How Do We Ensure the Assessment of Infrastructure Resilience is Proportionate to the Risk?

Matthew Holmes\textsuperscript{a}\textsuperscript{*}  
Anna Provost\textsuperscript{b}  
Derek Clucas\textsuperscript{b}  
Sean Wilkinson\textsuperscript{a}

Abstract: As infrastructure becomes increasing integral to daily lives, society becomes more vulnerable to potential failures. We mitigate against this by investing some of the increased prosperity afforded by infrastructure to treat the most salient risks and increase the resilience of the system. Therefore we enter a cycle where our ability to identify and prioritise vulnerabilities is crucial to the future development of infrastructure. It is easy to compose a list of risks occupying the whole spectrum from probable through to fanciful, but, how do infrastructure owners define defensible boundaries between the credible risks they should assess and those that can be set aside? This paper tests the hypothesis that incorporating information on the uncertainty of risk assessments provides risk managers with a more robust process to justify their choice of credible risks.

Key words: Infrastructure; Resilience; Risk assessment; Risk management; All-hazards

I. Introduction

There is increasing evidence to suggest that infrastructure and sustainable development are tightly coupled. Effective and efficient infrastructure encourage economic, environmental and social development\textsuperscript{1,2}, while development creates the demand for better infrastructure and, importantly, the means by which to afford it.

Which factor is the chicken and which the egg has caused much debate among economists\textsuperscript{3,4} but the coupled nature of these factors is central to an emerging challenge for risk managers as Figure 1 illustrates. The cycle of development and infrastructure provision is shown is solid lines. As infrastructure becomes increasingly integral to our daily lives we become increasingly vulnerable to its failure, and thus it must be more resilient (the base of the dashed cycle. The role of infrastructure owners and operators is to mitigate the risks to their system in order to achieve this continual improvement. Naturally there is a preference (as with any decision) to treat the more salient and certain risks\textsuperscript{5,6} but as the cycles in Figure 1 continue these risks are eliminated.

\textsuperscript{a} Civil Engineering and Geosciences, Newcastle University, Newcastle-upon-Tyne, NE1 7RU  
\textsuperscript{b} United Utilities Plc, Lingle Mere Business Park, Warrington, WA5 3LP  
\textsuperscript{*} Corresponding author: Matthew Holmes matthew.holmes@stream-idc.net  
http://dx.doi.org/10.14453/isngi2013.proc.23
and infrastructure providers are obliged to consider increasingly obscure, complex and tricky risks.

Of course this cycle is not operating in an environment with unconstrained resources and because infrastructure owners and operators’ budget are limited they need to target their investment carefully). In the aftermath of an event and with the benefit of hindsight it is easy to criticise owners and operators for failing to identify and act upon a risk. This is one reason for the growing impetus behind ‘all-hazards’ approaches to resilience. It is equally easy to compose a long list of risks, occupying the whole spectrum of plausibility, which could conceivably affect an infrastructure system. But neither hindsight nor long lists are of value to a risk manager; infrastructure systems are large, complex and have many interfaces with other systems making risk assessments time-consuming and expensive. To ensure the effort of assessment is proportionate to the risk, managers must choose at an early stage which risks they can afford to assess in detail and set aside those they cannot.

![Figure 1. The addictive cycle of infrastructure resilience.](image)

These decisions – often made with little available information - are pivotal to the analysis and errors of choice can easily result in catastrophic consequences if the wrong risks are selected. Moreover, these errors might then be hidden from immediate view because they are not made in the analysis but in establishing the problem. Risk managers must be careful to avoid these errors since their decisions need to be defensible under an inquiry from senior management and regulators, and under public scrutiny if risk becomes reality. Therefore they must be systematic
in choosing which risks to include and which to set aside. This paper assesses three approaches to making these decisions which employ different levels of complexity to explore the balance between the information provided to the decision maker and the costs of obtaining this information.

II. Approaches to selecting risks

A. Likelihood versus consequence

The obvious approach is to make a precursory assessment of the risk, considering the consequence and probability of occurrence. Figure 2 is a useful diagram produced by the UK Cabinet Office in 2010 which plots major risks according to these two factors. Can a risk manager choose which risks to assess based solely on this information, for example by excluding risks above the dashed line?

The benefit of this approach is its simplicity; it matches the approaches that risk managers are used to taking and those expected by regulators. It is recognised the placement and shape of the dashed line is potentially contentious but deliberately excluded from the scope of this paper for this and the two subsequent approaches discussed below. Ultimately it reflects the risk appetite of the utility provider and therefore will always be an individual choice.

The main challenge to this approach is that it does not account for the uncertainty attached to each assessment or the relevance to different types of infrastructure. The complexity of infrastructure systems means there will always be errors in the assessment of impacts and likelihoods. Moreover, this level of uncertainty varies between different risks; some are simpler or have been studied in detail whereas others are more complex and vague. Aleatory uncertainty is also a factor; events show natural variation meaning risks do not occupy a single point. This is well illustrated in IPENZ’s New Zealand equivalent of Figure 2.
B. Subjective assessment of uncertainty

It is logical that risk managers should seek to account for this uncertainty as they select which risks to analyse. As a risk assessment become less certain it offers risk managers less information and therefore its value diminishes. In parallel, higher uncertainty makes risk assessments increasingly difficult and expensive. Accepting that they are working with finite resources – and that all uncertainty will never be eliminated – a trade-off must be made between the cost of assessing the risk and the value of the information the assessment will provide.

