect exposure to technological failure can reduce the total exposure by eliminating contributors to practical non-availability.

7.2.3 Technological breakthrough

It is reasonable to at least consider the effect upon a particular example’s exposure should a specific technological capability become available. “Become available” could include several categories.

(a) A technological capability that does not currently exist, e.g. a technology capable of the economical storage of MWh of electrical power at household scale. “Flow batteries” exist but are technically immature; pumped hydro is the only technically mature option for the storage of large quantities of power, and is restricted to very specific geographies.

(b) Technology that is immature (in the terms of the NASA technology maturity index (2015)), e.g. “lab-on-a-chip” or “universal chemical fabrication” capabilities, or three-dimensional printing with engineering materials.

(c) Technologies that are moderately mature but require optimisation for large-scale use (macro-algae for sewage treatment and transport fuel production, at “village” scale).

Hypothesised changes identified under this category do need some comment on both scientific possibility, i.e. precluding those that contravene laws of physics, and practicality, but that leaves a wide scope. It seems to be quite reasonable in the context of this study to consider advances that are currently only mentioned in SciFi literature, yet do not contravene any laws – e.g. technology that can synthesize fresh
food that is indistinguishable from “real” fresh food, but is synthesised from very basic raw materials. A number of technologies could be considered in this category, and would therefore include solar pyro-metallurgy, lab-on-a-chip, small-scale general-purpose chemical synthesis and small-scale micromachining and fabrication.

7.2.4 Re-purposable components

The analysis of exposure considers the “availability” of a stream or process, with the general implication that a process is single purpose. It is quite possible to hypothesise a case where a multi-purpose component is substituted for a single-purpose component, and thus reduces the “exposure”. Well-written instructions allowing a member of the public to carry out the functions of a specialised employee would be an example of this type. The human being is perhaps the best example of a re-purposable component. The level of diagnostic capability, tailored instructions and operational capability of the common external cardiac defibrillation units are an excellent example of the implementation of this principle.

7.2.5 Repair priority or inherent difficulty of attack

It is possible to consider that a specific failure would have such a major effect that heroic repair efforts would immediately be launched; hence repair would probably be completed before the effects of the outage were fully felt. It is also possible to hypothesise a case, such as the severance of an undersea cable, where the preliminaries to an attack would be very likely to attract attention before they succeeded. Such cases would allow hypothesising that, even though an exposure locus exists, its significance should be deprecated, on the assumption that either a hazard would be avoided or repair would be rapid and certain; for example, consideration that the outage of a very large utility will attract major repair efforts, whereas a localised sewage pipe defect may take a utility many weeks to address if there are thousands of others. This is a matter for comment within the analysis, rather than offering a hypothesis for change, and hence is not noted as a category of hypothetical change. Local bodies will give high priority to maintaining the function of sewage systems, but, following the Christchurch earthquakes in 2011, untreated sewage has leaked from the system for over 5 years; “portaloos” on residential street corners were still in use 4 years after the earthquake, and the whole pipework system
is to be abandoned and replaced by a new pressurised system. Despite urgency, quick repairs have not been possible. Under this heading, it is also relevant to note that commentators have periodically drawn attention to significant factors that are easily omitted from even well-structured analyses. Examples include the preponderance of internet services that are totally dependent upon advertising revenue for continuance, as no effective mechanism to enable user-funding has been set up.

7.2.6 Standardised independent units and interfaces

Where there are standardised components and/or standardised interface specifications and/or very many readily available substitution units, the actual exposure is reduced. Where publicly available interface specifications exist, the production of multiple options for use of the interface will tend to be encouraged. It may be argued that the success of the internet has been possible because the packetising of information allows standardised handling approaches and the well-publicised TCP/IP protocols and mail, http, ftp etc., as defined by W3C, the Worldwide web consortium. All services allow very many suppliers to offer interoperable equipment. Other examples would include ISO-standard nuts and bolts, international fuel specifications, containerised shipping, micro-USB charging plugs and voltages, and Ethernet standards for communications protocols. An equally important application of this principle is the design of components for operation by multiple readily available tools – examples range from standardised nut and bolt sizes to a DVD format that can be read using a microscope rather than relying on a completely opaque specification plus firmware plus hardware and software. This concept is well understood in the mechanical engineering field, but has not yet been assimilated in the IT field. Programming languages appear to fail to implement this principle, although Java™ and, to a lesser extent, Microsoft’s .Net™ framework have attempted to do so. For data representation, the use of mark-up languages implemented in software is a good example of such an approach, because a text reader will allow a user to discern and edit the information represented. Open source document formats such as ODF (ISO/IEC 26300-3:2015 – “Information technology – Open Document Format for Office Application”) are another example of such an approach.
7.2.7 Minimise exposure contributed by common subsystems

**Contributory systems:** The analysis of examples has shown that large levels of end-user exposure are incurred when the provision of the goods or services is dependent on a significant technological subsystem that itself incorporates large levels of exposure. Use of a standardised subsystem such as internet communications may offer utility to the end-user, but the utility is associated with a very significant exposure. Technological alternatives that preserve the essential utility, but avoid the exposure contribution, need to be considered carefully. Small sensors and single-purpose devices can be created at low cost and can be connected to the internet; the functionality added by each is small, but the “exposure” added by each is significant and avoidable. Although disruption of major T1 links and associated routers is unlikely except briefly, the “Internet of Things” (IoT) allows burgeoning points of exposure for even local networks and other connected devices. Of particular concern are implanted medical devices, for which “exposure” is life threatening, and for which the addition of a significant contributory exposure (by internet connection) is a very dubious trade-off against functionality.

“Effectively unavailable”. This thesis has already noted that various quite disparate categories of fault or event can cause a system to become “effectively unavailable”: these can include physical fault, but can also include situations in which other factors make the “system” become effectively unavailable. Although such “effective unavailability” may be manifested as a contractual issue, the technological basis is clear: economies of scale and non-availability of user-controlled technological options have led to a highly centralised privately owned technological system with many users. Those technological drivers have, almost inevitably, provided the foundations for situations in which either contractual practices or known operational practices of the owners, e.g. data sharing, blatant snooping, censorship or the injection of information intended to entrap or mislead, exist and may cause the service to be effectively unavailable to a user. The applications of internet services are currently resulting in the carriage of both very broad and very fine-grained data relating to individuals. It has been noted elsewhere that “unavailability” can mean “unacceptable availability” as well as non-availability. Media reports (e.g. "NSA slide shows surveillance of undersea cables" (Washington Post, 2013)) have strongly
suggested that various powers have taken advantage of the common landing points of several high-capacity undersea data cables to install surveillance equipment; this cannot be confirmed with certainty but end-users with concerns for privacy may consider that the internet communications system is effectively unavailable to them. The data generated by electronic financial transactions provide a very detailed picture of users’ life patterns and the users have no effective control over the usage of the information exchanged. It is not hard to envisage situations (a citizen of a totalitarian country making regular donations to a democracy advocate or climate change scientists in a country ruled by climate change sceptics) where such a system could become effectively unavailable to a user. It can be observed that an individual living in a typical urban environment would find existence without a bank account very difficult – a situation that allows banks to impose terms and conditions with very little regard to user wishes.

**Reduction of specific internet exposure.** Individual users’ subscriptions to ISPs allow the funding of access, and contributions are aggregated to generate revenue for such commercially driven ventures as the provision of undersea cables. Internet infrastructure, e.g. administrative controls, router update costs, DNS server costs etc., are also funded by user contributions. Some indirect revenue, e.g. access to cable corridors, is still likely to originate from government sources. Internet services, which include major news providers and services offering free web searching, free web-based email and free document processing and storage facilities, are still generally funded by advertising and an economic downturn would put pressure on advertising revenue and perhaps drive content providers towards pay-to-use content.

**Reduction of financial system exposure.** The analysis of the EFTPOS system’s exposure shows the very large level of technological exposure incurred by this system. Previous notes on the potential for such a system becoming effectively available provide a quantitative basis for supporting the continued legality of a physical medium of exchange, whether cash or bullion. The recent emergence of machines capable of recognising large-denomination banknotes will assist this option. It may be observed that calls for the abandonment of cash as a legal tender have never gained wide support. Arguments that the tracking of financial transactions assist with the detection of criminal activity are commonly used; an equally valid argument
that such an aim does not require total and ongoing surveillance of all transactions can be made.

**Reduction of transport system exposure.** Many aspects of transport systems are already standardised: fuel specifications, vehicle dimensions, vehicle speeds aligned with road design standards and the use of containers for bulk material movement. A private motor vehicle with a full tank of fuel has a very low level of "exposure" within an operational time-frame – it is noteworthy that many persons perceive a private motor vehicle as giving them freedom and options. It seems to be possible that the future availability of easily hired utility vehicles will offer yet lower exposure for the user, but the current low levels suggest that transport vehicles are not a high priority for the reduction of user vulnerability. Bulk fuel supply has been shown not to be a major source of exposure for the short term, i.e. within an operational time-frame, as several strategically mandated stores offer alternative sources. For a longer time-frame, the supply of bulk fuel would contribute to the user's exposure and options for local fuel synthesis would offer attractive options.

### 7.3 Hypothesised modifications to examples

In this section, changes are hypothesised. Not all hypothesised changes are considered as worthy of analysis. For changes considered to be useful, the incremental change to exposure is noted. As hypothesised changes are identified, changed aspects rather than the complete system are described and incremental, rather than full, analyses of exposure are reported. The identification and assessment of hypothesised changes to each example will be considered under four headings.

(a) Observations on example analysis, particularly large contributors to vulnerability, and specific features of note.

(b) Review of applicability of types of hypothetical change, considering possible changes within each of the identified categories.

(c) Proposal of actual hypothetical system re-designs, in sufficient detail to allow analysis, and presentation of the assessed effects.

(d) Summary of effect of hypothesised changes, commenting on the effectiveness and implications of the proposed changes.

The effort required to effect a given change will be categorised as "Major", i.e. widespread replacement of high-cost infrastructure, "Moderate", i.e. requiring partial...
changes to infrastructure, or “Minor”, i.e. works that can be accomplished with little more than maintenance budgets and without major disruption. The effects of hypothesised changes are also categorised as “Major”, “Moderate” or “Minor” according to the proportional change in the total exposure.

7.3.1 Effect of hypothesised changes to communications

Options for eliminating or reducing the exposure incurred by any contributory system should be investigated. The high values of exposure incurred by the internet communications system justifies efforts to reduce its contribution.

(a) Observations on example analysis

The packet transmission protocols allow detection of corrupted packets and hence requests for resends, acknowledgement of valid packet receipt and robust protocols for reassembly of files from packets without regard to arrival times and routes. Commentators have noted that the protocols contain good error detection and correction approaches; they are inherently unencrypted and hence the contents are insecure. ISO OSI protocols (ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model) have never achieved significant uptake, particularly compared with TCP/IP protocols, but, unlike the TCP/IP protocols, the ISO OSI protocols were designed to allow both open standards and seamless integration across all process "layers" – an outcome that has not been achieved with TCP/IP. The internet originated as a highly decentralised network that would allow messages to be re-routed over many optional routes with semi-automated route selection, in response to outages. It has evolved into a state where a very large proportion of data is transmitted by a relatively small number of high-capacity undersea fibre-optic carriers. As well as increasing exposure to physical failures, this centralisation increases the exposure to practical non-availability because of issues such as surveillance.

High-capacity overland data transmission has also evolved, driven by economy-of-scale considerations, into a situation where small numbers of high-capacity lines carry the majority of data, and incur significant exposure. Although the re-routing of data transmissions is the mechanism that provides the internet’s robustness, and the DNS lookup methods are the key to usability for many applications, effective re-routing of packets depends upon the updating of router
tables and protocols and valid DNS lookups are essential for finding data. The mechanisms for reliably updating router tables and DNS server tables are both weaknesses within the definition developed in this thesis. In addition to the centralisation of data transmission paths, the internet has also progressively evolved into a state where large portions of the total online data storage are provided by a small number of well-resourced companies. The effects of this situation have been noted, e.g. New Scientist (2016).

(b) Review of applicability of types of hypothetical change

Local storage. Although many routers will include limited storage, increased storage will result only in excessive re-send requests rather than significant actual changes to exposure. This option is not considered further.

Technological substitution. Wireless access is used increasingly and, assuming that wireless communication modules are readily replaceable, these reduce the vulnerability associated with last-mile cable access.

Technological breakthrough. It is possible to consider a completely ad-hoc, self-discovering wireless network that will allow completely automated re-routing without cables. Self-discovering networks have been proposed, and are certainly feasible. Provided that a funding mechanism were developed and nodes were solar powered, a genuinely self-discovering network would reduce a user's exposure to negligible levels.

Semi-dynamic effects. Although store-and-forward systems could be considered, the current protocols have extensive provision for detecting and re-requesting corrupt packets. This approach appears to offer limited opportunities for significant gain. The use of uninterruptible power supplies for routers is the most promising application of this type of option.

Re-purposable components. The internet already makes extensive use of re-purposable components including PCs and hard drives, and this approach seems to offer limited additional opportunity for vulnerability reduction.

Standardised independent units and interfaces. The internet already makes extensive use of standardised independent units.

Minimisation of contributory systems. For many large components of the internet system, e.g. undersea cables and high-speed router centres, uninterruptible power supplies and un-manned operations are normal, reducing two common
contributory causes of exposure. The issue of commercial access and personally acceptable terms and conditions make very significant contributions to the issue of internet service availability.

**(c) Proposal of actual hypothetical system re-designs**

No claim to consider all possible changes is made. No claims for economic desirability or affordability are made. Options must not be clearly impossible, i.e. violate basic scientific principles, but may not necessarily be technically feasible at present. The following list has been developed from a consideration of the sources of exposure identified in the example study, and the identified change categories. It must be noted that the scope of these changes applies to systems from the outward-facing domestic router port onwards, i.e. within the scope of the internet communications subsystem.

**Last-mile wireless.** The last-mile cable between the DSLAM router and multiplexer and the household router is exposed to breakage, corrosion and other hazards. It would be possible to use a secure wireless carrier between the domestic router and the DSLAM router, with no changes to the remainder of the system. This change would eliminate a current $E_1$ vulnerability for the user.

**DSLAM power.** The power supply to the DSLAM router and multiplexer is a locus of exposure. Provision of a backup power supply to each DSLAM router reduces that exposure, with no changes to the remainder of the system. Provided the backup power supply met the criteria for a local storage solution, this change would eliminate a current $E_1$ vulnerability for the user.

**Redundant paths.** The original internet design provided multiple reconfigurable paths, and, although this design concept has survived, economies of scale have led to a situation in which the bulk of the total internet traffic is carried by a relatively small number of very-high-speed fibre-optic cables. These high-speed links have achieved high levels of availability but each represent a point of exposure. Even nation states may actually depend on a single high-speed connection to the rest of the world, and there have been cases (The Guardian, 2011) when a nation was in fact disconnected from the internet by the disruption of a single cable. Additional transmission routes, most probably additional undersea cables, with backup to satellite paths, with no changes to the remainder of the system, reduce this exposure.
The hypothesised change ensures that $E_1$, $E_2$ and $E_3$ are all zero for transmission paths between peering points.

**Acceptable access, the issue of practical availability.** The user currently requires the services of an ISP, who sets terms and conditions for the provision of services. The ISP will purchase transmission services and bandwidth from national and international providers, each of whom will offer services under set terms and conditions. Both the local ISP and the upstream providers are subject to the legal framework of the various jurisdictions in which they operate. Collectively, these commercial and legal conditions all represent loci of exposure that may make the service practically inaccessible to the end-user. Although it has been proposed that internet access should be considered to be a human right, these issues have not actually been addressed. It is reasonable to hypothesise a situation in which all users are assured of the privacy of their data and metadata and are required to offer terms and conditions that meet minimum standards, possibly via a "bill of rights" for consumers, and certainly by an acceptance of the acceptability of strong encryption. This hypothesised change would require contractual, technical and commercial aspects, as commercial provision would be required to ensure the provision of resources for expansion, repair and maintenance and operation, with no changes to the remainder of the system. This would reduce a current $E_1$ vulnerability to users.

**Widely distributed wireless access.** The hypothesised wireless link between the domestic router and the DSLAM would eliminate the exposure associated with the last-mile cable. A more generalised approach envisages modifications to the DSLAM to allow services similar to the GSM cell phone system to be offered, allowing any device to connect wirelessly, and hence offering mobile and near-anonymous wireless access to the current DSLAM level of connection. Such a change would also eliminate the "practical availability" $E_1$ contributor and would provide massively redundant access points.

**Alternative router table update.** According to Mr. Christopher Williams, Technology Correspondent (The Guardian, 2011)

"Organisations that track global internet access detected a collapse in traffic in to and out of Egypt at around 10.30GMT on Thursday night...The shut down involved the withdrawal of more than 3,500 Border Gateway Protocol (BGP) routes by Egyptian ISPs, according to Renesys ... BGP routes are one of the most vital parts of the
internet. They are mostly used by ISPs so their networks can exchange information about how to best route the packets of data that make up all internet communications. This action, carried out for political reasons, illustrates the issue of “exposure”. The internet was technically capable of routing data internationally but, once the government of the day decreed the non-availability of BGP information and the non-acceptability of alternative data routes, citizens of the country effectively had no internet access. The BGP router information was a point of exposure, and provision of an alternative approach would allow the removal of a contributor to user vulnerability.

**Ad-hoc, self-discovering routing system.** All of the previously hypothesised options assume packet transmission through a set of semi-automated routers connected by high-speed physical links. Re-routing is possible by arranging for the routers to select alternative paths, i.e. alternative cable or fibre-optic lines, en-route to the same destination. Although alternative paths decrease exposure, the total number of paths cannot be expected to be large. Significant work has been carried out, e.g. by Robertson (2007), to develop principles for self-discovering, ad-hoc free-field networks that effectively comprise a massively parallel network of independently powered, radio-connected and identical nodes with no interconnecting independently powered cables. A system using ad-hoc networks established by nodes using a self-discovery approach is effectively a significant internet re-design. However difficult technically, much has been learned about self-discovering ad-hoc networks and such are possible. This hypothesised approach would assume wireless access from the user’s router to the nearest available network node. Such a change would represent almost a complete technological development and substitution, but would remove all practical vulnerability from communications systems.

(d) **Summary of effect of hypothesised changes**

Simple and technically feasible approaches are able to reduce several (E1) contributors to vulnerability. More costly and difficult approaches, such as router updating and the provision of redundant capacity, are able to reduce exposure but rely on commercial and statutory enablers. Despite having been proposed as a "basic human right", the internet grew from a small network within a friendly environment, and the lack of inbuilt security and privacy measures have frequently been
commented upon. An invulnerable communications system is possible technically, but would require the transition to a significantly changed technological approach.

