University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2007

Managing Business Process Risk Using Rich Organizational Models

M. Bhuiyan
University of Wollongong

M. M. Islam
University of Wollongong

G. Koliadis
University of Wollongong

A. Krishna
University of Wollongong, aneesh_krishna@uow.edu.au

Aditya K. Ghose
University of Wollongong, aditya@uow.edu.au

Publication Details

This conference paper was originally published as Bhuiyan, M, Islam, MMZ, Koliadis, G, Krishna, A, Ghose, A, Managing Business Process Risk Using Rich Organizational Models, 31st Annual IEEE International Computer Software and Applications Conference COMPSAC 2007, 24-27 July, Vol 2, 509-520.

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

Managing Business Process Risk Using Rich Organizational Models

Abstract

Business processes represent the operational capabilities of an organization. In order to ensure process continuity, the effective management of risk becomes an area of key concern. In this paper we propose an approach for supporting risk identification with the use of higher-level organizational models. We provide some intuitive metrics for extracting measures of actor criticality, and vulnerability from organizational models. This helps direct risk management to areas of critical importance within organization models. Additionally, the information can be used to assess alternative organizational structures in domains where risk mitigation is crucial. At the process level, these measures can be used to help direct improvements to the robustness and failsafe capabilities of critical or vulnerable processes. We believe our novel approach, will provide added benefits when used with other approaches to risk management during business process management, that do not reference the greater organizational context during risk assessment.

Disciplines

Physical Sciences and Mathematics

Publication Details

This conference paper was originally published as Bhuiyan, M, Islam, MMZ, Koliadis, G, Krishna, A, Ghose, A, Managing Business Process Risk Using Rich Organizational Models, 31st Annual IEEE International Computer Software and Applications Conference COMPSAC 2007, 24-27 July, Vol 2, 509-520.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/624

Managing Business Process Risk Using Rich Organizational Models

Moshiur Bhuiyan, M.M.Zahidul Islam, George Koliadis, Aneesh Krishna, Aditya Ghose
Decision Systems Laboratory
School of Computer Science & Software Engineering (SCSSE)
University of Wollongong (UOW), Northfields Avenue, NSW 2522, Australia
{mmrb95, mmzi44, gk56, aneesh, aditya}@uow.edu.au

Abstract

Business processes represent the operational capabilities of an organization. In order to ensure process continuity, the effective management of risk becomes an area of key concern. In this paper we propose an approach for supporting risk identification with the use of higher-level organizational models. We provide some intuitive metrics for extracting measures of actor criticality, and vulnerability from organizational models. This helps direct risk management to areas of critical importance within organization models. Additionally, the information can be used to assess alternative organizational structures in domains where risk mitigation is crucial. At the process level, these measures can be used to help direct improvements to the robustness and failsafe capabilities of critical or vulnerable processes. We believe our novel approach, will provide added benefits when used with other approaches to risk management during business process management, that do not reference the greater organizational context during risk assessment.

1. Introduction

A Business Process can be described as a set of dynamically coordinated activities, controlled by a number of socially dependant participants, aimed towards the achievement of a specific operational objective [7] [11]. Business Process Management is a re-emerging discipline, aimed towards supporting the effective and automated [11] management of business processes within an organization via specialized tools and methods. Business Process Management promotes that a clear understanding through the explicit modelling of the processes underlying an organization is required to support effective organizational management / improvement practices [4].

An effective means to represent and manage operational risk is one of the most important capabilities within an enterprise. Some of the most prominent applications of risk management techniques include financial / operational management and modelling of organizations. Risk management techniques have also been extensively studied and applied within software process management, requirements engineering and project management disciplines [20] [24]. More recently, risk management has been applied to the business process management and modelling domain that as a whole, aims to bridge the gap between organizational and I.T. level conceptual / management concerns [16] [18] [19]. These approaches provide a more direct association between organizational risks at an activity level.

