Responsibility Modelling for Contingency Planning

Ian Sommerville, Tim Storer and Russell Lock

August 23, 2007

Extended Abstract

This paper proposes the use of responsibility modelling as a tool to support the process of contingency planning for civil emergencies. The objective of traditional contingency planning is to provide a mechanism whereby disparate organisational agents are able to prepare in order to respond effectively during an emergency. A contingency plan document may be a by-product of this process, but it is unlikely to be used actively during an emergency.

Emergency planning processes must accommodate the need for response organisations to discharge their responsibilities dynamically; that is, by actions that are dependent on the particular context of an emergency and the impact of on-going events. In addition, responses are also complicated by the specific information that agents may need in order to discharge their assigned responsibilities. A recurring theme identified in debrief reports of emergency response exercises are failures related to communication arrangements. Such reports describe how participants do not receive necessary information in order to discharge their responsibilities in a timely fashion, or similarly do not distribute information to others appropriately. The distribution of information is complicated by the need to anticipate who needs to know what to perform a given task, when they need to know it, and the consequences of inappropriate distribution of sensitive information.

The notion of employing responsibility modelling for assessing the vulnerabilities in a socio-technical system has been investigated by several authors. Recently, we have developed a formal model of responsibility assignment for the purpose of providing partially automated support for the analysis of responsibilities as they are assigned across a socio-technical system. In addition, we have developed a suite of graphical views which illustrate different, but consistently related aspects of the formal model. The views are implemented as a CASE tool in order to support the assisted construction and analysis of diagrams of responsibility assignment.

The paper presents a selection of example models of responsibility assignment derived from traditional contingency planning documents, constructed using the graphical notation we have developed. Using an approach comparable to the HAZOPS methodology, we illustrate how these models can be used to analyse the information requirements for each responsibility and associated vulnerabilities. Whilst the work described in this paper represents research in progress, the example models presented do illustrate the potential use of responsibility modelling concepts to assist in the contingency planning process.

Responsibility Modelling for Contingency Planning

Ian Sommerville, Tim Storer and Russell Lock

August 23, 2007

Abstract

This paper proposes the use of responsibility modelling as a tool to support the process of contingency planning for civil emergencies. Existing contingency planning techniques produce documents which are difficult to analyse for vulnerabilities, particularly across organisational boundaries and are likely to be largely unused during an actual emergency. This paper presents a new approach to contingency planning based on the notion of *responsibility modelling* combined with HAZOPS analysis of information requirements. Whilst the work described in this paper represents research in progress, the example models presented do illustrate the potential use of responsibility modelling concepts to assist in the contingency planning process.

Contents

1 Introduction

The task of planning for contingencies takes place in the wider context of civil defense. Associated activities include risk assessment and business continuity management. In addition, contingency planning requires inter–organisational communication to support planning for contingencies which cross organisational boundaries, as well as the coordination of communication with the wider public. Civil defense activities are undertaken by a wide variety of organisations, including, for example, police forces and charities. The purpose of contingency planning on an organisational basis, is to provide guidance on the procedures, resources and training that are likely to be required for a particular emergency response by those organisations involved. From an inter-organisational perspective, it is useful to understand the responsibilities that other agencies are expected to discharge, with less concern for detailing the manner in which this will be achieved.

The process of contingency planning involves multiple organisations, often with both individual and shared objectives. The complex relationships which are developed between organisations during contingency planning suggest that techniques previously used for the analysis of large scale complex socio-technial systems could be sucessfully applied to this area. In particular, this paper focuses on analysis of contingency planning and from the perspective of responsibilities. The papers proposes that *responsibility modelling* can be effectively employed to model and analyse the responsibilities that may need to be discharged during a response to a civil emergency.

Construction of responsibility models of contingency plans clarifies the analysis of modelled relationships for their appropriateness - whether an agent has been assigned a reasonable responsibility to discharge, for example. HAZOPS style "what if" risk analysis can also be applied to identify other vulnerabilities in the contingency plan. HAZOPS methodologies were designed to analyse industrial processes, predominantly in the chemical industry; however they have also been employed for the analysis of information systems [4, 14], in order to establish the consequences of failure of particular information flows. Some HAZOPS-type analysis is provided as part of the case study examples within this paper, to illustrate the potential of this approach.

1.1 Definition of Responsibility

The working definition of responsibility employed in this paper is as follows:

> *A duty, held by some agent, to achieve, maintain or avoid some given state, subject to conformance with organisational, social and cultural norms.*

The term 'duty' refers to more than simply a statement that a given task should be completed, it also encompasses aspects of accountability. It is important to note that failure to fulfill a given duty could in fact be due to circumstances beyond the control of the agent in question. It does not therefore follow automatically that the agent should be blamed for a given failure. The terms organisational, social and cultural norms relate to the inherent nature of responsibilities. Responsibilities are rarely broken down to individual instructions (for anything but the most trivial of system this would extremely difficult), instead they represent higher level constructs encompassing a remit for initiative. Initiative is bounded by professional conduct, from an organisational perspective as well as the wider social and cultural ones.