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Last-mile wireless.</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>2 DSLAM power</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>3 Redundant paths</td>
<td>TECH_SUB</td>
<td>Major</td>
<td>Major</td>
</tr>
<tr>
<td>4 Acceptable access</td>
<td>CONTRIB’Y</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>5 Widely distributed wireless access</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>6 Alternative router table update</td>
<td>TECH_NEW</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>7 Ad-hoc, self-discovering routing system</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
</tbody>
</table>

Table 16: Effect of hypothesised changes to internet system

7.3.2 Effect of hypothesised modifications to financial transaction systems

Several of the studied examples, and many examples that have not been studied but that clearly affect users, depend upon financial transactions. This justifies consideration of these systems as standard contributory systems. The studied examples assume the use of an EFTPOS transaction system.

(a) Observations on example analysis

Considering the EFTPOS system used in the representative example, the computer hardware systems of two banks need to operate to allow the transaction. The acquirer-to-merchant transaction can be run in batch mode and hence does not incur the same exposure as the acquirer and user bank systems. Of equal importance, both the user and the merchant can have any access to the EFTPOS system only if the merchant accepts the acquirer bank’s conditions and their own bank’s conditions – and the end-user can access the EFTPOS system only if the user accepts their bank’s EFTPOS card conditions, which may include disclaimers regarding the accessibility of data to either official or commercial entities. The EFTPOS system makes use of the internet and the example assumes the subsystem boundaries identified for the internet communications subsystem, but also requires secure processing systems at each of the three relevant banks.

(b) Review of applicability of types of hypothetical change

Local storage. No useful contributions.
Technological substitution. Several media of exchange avoid the use of the EFTPOS system entirely; ensuring that these media remain available and acceptable will eliminate all of the vulnerabilities associated with the EFTPOS system. The electronically verified credit card systems eliminate few of the vulnerabilities of the EFTPOS system.

Technological breakthrough. Currency notes and coins are generally only recognised within a single country; an internationally recognised medium of exchange that is suitable for consumer transactions could be developed. Legal tender currency is storable, but is subject to theft; cryptocurrencies are less vulnerable to physical theft, but incur vulnerabilities associated with bitcoin wallets, cryptographic schemes and other hardware and software components.

Semi-dynamic effects. None identified.

Re-purposable components. None identified.

Standardised independent units and interfaces. See above.

Minimisation of contributory systems. As the EFTPOS system depends upon internet communications, it incurs that contributory system's vulnerabilities.

(c) Proposal of actual hypothetical re-designed systems

Several options are considered to be worthy of analysis.

Credit card transaction. Many modern credit cards include electronically readable systems within the user's card to ensure identification of the user. An EFTPOS transaction involves a real-time interaction between the terminal, the user’s bank and the acquirer’s bank and a batch-mode interaction with the merchant’s bank. In contrast, a transaction using such a card requires only a real-time interaction with the card-issuer’s bank and batch-mode interactions with the user’s bank and the merchant’s bank. All of the exposure values associated with real-time interactions with user and merchant banks are eliminated, because transactions with the user and merchant banks are stored and executed whenever possible. Practical availability issues are not avoided and, as the credit card issuer carries some risk, the practical availability vulnerabilities may actually increase.

Paper-based credit notes. For credit card systems using “zip-zap” machines, effectively the merchant collects a promissory note from the user on the credit card issuer. The credit card issuer’s conditions could become unacceptable to the user,
rendering the system effectively unavailable. The effect on vulnerability is the same as for the credit card option.

**Cash transaction (notes or coins).** Cash transaction options include banknotes and coins or tokens (legal tender), all representing agreed physical media of exchange. Notes and coins are tokens of wealth, and their usage and acceptability are dependent upon banks or national exchanges and incur exposures related to issue and acceptance. They are generally recognised only within one country. The use of cash eliminates all of the vulnerabilities associated with an EFTPOS system, but is dependent upon the merchant’s willingness to accept cash and to tender change. It does incur an exposure to physical theft.

**Cash transaction (bullion).** Cash and coin depend on national or local bank issue. It is possible to consider a transaction system based on rare metal (bullion). Confirmation of authenticity is feasible based on physical properties including density and resistivity, and no dependence on external bodies is required. A technological development, capable of issuing small but accurately measured quantities of 99.999% gold, is possible and would offer an internationally acceptable payment system, eliminating all of the vulnerabilities of the EFTPOS system although incurring an exposure to physical theft.

**Promissory note (cheque).** This is a document that is signed or otherwise authenticated by the user, authorising the bank to pay the bearer the transaction amount. In some countries, bank cards would be issued to users, guaranteeing the honouring of transactions up to an agreed limit (a limit of £50 was common in the 1980s). Technologically, this system involves no more than paper, pen and bankcard at the point of transaction, and thus avoids the vulnerabilities of the EFTPOS system; however, as for credit card systems, vulnerabilities associated with practical availability are likely to be onerous as the bank bears some risk.

**Personal debit system to phone.** In many developing countries, particularly regions of Africa, it is common for users to treat their cell phone prepay balance as a personal bank, and find it convenient and simple to make transactions either from or to their prepay balance. Such a system avoids the vulnerabilities of an EFTPOS system but incurs the vulnerabilities of the cell phone system. The vulnerabilities of the cell phone system avoid the last-mile vulnerabilities; also, the fact that this is a debit system will tend to reduce the practical availability issues.
Personal debit system. The concept of a personal debit system is that the user carries a smart card or equivalent that both retains a verifiable record of the user’s credit balance and the means of authenticating this and a transaction. Such systems are not commonly available, but require only technology that is currently available. Such a system requires the card technology and also vendor technology that can transfer credit securely and reliably between the parties. This avoids almost all of the vulnerabilities of the EFTPOS system but incurs the few vulnerabilities of the card electronics and the vendor’s card reader.

Bitcoin transaction. The “bitcoin” transaction (as an exemplar of several blockchain-based “cryptocurrencies”) approach effectively requires both users and merchants to have access to bitcoin wallets. The hypothetical approach assumes that the user carries a hardware version of the bitcoin wallet, whereas the merchant has access to an online version. Both need access to the blockchain system. The technology for this system is available although not widely used. Although this hypothesised approach still requires access to the internet and computing power, it does not rely on the acceptance of financial institution terms and involves only two parties directly. The internet vulnerabilities remain, the additional vulnerabilities of the bitcoin wallet and the merchant wallet-reader are added, and the practical availability vulnerabilities of commercial and contractual access to EFTPOS and/or credit card systems remain.

Barter. Simple transactions between willing buyer and willing seller, with personal agreement on the value of dissimilar goods/services are possible and have effectively no exposure to technological systems.

Regulation of terms and conditions. Terms and conditions offered by financial institutions as a condition of holding an account may cause such accounts be practically unavailable to either users or merchants. Regulation constraining such terms and conditions may effectively remove such issues and allow users to consider the existing EFTPOS system to be available. Such regulation could remove one contributor (E₁) to the user’s vulnerability.

(d) Summary of effect of hypothesised changes

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Credit card transaction</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>2 Paper-based credit notes</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
</tbody>
</table>
Table 17: Effect of hypothesised changes to EFTPOS system

<table>
<thead>
<tr>
<th></th>
<th>Cash transaction (notes or coins)</th>
<th>TECH_SUB</th>
<th>Minor</th>
<th>Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Promissory note (cheque)</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>5</td>
<td>Personal debit system to phone</td>
<td>TECH_NEW</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>6</td>
<td>Personal debit system</td>
<td>TECH_NEW</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>7</td>
<td>Bitcoin transaction</td>
<td>TECH_NEW</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>8</td>
<td>Regulation of terms and conditions</td>
<td>CONTRIB'Y</td>
<td>Minor</td>
<td>Major</td>
</tr>
</tbody>
</table>

7.3.3 Effect of hypothesised modifications to sewage system

(a) Observations on example analysis

The largest contribution to the $E_1$ values is from the non-duplicated major components of the sewage treatment plant. As far as the apartment dweller is concerned, most of those systems could be bypassed, allowing service to continue, but with raw sewage discharged to waterways. This observation illustrates the importance of clarifying the “service”. The second largest contribution is from the extensive pipework system that is required to transport sewage from the apartment to the treatment plant – this is effectively a result of the highly centralised nature of the processing – which requires an extensive collection mechanism. Power to the pumping stations contributes to exposure and, although some pumping station equipment is duplicated, this still contributes to user vulnerability. Although the sewage treatment station discharges treated solid waste to landfill, as there are storage and alternative transport options for this function, its contribution to vulnerability is relatively small.

(b) Review of applicability of types of hypothetical change

Local storage. Local storage of sewage, i.e. close to the apartment, is actually quite practical for terms of a few days or weeks. “Pump-out” systems are actually increasingly commonly in peripherally urban areas where septic tank discharges are unacceptable but pipework and centralised treatment systems are also not practical. The exposure analysis demonstrates the contribution of local power supplies, and the difficulty of avoiding such exposure in the absence of an adequate power storage...
technology. For typical industrial processes (requiring MWh power levels), there are currently no processes for the storage of power that are technologically mature and close to economically viable. A capability for storing MWh quantities of electricity would have a significant effect on the exposure of processes such as this. Noting the value of standardised approaches, it would be possible to consider a system using local storage in container-sized vessels, allowing either pump-out or transport substitution.

**Technological substitution.** The 2011 earthquakes in Christchurch, New Zealand, caused very extensive damage to the clay pipework of the original gravity-fed sewage system, with very large numbers of fractures within the estimated 1400 km of pipes and major damage to the 16 pumping stations and also to the downstream facilities. Christchurch has decided that the cost of replacing the system is too great and has elected to install a completely new “pressure” system in which household-scale disintegration and pump units allow the use of small-bore flexible pipework rather than large-diameter and inflexible gravity-fed clay pipe systems. This avoids the huge repair costs of gravity reticulation and the disruption to other infrastructure.

**Technological breakthrough.** The development of an economical and convenient local (i.e. toilet) sewage breakdown technology is certainly technically possible and such technologies as composting toilets exist. It is not currently practical to use macro-algae to treat sewage and to generate biofuel at a village- or suburb-scale system. However, as the power requirements of such a system are modest, this could be considered as a target for a technological advance. A smaller scale system of this type would possibly allow consideration of local power sources such as a solar photovoltaic system plus battery systems.

**Semi-dynamic effects.** Raw sewage could be stored at the treatment plant, pending the repair of a component. When the volumes to be stored and the likely repair times are considered, this approach is not practical for other than the very short term at a city level. However, the storage of a few days’ volume is quite practical in the medium term at a household level.

**Re-purposable components.** It has been assumed that at least three persons at the treatment plant are able to operate each item – hence $E_3$ contributions. If plant item operating instructions were readily available, this contribution could be taken to below the $E_3$ level. Trucks for the disposal of landfill waste are assigned to
the E₃ level; if compaction and dewatering allowed the use of standard shipping containers, then this contribution could be moved to beyond the E₃ level.

**Standardised independent units and interfaces.** Many components of the sewage system are already standard mechanical components.

**Minimisation of contributory systems.** Although power and transport systems are used in many sections of the sewage system, the specific sources of the power vary, reducing the gains possible by substitution of a specific contributory system. The road transport system already has many alternative service options and is not considered to be a large contributor to exposure.

*(c) Proposal of actual hypothetical re-designed systems*

**Storage systems.** Containerised local tank systems would allow options of either pump-out or transport substitution; even at apartment scale, the criteria of sufficient storage to allow repairs to critical components would be feasible. At household or apartment locations, modest volumes would allow significant repair times and would meet the criteria to deduct the exposure associated with pump system failures and treatment plant failures, although it is unlikely that the storage volume could practically allow major pipeline repair.

**Pressure system.** Historically, the primary causes of failure to the nominated service level have been physical damage to the pipework leading to the treatment station, or overloading because of excessive storm water ingress. Power failures and equipment failures have not been significant contributors to failure. For small communities installing a sewage system for the first time, and even for Christchurch replacing its extensively damaged “conventional” sewage system following the 2011 earthquakes, it is common to select a “pressure” system in which household-scale pumps/disintegrators are used to process sewage and forward the low-viscosity liquid at pressure via a small-diameter flexible pipe. Such a system reduces capital cost, and decreases the maintenance cost and repair time of the pipework system; however, it depends upon the operation of the local disintegrator, the power supply and controls. This system effectively replaces all systems up to the main feed into the treatment plant. Combined with minimal local storage, such a system can reasonably be claimed to avoid the exposure of the pipework and local pumping systems.
Pumping station power supplies. Large-scale electrical power storage is not currently practical. If such a technology is developed, the exposure associated with both pumping stations and sewage treatment plants can be reduced.

Pumping station alternative power. Pumping station exposure can be reduced by providing either ICE-based backup power or additional power feeds. The economics of such approaches are not considered in this analysis.

Treatment station power supplies. Reductions to $E_2$ values associated with power supplies are possible, by providing alternative power supplies to the treatment plant distribution board. It is technically feasible at present to provide most of treatment plant power from biogas generated from sewage and, although the cogeneration and digester plants have vulnerabilities, as these are alternative power sources, they effectively move the $E_1$ contributors to $E_2$ levels.

Power storage for pumping stations and treatment plants. The storage of several hours’ power for pumping stations and treatment plants would require a technological breakthrough. If such a technology became available, the associated exposure at both treatment plant and pumping station would be avoided.

Treatment plant manual control. Reductions to exposure are possible by providing manual control of all pumping station, sewage treatment station plant and bypass functions, and instructions for operation by non-specialised staff. These changes do not affect the remainder of the system.

Solar-powered local system. As the development of an apartment-scale treatment system, requiring no more power than could reasonably be produced by solar thermal plus a photovoltaic system and generating environmentally acceptable waste streams, is technically feasible, this approach is proposed as a hypothesis to be examined. Although the hypothesis requires technological development, it is reasonable to postulate a gravity-fed system that uses solar-powered controls to maintain optimal conditions for biological degradation, uses solar-powered materials handling including pumping and aeration functions, and thus generates environmentally acceptable discharges at an apartment scale. Such a hypothetical system would avoid the need for extensive pipework, pumping stations and centralised treatment processes. Transport of treated waste would be required, but this contributes little exposure. An advanced treatment system, similar to this, but on
a household scale, can also be postulated, with identical exposure reduction for the individual end-user.

**Hybrid fuel system.** Household or suburb-scale macro-algae fuel generation would require a complete technological change, providing the processing of sewage using either high-rate ponds or a photo-bioreactor with the generation of hydrocarbons suitable for raw fuel feedstock, using solar power and technology that is feasible on a suburb scale. This eliminates all major pipework systems, centralised power supplies and treatment plants. The treatment of the exposure of such a system requires care, because the production of treated sewage is not the only output and redefinition of the "service level" would be required. The overall exposure of the user would however be reduced.

(d) Summary of effect of hypothesised changes.

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Storage systems</td>
<td>TECH_SUB</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>2 Pressure system</td>
<td>TECH_SUB</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>3 Pumping station power supplies</td>
<td>TECH_SUB</td>
<td>Moderate</td>
<td>Minor</td>
</tr>
<tr>
<td>4 Pumping station alternative power</td>
<td>TECH_SUB</td>
<td>Major</td>
<td>Minor</td>
</tr>
<tr>
<td>5 Treatment station power supplies</td>
<td>TECH_SUB</td>
<td>Major</td>
<td>Minor</td>
</tr>
<tr>
<td>6 Power storage for pumping and treatment stations</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
<tr>
<td>7 Treatment station manual control</td>
<td>REPURP</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>8 Solar-powered local system</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
<tr>
<td>9 Hybrid fuel system</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
</tbody>
</table>

*Table 18: Effect of hypothesised changes to sewage system*

7.3.4 Effect of hypothesised modifications to work information system

(a) Observations on example analysis

It is important to note the major differentiation between this example and the first-aid example: in the first-aid example, both the diagnostic information and the treatment information are generally static and hence durable non-volatile storage is possible; in contrast, work information is volatile, i.e. frequently created and/or edited, and commonly has a limited temporal relevance. The major exposure contributors are the remote server holding the work information, the internet (all aspects) and the local PC. The local PC can simply be duplicated, and its real exposure points are the
remotely changeable operating system, a situation where all duplicated PCs are affected by the same change, or local power supply issues. The remote server exposure can be at least reduced by continuous backup systems. The internet is the single largest contributor to exposure; the extent and the nature of the exposure have been considered elsewhere, and changes could be considered. The local PC operating system can be attacked separately and hence is identified as a contributor to $E_1$; an operating system can be implemented in firmware and signed by a trusted supplier. PC applications (software) can also be attacked separately and hence are identified as a contributor to $E_1$; standardised file formats (ODF) and adequately robust development can, in principle, allow software applications to be implemented in firmware and signed by a trusted supplier. Reductions in the power consumption of PCs is progressively allowing operation from USB power supplies (power packs), which will reduce exposure to domestic 230 V power supplies. Currently, most household routers are still powered directly from 230 V supplies and could be operated via a power pack (battery with trickle charge). The data format for spreadsheets has achieved a degree of standardisation, and a significant number of applications allow users to view and update spreadsheets. Full adoption of publicly available ODF standards will further reduce both current exposure to the possibility of being unable to view and edit data, and future exposure to an inability to access today’s data, i.e. avoiding the "digital dark ages" issue.

(b) Review of applicability of types of hypothetical change

Technological substitution. The internet communications subsystem has been identified as the subsystem that contributes the largest single exposure to the end-user in this case. The internet’s exposure contribution arises from the relatively small number of T1 lines, the centralised process for distributing key international routing information and the multiple single points of failure close to the end-user.

Several interlinked socio-economic factors also add to the exposure contributed by the internet: centralisation allows the internet to be subject to surveillance that may make the system practically inaccessible to groups; the anticipated proliferation of connection points (IoT) will significantly increase the number of sources of malicious software and/or surveillance. The ubiquitous nature of internet use makes it an attractive target, and commentators such as Bruce Schneier have noted sophisticated activities that are likely to be unfriendly (Schneier,
Media commentators have also drawn attention to the vulnerability of accessible data, caused by the lack of a robust funding model; this causes two types of exposure. Large providers such as “Facebook” and “Google” are funded by advertising revenue, and will try to maximise this revenue by making strong efforts to give their advertisers the best-targeted access to users. It is noted that infrastructures such as undersea cables are funded as investments by international carriers, who obtain revenue directly from consumers but are subject to national regulation (including access to users’ information), which may also make the network unavailable to a specific user.