There are difficulties associated to addressing risk at process level. We believe that by taking actor-level considerations such as vulnerability and criticality (at organizational level) as major considerations is important for process-level risk management. We provide an approach to support risk management by supporting the identification of risk factors (in terms of vulnerability and criticality) at organizational level prior to their propagation and reflection at a process level. We believe that such an approach will provide a higher-level scope for risk that may span numerous processes within an organization. Business process risk analysis should be based on higher-level organizational models. A high-level approach to iterative risk assessment should be integrated throughout the business process lifecycle. Therefore, risks may be identified and managed at an organizational level prior to their delegation to actual business processes. We provide an enhanced capability to relate risk at an organizational level by looking at the strategic relationships between functional units and process participants. We define risk at organizational model level on the basis of vulnerability and criticality. For organizational modelling we use the agent-oriented organizational modelling notation – *i** [13] that describes the organizational relationships among various actors and their rationales. For business process model representation we use a standardized, operational and executable process modelling notation – BPMN [12]. The authors consider that the majority of risks identified lie in mismatch with the methods employed within the various phases of the process lifecycle, a lack of clarity who is responsible for the individual phases or their results and a mismatch of process design, automation and evaluation objects. We believe that risk can be better viewed by using a combined notation proposed in [12].

The following section starts with a discussion of risk and risk management and our chosen notations. We then describe our approach to identify risk factors including our proposed measurement for vulnerability and criticality of actors at organizational level. Finally we illustrate the integration of risk factors in process model with examples and then some concluding remarks.

31st Annual International Computer Software and Applications Conference(COMPSAC 2007)
0-7695-2870-8/07 $25.00 © 2007 IEEE

2. Background

Agent Oriented Conceptual Modelling

The agent metaphor is powerful in modelling organizational contexts. Agent-Oriented Conceptual Modelling (AOCM) in notations such as the *i** framework [13] (see: figure 1) have gained considerable currency in the recent past. Such notations model rich organizational contexts and offer high-level social/anthropomorphic abstractions (such as goals, tasks, soft goals and dependencies) as modelling constructs.

It has been argued that notations such as *i** help answer questions such as what goals exist, how key actors depend on each other and what alternatives must be considered. Furthermore, *i** has been acknowledged as illustrating the key social/strategic inter-relationships between actors [6] [13] required for effective business process redesign. This is achieved via support for reasoning about organizational activities and their assignment to various organizational agents [13] in respect to: the ability, workability, viability, and believability of their routines; and, level of commitment [13].

The central concept in *i** is that of intentional actor. These can be seen in the Meeting Scheduling model as nodes representing the intentional/social relationships between three (3) actors required to schedule a meeting: a Meeting Initiator (MI); Meeting Scheduler (MS); and Meeting Participant (MP).

The *i** framework consists of two modelling components: Strategic Dependency (SD) Models and Strategic Rationale (SR) Models [13]. The SD model consists of a set of nodes and links. Each node represents an actor, and each link between the two actors indicates that one actor depends on the other for something (i.e. goals, task, resource, and soft-goal) in order that the former may attain some goal. The depending actor is known as depender, while the actor depended upon is known as the dependee. The object around which the dependency relationship centers is called the dependum. The SR mode further represents internal motivations and capabilities (i.e. processes or routines) accessible to specific actors that ensure dependencies can be met.

The intentional properties of an agent such as goals, beliefs, abilities and commitments are used in *i** for modelling organizations [13]. Actors are [inter]related through dependencies that may involve goals to be achieved (e.g. Evacuation & RescueMission), tasks to be performed (e.g. GatheringLocalInformation), resources to be furnished (e.g. FieldInformation), or soft-goals to be satisfied (e.g. RespondFast).

Business Process Modelling with BPMN

Many existing BPM notations primarily focus on technical process aspects including the flow of activity execution/information and/or resource usage/consumption [13]. This perspective is aimed at describing the sequence of activities, events and decisions that are made during process execution, however social and intentional components lack representation. The technical focus of these notations is especially suited for applications in the description, execution and simulation of business processes but is lacking in support for process redesign and improvement [13].

One such notation is the Business Process Modelling Notation (BPMN), developed by the Business Process Management Initiative (BPMI.org). BPMN can be seen as primarily a technically-oriented notation that is augmented with an ability to assign activity execution control to entities (e.g. roles) within an organization with 'swim-lanes'. This effectively provides a view of the responsibilities and required communications between classes of process participants, but does not provide a view of other social and intentional characteristics including the goals of participants and their inter-dependencies.