Given this abstract definition of both responsibility, this paper proposes that responsibility modelling can usefully be employed in the following general areas:

1. As a means of supporting discussion about systems that cross organisational boundaries. Responsibility misunderstandings in such situations are common and by making responsibilities explicit there is the potential to expose such misunderstandings.

2. As a means of supporting vulnerability analysis related to responsibility failure. Responsibility failure occurs when an agent does not discharge a responsibility as expected by other agents in the system.

3. As a means of helping to identify information requirements and vulnerabilities. Essentially, given an agent requiring specific information to discharge a responsibility what information is required, where does it come from, and what problems occur if it is unavailable, incomplete or incorrect.

4. As a means of conceptual system modelling. When attempting to understand and explain complex socio-technical systems, it may be helpful to create a conceptual system model in terms of the responsibilities in that system.

The paper will discuss how the different tasks within contingency planning can be supported by the different applications of responsibility modelling enumerated above.

1.2 Outline of this Paper

The paper is structured as follows. Section 2 provides background information on the process of contingency planning. Section 3 surveys the existing work on the use of responsibility modelling for the analysis of socio-technical systems. Section **??** presents the conceptual basis for the responsibility models used for the case study, discussed in Section 5. The case study presents a variety of examples of responsibility models constructed from a real world contingency plan. Section 6 describes future areas of research to be development and investigatedin line, as well as summarising the work described in the paper.

2 Contingency Planning

The process of preparing and planning for a civil emergency is illustrated in Figure 1, extracted from the UK government's guidance on the Civil Contingencies Act 2004 [13, 5]. Contingency planning is a cyclic activity, divided into two major processes.

For the consultation phase it is first necessary to identify which emergency scenarios are of interest. Emergency scenario selection is informed by the risk assessment process, which identifies vulnerabilities in civil infrastructure. However, it should be noted that the criteria for selecting scenarios, the next stage of planning, are not necessarily based on the severity or expected frequency of an incident, but are often politically motivated. For example, planning for the provision of fallout shelters during the Cold War was motivated largely by political considerations, as the probability of use was relatively low, the envisaged costs considerable, and the end benefits difficult to quantify [20].

Before plans can be established for a specific emergency scenario, it is first necessary to consult with the organisations which would be involved in the response to an incident. In the

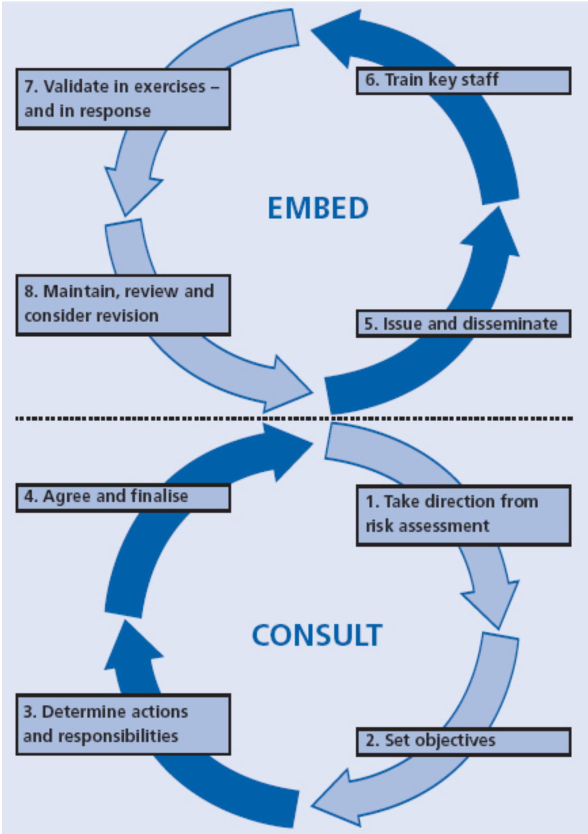

Figure 1: The emergency planning cycle, extracted from [13]. The cycle consists of two major processes; consultation and implementation.

United Kingdom, response organisations are coordinated by Civil Resillience Forums, which provide an administrative basis for contingency planning across organisations. The outcome of the consultation process is a set of responsibilities assigned to different agencies in the event of an incident. It is important to note that the contingency planning process brings together organisations with conflicting, rather than wholey complementary objectives, as such efforts towards providing greater clarity in the contingency planning process are beneficial, especially in preventing misunderstandings at later stages of the process.