**Technological breakthrough.** A truly ad-hoc peer-to-peer network protocol, with self-discovery of alternative routes.

**Semi-dynamic effects including local storage.** Adequate IT provisions for the duplication of user files across geographically remote servers is quite practical using existing technologies.

**Re-purposable components.** Although it cannot be assumed for the purposes of this study, it can be noted that many households do have more than one device, e.g. a PC and a smart phone that is capable of internet access and basic messaging. The progressive reduction in power requirement is allowing more communications devices to operate from low-capacity battery systems and to allow realistic charging from photovoltaics.

**Standardised independent units and interfaces.** Although progress has been made towards the standardisation of file formats for word processing, spreadsheets, presentations and database files, a more complete standardisation would reduce the exposure of all users, and would contribute to the long-term accessibility of material. Less than two decades ago, 8 inch floppy disks were used by Wan Corporation word-processing stations, audio cassettes were used for data storage and punched paper and cards were not uncommon. Equipment to read data from such sources would be exceedingly rare today and it cannot be assumed that all data have been moved to more modern formats. Even within the last two decades, common data formats have become inaccessible. This issue has been mentioned by authors, including Cerf (2015), who have proposed the term “digital dark ages” to describe situations in which data become inaccessible when the storage method, e.g. on closed-format storage systems such as DVDs, is no longer available. In the context
of this thesis, it is useful to observe that old data storage media such as microfiche have very low exposure (as defined in this thesis), and could be read using an improvised microscope. An open-format, non-volatile data storage technology would make very significant long-term reductions in exposure to data loss; the approach proposed by the Longnow Foundation’s (02016) “Rosetta project” concept is noteworthy.

**Minimisation of contributory systems.** A significant approach to reducing exposure is to eliminate the subsystems that contribute huge levels of exposure.

(c) **Proposal of actual hypothetical re-designed systems**

The portion of the internet system that has been defined in Chapter 5 of this thesis as a standard subsystem has been considered to include all aspects between the outputs of the domestic routers, i.e. communications to city ISP, intra-national peering systems, connections to international undersea cable service providers etc. Options for a reduction of exposure of this internet subsystem are considered separately.

**Backup power for household router.** As the household router is generally powered from a 230 VAC power pack, it is unusable if a mains power failure occurs. An uninterruptible power supply (UPS) or battery backup reduces one point of vulnerability without requiring changes to the remainder of the system.

**Backup power for PC.** Household PCs are generally powered from a 230 VAC supply and, even for PCs with batteries, a PC is commonly unusable after a few hours if a mains power failure occurs. A UPS or significant battery backup reduces one point of vulnerability without requiring changes to the remainder of the system.

**Online storage.** Data storage is a significant locus of exposure for users at both ends of this example. A duplicated (RAID) approach to local data storage will eliminate the exposure to local hardware failure causing data loss.

**Hardened router.** Router operating systems and applications are currently exposed to malicious changes, and hardwired “admin” access options have occasionally been found. The router applications could be hardened, checked and

---

3 It seems entirely appropriate, for an organisation whose projects include the design of a “10,000 year-clock”, to use the date format “02016” instead of “2016”. 
signed. Such a change would effectively eliminate the exposure associated with the router software.

**Hardened PC.** PCs currently have components including operating systems and applications as well as drivers that are potentially remotely alterable, either by targeted intrusion or by malware. Whether arising from poor design or oversight, all of these incur vulnerabilities to the user. There is no fundamental principle that prevents the construction of a secure, un-alterable suite of operating system plus system and application software that will ensure that these components will not be vulnerable to external threats. The implementation of such a system would eliminate the exposure contributions currently noted for PCs.

**Standardised data formats.** Data formats for spreadsheets have achieved a degree of standardisation, and a significant number of applications allow users to view and update spreadsheets. A full adoption of publicly available ODF standards will further reduce both current exposure to the possibility of being unable to view and edit data and future exposure to an inability to access today’s data, thus avoiding the "digital dark ages" issue.

### (d) Summary of effect of hypothesised changes

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Backup power for household router</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>2 Backup power for PC</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>3 Online storage</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>4 Hardened router</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>5 Hardened PC</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>6 Standardised data formats</td>
<td>INDEP'T</td>
<td>Minor</td>
<td>Major</td>
</tr>
</tbody>
</table>

*Table 19: Effect of hypothesised changes to work information system*

### 7.3.5 Effect of hypothesised modifications to local fuel supply system

#### (a) Observations on example analysis

Although the example is designed to be broadly representative of typical systems, real systems vary significantly. Some options for improvement are already found occasionally, and it is reasonable to note them and assess their effects. The representative system could be characterised as being “semi-automated”, with
requirements for staff, but with many functions that can be carried out only via the automated subsystems. The staff systems, including potable water supply and sewage removal, and the EFTPOS transaction system are the main contributors to system exposure. The road and vehicle systems required for bulk supply are considered to contribute little additional vulnerability because of their high level of duplication. Many petrol station forecourt systems include four to six replicated systems, but forecourt control systems are not duplicated and contribute to vulnerability. For short-term operation, multiple national reserves of bulk fuel reduce exposure, but, for longer time-frames, the capability to generate fuel onshore would reduce New Zealand’s exposure to multiple vulnerabilities associated with our single refinery.

(b) Review of applicability of types of hypothetical change

Local storage options can be applied to some of the staff facilities, allowing these to be provided on a temporary basis, pending repair, rather than forcing an immediate “failure” of the service. This option was covered when the sewage system was considered.

Technological substitution. Alternative technologies for many of the functions required by this example, including electrically powered pumps and electronic reading of amounts dispensed, can be offered.

Technological breakthrough. The science required to produce fuels, within standard specifications, from macro-algae sources, is close to maturity and is potentially practical at city or village scale. The practical availability of such technology would affect the exposure of national refining systems and bulk delivery systems.

Semi-dynamic effects. The example station requires staff and hence is inoperable without basic staff facilities including sewage and water systems.

Re-purposable components. As with many other examples, in this case, the human being is the most versatile component; thus, any capability for enabling human intervention is likely to reduce the actual vulnerability incurred.

Standardised independent units and interfaces. Limited opportunities of this type have been identified for this example.

Minimisation of contributory systems. Subsystems that make significant contributions to the exposure of the example include the sewage subsystem and the financial transaction subsystem. Both are addressed elsewhere.
(c) Proposal of actual hypothetical re-designed components and subsystems

**Staff service options – sewage.** All optional changes to the sewage system, as proposed under that example, can be considered.

**Staff service options – water.** Potable water is also required to enable staff occupancy. Rainwater collection to offer a supply for perhaps 3–7 days’ usage would eliminate the exposure to a potable water supply failure. This is an eminently practical measure.

**Staff service options – automation.** The example has considered a petrol station that is fully manned. A fully automated station must be considered. The elimination of requirements that are essential for staff presence will allow the exposure of those contributory systems to be eliminated. If the provisions for a reduction of the exposure of computing systems, financial transaction systems and communications systems were also eliminated, exposure would be very substantially reduced.

**Manual operations.** Provision for the manual operation of dispensing pumps and the manual recording of amounts dispensed would eliminate the exposure to both metering and pumping systems and local power supplies for these.

**Financial transaction options.** Options for a reduction of exposure to financial transaction systems have been considered separately.

**Alternative fuel sources.** It is possible to hypothesise a future technological option to generate standard-specification fuels from a macro-algae source. A likely technological option would also use sewage as part of the nutrition for the macro-algae, although the energy source is actually solar. This is noted as a “technological breakthrough” option; however, the components are at about 6 or 7 on the NASA scale of technological maturity (NASA, 2015), and hence this is a technological option that could reasonably be contemplated within a 10-year term. Macro-algae strains are already capable of achieving over 30% by weight of hydrocarbons. The generation of standard-specification fuels from macro-algae is not economically attractive at present, but the process engineering and chemical processes are known and technically feasible. The existence of multiple national reserves of fuel mean that bulk fuel is considered to contribute to user exposure in the shorter term; however, a consideration of fuel supply disruptions on a longer time-frame would require...
consideration of this exposure, and the potential for reduction by local fuel supply synthesis.

**Summary of effect of hypothesised changes**

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Staff service options – sewage</td>
<td>CONTRIB’Y</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>2 Staff service options – water</td>
<td>CONTRIB’Y</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>3 Staff service options – automation</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>4 Manual operations</td>
<td>REPURP</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>5 Financial transaction options</td>
<td>CONTRIB’Y</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>6 Alternative fuel source</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
</tbody>
</table>

*Table 20: Effect of hypothesised changes to local fuel supply system*

7.3.6 Effect of hypothesised modifications to targeted first-aid system

**Observations on example analysis**

The example differs from the work information example because the service delivered to the user is specific information selected from a static information storage system. Apart from the integrity of the storage system, the exposure is primarily associated with the selection and the transmission of the information, and with the systems for searching and identifying the information to be supplied. This example therefore offers a range of options for a reduction of exposure.

**Review of applicability of types of hypothetical change**

*Technological breakthrough.* The need is for a store of medical knowledge that can be searched based on symptoms. Although a colonial medical encyclopedia achieved this function, carrying such a tome is marginally impractical for the representative urban-dwelling user. The use of appropriate software and storage facilities in a mobile electronic device is possible and would avoid the exposure incurred by the communications system, although retaining the exposure associated with the mobile electronic device. Taking the hypothesising process further, it would be possible to consider a high-density portable storage system similar to the microfiche systems used in the mid–late 20th century, with a portable reader system requiring backlight and lenses only. Several other long-term and dense storage technologies have been proposed, including the Longnow Foundation’s “Rosetta” disk approach and the “1000 year storage medium” proposed by Kazansky et al. (2016).
Many media commentators and notable thinkers, including Cerf (2015), have noted that media such as DVDs may have quite short commercial lives and that, if proprietary technologies and software are required to read data from them, these technologies add to the exposure incurred by those storage media. This particular type of exposure illustrates the possibility of a “digital dark age” characterised by a lack of capacity to access large stores of information contained on media using inaccessible format or encoding systems. Both the Rosetta disk and the durable storage approach proposed by Kazansky et al. (2016) reduce this exposure.

**Technological substitution.** The use of a paper-based first-aid manual is certainly possible and, for simple first-aid issues, would represent a technology with negligible exposure.

**Semi-dynamic effects.** Limited applicability to this example.

**Re-purposable components.** Limited applicability to this example.

**Repair priority.** Limited applicability to this example.

**Standardised independent units and interfaces.** Although marginally applicable to this example, the use of standardised and open-source data formats will reduce exposure.

**Minimisation of contributory systems.** The approaches described under “technological breakthrough” are effectively approaches to avoiding exposure arising from contributory systems.

(c) **Proposal of actual hypothetical re-designed systems**

**PC hardening.** PC hardening has been proposed under the work information example and should be considered here, although these proposals now apply only at one end of the communications chain.

**PC power, router hardening, router power.** These options have been considered within the work information example. Proposal details and conclusions are identical, although they apply only to one end of the communications system.

**Local electronic storage.** Software allowing the diagnosis of first-aid issues by the individual user, and showing recommended approaches, based on locally stored electronic data and data search, is currently available. Such an approach would avoid the exposure associated with internet communications, but the local device and the associated storage and search mechanisms still contribute exposure.
**Local experts’ options.** The example has defined a representative situation in which the diagnosis and the proposed approach are obtained via an internet communication with an automated diagnostic tool, perhaps making use of an artificial intelligence technology. The proposed alternative is a telephone call to a number obtained from a hard-copied set of emergency contacts. The telephone hardware (POTS) is the only contributor to the user’s exposure, provided this is not routed through the internet.

**Local hard storage – paper.** Paper-based local storage is made practical by the static nature of the information. As long as an adequate indexing system is available, a local, static information source is quite adequate. A printed first-aid manual is hypothesised, and avoids all of the exposure sources within the described example.

**Local hard storage – Rosetta.** For the storage of static information, a book has two disadvantages – its volume-to-weight ratio is high and it has specific vulnerabilities, including damage by water, fire, insects and small children. Organisations such as the Longnow Foundation (02016) have proposed storage media that can be read using simple microscope technology; the information storage is minute images on media that are very significantly more robust than paper, specifically a metal disk encased in polycarbonate. As the technology for simple lens creation has been shown by Lee et al. (2014) to be simple, this hypothesised approach is realistic and offers an approach that requires only modest technological development, and a significant reduction in exposure.
(d) Summary of effect of hypothesised changes

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PC hardening</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>2 PC power, router hardening, router power</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>3 Local electronic storage</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>4 Local experts’ options</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>5 Local hard storage – paper</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Moderate</td>
</tr>
<tr>
<td>6 Local hard storage – Rosetta</td>
<td>TECH_NEW</td>
<td>Moderate</td>
<td>Major</td>
</tr>
</tbody>
</table>

Table 21: Effect of hypothesised changes to targeted first-aid system

7.3.7 Effect of hypothesised modifications to perishable food system

(a) Observations on example analysis

For public health reasons, pasteurisation is normally required for fresh milk, and the process and the process control requirements, particularly for homogenisation, which requires heating to a point within a closely defined temperature range and then holding for a fixed time followed by rapid chilling, have commonly led to a centralised factory approach. Similarly, as supermarket retail facilities have become the norm for common foodstuffs, these are assumed in the example. Analysis of exposure for the example shows the effects of power and staff requirements for the factory operation, the effects of refrigeration, lighting and staff facilities for the retail facility and the effects of the financial transaction function. As the product is a relatively short-shelf-life and low-value product, it is not possible to store significant volumes.

(b) Review of applicability of types of hypothetical change

Technological substitution. Alternative technologies for pasteurisation, for example UV-C irradiation, have achieved acceptance in some countries and their lower power consumption could decrease dependence on centralised factory processes if these were assumed to be accepted for the example. Storage of power for small consumption items such as cash-transaction tills and EFTPOS terminals is possible by substituting UPSs for local low-voltage power supplies. Options for the substitution of financial transaction technologies is discussed elsewhere.
**Technological breakthrough.** Considering the analysis of exposure, a breakthrough technology allowing the achievement of bacteriologically safe milk using small-scale and low-energy-use processes would allow consideration of milk sales from closer to the point of production, avoiding most of the points of exposure associated with the processing factory. Options for financial transactions and communications that require technological breakthrough are covered elsewhere.

**Semi-dynamic effects – local storage option.** There are currently no technologies that allow the storage of electrical energy at MWh levels, and that are technologically mature and close to economically viable. Such a capability would have a significant effect on the exposure of this example. However, the storage of heat and cold (ice banks, eutectic capsules) is technologically mature and capable of useful durations of storage.

**Re-purposable components.** Although the operation of factory processes could be made accessible to unskilled persons (re-purposable units), the contribution of specialised staff to the total exposure is initially small.

**Repair priority.** No options identified.

**Standardised independent units and interfaces.** Although milk tankers are designed for a single purpose, the number that are available means that these contribute little exposure. The use of containerised systems would allow further reduction.

**Minimisation of contributory systems.** A significant approach to reducing exposure is to eliminate the subsystems that contribute huge levels of exposure, specifically financial transaction systems and systems needed to provide staff facilities.

**(c) Proposal of actual hypothetical re-designed systems**

**Factory operation.** Manual operation alternatives for the factory, and provisions to allow unskilled operators to carry out functions, will allow reduction of specialised staff exposure points.

**Factory power options.** Either further duplications of the power source by using additional line feeds or fuel-operated generators would reduce the exposure associated with the power requirement, but are unlikely to be economically attractive.

**Factory power storage.** The capability to store several hours’ power supply would require a technological breakthrough – this capability is not currently
technologically available but would make a very large reduction in exposure if it were possible.

**Factory heat and cold storage.** Much energy usage in the factory, except for that used in pumping and automation, is related to the supply of heated and chilled product. Technologies for the storage of significant heat and cold (ice banks) are available and marginally economic. Even if this technology were used, it would offer limited reduction in exposure because the heating and chilling services require pumping as well as the storage of heat and cold.

**Local pasteurisation.** Factory level pasteurisation is used to achieve economies of scale, but results in a need for significant power input. It is reasonable to hypothesise lower energy pasteurisation approaches (e.g. UV-C) using solar power sources, at farm scale. Although milk standardisation would not be practical at farm scale, this is of less concern to the user than food safety, which could be achieved. The primary functions of the factory and the associated exposure can be avoided.

**Direct sale.** Assuming that farm-scale pasteurisation can be achieved, direct sales can avoid all of the exposure issues associated with the factory treatment, and the wholesale and retail systems.

**Financial transaction options.** Options for technological change and associated reductions in exposure have been treated elsewhere.

**Local storage options.** Product shelf-life limitations preclude significant local storage of the foodstuff. Refrigeration is nevertheless the main power use at the retail location and ice bank technology effectively allows local storage of “cold”, reducing the exposure to power supply continuity. The storage of power for PCs and routers, associated with the completion of financial transactions, has been covered elsewhere.

**Staff facilities options – sewage.** All the options hypothesised for a reduction of exposure of sewage systems have been considered elsewhere.
<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory operation</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>Factory power options</td>
<td>TECH_SUB</td>
<td>Moderate</td>
<td>Minor</td>
</tr>
<tr>
<td>Factory power storage</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
<tr>
<td>Factory heat and cold storage</td>
<td>TECH_NEW</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Local pasteurisation</td>
<td>TECH_NEW</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Direct sale</td>
<td>TECH_SUB</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Financial transaction options</td>
<td>CONTRIB’Y</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>Local storage options</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Minor</td>
</tr>
<tr>
<td>Staff facilities options – sewage</td>
<td>CONTRIB’Y</td>
<td>Moderate</td>
<td>Major</td>
</tr>
</tbody>
</table>

Table 22: Effect of hypothesised changes to perishable food system

7.3.8 Effect of hypothesised modifications to essential specific medicine system

(a) Observations on example analysis

The long shelf life of the raw and intermediate streams in this example allow economies of scale to be achieved by a centralised production system. These same economies of scale have made possible a highly specialised approach to the delivery of the goods to the end-user, which in turn has created a very large number of points of exposure. This is a principle that can be observed for many cases, and suggests decentralisation as a primary approach for a reduction of exposure. The high value, long shelf life and small volume of both the intermediate product and the final product suggest a primary option of local storage. Although the synthesis of salbutamol is specialised, the processes are well publicised and are within the capabilities of a moderate chemical synthesis facility. The broad tolerance of the dosage of salbutamol makes local synthesis and distribution possible within safe usage parameters.