Processes are represented in BPMN using flow nodes: events (circles), activities (rounded boxes), and decisions (diamonds); connecting objects: control flow links (unbroken directed lines), and message flow links (broken directed lines); and swim-lanes: pools (high-level rectangular container), and lanes partitioning pools. These concepts are further discussed within [12].

Since its initial publication [12], BPMN has been accepted by the greater Business Process Management community [1] [11], due to its expressiveness and ability to map directly to executable process languages including XPDL [4] and BPEL [10] [12]. The wide uptake of the notation by most Business Process Modelling tool vendors is also a sign of its longevity [4]. Some practitioners have hailed BPMN as supplying a rich representation that allows Business Process Management Systems (BPMS) the ability to control the required interactions with humans and 3rd party applications [9]. Furthermore, an analysis of BPMN also stated its high maturity in representing concepts required for modelling business process, apart from some limitations in terms of representing state, and the possible ambiguity of the swim-lane concept [1].

3. Identifying Risk within Organizational Models

In this section we will describe our intuitive approach to analysis and design with regards to organizational risk. In order to achieve this task, we propose an analysis of strategic dependencies between actors in order to measure and identify each actor's vulnerability and criticality. Once determined, the design task will be focused towards the area of process modelling that requires most attention.

Vulnerability

The vulnerability of an actor plays a vital role for identifying and measuring risk. The *i** model provides an intentional description of a process in terms of a network of dependency relationships among actors [13]. We believe because of its richer modelling concepts, the model pro-

vides a better basis for an analyst to explore the broader risk implications of alternative organizational structure. It can help analyze opportunities and vulnerabilities and recognize patterns of relationship. A depender actor's intention is to have the dependency goal achieved, task performed, or resource available. Failure to obtain the dependum can affect the process by making it more vulnerable and hence increasing the likelihood of risk occurrence. In our work we propose a way of measuring vulnerability of actors at organizational model. The analyst can then take necessary steps to mitigate these vulnerabilities in process models. A stronger degree of vulnerability implies that a stronger initiative to mitigate vulnerability is necessary. Such initiative can be taken by increasing the monitoring process of dependee actor's activities.

We propose a metric for actor vulnerability. This metric is effectively divides the number of outgoing dependencies by the number of dependee actors. A depender actor with more outgoing dependencies implies a greater degree of vulnerability. We consider outgoing dependencies for vulnerability measurement as we believe that outgoing dependencies indicate delegation of tasks and activities. If the tasks are delegated to other actors the depender actor becomes vulnerable. In case of the failure of dependee actor to satisfy the dependency, the corresponding task/goal might not be satisfied (a considerable risk). The vulnerability of actors thus is related to the likelihood of a risk occurring. We believe if an actor is vulnerable, an increase in the overall likelihood of risk occurrence is apparent. Intuitively, if the likelihood increases risk will increase as well.

The formula we use to assess the vulnerability measurement (VM) of actors is as follows:

VM =No of Outgoing Dependencies / No of Dependee Actors

For example, for actor *EmergencyCoordinationCentre-Coordinator*,

No of Outgoing dependencies = 12

No of Dependee Actors = 4

So, Vulnerability, VM= (12/4) = 3

Table 1: Vulnerability Measurement of Actors

Name of the Actor	**No of Outgoing Dependencies**	**No of *Dependee* Actors**	**Vulnerability**
Emergency Coordination Centre Coordinator	12	4	3
Weather Bureau	0	0	None
Call Taking Supervisor/ System	0	0	None
Volunteer/Emergency Workers	4	2	2
Flood Control Centre Coordinator	7	3	2.33
Community	8	3	2.66

In a softgoal-dependency, a depender depends on the dependee to perform certain goals or task that would enhance the performance. The notion of a softgoal derives from the Non-Functional Requirements (NFR) framework [2] and is commonly used to represent optimization objectives, preferences or specifications of desirable (but not necessarily essential) states of affairs. So, softgoals are non-functional requirements of the system, which have positive or negative contribution toward achieving a goal, task, or resource. While measuring the vulnerability of actors we do not included the softgoal dependencies. We believe these non-functional requirements of the system have minimal impact on risk either in the organizational level or on the process level. When we calculate the outgoing dependencies of actors we exclude the softgoal dependency.