During the Embedding phase the outline plan is disseminated to relevant organisations in order to both inform and assess the appropriateness of the plan for each organisational domain. Appropriate training can then be planned and undertaken. The robustness of an emergency plan and the training provided to personnel is frequently evaluated using emergency incident exercises. Such exercises may be "table top", i.e. largely simulated, or larger scale live exercises with appropriate deployment of resources to test the speed of response, reliability of communications infrastructure and so on. The use of exercises of this type is widespread, with government policy stating that exercises should take place for each scenario emergency plan on a regular basis. Exercises are designed to test the resilience of a given emergency plan and often lead to substantive changes afterwards. It should be noted that this is not necessarily recognition of flaws in the original plans, rather that the assumptions on which the original plan were written no longer hold.

A recurring theme identified in debrief reports of emergency response exercises are failures related to communication arrangements. Such reports describe how participants do not receive necessary information in order to discharge their responsibilities in a timely fashion, or similarly do not distribute information to others appropriately. The distribution of information is complicated by the need to anticipate who needs to know what to perform a given task, when they need to know it, and the consequences of inappropriate distribution of sensitive information. These information flow aspects of contingency planning form an integral part of the responsibility model currently under development, contingency planning therefore provides a suitable source of case studies for research into the application of responsibility modelling.

3 Responsibility Modelling

Responsibility modelling has been proposed by several authors as a useful construct for analysing the dependability of socio-technical systems. The work partly originates from the perceived failure of technical solutions, such as role based access control (RBAC) [15], to provide a sufficient abstraction of system dependability requirements [16].

A key preliminary to the development of responsibility analysis is the identification of a system as consisting of both technical and social / organisational entities; both of which contribute to the achievement of the overall goals or objectives that are the systems purpose. The term socio-technical system has been adopted by the software engineering community, in reference to the interactions that occur between human and organisational agents and software systems. In addition to achieving system goals, both social and technical entities contribute to the broader dependability of a system. The notion that human agents in a system, if employed appropriately, can contribute positively to the dependability of a technical system is one that is often missed from discussions on the topic [1].

Different types of agent (both technical and human) generally contribute to the dependability of systems in different ways. For example, whilst technical components can perform repetitive tasks efficiently, their failure to do so does not necessarily lead to system failure; human operators, with their greater flexibility can often deal with unplanned situations before failures become observable to those interacting with a given system. Given that both types of system entity are responsible for contributing to the overall dependability of a system, this paper will argue that an analysis of how responsibility for dependability is distributed throughout a system provides an insight into potential vulnerabilities of the system. For example, analysis of a given responsibility model may show how the allocation of a given responsibility to a single agent could prove a central point of failure for a work process should that agent fail in their duties; or identify where a responsibility has been inappropriately delegated to an unqualified agent. The analysis itself should form part of the dialogue between system analyst and the various stake holders in a system (i.e. it is domain specific), and could evolve with time.

Models of responsibility were first proposed by Blyth et al in the ORDIT methodology [2], a graphical notation for describing the responsibilities that agents hold with respect to one another. Strens, Dobson and Sommerville have argued for the importance of analysing responsibility, and the need to view roles with respect to the responsibility relationships they hold [11, 12, 19]. Dewsbury and Dobson have edited a collection of papers [10] that describe

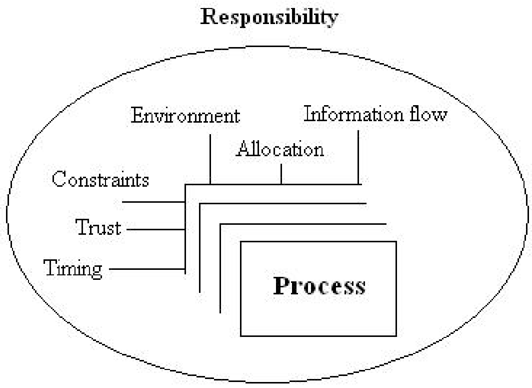

Figure 2: The responsibility concept

much of the research undertaken on responsibility as part of the DIRC project [1], presenting analyses of inappropriate responsibility allocation in socio-technical systems. The work also includes a graphical notation for responsibility by Sommerville. The purpose of the notation is primarily to support the discussion of responsibility allocations during a system development process [17], and in this respect is similar to the approach taken by proponents of the soft systems methodology [6].