(b) Review of applicability of types of hypothetical change

Local storage. All of the raw and intermediate streams for this product have long shelf lives, i.e. can be stored without degradation for long periods. Local storage at the input to and output from any process can therefore reduce the actual vulnerability of that process and ultimately the vulnerability of the complete...
technological systems. Local storage options are possible for the aluminium strip-stock, the bar-stock, the salbutamol synthesis feedstocks and reagents, the propellant and the packaging components. For the financial transactions (which include internet communications), the significance of small-scale power storage using available technologies has been covered under the hypothetical improvements for those subsystems. For typical industrial processes, there are currently no technologies for the storage of power at MWh levels that are technologically mature and close to economically viable. Such a capability would have a significant effect on the exposure of processes such as this.

**Technological substitution.** Within the example system, technologies for financial transactions can be substituted. These options are covered under the heading of contributory systems. Considering the end-user requirements, it is noted that salbutamol can be administered by several means (nebuliser, atomiser and intravenously) and that the safe dosage level is quite broad – hence the technological option of local synthesis, with relatively simple and/or standardised equipment and publicly available formulation and preparation information, is feasible.

**Technological breakthrough.** Small-scale, general-purpose chemical synthesis approaches have been mooted in the literature, and are possible in principle. A well-equipped chemical laboratory would be capable of synthesising salbutamol using common equipment.

**Re-purposable components.** No obvious options in addition to those stated above.

**Standardised independent units and interfaces.** Currently a small range of MDI canister sizes and configurations are produced; standardisation of these would facilitate the use of alternative manufacturing facilities for the canisters.

**Minimisation of contributory systems.** A significant approach to reducing exposure is to eliminate the subsystems that contribute large levels of exposure; these include the financial transaction system used at the retail level.

(c) **Proposal of actual hypothetical re-designed systems**

**Financial transaction option.** Financial transaction options and associated exposure reductions have been explored elsewhere.

**Local storage of empty MDI.** As the filling and packaging of MDI canisters is generally less centralised than their manufacture, a reduction in exposure can be
achieved by local stockpiling of empty MDI canisters plus metering valves and chambers.

**Local storage of diluted salbutamol.** As both salbutamol and the diluent have long shelf lives, it is possible to reduce the exposure of the complete supply system by stockpiling these at the locations at which the canisters are to be filled.

**Standardised MDI manufacture.** Currently, several sizes of MDI are made. By standardizing these (which might require adjustment of the diluent and dose numbers), the exposure from the non-availability of empty canisters, and also from incompatibility of the filling lines with available canisters, can be eliminated.

**Local major power storage.** For typical industrial processes (MWh levels), there are currently no processes for the storage of power that are technologically mature and close to being economically viable. Such a capability would have a significant effect on the exposure of processes such as this.

**Local creation of salbutamol.** Most example intermediate streams (except electrical power) have long shelf lives. Canister manufacture and filling facilities are also moderately standardised. Nevertheless, the use of a filled MDI to deliver salbutamol does involve very many specialised steps. Salbutamol can be effective via many different delivery approaches, and human tolerance to a varied dosage is high. The exposure associated with the specialised production can therefore be significantly reduced by a local creation of pure salbutamol. Although the technology for completely generic chemical synthesis is still not mature, proof-of-concept has been demonstrated and it is reasonable to examine the effect on exposure of the availability of a general-purpose synthesis technology that would allow the production of pure salbutamol from readily available feedstocks. Such a process, which is dependent only on open-source information and basic feedstocks, would eliminate all of the exposure points of this example.
(d) Summary of effect of hypothesised changes

<table>
<thead>
<tr>
<th>Measure</th>
<th>Type</th>
<th>Effort</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Financial transaction option</td>
<td>CONTRIB’Y</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>2 Local storage empty MDI</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>3 Local storage of diluted salbutamol</td>
<td>TECH_SUB</td>
<td>Minor</td>
<td>Major</td>
</tr>
<tr>
<td>4 Standardised MDI manufacture</td>
<td>INDEP’T</td>
<td>Moderate</td>
<td>Major</td>
</tr>
<tr>
<td>5 Local major power storage</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
<tr>
<td>6 Local creation of salbutamol</td>
<td>TECH_NEW</td>
<td>Major</td>
<td>Major</td>
</tr>
</tbody>
</table>

Table 23: Effect of hypothesised changes to essential specific medicine system

7.3.9 Effect of hypothesised modifications to newspaper vendor model

The “newspaper vendor” example is included in this thesis purely as an illustration of the effect of treating a simple dynamic model using the exposure theory. The exposure metric of the original model is shown to be \((4, 0, 0)\). The \(E_1\) value (4) reflects the possible failure of the input stream (papers from the newspaper producer), failure of fuel or roads to allow transport from the point of bulk supply purchase to the point of sale and non-availability of the newspaper vendor. As the model relates to a single vendor, selling a single product that is sourced from a single point, there are no contributors to \(E_2\) or \(E_3\) values (there are no combinations of two or three failures, where neither failure alone would cause output failure that would cause a service failure. The whole newspaper vendor “problem” is an operational research problem of optimising a variable (profit) under conditions of uncertain demand and fixed supply cost – a semi-dynamic effect. If the vendor could download an electronic copy of the paper, and use a local printer to generate papers as required (paying the printer only the royalty for each copy sold), the problem of predicting demand would become irrelevant, but this technological change would introduce all the technological vulnerabilities of the printing process, which include the provision of power, paper and communications to the newspaper file supplier, and would probably actually increase the exposure of the end-user. It is concluded that, assuming that only cash transactions are possible, the newspaper vendor is one of the examples that has the lowest technological exposure of all of the example studies, and it is difficult to develop
a technological solution that has lower exposure. The example almost epitomises a case where the end-user is minimally vulnerable to technological failures.

7.4 Conclusion: exposure reduction from changes to examples

This chapter has set out the results of the analyses of hypothesised changes to the technological systems described in the initial examples. The effectiveness of these changes (in terms of vulnerability reductions) will allow conclusions both on the options for reducing the vulnerability of specific systems, and also on the most general approaches to a reduction of technological vulnerability. This analysis and the summary have answered RQ(b): “For goods or services delivered to end-users, what reductions of vulnerability can be obtained by changes to the technological approach or configuration”? 
8. CONCLUSIONS

8.1 Vulnerability of end-users to existing technological systems

8.1.1 Description of vulnerability

Published definitions of “vulnerability” have been extensively examined in Chapter 2 and also Chapter 4 of this work. Significant divergence and lack of clarity among published definitions have been noted. The proposed approach to improving the precision of these definitions is to constrain the term resilience to describing the dynamic response of a functioning system to a specified perturbation. Resilience improvement measures, which are not analysed in this thesis, would then take account of the instantaneous state of all system components and the magnitude of nominated perturbations, and would assume that the system will not actually fail. Metrics of resilience would measure the response of a system, starting at a defined status, to a defined perturbation.

Once a level of service output to users is defined for a technological system, the capability of a system to deliver or fail to deliver a service can be considered. This thesis is concerned with the failure of technological systems to deliver, at identified service level, their designed outputs and the thesis scope is thus distinguished from a consideration of the resilient, dynamic response of a functional system. A recursive application of a defined service level output will also establish the nominal state of all streams and processes "upstream" of the final delivery of goods or services. This set of states, which corresponds to nominal operating conditions for the defined service level, allows a clear definition of a maximum tolerable disturbance for each stream or process variable, as the perturbation from the nominal state that will cause failure to achieve the service level output.

Having defined “resilience” in terms of described dynamic and continuous responses and having defined the scope of that term, the term “vulnerability” has been proposed to describe the combination of risk and exposure. The research question upon which this thesis is based, relates to vulnerability and, for the situation where risks are considered to have \( p = 1.0 \), the “vulnerability” of an urban dweller to the loss of a specified service can be equated with the exposure of the technological system supplying that service. The work of Chapter 4 has been to show that the proposed exposure metric is a valid measure of vulnerability.
Under these definitions, exposure is a precise antonym of robustness, noting that robustness is commonly associated with the design and configuration of a technological system, rather than the margin between design and overload performance. These definitions fall within the scope of other published definitions, whose scope in some cases is very wide, but the refined definitions allow clear distinctions to be made. The clear distinctions demonstrate both the specific contribution of this thesis and the alignment of the work of this thesis with other related works.

8.1.2 Distinctive aspects of end-user vulnerabilities and exposures

End-user vulnerabilities have several distinctive aspects: there are differences in the attribute being measured, distinctive scope elements, distinctive types of vulnerability and distinctive effects.

**Difference in what is measured.** Failure options within an infrastructural system could potentially include geographically localised failures, percentage reduction in full performance or reduced annual availability. For a supply chain, decreased capability, temporary delays in supply or the inaccessibility of an optimal route could all be considered to be possible vulnerabilities. The variety of possible definitions of infrastructural system and supply chain vulnerabilities leads to a corresponding difficulty in defining the level of exposure to failure, or the infrastructural system. The end-user’s static vulnerability is distinctively and relatively easily defined in terms of the non-availability of goods or services at a specified service level. The relatively clear definition of the vulnerability of the individual user also allows the development of a clear definition of the actual exposure of that individual to the systems providing the vulnerable services. Although many end-users may be served by a technological system, all will be subject to the same vulnerability; thus, the distinctive end-user vulnerabilities are applicable to the full complement of end-users.

**Difference in scope.** Chapters 5 and 6 of this work argue that typical and representative individual end-users are subject to a range of “exposures” in addition to those that affect the major infrastructure and typical supply chains. The scope of the technological system that supplies the end-user includes not only the "last-mile" systems that are outside common definitions of national infrastructure, but also connected and contributory subsystems.
Difference in nature. The theoretical basis of analysis has deprecated the importance of identifying specific hazards that may cause a non-availability, but has drawn attention to the effect of non-availability. The analysis has included the observation that “non-availability” can result from causes that are related more to the interface to a component than to the technological functionality of a component. In specific cases – communications systems and financial systems – it has been observed that a system can become practically unavailable to a user, as a result of unacceptable terms of use imposed by system owners. Contracts for services therefore contribute exposure because the user may be offered terms that are unacceptable, in situations where service options with acceptable terms are not available.

Difference in effect. This thesis has argued that the individual’s vulnerability is clearer, i.e. more readily defined, than the infrastructural system vulnerability. This thesis has also argued that the magnitude of the end-user vulnerability, i.e. the effect upon the user if the event to which they are vulnerable comes to pass, is qualitatively different from the magnitude of the same vulnerability for the infrastructural system owner. The non-availability of a working sewage system will force the apartment dweller to relocate, but the non-availability of a single-dwelling sewage connection will be of limited consequence to the system owner or operator. This qualitative difference justifies the focus of the thesis on the vulnerability of the end-user.

In summary, it is argued that there are a number of distinctive aspects to the end-user's exposure in regard to the supply of specific goods or services. These distinctive exposures are described and considered in this thesis.

8.1.3 Investigation of vulnerability of end-users to selected technological systems

This work has considered the effect of technological systems on an individual user, and has justified the consideration of a representative individual user, dwelling in an apartment in a city of about 200,000 to 500,000 people. For each of the examples studied, it has been shown that the lack of the goods or services supplied would force significant changes to the lives and lifestyles of the intended recipients. This is sufficient justification to study the examples, as the research question did not anticipate studying more than a selection of goods or services. However, the
examples have been selected to demonstrate a broad range of types of goods or services.

For each example studied, the technological system has been justified to be typical of that used in cities of the size proposed. As the systems studied are "typical", it is inevitable that some actual examples will have already incorporated at least some of the hypothesised changes – this does not negate the conclusions from the study of the exemplar systems and hypothesised changes.

Several technological sub-systems were considered to be sufficiently common as to warrant separate analysis. This approach also ensured identical treatment for each case where these sub-systems contributed to a studied example. Internet communications and EFTPOS financial transaction systems were considered to be standard contributory subsystems. Road systems, power supply and potable water were considered for analysis as standard contributory systems but did not appear to be sufficiently standardised across the studied examples. For an end-to-end transfer of data over the internet, an exposure metric of \( \{25, 19, 0\} \) was calculated, however, some variation is needed for systems that do not involve end-to-end international data transfer. Exposure points include "last-mile" communications issues, router and national transfer systems and international transfers via undersea cables. The commercial issues of acceptable access to ISPs also contribute to this vulnerability. An EFTPOS transaction includes interactions between an EFTPOS terminal, three banks and several communications paths, generating an exposure of \( \{49, 12, 1\} \). That exposure scope includes the power supply, standard communications and bank processes and the commercial acceptances for the parties involved in the transaction.

**Example study #1: sewage system.** The sewage evacuation and treatment system has been calculated to have an exposure metric of \( \{34, 4, 6\} \). This level of exposure considers the apartment systems, the pipework system connecting to the treatment plant, associated power supplies and control systems and the significant treatment plant systems. It is noted that the exposure of this system is significantly affected by the specification that "service" includes the treatment of sewage to an environmentally benign state.

**Example study #2: collaboratively developed work information.** The work information exchange is calculated to incur an exposure of \( \{38, 21, 2\} \), the metric being
dominated by the internet communications contribution, but also reflecting the contribution of the PC hardware, the PC software and power supplies at each end.

**Example study #3: local fuel supply.** The supply of fuel at a local petrol station is calculated to have an exposure of \{98, 20, 12\}, which reflects both dispensing functions that include pumping, control and metering systems, financial transactions, the amenity functions including water provision and sewage evacuation, which are required for a staffed facility, and the provision of bulk fuel supplies.

**Example study #4: targeted first-aid.** Obtaining a diagnosis and treatment instructions in the specific first-aid example is calculated to incur an exposure of \{23, 14, 1\}. International internet communications are not required, but local communications, a local PC and a search system for information to be returned (first-aid instructions) contribute to the total exposure.

**Example study #5: perishable food.** The supply of perishable food (fresh milk) has been calculated to have an exposure of \{128, 22, 12\}, with contributions from a financial transaction (which includes communications), the milk treatment factory (including power supply, staff, equipment and fuel), the wholesale processes, the retail facilities (including staff amenities (sewage, water and power)) and the user’s transport and local storage facilities.

**Example study #6: essential specific medicine.** The supply of a selected specific medicine has been shown to have an exposure metric of \{58, 15, 10\}. Although several specialised processes are involved, these are duplicated and moderately standardised. The user must use a financial transaction, and also a permission (a doctor’s prescription) process in order to access the medication. Clearly, these values will be specific to the selected medicine; however, the selected example has been justified as being reasonable.

This section has described the vulnerabilities of the examples studied, and on the causes of the vulnerabilities identified. As such, this section has provided interpreted answers to the first part of the research question (RQ(a)).

As all the studied examples represent items whose non-availability would have significant effects on the lifestyle of the representative individual, and have been selected to illustrate a broad variety of technological systems, the study has demonstrated that the representative apartment-dwelling end-user is significantly vulnerable to a range of technological systems.
8.1.4 End-user vulnerability to other systems

Table 6 sets out a selection of examples that could be studied, and makes the final selection. Of the candidate examples that were not studied, arguably the international travel example includes the largest range of components that are not covered in the studied examples. These include international travel permissions, several skill sets that cannot be substituted, equipment that is not duplicated, e.g. aircraft, and such items as navigation satellites. This example is mentioned as one that appears, upon superficial inspection, to incur a very high vulnerability for the end-user.

An initial examination of a small selection of other examples, such as water supply, power supply and the supply of non-perishable foods, strongly suggests that analysis would reveal very similar issues to those found in the selected examples, and in many cases the same contributory subsystems are relevant. For these reasons, it is considered that the conclusions developed for the selected examples can be applied more generally.

8.1.5 End-user vulnerability conclusion

The basis for the selection of the example technological systems is presented in Section 3.4.1. Although the research question for this thesis only requires the examination of selected systems, it is useful to consider the extent to which the selected systems are representative of other systems that supply goods or services to the target category of end-users. The target category of end-users has been described as apartment dwellers in cities of approximately 200,000 to 500,000 individuals. A broad inventory of the needs of the target group could be generated by several approaches; one such approach could involve identifying each service or stream of goods that falls within a category in the hierarchy of needs proposed by Maslow (1943). Less rigorously, it is possible to simply itemise needs starting with shelter, warmth, food, water, sanitation, the means of earning a living, mobility, communication, security for possessions and resources, including material and financial resources, storage and communication of information.

The exemplar technological systems studied in this thesis are shown to be broadly representative of the categories of needs of the target group. The short-shelf-life food example is expected to be broadly similar to many other short-shelf-life items.
such as fresh vegetables, fresh meat and fruit; each will have post-harvest treatment, packaging, wholesale and retail functions with financial transactions and the need for user transport. The sewage example is expected to be broadly similar to services such as water and power supply systems, incorporating centralised bulk supply, with progressive change and distribution, e.g. voltage breakdown for the power system, and a “last-mile” supply line, without immediate pay-for-service. This thesis has intentionally not considered long-life items such as the dwelling itself, clothing or vehicles, where the expected lifetime is significantly greater than the time required to recreate the technological system for the production of the item.

Two important conclusions can be drawn: firstly, that the studied examples are likely to be representative of other examples of goods or services supplied to the end-user, and without which the end-user is faced with significant and unwanted life-changes; secondly, that the vulnerability of the end-user to the technological systems (as measured by their exposure) is very high.

8.2 Contribution of exposure analysis approach

8.2.1 Contributions to the analysis of vulnerability

Many published studies and popular media articles include degrees of acknowledgement of the vulnerability of individuals to technological systems. Specific examples are sometimes quoted, but generalised analyses are rare. The definitions of vulnerability that are used in these studies vary considerably. Specific examples are sometimes quoted, but generalisations are rare and the term vulnerability has no definition that is well accepted, constraining or quantitative. Not only do definitions of vulnerability vary, but also the authors who supply definitions of vulnerability do not always supply definitions of other terms such as resilience, risk etc. The result is that not only are there a variety of published definitions of "vulnerability", but also these varied definitions do not align with definitions of other related terms. There is a need for a set of definitions of all common terms that preserve internal consistency and are related to the field of this thesis topic.

Section 4.7 of this thesis develops a set of definitions that are internally consistent and precise. These are necessary for the development and defense of a metric that will answer the research question. In particular, the definitions establish
that resilience may be defined in terms of a system response to a perturbation that is below a maximum tolerable level, and hence refers to a system that has not failed. This definition allows the field of study of the thesis to be clearly distinguished from the study of dynamic responses, which are outside the scope of this thesis. The definitions establish that both vulnerability and harm are indexed to a "failure to deliver" concept and are not related to the concept of "consequences of failure to deliver". The consequences of failure to deliver justify the study of the field. The definitions proposed in section 4.7 also establish that "risk" refers to the probability of a hazard occurring within a time-frame and that, within the context of this thesis, a hazard is any event that can threaten a weakness in a technological system. The description and definition of vulnerability and the indexation to an end-user enables a quantitative analysis of vulnerability.