If any actor has no outgoing dependency with other actors, we do not take that actor for vulnerability measurement. We believe such actor has no vulnerability as it can not affect the likelihood of occurrence. From figure-1 we find that the actors *WeatherBureau* and *CallTaking-Superviosr/System* do not have any outgoing dependencies. It means they have not delegated their responsibilities or tasks to other actors. But, actor with no vulnerability does not necessarily mean that it is not critical enough to affect the consequences if it fails. In this case criticality of the actor is considered to measure the risk.

Criticality

Criticality is the consequence factor that is measured from the impact of an actor's performance where the actor is assigned to satisfy responsibilities/incoming dependencies. The more critical an actor is, the more ability it carries to impact other actors and the organizational context. Incoming dependencies towards an actor are taken into consideration to measure the criticality of an actor. The incoming dependencies describe responsibilities are assigned to an actor from other actor. By receiving dependencies from other actor makes the dependency receiving actor crucial. If it fails to satisfy the incoming dependencies the depender actors are widely affected which possibly affect the context as a whole. In order to mitigate the risks associated with the system the criticality measurement of actors should be taken into consideration. Measuring critical factors of actors helps the analysts to analyze and

construct alternative options to achieve the aim of the system. This will alleviate the risk management and increase the robustness of the system.

Criticality of actors is measured by multiplying number of incoming dependencies and number of depender actors. The formula we use to assess the criticality measurement (CM) of actors is as follows:

CM = No of Incoming Dependencies * No of Depender Actors

For example, for actor *Volunteer*,
No of Incoming Dependencies = 10
No of Depender Actors = 3
So, Criticality, CM= 10*3 = 30

Table 2: Criticality Measurement of Actors

Actors	No of Incoming Dependencies	No of *Depender* Actors	Criticality
Emergency Coordination Centre Coordinator	4	1	4
Call Taking Supervisor/System	9	3	27
Volunteer/Emergency Workers	10	3	30
Flood Control Centre Coordinator	9	3	27
Weather Bureau	2	1	2
Community	2	1	2

According to the result from Criticality Metrics, *Volunteer* actor is more critical than other actor in the model. Volunteer has ten incoming dependencies from three other actors and its existence is more crucial because if it fails to satisfy any of the incoming dependencies received from other three actors it will have greater impact on other actors and to system as a whole. We have not considered the softgoal dependencies while calculating the criticality of the actors for the same reasons of vulnerability measurement.

If an actor does not have any incoming dependencies from another actor of the model then it portrays that the actor has distributed his dependencies to other actor but no other actor has delegated any tasks, resources and goals into this actor. So the actor will have no impact on the consequences of the performance of other actors in the strategic context of the model. For this reason an actor with no incoming dependencies will be positioned with no criticality fact towards it but the vulnerability factor of that actor will take it into the consideration of the risk measurement in the strategic framework.

4. Integrating Risks in Business Process Models

Treating Vulnerable Actors

We believe that every actor in the business processes should be given a relative level of effort to mitigate vulnerability via robustness and efficiency. We suggest for the more vulnerable actors more monitoring of the tasks/ sub-tasks is necessary. Monitoring of the business process means tracking the individual tasks or subtask in a process so that information on their state can be easily made visible. It is done to measure the satisfactory performance of a business process. Business process tasks of the vulnerable actors need more monitoring so that we can continually refine them based on feedback that comes directly from operational level.

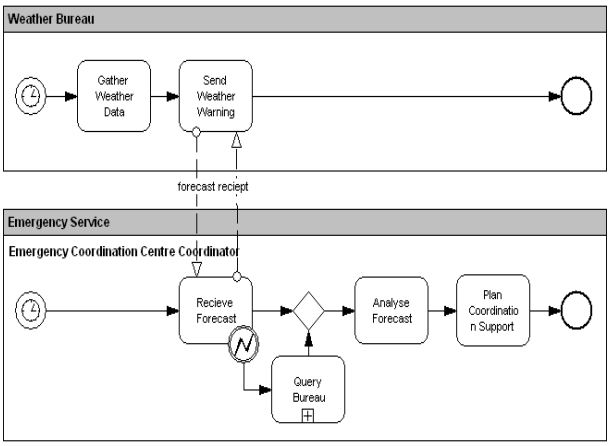

Figure 2: Business Process Model in BPMN

This process model has two actors *WeatherBureau* and *EmergencyCoordinationCentreCoordinator (ECCC)* with few tasks and subtask. The model also represents exception handling procedure for *RecieveForecast* task. From table-1, we find that *ECCC* is the most vulnerable actor which implies more monitoring of the tasks and subtask inside this process is required.