Research on responsibility modelling differs from existing goal based techniques in a number of ways, despite appearing similar at first glance. Goal based modelling as seen in $i*$, and KAOS is designed to expose high level dependencies between objectives in a given system[CITATIONS,CITATIONS,CITATIONS]. Whilst responsibility modelling also encompasses the specification of high level objectives, its main benefits lie in the specification of more detailed information. For example the specification and analysis of information flows, concepts of temporal specification, branches within work flows, and most importantly the concept of environment when specifying a given decisions rationale. The approaches can more clearly be differentiated in 2 which illustrates the multi-fauceted nature of responsibilities beyond the mere definition of a process. The terms goal and process both define a state to achieve, and do not relate other information necessary to realistically make an agent responsible for them. For example doctors operate subject to ethics, companies operate subject to the data protection laws. These societal constraints are one example that would not necessarily be adequately explored by a goal model, or a straight forward workflow one.

More recently, we have revised the graphical notation proposed by Sommerville as a suite of related graphical views for a corresponding formal semantics of responsibility[18]. The views simplify the process of diagram (and hence model) construction by permitting inexperienced users to concentrate on particular aspects of a responsibility model at a time. In addition, tool support for the notation guides a user between different views, providing a sense of interconnection between the different views of responsibility. In this paper, we briefly discuss the basis for the revised model of responsibility, and present a selection of example diagrams in a case study, which illlustrate the different views of the responsibility model.

[1] `http://www.dirc.ac.uk`

4 Model of Responsibility

This section provides an informal explanation of the underlying model of responsibility adopted for use in the graphical views employed here; for more detail see [18]. Figure 3 provides a visual guide to the representative shapes used for examples in this paper. Intuitively, the model of responsibility presented in this paper is as follows. An *agent* (a generic abstract agent, or either technical, human or organisational) may become the holder of a *responsibility* for either an *objective* or a *process*, through an act of *delegation* by another agent, the responsibility *authority*. This relationship can be seen in Figure 4 Objectives and processes are collectively termed *targets* of responsibility. We distinguish between an objective, as a desirable state of affairs to be obtained or maintained, and a *process*, as a well defined activity to be followed by an agent or agents who are responsible for it. Note that in this definition, a responsibility bears closer resemblance to the "responsibility relationship" proposed by Dobson and Sommerville [12]. Similarly, the notion of a responsibility as an entity which may be discussed in isolation from other considerations as adopted by Sommerville [17], resembles the target of responsibility concept discussed here.

Both objectives and processes may be decomposed, effectively sub-divided, by the responsibility owner. An objective may be divided into a combination of sub-objectives and processes, whilst a process may only be divided into sub-processes. The extent to which this sub-division occurs is dependent on the context of a particular model, so no limitation is defined within the model. When the agent responsible for a given responsibility target decomposes that target, they are considered responsible for the decomposed responsibility targets, be they processes or objectives, until they have been explicitely delegated to others. The symbolism used to describe this process is visually is straightforward. The decomposition appears on a different diagram from its aggregate, to which it is then linked. Figure 5 illustrates this.

Process A indicates a process that is currently atomic, with no lower level of decomposition present at the time. Process B indicates a process that has been decomposed further, allowing traversal to its decomposition. Process C represents the lower level of decomposition, allowing traversal to its aggregation. In line with the conceptual model a given process can be decomposed, but cannot directly be decomposed a further time. Instead a given process is decomposed into a set of separate sub-processes, each of which could in turn be decomposed further. The same mechanism and graphical representation is employed for the decomposition of objectives to maintain consistency.

An agent may choose to delegate a responsibility relationship it created; creating a new responsibility relationship with a delegatee. Note, this approach explicitly excludes an agent delegating a responsibility for which it was the delegatee. Rather, two responsibility relationships may exist for the same target. For example if agent Ag is responsible for a given process to an Authority Au, if Ag delegates responsibility to another party, Ag would still be responsible to Au from Au's perspective.

The description of process decomposition given above, implies further relationships between processes as decompositions occur. When a process is decomposed, a set of "follows in sequence" relationships can be defined by a user, which indicates that processes must be completed sequentially. Further, follows in sequence relationships may be associated with information flows, indicating the information that a process requires before it may be executed, or information it passes, creates or modifies.

Thus far, the discussion of the responsiblity model has referred to two basic types, targets