8.2.2 Contribution from the measure of exposure

The "exposure" metric was developed within a well-defined context. The field, linked to the research question, assumes a technological system supplying goods or services to a user. A heterogeneous system consideration was essential, because the "technological system" included the creation of the goods or services rather than just the delivery. The technological system was understood to be a system that creates and finally delivers the target service or supply of goods, and hence is clearly heterogeneous. A metric relevant to the research question therefore had to be applicable to a heterogeneous system. To achieve clarity of the analytical results, it was proposed that the delivery of a single, defined service or supply of goods, to a single end-user, at a defined rate should be the basis for the analysis metric. This approach did not preclude separate analyses at different supply rates but allowed the system output to be represented by a simple yes/no variable indicating successful supply at the defined rate. The definition of a single output also allowed the scope of the technological system under consideration to be unambiguously defined. The definition of vulnerability developed in Section 4.7 of this thesis has clarified the scope of the research question and distinguishing this from any consideration of the dynamic response of the technological system. The research question is therefore also clarified to relate to static contributions of the technological systems studied. It is argued that
the clarification of these contextual principles allows a clear and valid metric to be developed.

Starting from the observation that any hazard is only such if it is aligned with a weakness, it has been argued that the number and the types of weaknesses are significant and are reasonably described as the "exposure" of a defined technological system. It has also been argued that, for either guided hazards or long time-frames, the probability of any hazard occurring approaches 1.0; hence, using the definitions from Section 4.7, "vulnerability" is measured by the supplying system's "exposure" and this exposure metric is mapped directly from the configuration of processes and streams within the technological system.

The exposure metric is refined in Chapter 4 of this thesis, by categorising weaknesses and summing them according to the number of simultaneous failures required to cause the system's output to fail. Refinements to clarify the granularity of representation are presented, and it is noted that appropriate re-drawing and representation of the Boolean expression will allow subsystems (e.g. power supplies) that affect more than one part of a technological system to be correctly represented. Many practical systems are dependent upon inputs from specialised (sub)systems; the basis for calculating the effect on the total exposure, for contributory subsystems, is developed. The effect of the contributory systems is shown (in Chapters 6 and 7) to have a major effect on the total system exposure.

Section 4.6 of this thesis considers whether the proposed quantification of "exposure" can be claimed as a valid metric to answer the research question. The validity is considered by reference to "measurement theory", and it is argued that the metric meets criteria proposed by Hand (2004). The theoretical basis for the calculation of exposure is shown to reasonably represent the issues raised in the research question, and is also shown to achieve the fundamental goals of the measurement, i.e. allowing informed decision and allowing comparison of alternative technological systems.
8.3 Reduction of vulnerability

8.3.1 Identification of options

The description of the example cases, in terms that can be translated into an exposure metric, has allowed the identification of the points, e.g. streams and processes, within the examples that contribute to the exposure metric. As the metric is demonstrably correlated with vulnerability, an inspection of the contributors to the metric clearly and quickly identifies the aspects that can most profitably be modified to reduce the end-user’s actual vulnerability. A standard set of categories of possible exposure reductions has been proposed. These are: "local storage" “technological substitution”, “technological breakthrough”, "re-purposable components", "repair priority or inherent difficulty of attack", "standardised independent units and interfaces" and "minimisation of exposure contributed by common subsystems". These categories are not shown to be exhaustive, and hence other opportunities must be considered for the elimination of each identified point of exposure. The categories are also not mutually exclusive, and overlap in their definitions. Nevertheless, the use of a standardised set of categories is helpful in identifying practical hypothetical approaches to the elimination of exposure; of equal importance, the use of standardised categories is helpful in identifying generalised conclusions.

8.3.2 Effectiveness of hypothesised approaches

This section describes notable findings resulting from the analysis of hypothesised changes to the example cases and hence summarises the answer to the second part of the research question (RQ(b)). The fresh food (milk) and the essential medicine (Ventolin™) examples illustrate the relative effects of local storage options for short- and long-shelf-life goods. For high-value, low-volume and long-shelf-life goods such as Ventolin™ MDIs, local stockpiling at a level that will allow new supply options to be identified is shown to allow a substantial reduction in exposure. For the first-aid example, the static nature of the information allows a major reduction in exposure by using local information storage. Local storage of such reference information on a common personal electronic storage device (cell phone) is quite practical, and devices allowing optical reading of dense storage, such as microfiche or the University of Southampton’s (2016) “5D glass”, allow exposure to be brought
to a very low figure for this example. The work information example describes the exchange of an editable spreadsheet via the internet and two (remote) PCs. The delivery of the "service" actually depends on standardised data formats at several levels, i.e. file formats, data packet formats and routing information formats. Exposure within this example is contributed by the internet, by each local PC and by the "last-mile" communication between the PC and a central internet system. For both petrol and fresh food, dependence on EFTPOS systems contributes significant exposure to the examples as described, and this exposure contribution can be avoided by ensuring the acceptability of other legal tender such as cash. For the time-frames considered, the raw materials (such as raw milk and bulk petrol) were, perhaps surprisingly, shown to have several alternative sources and hence did not contribute to high "E" values.

The analyses have deliberately considered some options for which practical implementations are not yet available, or where implementations are at a low level of technological maturity. Of particular note is the large reduction in exposure that would become available if large-scale storage of electrical power became feasible.

Significant reductions in exposure could also be achieved (without awaiting technological breakthrough) should the internet transition to an anonymously accessible network with increased design redundancy for such components as DNS servers and router information updating, as well as international transmission paths and widespread use of end-to-end strong encryption.

8.3.3 Development of general principles

The analysis of hypothesised changes to the example studies allows some broad principles for a reduction of end-user vulnerability to be proposed.

**Exposure is contributed by system components close to user.** Single points of failure (contributors to user $E_1$ value) commonly occur close to the point of service delivery. Although this result may be expected, it does focus attention on options for exposure reduction, and it also justifies the distinction between end-user vulnerability and national infrastructural vulnerability.

**Exposure is contributed by connected subsystems.** The study has shown, both in theory (Chapter 4) and for particular examples (Chapters 5, 6 and 7), the extent to which subsystems contribute to the total exposure value. Where some output
of a large subsystem is required in order to deliver some specific goods or services, this will contribute all of its exposure metric to the final exposure. This observation has important effects: to reduce exposure and hence end-user vulnerability, it is important to avoid creating dependence on large contributory systems, either by ensuring options for bypassing these systems or by simply avoiding their connection. There is currently much interest in an “internet of things”, which assumes multitudes of internet-connected sensors and even implanted medical devices; whatever the utility of having such devices connected, the connection contributes very large increases in the exposure of the delivery of goods and services. Considering the specific case of an implanted medical device that is essential for life, connection of the device to the internet significantly increases the exposure of the patient to failure or unplanned operation of the device.

**Exposure is contributed by dependence on large centralised systems.**

The sophistication of some technological systems, plus opportunities for achieving economies of scale, has contributed to a very marked trend for large and sophisticated technological systems to be owned and operated by corporates. These drivers may or may not still be valid but, in any case, the user seldom has options for selecting more robust and less-exposed options.

For large technological systems owned by either a public or private entity, the consequences of a failure for the owners may be orders of magnitude less than the consequences for the end-user. A commercial entity that is responsible for a complex technological system is quite likely to conclude that a level of loss-of-service for end-users is an optimal commercial position; the user’s economic resource is limited and the cost of the provision of high levels of reliability is high compared with the likely financial penalties for service failure. Commercial entities such as banks and petrol stations also have no obligation to provide facilities at all and can decide to cease to offer services or change terms of offer, on purely commercial grounds.

Alternative sources of supply of, for example, water, sewage, internet connection and power for the user may or may not be available, and are unlikely to be readily available. With the exception of civil-defense-type measures, public policy seldom considers the capacity of the individual to continue their lifestyle, on a long-term basis, without current centralised systems. By definition, a large system includes many points of weakness (even if only because the commercial viability of a large
system depends on many paying customers – undersea fiber-optic cable is a good example); therefore, it is possible to generalise a conclusion that dependence on a large and centralised system always results in large exposure for the end-user.

**Exposure tends to be decreased by use of decentralised systems.** Although many systems are highly centralised, there are notable cases where powerful components are sufficiently accessible to allow decentralisation and hence decreased exposure of users for specific services. Notable cases include three-dimensional printers, allowing the fabrication of complex objects by individuals. The Royal Society of Chemistry’s journal "Lab-on-a-chip" is devoted to disseminating developments in the field of highly integrated and portable analysis systems. Chemical unit operations are often relatively simple, and the availability of process simulation software, public information on compounds and synthesis methods does make the synthesis of complex substances possible for individuals, e.g. the synthesis of aspirin, salbutamol and Daraprim as reported by the New York Post (2016). More versatile (and less technologically mature) options for general chemical synthesis have also been proposed, e.g. a “molecular assembler” as envisioned by Drexler (2007). Taken to a logical conclusion, this trend will result in fully capable von Neumann machines as envisioned by such authors as Freitas and Merkle (2004). Although such concepts have been the diet of science fiction literature, they are actually close to technological maturity, and allow a very highly decentralised society with very low technological exposure to be envisaged. It is therefore entirely reasonable to hypothesise systems based on foreseeable technology, which enable functionality that was previously confined to national-scale systems to be available at household or suburb level. Such hypotheses show the real possibility of significantly reduced exposure of not only a representative individual but also potentially ALL such representative individuals.

**Practical unavailability contributes exposure.** Access to highly centralised systems is generally via commercial contract, and users are vulnerable to systems being practically unavailable or inaccessible because of unacceptable contractual terms. The analysis has, for example, highlighted the reduction in exposure that is possible by retaining cash-payment options rather than enforcing dependence on electronic payment systems.
Standard and re-purposable components decrease exposure. Many useful examples of standardisation, including simple mechanical and electrical components, fuel specifications etc. exist; however, the analysis has also drawn attention to the high levels of long-term exposure arising from issues such as non-standardised data storage formats, leading to the threat of a "digital dark age". It could be argued that the most versatile component of any system is the human operator, and the consideration of re-purposable components has drawn attention to the value of including options for human intervention wherever possible in a technological system. Because people can re-purpose and re-configure, their capability to intervene in a technological system offers a primary approach to decreasing exposure; at almost any point, introducing a "person" means that the criterion of "no contribution at the E_2 level" is met.

Deprecation of importance of specific nature of attacks. This study has deprecated the importance of characterising the specific nature of possible attacks upon a process or stream within a technological system; it has not even distinguished between technological and commercial failure. It is valid to consider that there is a very wide range of possible issues that can result in a process becoming effectively unavailable to the end-user. In addition to physical failure, strictly non-technological issues such as unacceptable terms of business, inevitability of unfriendly surveillance and a lack of security may be significant factors in causing the effective non-availability of a process or subsystem. The “exposure” metric can take account of such potential sources of unavailability, which contributes to its validity as a true measure of the end-user’s vulnerability.

Importance of definition of scope. The analysis of the examples and the hypothesised changes to each have emphasised the importance of carefully describing the boundaries and service levels under consideration. Applying adequate definitions of these constraints has allowed hypothesised changes to be investigated; less precise definitions would probably result in indeterminate conclusions. It has also been shown that consideration of common time-frames is essential for useful results. The petrol station example assumes the availability of bulk petrol; however, a longer time-frame could lead to consideration of a scenario where this was not necessarily available and hence contributed exposure.
8.4 Contributions of the research

The research contribution is considered under three subheadings: contribution to academia, contribution to practice and contribution to society.

8.4.1 Contribution to academia

The introduction to this work identified that a large group of persons live in urban environments, and are likely to be vulnerable to systems that are commonly used to supply essential goods and services. The work has described two distinctions between the individuals who are representative of the target group and the owners of supply chains and of national infrastructure. These distinctions are described in terms of the comparative effects of adverse outcomes, and the specific threats that may be relevant to the end-user but not to either the infrastructural owner or the supply chain owner or operator. The description of these distinctive features and the identification of a defined field of interest is considered to represent a contribution made by this work. Having established that a distinct field of study exists, specifically that the described representative end-user is vulnerable to the loss of several essential goods and services, the introduction has also established that there is a need for an analytical method for assessing the vulnerability incurred by current approaches to the supply of these services.

A number of criteria for assessing the technological contribution to end-user vulnerability have been identified, and this work has presented a tabulated assessment of the capabilities and limitations of (many) techniques appearing in the literature. The techniques considered include graph theory, risk analysis and various accumulated scoring approaches. The classification has also considered whether the techniques offer static or dynamic analyses, and whether these are applicable to systems in which a single service is transported, or where a service is progressively created from intermediate streams and a range of processes within homogeneous or heterogeneous systems. The comparison of assumptions and the fields of applicability of a diverse range of published analytical techniques (considerations of applicable time-frame, homogeneity of technological system, accuracy of definition, classification of hazards, result type and nature of input data) is considered to represent a contribution. This work has concluded that the published material has not fully or quantitatively considered the significance of the configuration of the
technological systems under consideration. This work has developed a practical approach to quantifying the exposure of a technological system and has provided a good theoretical basis for concluding that the metric is indeed a valid measure of the contribution to end user vulnerability. This is proposed to be a specific contribution to the theoretical basis of the field of study.

It has been noted that, whenever any process or stream is essential for a final delivery of goods or services, its presence is a potential locus for a hazard(s); conversely, if the necessity of a process or stream is eliminated (for example by the elimination of a contributory sub-system), then the hazards previously associated with it are no longer valid and it is no longer a potential locus for disruption or denial. This work has drawn attention to the significance of a technological system’s component, process and stream configuration, for the assessment of the end-user’s vulnerability. Ancient military wisdom noted the dangers associated with long supply chains: defining the basis for this observation and applying it to technological systems upon which people depend is considered to be a contribution.

Risk analyses commonly assess the probability of a particular hazard occurring, and sometimes identify a time-frame for that occurrence. This work has argued that, for either guided (i.e. intentionally generated) hazards or long time-frames, it is more realistic to assume that a hazard will occur, and therefore a probability of 1.0 is the reasonable value to be applied to the probability of occurrence. It is noted that there is no specific limit on the number of possible hazards that could be associated with an essential process or intermediate stream. When the probability of at least one hazard having a probability of 1.0 is assumed, then the existence of a critical locus for the hazard becomes the factor that actually determines the final vulnerability of the user.

A number of published definitions of vulnerability have been analysed; these vary considerably. Although all contain recognisable elements, there is no definition that either would be accepted as authoritative or would provide the rigour of a definition required for a quantitative analysis of a technological system.

This work has proposed that a service level be defined for each service or supply of goods to be studied. Such a definition allows a rigorous study, and does not preclude studies of more than one service level (e.g. "normal supply" and "emergency rationed supply"). Defining a service level does allow the state of the supply to be
quantified as "true" or "false". For many services, e.g. the supply of electrical power, a Boolean representation of the state of supply is obvious. However, a Boolean representation can also be applied to any nominated service level.

A technological system supplying goods or services will require inputs, and the achievement of a service level output will also require the supply of service level inputs. By applying the "service level" criteria recursively, this work has illustrated that it is possible to describe a complete technological system by a Boolean representation of all the processes and streams. The correlation between the inputs and outputs of a Boolean expression (describing an actual system) can be described and demonstrated by a "truth table" that shows the correlation between any combination of input conditions, i.e. the status of processes and input streams. The nature of the exposure metric, including the business rules such as dealing with streams that are essential at more than one location, has been defined and justified. This, together with the practical experience of application to examples, is evidence that the definition is both practical and adequately complete.

The theoretical background for this work has been developed in Chapter 4, and describes a metric of "exposure", detailing not only the rationale for the metric but also the proposed method of calculation, and the justification for using the "exposure" descriptor. It is not claimed that this approach supersedes other approaches, but it is claimed that, as it is well founded and allows the demonstration of valuable results, this represents a contribution to academia.

Starting from the assertion that end-user vulnerability is an "attribute of interest", the discipline of measurement theory has been applied to the proposed "exposure" metric, and this application has shown that the proposed metric is indeed a valid metric representing the attribute of interest. Several other theories or concepts related to personal vulnerability have been published; these include "normal accident theory" applied to complex and interlinked systems having large potential consequences, as noted by Perrow (1984), chaos and complexity theories linking small perturbations to large changes in output conditions and utilitarian theory applied to populations rather than individuals. Some less academic approaches have been proposed in specific fields – e.g. the "bus hit factor" applied to software development teams. The relationships between these approaches and the exposure analysis approach are explored and are considered to offer a contribution. Of equal
importance, the relationships between terms such as “robustness”, “survivability”, “resilience”, “fragility” and “exposure” have been explored. Although the lack of fully accepted and adequate definitions of terms precludes an unambiguous analysis, it is particularly proposed that robustness is synonymous with low levels of exposure and that a reduction in exposure can be stated to imply an increase in robustness. This in itself is considered to be a useful contribution.

8.4.2 Contribution to practice

The topic of this work is applicable to public policy, technological system design and application, and public interest. "Practitioners" can therefore be claimed to include policymakers concerned with the vulnerability of citizens and the use of public monies to decrease that vulnerability, persons engaged in the design of systems, e.g. those designing implanted medical devices and those considering the application of IoT devices, and members of the public concerned for their own vulnerability and wishing to make effective changes to it.

A "contribution to practice" will therefore assist those who "practice" in one of these fields, i.e. policymakers, designers and members of the public. The actual contribution to practice is similar for all these categories of "practitioner". It is the additional insights available, and specifically those arising from the more complete identification of the nature and numbers of contributions to vulnerability, and the analysis of the effectiveness of hypothesised changes. In the course of the investigation, a classical risk analysis was commissioned for a system identical to the exemplar sewage disposal system. Care was taken to ensure that the scope of the risk analysis was identical to the representative system, and was carried out by a professional engineer. The risk analysis did, as argued, proceed via a brainstorming of hazards without initially clarifying the nature and the interdependencies of the processes and intermediate streams that were necessary to deliver the service. The results of the analysis failed to identify specific processes whose disruption would have caused the service delivery to fail. The exercise of comparing the practice of a classical risk analysis with an analysis of exposure has demonstrated the practical gains achievable from representing the complete technological system in terms of processes, intermediate streams and interconnections and the quantification of exposure that this representation enables. A defensible approach has been set out to
define a technological system and to ensure its completeness within defined boundaries, and hence to define the processes and streams contributing to the provision of the defined services or goods. Practitioners of each type share a concern at the possibility of failures caused by hazards to un-identified vulnerabilities, despite expenditure to reduce vulnerability associated with previously identified hazards and points of exposure. A detailed consideration of exposure for the system will generate some confidence that all significant points of exposure have been identified.