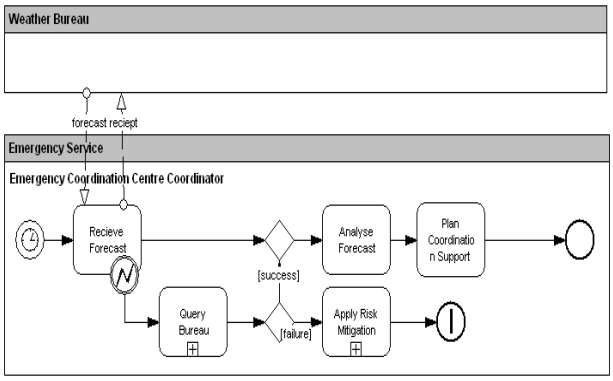

Figure 3: Extended Process Model Reflecting the Vulnerable Actor.

The process model in figure 2 is improved in figure 3 by using our notion of vulnerability. The exception for *RecieveForecast* task is handled by *QueryBureau* sub-process. We extend this model by integrating *ApplyRiskMitigation* sub-process. This sub-process includes the risk mitigation procedures which takes place in case of the failure of *QueryBureau* sub-process.

The analyst should design the organizational model or process model carefully while delegating the dependencies from one actor to other actors. Actor with dependencies over only one actor is more vulnerable then actor with dependencies with multiple actors. For example, the vulnerability level of actor A1 is 4 and actor B1 is 1. Actor A1 has four dependencies over A2. If actor A2 fails then all the dependencies will remain unsatisfied. On the other hand actor B1 has delegated its dependencies over four actors. If any of the four dependee actor fails one dependency will remain unsatisfied, but the others might be satisfied. Thus actor A1 is more vulnerable than actor B1.

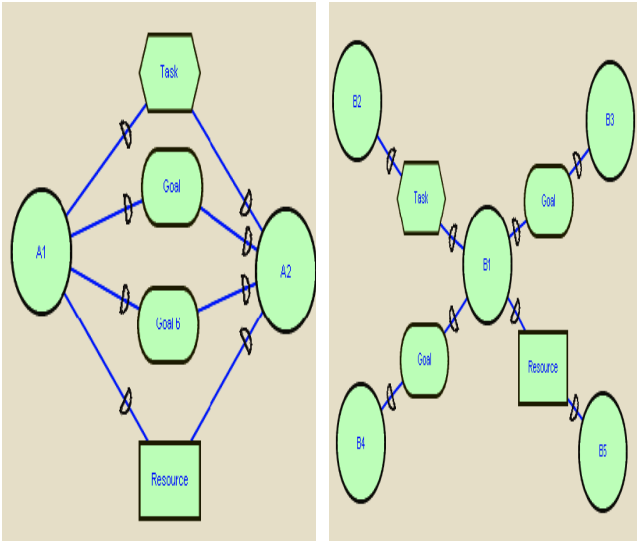

Figure 4: Delegation of Dependencies among Actors.

Treating Critical Actors:

Volunteer actor is the most critical actor according to the the matrix. In this case the three actors *ECCC*, *FieldControlCentreCoordinator(FCCC)* and *Community* are dependant on *Volunteer* actor to accomplish their certain objectives. Failure to satisfy these objectives/incoming dependencies will have a big impact on the performance of the depender actors and to the system as a whole. To minimize the criticality levels of actors, the analyst needs to have pragmatic and profound process delegation strategy.

The tasks and sub-processes of the most critical actors should be robustly planned to make the whole process successful. To make the process robust the analysts need to identify what is the overall objective of the process. This should describe problems to be solved, issues to be addressed, key participants, whether all the tasks are well integrated within the process and how the process add values and quality to the system.