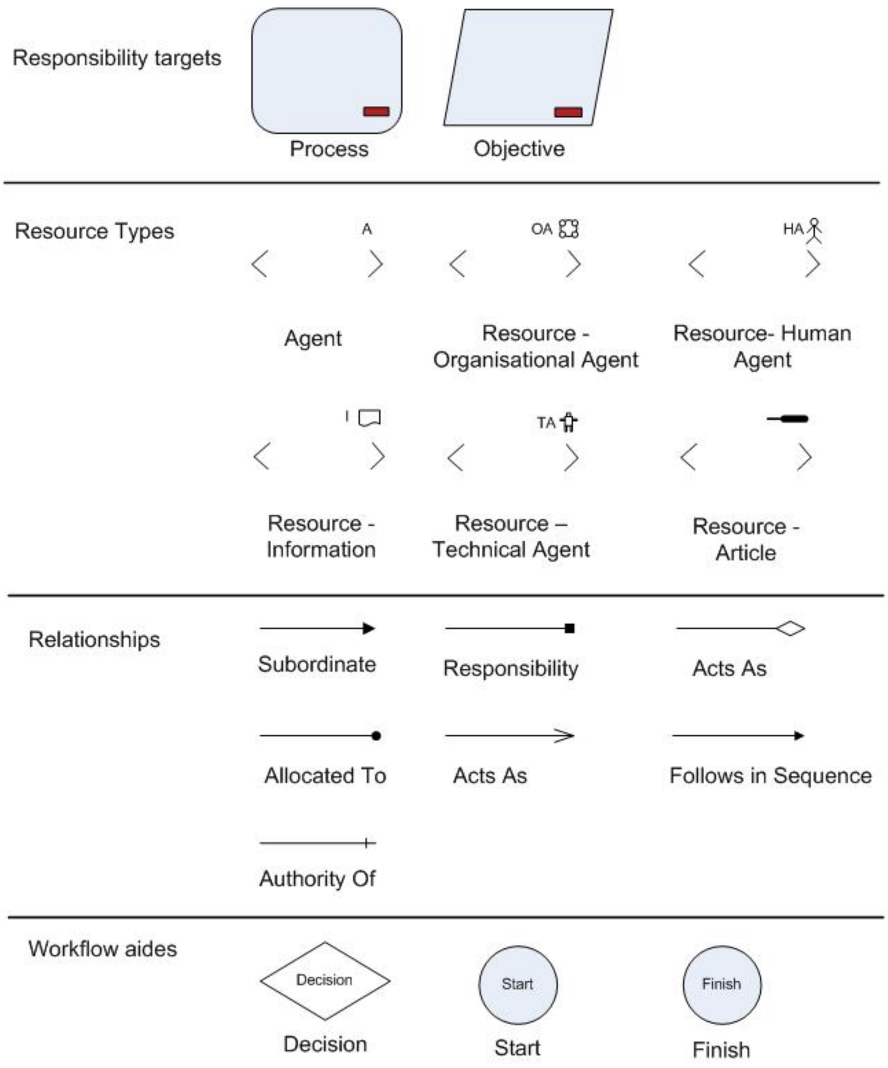

Figure 3: Responsibility Modelling Key

and agents. However, to provide more detail for responsibility scenarios, the notion of an agent may be generalised to that of a *resource*. Resources are artifacts in a responsibility model, and are categorised as agents, information and articles. Information resources are used to model the information requirements needed to discharge a responsibility, such as an evacuation priority list. Agents refer to resources with some degree of autonomy or ability to act independently, and are further sub-categorised as human, technical and organisational, to reflect the emphasis of the model on socio-technical systems. Physical resources refer to artifacts employed by an agent in order to discharge their responsibility, a web server to distribute public service information, for example. The distinction between a technical agent and an article, is to some degree undefined; it is anticipated that such a distinction should be made in individual contexts, dependent on the degree of autonomy a technical agent/article is considered to demonstrate.

Different subsets of the model of responsibility are employed in a suite of graphical views of responsibility. The views are implemented in a CASE tool, which provides users with

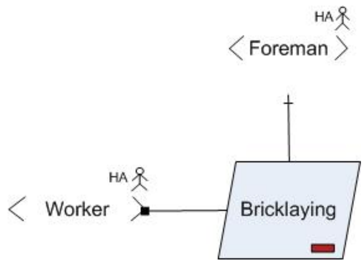

Figure 4: Responsibility Assignment

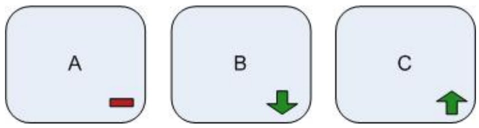

Figure 5: Process Decomposition

support for construction of model instances. The next section illustrates a selection of views on a particular instance of the model constructed on a case study of contingency planning. The views are illustrated graphically, rather than referring directly to the underlying responsibility model, in order to convey the manner in which the tool will be used.

5 Case Study

The case study material presented here has been gathered from a number of real world contingency planning documents. As the presentation of this research investigates the use of responsibility modelling rather the vulnerabilities in any particular councils preparations, the source of the documents is not stated.