The evaluation of hypothesised changes to exemplar systems (Chapter 7 of this work) has shown that changes that effect significant reductions in actual end-user vulnerability are often simple and should be relatively inexpensive. The detailed evaluation of cost was not in the scope of this study but the observation suggests a need for detailed evaluation by the practitioner. The exemplar systems analysed are representative of real systems, and hence the analyses of these specific systems do provide guidance for practitioners. As the exemplar systems also address subsystems that will be common to the systems that supply many other goods and services, the results from the analysis of hypothesised changes will have a wider validity.

The analysis of representative systems has demonstrated clearly that the vulnerability of end-users is greatly reduced by attention to the single-source-of-failure loci that are commonly found close to the point of consumption – and hence beyond the scope of more conventional analyses of infrastructural or supply chain systems. The analysis of representative systems has also drawn attention to the exposure that a technological system accrues from contributory systems. Whenever a subsystem is made essential to the function of a system, the exposure of the system is incrementally increased by the exposure metric of the contributory subsystem; this accrual can be defined mathematically. The accrual actuality can, and should, contribute to the practitioner’s design process. As a primary example, the creation of an internet-connected essential input to any process will essentially and inevitably cause the exposure of the host system to be increased by the exposure of the internet. For technological systems delivering goods or services to an end-user, the practitioner’s leaning should be that contributory systems need to be non-mandatory in every case and no more than informative. The process of hypothesising changes to the representative example systems has also proposed a set of categories of types of change. These have been shown to generate useful options, leading to the
reduction of exposure of the exemplar systems. As such, these categories of hypothetical change are proposed for practitioners.

8.4.3 Contribution to society

This work has considered the vulnerability of end-users, noting that this group has concerns and vulnerabilities that are different in nature and personal impact from those of the authorities controlling national infrastructure and the owners of supply chains or large systems. This work has further considered the particular group of end-users who live in cities, and has given particular attention to those living in apartments. The proportion of the world’s population living in an urban context increased to over 50% in 2016 and is predicted to reach 75% by 2030. The total number, and the total proportion, of users whose vulnerability is represented by this study is therefore both large and increasing. The issues contributing to the vulnerability of the end-user have been distinguished from those affecting the owners or operators of national infrastructure, and from the owners or operators of supply chains. These distinctions are primarily the large difference between the consequences of supply failure and the specific hazards that apply distinctively to the end-user. The end-user is vulnerable to significantly different consequences from the failure of a technological system supplying services: an inoperable sewage system will make an apartment uninhabitable, whereas the same failure will probably cause no direct consequences to the city authorities who are responsible for the installation and operation of the sewage system. A user who is, for whatever reason, unable to make electronic financial transactions is effectively confined to a mode of life that is very significantly different from that of others. The individual user actually has few advocates: corporates focus on profitability (revenue-to-expenditure ratio); public policy focuses on utilitarian principles (greatest good for greatest number) and assumes a continuation of major systems. With the exception of civil-defense-type measures, public policy seldom considers the capacity of individuals to continue their lifestyle, on a long-term basis, without current centralised systems. For the representative individual, there is nevertheless a significant suite of needs that, if not supplied, will require immediate, major and unwanted lifestyle changes. The user can therefore quite simplistically be described as vulnerable.
Sophisticated technological systems have commonly become centralised and of large scale, driven by the economies of scale available from mass production (the per-unit costs of production, which decrease with plant capacity) and the related technological impracticality of small-scale operation. A high-bandwidth undersea fibre-optic cable illustrates the issue well: the capital cost of such a cable can be justified only when spread across many users for many years – and there is no technology for single-user bandwidth with a pro-rata cost. Although this has been a trend since the start of the industrial age, there are significant reasons to explore options to reverse this trend: the consideration of end-user vulnerability studied in this work, is one such reason. Chapter 7 of this work has considered hypothetical changes to the example studies.

Those analyses have specifically examined change options that involve either technological breakthrough or technological substitution, and the consideration of options under these categories has shown that there are currently many examples of technological decentralisation. Manufacturing that would have required a sophisticated factory can be achieved with a garage-scope three-dimensional printer; household-scale solar power options are rapidly maturing. Other capabilities such as on-demand chemical synthesis are less mature but are under active investigation, and the analysis of the specific medicine example has illustrated the effect on the vulnerability of drug users of such capabilities. No approach to small-scale fabrication of computing components is realistic at present, and technological substitution or technological breakthrough approaches to reducing dependence on very-large-scale facilities for the production of CPU, memory etc. devices are not available. As computing elements are moderately standardised components, the very widespread availability of mass-produced units and their longevity have however reduced that associated exposure.

Within the category of technological breakthrough, the analysis of the fuel supply example has examined the option of creating in-specification motor fuel from macro-algae, at a "suburb or village" scale. This approach is technically feasible at present (i.e. the required technology exists but the fuel can be assumed to be significantly more expensive per litre than that from current supply systems). It is not within the scope of this work to examine the relationship between vulnerability reduction and acceptable cost increase but this relationship certainly exists. Although
sales of household-scale photovoltaic cells have increased markedly in New Zealand and Australia since about 2014, the full price of power from a photovoltaic system is judged to be significantly higher than that from the grid, for the foreseeable future. The analysis of actual vulnerability incurred, and the reductions available from options, should usefully inform the social question of price versus vulnerability. A facility that serves many end-users also is likely to be financed and operated by a corporate entity whose function will be to maximise ongoing financial return for that entity and hence ensuring both ongoing permission to operate with high availability. These dual requirements almost inevitably lead to the assignation of low priority to each individual user’s needs.

This work has drawn attention to the distinction between guided and random hazards. The entity who purposely determines to disable a technological system will search out processes or streams and will create hazard(s) – i.e. probability 1.0 – to target those weaknesses. This phenomenon is qualitatively different from an extreme weather event. Whether the motivation is terrorism, vandalism, or civil disobedience does not change the essential difference between a (mis)guided hazard and a random hazard. It can be observed that, for very large and near-monopolistic systems (national power, telecommunications and finance), the potential effect of disruption is very high; hence, these will be perceived as high-value targets by any contemplating disruption. This observation must be distinguished from the "normal accident theory" proposed by Perrow (1984) because it is not simply the complexity of the large system per se that is responsible for an incurred vulnerability but the attractiveness of the "target" that leads ill-wishers to expend effort on identifying weaknesses.

This work has also highlighted the issue of potential "practical non-availability", which is relevant for individual users of near-monopolistic systems. Particular fields of concern are financial and communications systems. In addition to profit-to-loss considerations, owners or operators of such systems are themselves vulnerable to statutory requirements (good or bad) and hence are likely to impose non-negotiable terms of access upon individual users. If those terms of access are unacceptable to the individual user, the service becomes practically non-available or inaccessible, and there is no certainty that an alternative system with different conditions will be available. Highlighting this issue is considered to be valuable, because such systems are increasingly common (New Zealand has one motor fuel refinery, there are only
two main EFTPOS clearing systems, there are only two undersea fibre-optic cables and there is almost monopolistic ownership of power and "last-mile" communications systems). Within a city, there is generally a single owner for sewage systems. A "practical non-availability" might occur as a result of unacceptable terms, inevitability of surveillance or lack of security. It is significant that the "exposure" metric measure is applicable regardless of the cause of the unavailability, and hence is a valid measure for the end-user.

The analysis of the example systems has shown that local power supplies and local communications systems contribute significantly to the end-user's vulnerability. Perhaps the most significant observation from the analysis of the example studies is the significant vulnerability incurred by the electronic financial transaction system, and the marked reductions in exposure that can be achieved by simple retention of cash-based systems or other systems that do not force major "contributory system" exposure values. A more general conclusion, which has been clarified by the analysis, is the end-user's vulnerability to the simple availability of services provided on a strictly commercial, rather than statutory, basis. A number of trans-national banks and national petrol retailers have recently withdrawn services from rural towns; such actions have occasioned much public outcry but have starkly clarified the fact that the banks and the petrol retailers have only one duty, which is to maximise the profit of their shareholders – they have neither obligations to communities nor even a legal "duty of care" to make services available, regardless of the consequences for end-users.

The analyses in this work have also shown many cases where an exposure point is created by the use of a single specific-purpose component such as a person with particular skills. It has been noted that, in many of these cases, simple design changes will ensure that multi-purpose components can be used, eliminating a single point of failure. For examples that include intermediate or final products that can be stockpiled, the analysis has noted both the previous work of stockpile effects on supply chain vulnerability and also the previous work by Robertson (2010). The analyses have also drawn attention to the significant cases where stockpiling is not currently technologically feasible, e.g. MWh storage of electrical power or long storage of perishable foods.
There has been a great deal of effort on the theoretical and practical approaches to minimising natural disaster effects. That work has noted that natural disasters are characterised by the disruption of multiple services that have key components within a defined geographical area. The focus of this work has been on functionally connected systems regardless of geographical proximity. Those who prepare for either natural or politico-economic disasters do anticipate the cessation of many services that are considered to be essential to their lifestyles; to this extent, the interests of the "preppers" do somewhat overlap with the concerns that have motivated this work. In contrast, this work does not assume geographically multiple failures, and has illustrated the vulnerabilities that are not strictly geographically bounded as for natural disasters.

This work has explored mathematically the relationship between the exposure values of a contributory subsystem and the exposure of the individual end-user. This conclusion has significant effects for the design of all systems that are essential to the life and lifestyle of the individual, and is of particular concern to such issues as the “Internet of Things”, implantable medical devices etc. This analysis has particularly drawn attention to the effects upon the end-user's exposure of "internet-connected" services. Explaining this example simply, in each case where a service to an end-user is made to be dependent on an internet-supplied input, the end-user's service becomes exposed to each and every locus of vulnerability on the connected internet. Attention has been drawn to cases where an individual user may effectively be unable to access a service because of quasi-technological issues (e.g. a service that routinely makes private information available to inimical users). For near-monopoly services, e.g. internet use and international banking, this could generate a situation where large numbers of users are affected, yet where it is unlikely that a pure "market forces" approach will encourage the development of an acceptable service. Current debates over the acceptability of strong end-to-end encryption are closely related to this issue. The capability of national governments to technologically prevent citizens from accessing selected internet services is another clear example of this issue.

A review of the hypothesised options for reduction of exposure has demonstrated that there is no longer any absolute need to equate sophistication of services with a high degree of centralisation and exposure. Household-scale equipment both for analysis (diagnosis) and for sophisticated fabrication are quite
foreseeable. A sophisticated and highly reconfigurable capability also offers the possibility of von Neumann machines having the capability to self-replicate, and completely obviates the economy-of-scale issues that have driven our current centralisation of services. The banking system or, more accurately, the systems for holding financial reserves and carrying out electronic (EFTPOS, online banking) transactions have been shown to contribute a very large level of vulnerability to the end-user. The study has shown the value of retaining provision for a cash- or bullion-based transaction system, specifically offering a huge decrease in exposure, and for a system such as bitcoin, which is decentralised and independent of a centralised provider. The "internet" has become essential to so many normal functions that there have been serious proposals, e.g. by La Rou (2011), to include "internet access" within a list of basic human rights; however, the capability of state and other bodies to either technologically deny access to services or to create practical unavailability by ubiquitous surveillance causes significant exposure to all user-systems reliant on the internet.

Much information used by individuals is actually relatively static. The analysis of the first-aid example illustrated a case where exposure could be realistically reduced by exchanging an online information option for a local reference source. Such an option is technologically feasible, and it is likely to be economically practical to store large volumes of non-transient information in robust formats that are directly accessible to users. Such an approach is contrary to the current trend to move all information online, and illustrates both the exposure incurred by online information sources and the reduction in exposure that is possible by local storage.

By hypothesising changes that are reliant on major technological breakthroughs, this study has also highlighted specific advances that would allow major reductions in the exposure of technological systems and the resultant end-user vulnerability. The specific examples include large-scale (MWh) electrical power storage capability, general-purpose chemical synthesis capability, general-purpose or re-purposable chemical processing capability and ad-hoc point-to-point network communications capability.
8.5 Future work

Much valuable work is beyond the scope of this thesis; this includes further development of the theoretical basis and further application of the theories. This section describes the further work that can currently be envisaged. The definition of the exposure metric means that $E_1$, $E_2$ etc. values impose limits on each other. If a system has $n$ processes plus inputs and $E_1 = m$, then $\sum(E_2..E_n) \leq 2^{(n-m)}$. It can also be observed that, if $E_n = 1$, then $E_1..E_{(n-1)} = 0$. These rules could be further developed.

An algorithm to examine each line item of a truth table and to generate the exposure values could be developed. For the real studies examined, this was not considered to be necessary. Similarly, a computerised approach to generating exposure values for a parent system, from an arbitrary combination of contributory systems, could be developed. This was also not considered to be necessary for the real studies examined. This thesis has examined the exposure of a (representative) end-user. However, in many cases (e.g. the fresh food example), the same systems supply many users and it would be possible to extend the concepts to reflect this.

Authors such as Alderson and Doyle (2010) refer p. 849 to the "new sciences of complex networks (NSCN)" and refer extensively to the learnings that technological system might derive from complex biological systems. Noting the long-term survival of biological system despite complexity and multiple threats, this must indeed be considered as a fruitful field for additional work.
REFERENCES


La Rou, Frank (2011) Within a list of basic human rights, Frank La Rou (UN Special Rapporteur) states that, “the Internet has become a key means by which individuals can exercise their right to freedom and expression.” – Report presented to General Assembly of UN. June 2011). Viewed June 2017 <http://documents.latimes.com/un-report-internet-rights/>.


Longnow Foundation’s “Rosetta” project has created an extremely durable disk containing high-density information which can be read using a microscope. Viewed May 2017 <http://rosettaproject.org/>.


Shen, Y. Nguyen, N P; Thai, M T (2011). Exploiting the robustness on power-law networks, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 6842 pp. 379-390.


Deliverable D12. (Also Technical Report DI/FCUL TR-07-26, Department of Computer Science, University of Lisbon, November 2007).


APPENDIX A: INDEPENDENT RISK ANALYSIS EXAMPLE
Project Risk Management Register
Risk analysis: Technology System

Independent Sewage System Risk Analysis

1. Introduction

An independent risk analysis on risks associated with failures within a reticulated sewage system has been undertaken for Lindsay Robertson as part of his PhD research into the extent to which technology contributes to the vulnerability (exposure) of end users. The analysis has been based on the terms of reference for Risk Analysis Technology System October 2014. The terms of reference are included as part of this report as Appendix 1.

Several approaches to the risk analysis for a sewage system were considered. The potential scope and extent of such analysis was very large given the number of components and range of risks associated each element/component of such system. It was decided that given the risk context of the analysis was to be based on a single end user, the focus of the analysis would be on probability of occurrence and consequences or impacts of any “failure” within the system as might be perceived by that end user rather than detailed risk analyses around each component of the system.

By way of context and terminology around risk management the introduction to the Australian/New Zealand Standard “Risk Management- Principles and Guidelines AS/NZS ISO 31000:2009 has been included in this report as Appendix 2.

2. Methodology

The methodology used has been a broad brush screening of risk, based on a standard risk matrix approach linking probability or likelihood of an event affecting the system component with the impact or consequence of that event on the system. to give a “risk rating” for the failure of that component. In this case the focus of the consequence of failure within this technology system in question, the sewage system, is on the end user.

As outlined in the terms of reference for this case the end user is an upper apartment dweller within a City of about 500,000 people. In terms of a time frame for the analysis it was considered that for events/failures of components within this type of technology system then a nominal 20 year time frame as the risk perception period would be adopted.

The results of the analysis are presented in the form of a project Risk Management Register with relative assessments of failure probability and associated potential impacts of the failure shown in the register along with the combined “risk rating”. The risk rating has been derived from the attached risk matrix table which gives a nominal risk rating range from low to extreme.
3. Conclusions

i) The analysis has shown that the higher risk issues will be perceived by the user at the end user end of the system with the "failures" of the system closest to the WC in the apartment. As part of the peer review of the analysis it was agreed that failures at the pump station and at the treatment plant are unlikely to impact on the end user directly and would not necessarily be perceived as a significant risk affecting his/her day to day living.

ii) The risk of failure and the impact of failure further along the system may eventually impact financially on the end user with the need for the City Council to upgrade or build in redundancies into the system. These costs will ultimately manifest themselves through an increase in the Council rates. However direct financial impact from these actions on the end user would also depend on whether the end user was a tenant or an owner.

iii) The analysis ultimately indicates there is potentially an environmental risk to the end user impacting or his/her standard of living if the treatment plant doesn't perform according design or fails to meet discharge consent standards. This environmental risk and impact on living standards is real and is reflected in the analysis, however, the actual risk as perceived by the end user will also depend on the end users perception and appreciation of the environment and standards set to protect the environment.