We can get a new perspective by taking the concept from Figure 2 and replacing the likelihood with the uncertainty around the probability assessment. Risk managers can then use the expert judgement available to them to populate the diagram with potential risks. For example, they can assess day-to-day operational risks such as burst pipes with relative accuracy; they realise that some conventional risks, such as flooding, are uncertain but still feel they can reach a sensible estimate; and they acknowledge there are some risks which are too uncertain to reach a credible estimate, for example war or solar flares. An example is shown in Figure 3.

In the same manner as the dashed line in Figure 2 a threshold can be added to this approach to delineate which risks are worth assessing. The value of the information provided is influenced by the size of the risk (hence the curved line). There is little value in an uncertain estimate of a low risk but a similarly uncertain estimate of a high risk will have greater value; because the stakes are higher a decision maker may be more cautious and act on less certain evidence. The line approaches vertical as scenarios become too far-fetched for executives, shareholders and regulators to find them credulous. At this point we are entering the territory of ‘black swan’ risks as outlined by Taleb12.

Figure 3. The limit of resilience planning set by the precision of the probability assessment.
The challenge to this approach is that it is subjective, based upon a personal or organisational perspective of the risks and for rare risks they are likely to have no experience of the event. There will be inconsistency between different infrastructure providers and between them and regulators. This creates a significant risk for providers if their processes come under scrutiny.

C. Formalised assessment of uncertainty

It is anticipated that by formalising the estimate of uncertainty the process becomes more transparent and therefore more accountable so this hypothesis is tested on a model of a real-world wastewater system. For the purposes of illustration four different risks – public disorder, storms and gales, cold weather, and cyber-attacks on infrastructure - are selected from the latest UK National Risk Register\textsuperscript{13}. Basic event trees are then used to estimate the probability of the national scenarios having an impact on this particular network. Where a probability within the fault tree is subject to uncertainty a probability distribution derived from expert knowledge is used in the place of a deterministic value. 1000 realizations of the model are then used to assess how this uncertainty affects the risk of flooding.

1) For each realization the probability of at least one failure as a consequence of the scenario is calculated, the mean of these gives the likelihood shown on the x-axis.

2) The coefficient of variation, shown on the x-axis, is calculated as the standard deviation of the probability of at least one failure divided by the mean probability of at least one failure. Note the reverse scale on the x-axis.

A comparison between the results of this method and an assessment of only likelihood and consequence indicates that it does present new information, showing that the threat of cyber-attacks is highly uncertain and that public disorder could be assessed with relative ease. This is a useful outcome from the perspective of an audit trail demonstrating to others that a robust process has been followed; however, it does not materially affect the outcome of the assessment; that storms and gales and cold weather are the principal risks, and cyber-attacks and public disorder should be discarded from a proportionate risk assessment. In addition, whilst the process may make the subjective choices less opaque we have not addresses the accuracy of these expert judgements, in particular the difficulties of estimating the probability distributions of rare events. Therefore we return to the issue of balancing information and the effort of collecting it; does the benefit of the audit trail exceed the extra costs incurred in assessing the uncertainty even at a basic level?
III. Discussion

Three different approaches have been used to identify which risks are most important for further analysis. The simple assessment of likelihood and consequence benefits from its simplicity and it matches the expectations of regulators and policy makers. The omission of uncertainty at the risk screening phase is not a flaw in itself; however, its inclusion does present risk managers with an opportunity to justifiably eliminate those risks whose assessment adds little value. The second approach, subjective assessment of uncertainty, achieves this based upon the personal opinion of the assessor. The benefit of this is that it can be undertaken with limited extra input however it becomes an opaque process and its worth for very rare events is questionable. The third option which formalises the assessment of uncertainty increases transparency but increases the complexity and therefore cost of making the decision and still relies on the judgement of experts. This extra cost undermines the approach’s purpose as a simple precursor to enable a more proportionate detailed risk assessment and, given the results also suggest that it offers little extra information compared to the simpler analyses, it is tempting to discount it. However the extra cost may be justified by its auditability and the possibility of easily updating the analysis as new assessments of risk come to hand.

It is also tempting to suggest the value of the likelihood versus consequence approach is limited by its simplicity. Whilst it provides a useful initial estimate of the risk it does not account for the effort which a risk manager will have to expend to convert this estimate into a more reliable assessment.

IV. Conclusion

As reliance on infrastructure increases so does our vulnerability to failure, requiring risk managers to consider increasingly rare risks. This problem of dealing with very rare threats is
only going to get worse and, due to the cost of assessing such risks, new and robust methods of identifying which risks should receive the most attention are vital. Incorporating high level subjective information on the uncertainty of the probability estimates allows them to do this in a more perceptive way, though subjective and opaque. Formalising this process by estimating the uncertainty of individual elements improves the auditability of this process but the extra complexity and cost may exceed the value of the new information obtained.

References

http://dx.doi.org/10.1111/j.1468-0297.2011.02420.x


http://dx.doi.org/10.1016/S0304-3878(02)00105-0

http://dx.doi.org/10.1257/jep.6.4.189

http://dx.doi.org/10.1017/CBO9780511609947


http://dx.doi.org/10.1111/0272-4332.00020