Figure 6 shows the use of organisational entities. (ed: The plan does not care who co-ordinates these responsibilities, only that they are completed by that group of people)

Figure 8 shows the responsibilities associated with evacuation of the general public due to flooding. The diagram illustrates that although the police retain authority over such an operation, they delegate responsibilities to other agencies to aide in the undertaking of such activities. Focusing in on one particular aspect of this, prior to any given flooding incident data is collected, and presumably updated, to reflect the population occupying flood risk areas to aide in decision making and resource allocation when flooding takes place. Taking a simplified HAZOPs approach we can analyse this aspect of the plan for vulnerabilities related to this particular input. HAZOPs focuses discussion on the risk of problems occurring related to information flow, as well as aiding in the development of mitigation strategies.

Table 1 shows a HAZOPS description of the risks associated with the evacuation data information Resource. The guide words employed in the analysis are: never arrives, arrives late, arrives early, and arrives inaccuate. In each case, the probability and consequences of the risk occuring are stated. For example, inaccurate information on evacuation data is likely. Such information would need to be update on a regular basis, must take into account seasonal shifts. For example caravan parks may be empty during the winter. Such data is inherently innacurate, partly due to the need for statistical averaging in order to make the task of information gathering tractable. Some contingency plans make use of the family

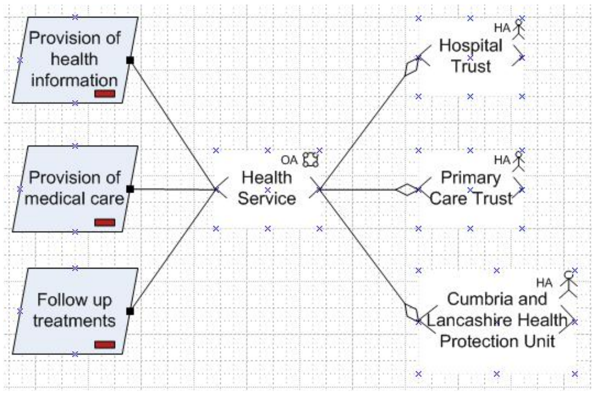

Figure 6: Health Service Responsibilities

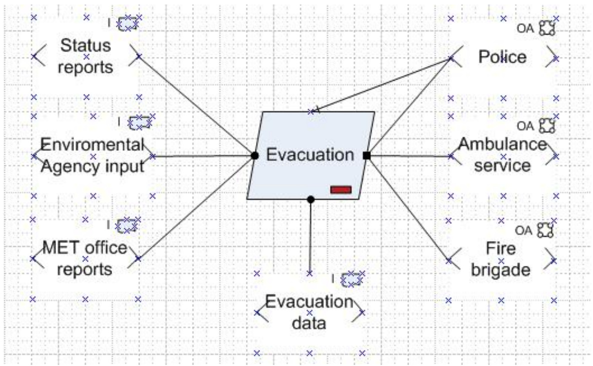

Figure 7: Evacuation responsibilities

2.4 multiplier, which would never be completely accurate, and would be dependent on the makeup of the area it was applied to. The level of risk identified here may, for example highlight the importance of keeping reserves in place to deal with sudden surges of demand due to inaccurate data.

Note also that the “early” guide word is included in the HAZOPS analysis for completeness. The ”early” guide word could for example be used to illustrate that overloading agents with information before it is needed could cause issues.

Analysis of this type would allow planners to highlight vulnerabilties which require remedial attention, and although much of the information held therein could be percieved as obvious to an experienced planner, may not to an unexperienced one. The very nature of contingency planning makes the availability of experienced personnel during actual emergencies something that cannot be entirely determined in advance.

Figure 9 shows responsibility assignment, at a very high level of the organisations involved in flood assistance. There are in fact a number of important tertiary organisations including the salvation army etc, but these have been left of for brevity. Whilst many organisations have specific roles to play in inland flooding there are also organisations which cannot necessarily be counted upon to give assistance, but may be able to. The RNLI is a voluntary organisation and as such cannot be an integral provider of resources and skills to a given emergency but can still provide important aide when appropriate. This can be seen by the fact that the RNLI is listed on the diagram as a potential resource (illustrated by the line

Responsibility: **Evacuation**			
Information	Guide Word	Consequence	Probability
Evacuation Data	Never	Emergency services will have to deal with unanticipatable demands	Low
	Late	Emergency services may evacuate people in an ineficient order	medium
	Early	-	-
	Inaccurate	May lead to unanticipated demand for additional resources	High

Table 1: HAZOPS analysis of the evacuation list resource.