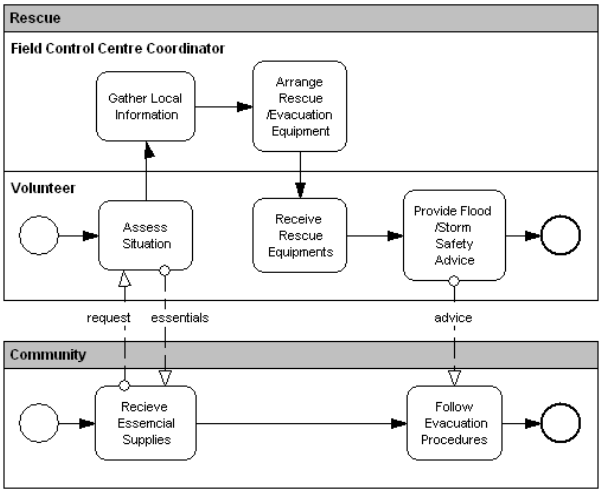

Figure 5: Business Process Model in BPMN

The objective of the process in figure-5 is to provide a Flood/Storm Safety advice to the *Community*. *Volunteer* provides the safety advice to the *Community*. For the well completion of the process *Volunteer* needs to have local information and rescue equipments which are done by *FieldControlCenterCoordinator* by accomplishing two tasks *GatherLocalInformation* and *ArrangeRescue/EvacuationEquipment*. Upon successful completion of the task *ReceiveRescueEquipments* the *Community* receives the message *ProvideFlood/StormSafetyAdvice* from *Volunteer* in the *FollowEvacuationProcedures* tasks which add values to the process of evacuation.

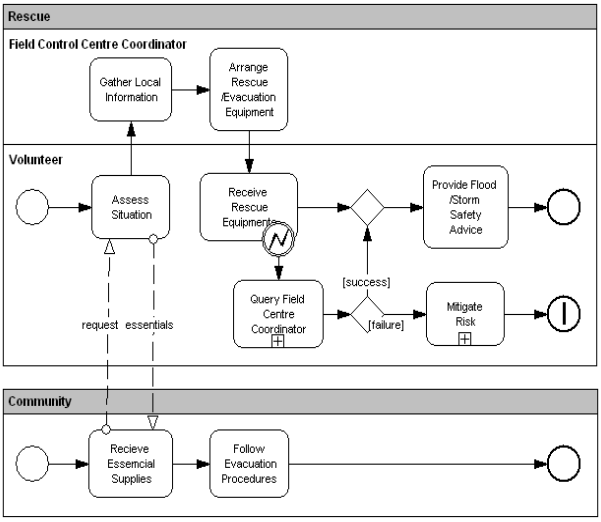

Figure 6: Extended Process Model Reflecting the Critical Actor.

The above process model is extended from figure 5 by introducing an exception handling technique in *Volunteer's RecieveRescueEquipments* task to manage its satisfactory performance. If the *Volunteer* does not receive the

rescue equipments from *FCCC* the process will throw an exception which sends query to *FCCC*. To handle the risks from negative response from the *FCCC* a *MitigateRisk* sub-process is introduced. Exception handling should be taken into thoughtful consideration by the analyst as exceptions may arise in any stages of the process.

The processes of the critical actors should have mutual consistency to reduce criticality and increases process performance. If a process is allocated to an actor, which the actor may not be capable of performing, it is likely to delay the process which could lead to a disaster. Clearly specified activities for the actors should be one of the most important priorities to the analyst. It makes easy to comprehend and allocate resourceful process design to ease the modification of processes.

5. Conclusion

In this work we have presented a discussion on how we can identify risk in terms of vulnerability and criticality in organizational models. We have also provided a way to integrate risks within the process model. We believe it helps the analyst while to design organizational models, delegate dependencies among various actors, choose alternatives, decompose tasks, maintain consistency among organizational and process models, handle exceptions etc. However, we have considered the concept of vulnerability and criticality of actors only. We have not considered our notions on the activities and sub-process for assessing risks. Our future work will deal with the combination of actors and their tasks and sub-processes. Our proposal is based on a combined notation (*i**-BPMN) which might not be suitable for organizations using different notations. However, we wish apply our proposal to different notations in the future.

REFERENCE

[1] Becker, J. Indulska, M. and Rosemann, M. Green, P (2005). Do Process Modelling Techniques Get Better? A Comparative Ontological Analysis of BPMN, in Campbell, Bruce and Underwood, Jim and Bunker, Deborah, Eds. Proceedings 16th Australasian Conference on Information Systems, Sydney, Australia.