Brian Kouvelis; BE (Cant), Dip Mgt, FIPENZ

Sustainable Futures NZ Ltd

18 February 2015
## Project Risk Management Register

### Risk Analysis Technology System

**Sewage System Risk Analysis (Terminology refer Risk Matrix Table)**

**Risk as perceived by an upper level apartment dweller**

<table>
<thead>
<tr>
<th>Component</th>
<th>Risk</th>
<th>Description of Risk</th>
<th>Cause</th>
<th>Prob*</th>
<th>Imp*</th>
<th>Risk rating*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal flushing toilet</td>
<td>No flush</td>
<td>Lack of water supply</td>
<td>Mains water failure</td>
<td>L</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>No flush</td>
<td>Lack of water supply (planned)</td>
<td>Mains water failure</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>No flush</td>
<td>Malfunction of flush system</td>
<td>Seal, pipe, flush connection</td>
<td>L</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>Spillage in</td>
<td>WC discharge failure</td>
<td>Blockage, seal leak</td>
<td>L</td>
<td>VH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WC room</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inability to</td>
<td>WC Bowl failure</td>
<td>Broken,</td>
<td>VL</td>
<td>VH</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>use WC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gravity to</td>
<td>Pipeline</td>
<td>No flow Backflow to WC</td>
<td>Pipe broken blockage</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>pumping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>station</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gravity line</td>
<td>No flow (planned)</td>
<td>Gravity main maintenance</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>out of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>action</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pumped to</td>
<td>Pumpstation</td>
<td>Power failure</td>
<td>Various</td>
<td>L</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Treatment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>station</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pumpstation</td>
<td>Pipe blockage</td>
<td>Lack of maintenance extraneous</td>
<td>M</td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>failure</td>
<td></td>
<td>material</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pumpstation</td>
<td>Mechanical failure of pumps</td>
<td>Lack maintenance Extraneous</td>
<td>L</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td></td>
<td>failure</td>
<td></td>
<td>material</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pumpstation</td>
<td>Scheduled maintenance</td>
<td>Pump station maintenance</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>operating</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Appendix A 4
<table>
<thead>
<tr>
<th>Component</th>
<th>Risk</th>
<th>Description of Risk</th>
<th>Cause</th>
<th>Prob*</th>
<th>Imp*</th>
<th>Risk rating*</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Primary solids removal</td>
<td>Plant failure</td>
<td>Mechanical failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Power supply failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>5 Grit removal</td>
<td>Plant failure</td>
<td>Power supply failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Screen failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>6 Primary sludge extraction</td>
<td>Plant failure</td>
<td>Mechanical plant breakdown</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Power supply failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>7 Triclir Fliter</td>
<td>Plant failure</td>
<td>Plant breakdown</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Power supply failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>8 Aeration through oxidation ponds</td>
<td>Plant failure</td>
<td>Pipe blockage</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aerator breakdown</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Lack of power supply</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
</tbody>
</table>

Appendix A 5
<table>
<thead>
<tr>
<th>Component</th>
<th>Risk</th>
<th>Description of Risk</th>
<th>Cause</th>
<th>Prob</th>
<th>Imp</th>
<th>Risk rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 Sludge biogas generation</td>
<td>Plant failure</td>
<td>Mechanical breakdown</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>10 Sludge dewatering</td>
<td>Plant failure</td>
<td>Mechanical break down</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Power supply failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>11 Transport sludge to landfill</td>
<td>Transport not available</td>
<td>No transport. Storage required on site</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>12 Clarification process</td>
<td>Plant failure</td>
<td>Mechanical breakdown</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plant failure</td>
<td>Power supply failure</td>
<td>Various</td>
<td>M</td>
<td>VL</td>
<td></td>
</tr>
<tr>
<td>13 Discharge to the environment</td>
<td>Discharge quality not up to standard</td>
<td>Damage to the receiving environment</td>
<td>Various</td>
<td>M</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pipe blockage</td>
<td>Overflow to adjacent land. Damage to the environment</td>
<td>Various</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>
## Risk Matrix Table

<table>
<thead>
<tr>
<th>Likelihood of Occurrence</th>
<th>Consequence</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likely</td>
<td>Critical</td>
<td>Medium</td>
</tr>
<tr>
<td>Likely</td>
<td>Critical</td>
<td>High</td>
</tr>
<tr>
<td>Likely</td>
<td>Critical</td>
<td>Extreme</td>
</tr>
<tr>
<td>Likely</td>
<td>Critical</td>
<td>Almost Certain</td>
</tr>
<tr>
<td>Possible</td>
<td>Major</td>
<td>Medium</td>
</tr>
<tr>
<td>Possible</td>
<td>Major</td>
<td>High</td>
</tr>
<tr>
<td>Possible</td>
<td>Major</td>
<td>Extreme</td>
</tr>
<tr>
<td>Possible</td>
<td>Major</td>
<td>Almost Certain</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Moderate</td>
<td>Medium</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Moderate</td>
<td>Extreme</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Moderate</td>
<td>Almost Certain</td>
</tr>
<tr>
<td>Rare</td>
<td>Minor</td>
<td>Medium</td>
</tr>
<tr>
<td>Rare</td>
<td>Minor</td>
<td>High</td>
</tr>
<tr>
<td>Rare</td>
<td>Minor</td>
<td>Extreme</td>
</tr>
<tr>
<td>Rare</td>
<td>Minor</td>
<td>Almost Certain</td>
</tr>
</tbody>
</table>

### Risk Ranks / Level of Risk

- **Low**: While further assessment may not be required, risk should be monitored. Typically managed at operational level using routine procedures.
- **Medium**: While further assessment may not be required, control evaluation should be undertaken and monitored. Also typically managed at operational or tactical level.
- **High**: Further assessment including control evaluation is required. Senior management review is necessary with escalation to Executive management (if required).
- **Extreme**: Immediate action is required including the attention of senior and executive management.

---

**Risk Management Table Terminology Cross Referencing to the Project Risk Management Register and the Sewage System Risk Analysis**

<table>
<thead>
<tr>
<th>Probability (Prob) = Likelihood</th>
<th>Impact (Imp) = Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability / Likelihood Ratings</td>
<td>Impact/Consequence Ratings</td>
</tr>
<tr>
<td>Very Low (VL) = Rare</td>
<td>Very Low (VL) = Insignificant</td>
</tr>
<tr>
<td>Low (L) = Unlikely</td>
<td>Low (L) = Insignificant</td>
</tr>
<tr>
<td>Medium (M) = Possible</td>
<td>Medium (M) = Insignificant</td>
</tr>
<tr>
<td>High (H) = Likely</td>
<td>High (H) = Insignificant</td>
</tr>
<tr>
<td>Very High (VH) = Almost Certain</td>
<td>Very High (VH) = Insignificant</td>
</tr>
</tbody>
</table>

---

Appendix A 7
Appendix 2

Risk Management Principles and Guidelines

INTRODUCTION

Organizations of any kind face internal and external factors and influences that make it uncertain whether, when and the extent to which they will achieve or exceed their objectives. The effect this uncertainty has on the organization’s objectives is “risk”.

All activities of an organization involve risk. Organizations manage risk by anticipating, understanding and deciding whether to modify it. Throughout this process they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk. This Standard describes a systematic and logical process in detail.

This is a new standard for managing risk that supersedes AS/NZS 4360:2004. It builds upon the processes contained in the superseded standard.

While all organizations manage risk to some degree, this Standard establishes a number of principles that need to be satisfied before risk management will be effective. This Standard recommends that organizations should have a framework that integrates the process for managing risk into the organization’s overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied across an entire organization, to its many areas and levels, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors to meet diverse needs, the adoption of consistent processes within a comprehensive framework helps ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this Standard is shown in Figure 1.

When implemented and maintained in accordance with this Standard, the management of risk enables all organizations to, for example—

(a) increase the likelihood of achieving objectives;
(b) encourage proactive management;
(c) be aware of the need to identify and treat risk throughout the organization;
(d) improve the identification of opportunities and threats;
(e) achieve compatible risk management practices between organisations and nations;
(f) comply with relevant legal and regulatory requirements and international norms;
(g) improve financial reporting;
(h) improve governance;
(i) improve stakeholder confidence and trust;
(j) establish a reliable basis for decision making and planning;
(k) improve controls;
(l) effectively allocate and use resources for risk treatment;
(m) improve operational effectiveness and efficiency;
(n) enhance health and safety performance as well as environmental protection;
(o) improve loss prevention and incident management;
(p) minimize losses;
(q) improve organizational learning; and
(r) improve organizational resilience.

This Standard is intended to meet the needs of a wide range of stakeholders including—

(i) those accountable for achieving objectives and therefore ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;
(ii) those responsible for developing risk management policy within their organization;
(iii) those who need to evaluate an organization effectiveness in managing risk; and
(iv) developers of standards, guides, procedures, and codes of practice that in whole or in part set out how risk is to be managed within the specific context of these documents.

Organizations with existing risk management processes can use this Standard to critically review, align and improve their existing practices. Those whose risk management framework has been based on AS/NZS 4360:2004 will thereby benefit from the additional concepts and practices in this Standard.

In this Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, and “managing risk” refers to applying that architecture to particular risks.
Figure 1 — Relationships between the risk management principles, framework and process
RISK ANALYSIS: TECHNOLOGY SYSTEM

Document control
Version 1
Created 11 Sept 2014  Updated 2 Oct 2014
Lindsay Robertson

Abstract
This document sets out the terms of reference for the group/person carrying out a risk analysis. The terms clarify the nature and the scope of the system whose output (service to the end user) may fail (i.e., is at risk).

Description of system
General
The system under consideration is the sewage system, typical for a city of > 200,000 residents, and defined in terms of the effect on a single end-user.

Components
The system under consideration has the following components:
• Normal flushing toilet
• Gravity fed to pumping station
• Pumped to treatment location
• Primary solids removal
• grit removal (electric power, mechanical screening)
• primary sludge extraction
• trickle filter minimal power
• Aeration/oxidation ponds
• sludge biogas generation and power generation.
• Sludge dewatering and transport to landfill
• Clarification of oxidised settled waste
• clarified discharge to environment

Scope inclusions
• the point where environmentally benign (in terms of BoD, CoD, coliforms) streams originating from the sewage are released to the environment.
• The point where multiple water sources are available without obvious common failure modes.
• The point where control systems are available with multiple routes and no obvious common mode failure points
• human operators where needed for control in the "operational" timeframe.

Scope exclusions
• Landfill disposal for treated solid waste
• Diesel supply beyond bulk storage tanks at local filling stations
• Assume that national grid is live, but consider power supplies to treatment plant as separate from supplies to apartment (potable water pumping), and to local pumping stations

Analysis required
The risk context is the single end-user, living on one of the upper floors of an apartment building, within central district of a city of about 500,000 persons.
The risk is to the end-user, from non-availability of the capability to dispose of sewage as required.
The group is request to consider the risks (to the user, and with the nominated context and system scope) using the practices and techniques of risk assessment that would normally be considered as good engineering practice, and generally aligned with the principles set out in ISO 31000:2009.

Deliverables
A risk analysis (risk register) IS needed but consideration of risk remediation options is NOT needed.

Appendix A 11
APPENDIX B: EXAMPLE ANALYSES
<table>
<thead>
<tr>
<th>Subsystem/Function</th>
<th>Gate #</th>
<th>Varname</th>
<th>Long Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intact file at local machine</td>
<td>001</td>
<td>L_003</td>
<td>Valid_packet_on_I/O_router_port</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_005</td>
<td>Local_operational_household_router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_007</td>
<td>Consumer (230V, single phase) power</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_008</td>
<td>File_from_local_DSLAM_router</td>
</tr>
<tr>
<td>File transferred from ISP to home</td>
<td>002</td>
<td>L_008</td>
<td>File_from_local_DSLAM_router</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_055</td>
<td>Disable_DSLAM_router_to_household_router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_056</td>
<td>DSLAM_router_multiplexer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_058</td>
<td>DSLAM_router_power</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_057</td>
<td>File_available_at_ISP_end_of_DSLAM_router</td>
</tr>
<tr>
<td>File transferred from peering point to ISP POP</td>
<td>003</td>
<td>L_057</td>
<td>File_available_at_ISP_end_of_DSLAM_router</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_060</td>
<td>ISP_POP_router_FO_to_DSLAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_011</td>
<td>Local_functional_POP_router</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_012</td>
<td>Local_250VAC_to_POP_router</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_013</td>
<td>Local_POP_router_Fo</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_014</td>
<td>Local_POP_router_OS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_015</td>
<td>Local_POP_router_storage</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_016</td>
<td>Local_POP_router_app</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_017</td>
<td>Local_POP_router_DNS_lookup</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_061</td>
<td>File_from_peering_point_router</td>
<td>1</td>
</tr>
<tr>
<td>File transferred from NAP to peering point</td>
<td>004</td>
<td>L_061</td>
<td>File_from_peering_point_router</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_053</td>
<td>Peering_point_power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_054</td>
<td>Peering_point_power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_054</td>
<td>Peering_point_power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_019</td>
<td>Local_FO_link_peer_point_NAP_router</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>L_020</td>
<td>File_from_local_NAP_router (undersea link)</td>
</tr>
</tbody>
</table>

**TOTAL for trans-national**

|                      | 1 7 0 |

File transferred across T1 links

<table>
<thead>
<tr>
<th></th>
<th>E1 E2 E3</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND L_020 File_from_local_NAP_router (undersea link)</td>
<td>1 5</td>
</tr>
<tr>
<td>AND L_025 T1_link</td>
<td>2</td>
</tr>
<tr>
<td>AND L_024 File_from_remote_NAP_router</td>
<td>1 5</td>
</tr>
<tr>
<td>AND L_049 T1_link_routers</td>
<td>2</td>
</tr>
<tr>
<td>AND L_050 T1_link_power</td>
<td>2</td>
</tr>
</tbody>
</table>

Appendix B 2
<table>
<thead>
<tr>
<th>Function</th>
<th>Code</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction completed at EFTPOS</td>
<td>031</td>
<td>I_001 Accept_transaction_msg_at_terminal</td>
<td>1</td>
</tr>
<tr>
<td>terminal</td>
<td></td>
<td>AND I_002 Local_power_to_EFTPOS_terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND I_003 Terminal_processor_operational</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND I_004 EFTPOS_keyboard_operational</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND I_005 EFTPOS_cardreader_operational</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND I_009 Accept ILOCAL_message_from_acquirer_bank</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND I_007 EFTPOS_terminal_display_operational</td>
<td></td>
</tr>
<tr>
<td>Comms EFTPOS to acquirer</td>
<td>002</td>
<td>Accept ILOCAL_message_from_acquirer_bank</td>
<td>1</td>
</tr>
<tr>
<td>Acquirer bank acceptance</td>
<td></td>
<td>AND Acquirer_bank_accept</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Acquirer_bank_power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Acquirer_bank_processor</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Acquirer_bank_NAS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_bank_SW_DS_operational</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_bank_accept_msg</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Merchant_accept_acquirer_conditions</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Acquirer_funds_to_Merchant</td>
<td>1</td>
</tr>
<tr>
<td>Comms acquirer banks to user bank</td>
<td>033</td>
<td>User_bank_accept_msg</td>
<td>1</td>
</tr>
<tr>
<td>User bank acceptance</td>
<td></td>
<td>AND User_valid_bank_account</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_accept_account_conditions</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_bank_power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_bank_processor</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_bank_NAS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND User_bank_SW_DS_operational</td>
<td>1</td>
</tr>
<tr>
<td>Comms acquirer to merchant bank</td>
<td>004</td>
<td>Acquirer_funds_to_Merchant</td>
<td>1</td>
</tr>
<tr>
<td>Funds to Merchant bank</td>
<td></td>
<td>AND Merchant_bank_power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Merchant_bank_processor</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Merchant_bank_NAS</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Merchant_bank_SW_DS_operational</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Merchant_valid_bank_account</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND Merchant_accept_account_conditions</td>
<td>1</td>
</tr>
<tr>
<td>Subsystem/function</td>
<td>Gate #</td>
<td>Varname</td>
<td>Sewage system</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>---------</td>
<td>---------------</td>
</tr>
<tr>
<td>Apartment systems</td>
<td>001</td>
<td>AND 3</td>
<td>Domestic water supply at building</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND 68</td>
<td>Domestic water at apt booster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND 2</td>
<td>Commercially open elec A/C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND 70</td>
<td>Apt Booster control signal</td>
</tr>
<tr>
<td>WC at apartment</td>
<td>13</td>
<td>Functioning sewage system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>AND 14</td>
<td>#Domestic water supply at cistern</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>AND 2</td>
<td>Local cistern ball valve</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>AND 70</td>
<td>Sewer connection at apartment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND 3</td>
<td>Commercially open elec A/C</td>
</tr>
<tr>
<td>Gravvy feed to first pump stn</td>
<td>002</td>
<td>18</td>
<td>Sewer connection at apartment</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>AND 12</td>
<td>Physical integrity to pump input</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>AND 1</td>
<td>Functional pumphouse systems</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>AND 11</td>
<td>3 Phase supply at pumphouse</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>AND 11</td>
<td>Pump discharge capability</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>AND 19</td>
<td>Functional control signal comms</td>
</tr>
<tr>
<td>Functional pumphouse systems</td>
<td>003</td>
<td>12</td>
<td>Functional pumphouse systems</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>OR 7</td>
<td>Functional pump A system</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>OR 11</td>
<td>Functional pump B system</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>AND 4</td>
<td>Functional pump A</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>AND 5</td>
<td>Functional pump A control</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>AND 6</td>
<td>Functional pump A control valve</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>AND 8</td>
<td>Functional pump B</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>AND 9</td>
<td>Functional pump B control</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>AND 10</td>
<td>Functional pump B control valve</td>
</tr>
<tr>
<td>Pump stn discharge to treat't stn</td>
<td>20</td>
<td>20</td>
<td>Bulk sewage at input to treatment station</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>AND 21</td>
<td>Pipework from pump to treatment station</td>
</tr>
<tr>
<td>Treatment station</td>
<td>004</td>
<td>22</td>
<td>Solids to truck</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>24</td>
<td>Functional solids screen</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>26</td>
<td>Treatment stn motor power supply</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>26</td>
<td>Functional screen discharge screw motor</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>26</td>
<td>Functional truck removal system</td>
</tr>
<tr>
<td>Grit removal (coarse screen)</td>
<td>26</td>
<td>26</td>
<td>Functional truck removal system</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>31</td>
<td>Functional grit removal air blower</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>24</td>
<td>Functional grit removal auger</td>
</tr>
<tr>
<td>Sedimentation output to trickle filter</td>
<td>34</td>
<td>34</td>
<td>Discharge to trickling filter</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>34</td>
<td>pump to trickling filter</td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>34</td>
<td>Treatment station power distrib system</td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>34</td>
<td>Treatment stations functional SCADA</td>
</tr>
<tr>
<td></td>
<td>38</td>
<td>34</td>
<td>Functional pipework to trickling filters</td>
</tr>
<tr>
<td>Trickle filter (a)</td>
<td>38</td>
<td>38</td>
<td>Filter output to contact tanks</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>28</td>
<td>Treatment station power distrib system</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>28</td>
<td>Trickling filter distributor motor</td>
</tr>
<tr>
<td>Trickle filter (a)</td>
<td>39</td>
<td>39</td>
<td>Filter sludge output</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>28</td>
<td>Treatment station power distrib system</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>28</td>
<td>Trickling filter distributor motor</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>44</td>
<td>Air to trickling filter</td>
</tr>
<tr>
<td>Contact tanks -Aeration/oxidation ponds</td>
<td>41</td>
<td>41</td>
<td>Low BOD stream to clarifier</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>28</td>
<td>Treatment station power distrib system</td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>42</td>
<td>Aeration chambers</td>
</tr>
<tr>
<td>Odour control</td>
<td>44</td>
<td>44</td>
<td>Air to trickling filter</td>
</tr>
<tr>
<td>AND</td>
<td>28</td>
<td>Treatment station power distrib system</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>45</td>
<td>Air pump for de-odorising</td>
<td></td>
</tr>
<tr>
<td>Clarification of oxidised settled waste</td>
<td>46</td>
<td>Clarified stream</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>28</td>
<td>Treatment station power distrib system</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>48</td>
<td>Clarifier rotor motor</td>
<td></td>
</tr>
<tr>
<td>Clarification of oxidised settled waste</td>
<td>47</td>
<td>Clarifier sludge</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>28</td>
<td>Treatment station power distrib system</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>48</td>
<td>Clarifier rotor motor</td>
<td></td>
</tr>
<tr>
<td>Power connection (supply and discharge)</td>
<td>27</td>
<td>Treatment stn bulk power supply</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>28</td>
<td>Treatment station power distrib system</td>
<td></td>
</tr>
<tr>
<td>Comms/SCADA/control system internal</td>
<td>66</td>
<td>Operational SCADA system</td>
<td></td>
</tr>
<tr>
<td>Treatment stn power dist'n system</td>
<td>24</td>
<td>Treatment stn motor power supply</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>28</td>
<td>Treatment station power distrib system</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>27</td>
<td>Treatment stn bulk power supply</td>
<td></td>
</tr>
<tr>
<td>Power system operator</td>
<td>55</td>
<td>Skilled operator - Power</td>
<td></td>
</tr>
<tr>
<td>Equipment operator</td>
<td>56</td>
<td>Skilled operator - digester/filter/clarifier</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>67</td>
<td>Transport fuel (petrol)</td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>62</td>
<td>Roading system</td>
<td></td>
</tr>
</tbody>
</table>

| Sludge digestion and cogeneration | 005 | 51 | Sludge treatment and pumping to digester |
| AND | 47 | Clarifier sludge |
| AND | 52 | Sludge pipework system |
| AND | 54 | Biogas supply |
| AND | 55 | Skilled operator - Power |
| AND | 56 | Skilled operator - digester/filter/clarifier |

| Discharge to landfill, environment | 006 | 58 | Dewatered sludge |
| AND | 64 | Sludge dewatering plant |
| AND | 28 | Treatment station power distrib system |

| clarified discharge to environment | 49 | Pipework to discharge |
| AND | 46 | Clarified stream |

| Sludge transport to Landfill | 65 | Dumped sludge |
| AND | 59 | Truck |
| AND | 60 | Transport fuel (diesel) |
| AND | 61 | Truck driver |
| AND | 62 | Roading system |
| AND | 63 | Operational landfill |