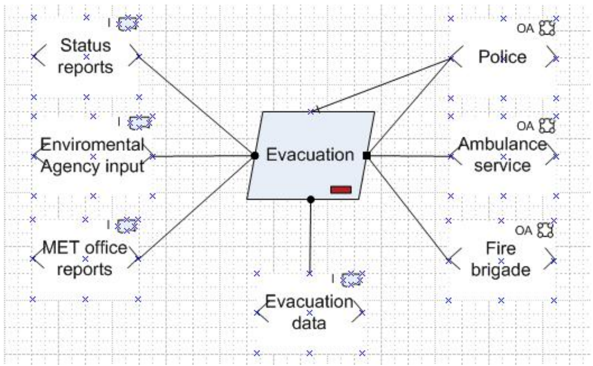

Figure 8: Evacuation responsibilities

with end circle connection), rather than a responsibility holding organisation (illustrated by the square connector). Further decomposition of the RNLI construct within the model could give information on its potential capabilities etc; all of which could prove useful during the contingency planning phase in addition to that of the handling of actual emergencies.

Figure 10 illustrates the need for constraint specification within responsibility models. The use of cellular networks in particular raise a number of issues that need to be outlined in order to identify possible responsibility vulnerabilities. In most emergency operations communications play an important role. Personnel equiped with mobile phones as resources could be affected by constraints including:

1. Power, both for individual units and for mast relays
2. Availability of specially equiped handsets in the event of the activation of the ”Access Overload Control System” which can, in emergencies filter traffic to allow communication only by enabled handsets
3. Operation of the existing fixed line system. Subject to power, the mobile network often operates beyond that of the fixed exchanges in flooding situations; however communication with fixed lines would still only be possible if the fixed exchanges were still in service.
4. Cost implications. Although in actual emergencies these constraints are often relaxed, contingency planning is designed to consider the provisioning of such resources in the

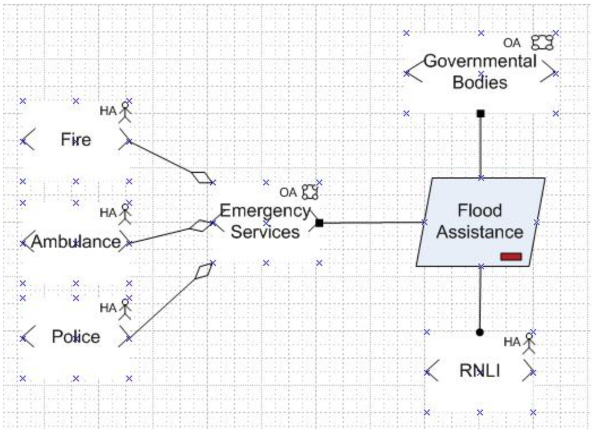

Figure 9: Flood assistance responsiility assignment

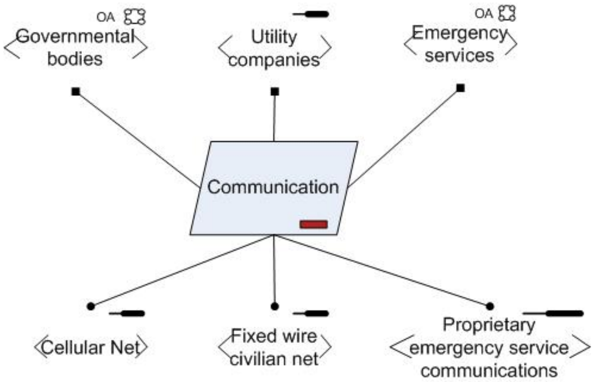

Figure 10: Communications

lonf term. This constraint could, for example affect the number of handsets in circulation for emergencies.

The use of data models for storage of such information allows easy cross referencing and analysis to enable users to determine vulnerabilties exposed by constraints breaking.

6 Conclusions and Future Work

This paper has described the potential for applying the notion of modelling responsibility to the task of contingency planning for civil emergencies. The paper represents a recently developed work in progress, with the intention that further work with organisations such as the Scottish Environmental Protection Agency (SEPA) will develop the work further. In particular, observations of emergency exercises will provide an opportunity to understand the manner in which contingency plans are executed in response to an incident (this does not necessarily refer to a plan document). Several specific avenues of future research are discussed below:

Timeliness One significant omission from the model of responsibility assignment used within these examples is the notion of timely discharge of an agent's responsibility. A desirable extension to the model would be to describe not only the dependencies of an agent, but the time constraints of those dependencies. One potential approach would be the integration of the model of timeliness proposed by Burns et al [3] into the semantics of responsibility assignment described above. Other possible approaches to this area can be seen in the literature for KAOS [8] and *i** [21].

Integration with Communications Infrastructure As noted above, the failure of communication between incident responders is a recurring theme of debrief reports. Whilst the CASE tool under development for responsibility modelling described here supports the description of information resource requirements for high level responsibilities, currently a user is still required to effect the results of analysing a responsibility model (i.e. convey information as suggested by the tool to the appropriate organisation). One potential avenue of future research is the integration of the responsibility model with a communications infrastructure, such that the communication infrastructure is able to query the model automatically for end point information for messages.