[2] Chung, L. (1993). Representing and Using Non - Functional Requirements for Information System Development. A Process-Oriented Approach. PhD Thesis, Graduate Department of Computer Science, Toronto, University of Toronto.

[3] Fischer, L. (2005). Workflow Handbook 2005, Workflow Management Coalition, (WfMC).

[4] Hall, C. Harmon, P. (2005). The 2005 Enterprise Architecture, Process Modelling & Simulation Tools Report, Technical Report, bptends.com.

[5] Hammer, M. Champy, J. (1993) Reengineering the Corporation: A Manifesto for Business Revolution, HarperBusiness, 1993.

[6] Katzenstein G. Lerch F. J. (2000). Beneath the surface of organizational processes: a social representation framework for business process redesign. ACM Transactions on Information Systems (TOIS), 18(4), (pp. 383-422).

[7] Koliadis G., Vranesevic A, Bhuiyan M., Krishna A. and Ghose K. Ghose (2006). A combined approach for supporting the business process model lifecycle. *Proceedings of the Asia-PacificConference on Information System*

[8] Loucopoulos, P. and Kavakli, E. (1995) "Enterprise Modelling and the Teleological Approach to Requirements Engineering," International Journal of Intelligent and Cooperative Information Systems, Vol 4, No1, pp. 45-79.

[9] Miers, D. (2004) The Split Personality of BPM, Business Process Trends, bptrends.com

[10] Ouyang, C. W.M.P. van der Aalst, Dumas, M. and ter Hofstede, A.H.M.(2006). Translating BPMN to BPEL, BPM Center Report BPM-06-02, BPMcenter.org.

[11] Smith, H. Fingar, P. (2003). Business Process Management – The Third Wave, Tampa, FL: Meghan-Kiffer Press, 2003.

[12] White, S. (2004). Business Process Modelling Notation (BPMN), Version 1.0, Business Process Management Initiative (BPMI.org).

[13] Yu, E. (1995) Modelling Strategic Relationships for Process Reengineering. PhD Thesis, Graduate Department of Computer Science, University of Toronto, Toronto, Canada, pp. 124.

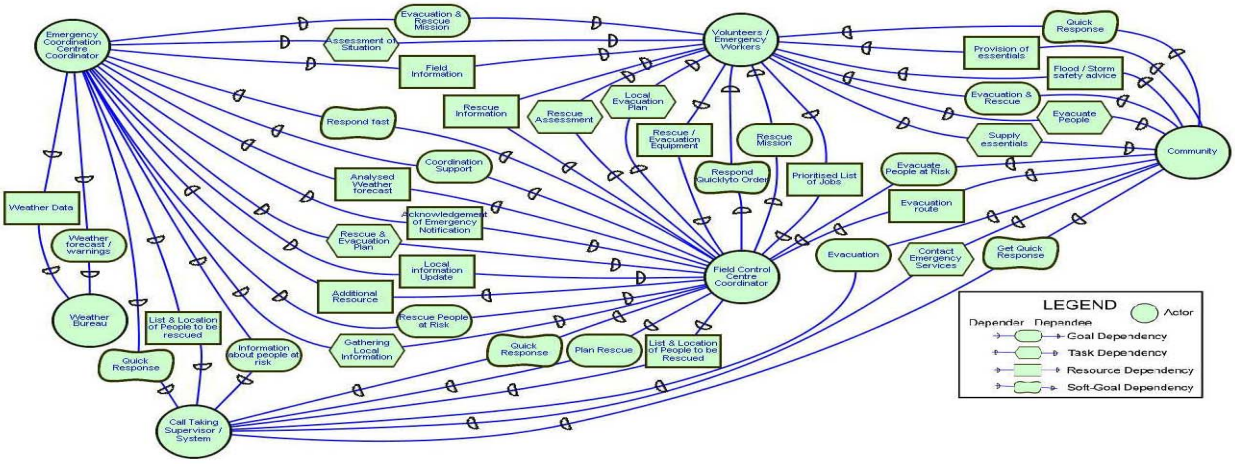

Figure 1: Strategic Dependency Model of an Emergency Service Provider.