Sludge landfill

[[ No longer needed ]]
<table>
<thead>
<tr>
<th>Subsystem/function</th>
<th>Gate #</th>
<th>Varname</th>
<th>Work Info</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fineal doc (spreadsheet) on screen</td>
<td>001</td>
<td>0.001</td>
<td>Spreadsheet on screen</td>
<td>E1: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.002</td>
<td>Functional PC hardwaro</td>
<td>E2: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.003</td>
<td>PC_local_Power_supply</td>
<td>E3: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.004</td>
<td>Functional PC_Os</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.005</td>
<td>Functional PC file display app</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.008</td>
<td>Functional PC email_client</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.023</td>
<td>Packets to/from local router</td>
<td></td>
</tr>
<tr>
<td>Power supply (to PC and router)</td>
<td>002</td>
<td>0.033</td>
<td>PC_local_Power_supply</td>
<td>E1: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.008</td>
<td>Local household wiring</td>
<td>E2: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.009</td>
<td>Local 240V distro sys</td>
<td>E3: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.010</td>
<td>Local substation_transformer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.011</td>
<td>Local grid power supply</td>
<td></td>
</tr>
<tr>
<td>Functional household router</td>
<td>003</td>
<td>0.023</td>
<td>Packets to/from local router</td>
<td>E1: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.024</td>
<td>Functional router</td>
<td>E2: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.003</td>
<td>PC_local_Power_supply</td>
<td>E3: 1</td>
</tr>
<tr>
<td>Comms subsystem (Internet)</td>
<td></td>
<td>[Comms from user router to Internal link]</td>
<td>12: 6: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Comms from Internal link]</td>
<td>1: 7: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Comms from remote router to Internal link]</td>
<td>12: 6: 0</td>
<td></td>
</tr>
</tbody>
</table>

Remote end is mirror image of user end.
<table>
<thead>
<tr>
<th>Subsystems/function</th>
<th>Gate #</th>
<th>G_Type</th>
<th>Vname</th>
<th>Petrol station example</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Petrol station forecourt</td>
<td>001</td>
<td></td>
<td>I_003 Petrol_dispersed</td>
<td></td>
<td>E1: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_002 Petrol_station_pumps</td>
<td></td>
<td>E2: 1</td>
</tr>
<tr>
<td>Local power supply</td>
<td>006</td>
<td></td>
<td>I_017 Service_stn_local_400V_3Ph_power</td>
<td></td>
<td>E3: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_016 Grid_power_available</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_017 HV_lines_operational</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_012 Substation_operational</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_018 Local_MV_lines_operational</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pump control and flow measurement</td>
<td>003</td>
<td></td>
<td>I_002 Pump_flow_metering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_005 Pump_flow_measurement</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_004 Display_total_I_$_</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_006 Service_stn_local_400V_3Ph_power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Petrol station staff</td>
<td>004</td>
<td></td>
<td>I_013 Forecourt_staff_available</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_014 Forecourt_staff</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_016 Local_road_network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_012 Local_staff_vehicles</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_017 Service_stn_local_400V_3Ph_power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Petrol station transaction</td>
<td></td>
<td></td>
<td>I_019 Service_station_transaction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk petrol supply to station</td>
<td>005</td>
<td></td>
<td>I_021 Bulk_supply_to_station</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_006 Tanker_driver</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_016 Local_road.Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_012 Tanker_operational</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_017 Bulk_petrol_available</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_018 Diesel_forTanker</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_017 Bulk_fuel_transaction</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AND</td>
<td>I_017 Bulk_fuel_processing_dispatch_power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk fuel production</td>
<td>006</td>
<td></td>
<td>I_006 Bulk_petrol_available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subsystem/Function</td>
<td>Gate #</td>
<td>Varname</td>
<td>Long Name</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>--------------------------</td>
<td>------------------------------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Use communications system</td>
<td>001</td>
<td>1_001</td>
<td>Net_connected_router</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_002</td>
<td>PC_local_power_supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_003</td>
<td>Functional_local_PC_hardware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_004</td>
<td>Functional_local_PC_OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_005</td>
<td>Workable_interactive_web_browser/connection</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_006</td>
<td>Responsive_FA_app</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Power supply (to PC and router)</td>
<td>002</td>
<td>1_001</td>
<td>PC_local_power_supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_002</td>
<td>Local_house_wiring</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_003</td>
<td>Local_dist_wiring</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_004</td>
<td>Local_substation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_005</td>
<td>Grid_supply</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Functional household router</td>
<td>003</td>
<td>1_001</td>
<td>Workable_interactive_web_browser/connection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_002</td>
<td>Functional_local_PC_hardware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_003</td>
<td>Functional_local_PC_OS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet services</td>
<td></td>
<td>1_001</td>
<td>Continue_to_international_system</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_002</td>
<td>International_communication</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Diagnosis and identification of advice</td>
<td>003</td>
<td>1_001</td>
<td>Responsive_FA_app</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_002</td>
<td>Functional_remote_PC_hardware</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_003</td>
<td>Functional_remote_PC_OS</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_004</td>
<td>Functional_remote_FA_app</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_005</td>
<td>Remote_PC_power_supply</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1_006</td>
<td>Functional_remote_power_supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subsystem/Function</td>
<td>Gate #</td>
<td>Varname</td>
<td>Description</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>--------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Refrigeration</td>
<td>017</td>
<td>60</td>
<td>End-user refrigerated storage</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>61</td>
<td>Power supply to end-user refrigeration</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>79</td>
<td>User refrigerator</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>57</td>
<td>End-user transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer transport</td>
<td>016</td>
<td>57</td>
<td>End-user transport</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>68</td>
<td>Petrol for end-user transport</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>59</td>
<td>Roadway access for end-user</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>52</td>
<td>Supermarket chilled storage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Retail transaction system**

<table>
<thead>
<tr>
<th>Retail outlet functions</th>
<th>015</th>
<th>50</th>
<th>Supermarket chilled storage</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>53</td>
<td>Supermarket power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>54</td>
<td>Supermarket stackers</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>55</td>
<td>Supermarket checkout operators</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>51</td>
<td>Chilled consumer packs delivered to supermarket</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>60</td>
<td>Supermarket staff facilities</td>
<td></td>
</tr>
<tr>
<td>Retailer staff facilities</td>
<td>90</td>
<td>61</td>
<td>Supermarket sewage disposal</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>62</td>
<td>Supermarket potable water</td>
<td>6</td>
</tr>
</tbody>
</table>

**Transport to retail outlet**

| Transport to retail outlet | 014 | 51 | Chilled consumer packs delivered to supermarket | 1 |
|                           |     | 50 | Chilled wholesale storage                        | 1 |
|                           |     | 15 | Operational roadways system                      | 1 |
|                           |     | 14 | Diesel fuel                                      | 1 |
|                           |     | 77 | Operational outershale                           | 1 |
|                           |     | 76 | Truck (outershale) driver                        | 1 |

**Raw Milk processing**

<table>
<thead>
<tr>
<th>Filtration and pasteurisation into pasteurised milk vat - regulatory requirement, no bypass</th>
<th>33</th>
<th>Pasteurised and chilled milk</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>26</td>
<td>Raw milk to pasteuriser</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>Operational pasteuriser PHE</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>Operational pasteuriser system (holding, pump etc)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>Hot water supply</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>37</td>
<td>Chilled water supply</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>Factory power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>Factory CIP automation (valves, bypasses)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>Factory automation system</td>
<td>1</td>
</tr>
</tbody>
</table>

**Standardisation (optional bypass)**

<table>
<thead>
<tr>
<th>Standardisation (optional bypass)</th>
<th>72</th>
<th>Pasteurised and standardised milk</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>71</td>
<td>Operational cream storage packaging system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>38</td>
<td>Operational separator</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>39</td>
<td>Operational metering system for cream</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>Standardised milk storage</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>71</td>
<td>Operational cream storage packaging system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Factory automation system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>Factory power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>Factory CIP system</td>
<td>1</td>
</tr>
</tbody>
</table>

**Processing CIP system (CIP solutions needed within the operational timeframe)**

<table>
<thead>
<tr>
<th>Processing CIP system (CIP solutions needed within the operational timeframe)</th>
<th>41</th>
<th>Factory CIP system</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>42</td>
<td>Factory CIP keftes</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>Factory CIP chemicals</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>Factory CIP automation (valves, bypasses)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>36</td>
<td>Hot water supply</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>Operational CIP waste treatment and discharge</td>
<td>1</td>
</tr>
</tbody>
</table>

**Bottle-filling system (takes PET bottles as Input)**

<table>
<thead>
<tr>
<th>Bottle-filling system (takes PET bottles as Input)</th>
<th>76</th>
<th>Milk in consumer packages</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>45</td>
<td>Factory bottle filling machine</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>73</td>
<td>Pasteurised and standardised milk</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>46</td>
<td>PET bottle supply</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Factory automation system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>Factory power</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>Operational CIP waste treatment and discharge</td>
<td>1</td>
</tr>
</tbody>
</table>

**Refrigerated storage for filled consumer packs**

<table>
<thead>
<tr>
<th>Refrigerated storage for filled consumer packs</th>
<th>50</th>
<th>Chilled wholesale storage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>48</td>
<td>Forklift</td>
<td>1</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td>Cost Code</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>AND</td>
<td>49 Forlift operator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>70 Milk in consumer packages</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Hot water system</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>018</td>
<td>36 Hot water supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>63 Operational factory hot water boiler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>62 Fuel for factory hot water system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Chilled water system</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>019</td>
<td>37 Chilled water supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>70 Operational factory chilled water system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cream holding and dispatch system</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>020</td>
<td>71 Operational cream storage packaging system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Factory CIP waste treatment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>021</td>
<td>32 Operational metering system for cream standardisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Processing facility power distribution</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>022</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>65 Processing facility power distribution system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>66 Processing facility bulk power supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>68 Operational factory transaction system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Raw milk collection system</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>004</td>
<td>15 Chilled bulk milk delivery to processing plant reception</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>11 Operational milk tanker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>12 Tanker driver</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>13 Operational roading system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>14 Diesel fuel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>15 Tanker electronic metering system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>7 Chilled raw milk: farm terminal point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>17 Payment to Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>9 Form CIP chemical supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>3 Power supply at milking shed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Metering and billing system</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Testing system - raw milk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Payment to Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>18 Operational central banking system</td>
<td></td>
<td>??</td>
</tr>
<tr>
<td>AND</td>
<td>19 Milk purchaser billing and recording system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>20 Milk purchaser administration staff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>21 Milk quality verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>22 Laboratory technician</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>25 Operational laboratory equipment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>24 Laboratory consumables</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Raw milk receipt and storage</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Raw milk to pasteuriser</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>15 Chilled bulk milk delivery to processing plant reception</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>31 Operational CIP system (valves/sprayballs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>21 Milk quality verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>29 Tanker and reception CIP chemicals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>30 Tanker and reception CIP lattices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>28 Factory automation system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>32 Operational CIP waste treatment and discharge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AND</td>
<td>64 Factory power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subsystem/function</td>
<td>Gate #</td>
<td>Varname</td>
<td>Medicine example</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>--------</td>
<td>---------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>User acquisition of functional MDI</td>
<td>001</td>
<td>L_001</td>
<td>User Owned Functional Inhaler</td>
</tr>
<tr>
<td>[financial transaction]</td>
<td></td>
<td>L_002</td>
<td>Functional Inhaler retail stock</td>
</tr>
<tr>
<td>[prescribing]</td>
<td></td>
<td>L_003</td>
<td>Inhaler purchase transaction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_004</td>
<td>Inhaler_permisssion_to_purchase</td>
</tr>
<tr>
<td>Functional inhaler in retail stock</td>
<td>002</td>
<td>L_002</td>
<td>Functional Inhaler retail stock</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_005</td>
<td>Bulk Inhaler local supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_008</td>
<td>Local Roading</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_007</td>
<td>Local Vehicle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_008</td>
<td>Local Driver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_008</td>
<td>Local Warehousing</td>
</tr>
<tr>
<td>Filling packaging and distribution</td>
<td>003</td>
<td>L_005</td>
<td>Bulk Inhaler local supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_009</td>
<td>Bulk Inhaler supply assembled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_010</td>
<td>International Transport</td>
</tr>
<tr>
<td>Filling and packaging of inhaler</td>
<td>004</td>
<td>L_009</td>
<td>Bulk Inhaler supply assembled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_011</td>
<td>Operational filling plant</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_012</td>
<td>Quality assured active ingred</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_013</td>
<td>Quality assured propellant</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_014</td>
<td>Bulk Inhaler bodies_unfilled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_015</td>
<td>Inhaler_packing Bulk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_016</td>
<td>Assembly Plant Power supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_017</td>
<td>Assembly Plant Staff</td>
</tr>
<tr>
<td>Manufacture of container and distribution</td>
<td>005</td>
<td>L_014</td>
<td>Bulk Inhaler bodies_unfilled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_018</td>
<td>Bulk Aluminium Strip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_019</td>
<td>Carister forming_machine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_020</td>
<td>Carister forming_power_supply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_021</td>
<td>Carister forming_staff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_022</td>
<td>Carister packing</td>
</tr>
<tr>
<td>Manufacture of active ingredient</td>
<td>006</td>
<td>L_012</td>
<td>Quality assured active_Ingred</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_023</td>
<td>6 Stage Reactor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_024</td>
<td>6 Raw Chemical stocks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_025</td>
<td>Salbutamol Cook</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_026</td>
<td>Salbutamol Cook_facilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L_027</td>
<td>Active Ingred Power supply</td>
</tr>
</tbody>
</table>
APPENDIX C: GLOSSARY
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Border gateway protocol</td>
</tr>
<tr>
<td>BoM</td>
<td>Bill of materials</td>
</tr>
<tr>
<td>BS OHSAS</td>
<td>British Standard, Occupational Health and Safety Assessment Series</td>
</tr>
<tr>
<td>CIP</td>
<td>Cleaning-in-place (food processing)</td>
</tr>
<tr>
<td>CNC</td>
<td>Computer numeric control (machining)</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain name server (Internet)</td>
</tr>
<tr>
<td>DSLAM</td>
<td>Digital subscriber line access multiplexer</td>
</tr>
<tr>
<td>EFTPOS</td>
<td>Electronic funds transfer, point of sale</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure modes and effects analysis</td>
</tr>
<tr>
<td>HV/LV</td>
<td>High voltage/Low voltage</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>ISNGI</td>
<td>International Symposium on Next Generation Infrastructure</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider</td>
</tr>
<tr>
<td>ISTAS</td>
<td>International Symposium on Technology and Society (IEEE)</td>
</tr>
<tr>
<td>MDI</td>
<td>Metered dose inhaler</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean time between failures</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean time to failure</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean time to repair</td>
</tr>
<tr>
<td>MW and</td>
<td>MegaWatt and MegaWatt-hour</td>
</tr>
<tr>
<td>MWh</td>
<td></td>
</tr>
<tr>
<td>NAP</td>
<td>Network access point</td>
</tr>
<tr>
<td>ODF</td>
<td>Open document format (ISO/IEC 26300-3:2015 – Information technology)</td>
</tr>
<tr>
<td>POTS</td>
<td>&quot;Plain old telephone system&quot;</td>
</tr>
<tr>
<td>RQ</td>
<td>Research question</td>
</tr>
<tr>
<td>SCADA</td>
<td>System control and data acquisition</td>
</tr>
<tr>
<td>SE</td>
<td>Systems engineering</td>
</tr>
<tr>
<td>SMS</td>
<td>Simple message service (TXT)</td>
</tr>
<tr>
<td>STD</td>
<td>Security through diversity</td>
</tr>
<tr>
<td>TEFC</td>
<td>Totally enclosed, fan-cooled (electric induction motor)</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible power supply</td>
</tr>
<tr>
<td>VAC</td>
<td>Voltage alternating current</td>
</tr>
</tbody>
</table>

Appendix C 2