This paper describes work undertaken within the InDeED project, which investigates the potential of applying the notion of responsibility modelling to the process of contingency planning. The paper describes the conceptual approach to modelling responsibility and some aspects of the associated graphical notation using examples extracted from a case study of a response to a flooding emergency. To support the use of responsibility modelling in realistic contingency planning case studies, a prototype CASE tool is under development. The tool will provide some automatic diagram construction features, as well as analysis tools for the model developed.

References

[1] Dennis Besnard and Gordon Baxter. Human compensations for undependable systems. Technical Report CS-TR-819, School of Computing Science, Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK, November 2003.

[2] Andrew J.C. Blyth, Jarnail Chudge, John E. Dobson, and M. Ros Strens. ORDIT: A new methodology to assist in the process of eliciting and modelling organisational requirements. In S. Kaplan, editor, *Proceedings on the Conference on Organisational Computing Systems*, pages 216–227, Milpitas, California, USA, 1993. ACM Press.

[3] A. Burns, I.J. Hayes, G. Baxter, and C.J. Fidge. Modelling temporal behaviour in complex socio-technical systems. Technical Report YCS-2005-390, University of York, 2005.

[4] David Bush. Modelling support for early identification of safety requirements: A preliminary investigation. In *Fourth International Workshop on Requirements for High Assurance Systems (RHAS'05 - Paris) Position Papers*, Paris, France, August 2005.

[5] Civil Contingencies Act, 2004. Ch. 36.

[6] Peter Checkland. *Systems Thinking, Systems Practice*. John Wiley & Sons, 1981.

[7] General emergency plan. Cumbria County Council, Arroyo Block, The Castle, Carlisle, CA3 8UR, August 2002.

[8] Robert Darimont, Emmanuelle Delor, Philippe Massonet, and Axel van Lamsweerde. GRAIL/KAOS: an environment for goal-driven requirements engineering. In W. Richards Adrion, editor, *ICSE'97: Pulling Together, Proceedings of the 19th International Conference on Software Engineering*, pages 612–613, Boston, Massachusetts, USA, May 1997. ACM Press.

[9] Anna-Louise Day. Carlisle storms and associated flooding multi-agency debrief report. UK Resilience, July 2005.

[10] Guy Dewsbury and John Dobson, editors. *Responsibility and Dependable Systems*. Springer-Verlag London Ltd, June 2007.

[11] John Dobson. New security paradigms: what other concepts do we need as well? In *NSPW '92-93: Proceedings on the 1992-1993 workshop on New Security Paradigms*, pages 7–18, Little Compton, Rhode Island, United States, 1993. ACM Press.

[12] John E. Dobson and Ian Sommerville. Roles are responsibility relationships really. To appear IEE Symposium on People and Computers, October 2005.

[13] Emergency preparedness. HM Government, November 2005. Guidance on Part I of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements.

[14] John. A. McDermid and David J. Pumfrey. A development of hazard analysis to aid software design. In *Compass'94: 9th Annual Conference on Computer Assurance*, pages 17–26, Gaithersburg, MD, 1994. National Institute of Standards and Technology.

[15] Ravi S. Sandhu, Edward J. Coyne, and Charles E. Youman. Role-based access control: A multi-dimensional view. In *Proceedings fo the 10th Annual Computer Security Applications Conference*, pages 54–62, Orlando Florida, December 1999. IEEE Computer Society.

[16] M. Angela Sasse. Computer security: Anatomy of a usability disaster, and a plan for recovery. In *Workshop on Human-Computer Interaction and Security Systems*, 2003.

[17] Ian Sommerville. Models for responsibility assignment. In Dewsbury and Dobson [10], chapter 8.

[18] Tim Storer and Russell Lock. An integrated model of responsibility for the analysis of the dependability of socio-technical systems. Project Working Paper 1, InDeED Project, 2007. `http://www.indeedproject.ac.uk/publications/responsibility-modelling.pdf`.

[19] Ros Strens and John Dobson. How responsibility modelling leads to security requirements. In *NSPW '92-93: Proceedings on the 1992-1993 workshop on New security paradigms*, pages 143–149, New York, NY, USA, 1993. ACM Press.

[20] Robin Woolven. Uk civil defence and nuclear weapons 1953–1959. UK Nuclear History Working Paper 2, Mountbatten Centre for International Studies, December 2006.

[21] Eric S. K. Yu. Agent-oriented modelling: Software versus the world. In Michael Wooldridge, Gerhard Weiß, and Paolo Ciancarini, editors, *AOSE*, volume 2222 of *Lecture Notes in Computer Science*, pages 206–225, Montreal, Canada, May 2002. Springer.