Responsibility modelling for contingency planning

This item was submitted to Loughborough University's Institutional Repository by the/an author.


Additional Information:

- This paper was prepared for Safety Critical Systems Club 2007, Workshop on Understanding Why Systems Fail, Contingency Planning and Longer Term Perspectives on Learning from Failure in Safety Critical Systems. It is a working paper from the InDeED project http://www.indeedproject.ac.uk/

Metadata Record: https://dspace.lboro.ac.uk/2134/8751

Version: Accepted for publication

Publisher: © InDeED project

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to: http://creativecommons.org/licenses/by-nc-nd/2.5/
Responsibility Modelling for Contingency Planning

Ian Sommerville, Tim Storer and Russell Lock

September 17, 2007

About Working Papers

Interdisciplinary Design and Evaluation of Dependability (InDeED) project working papers represent works in progress. Papers may be published in the series for internal project comment, or to the project website for external comment. Papers in the series may be incomplete as they represent working documents, and they explicitly do not describe the settled views of the authors concerned.
### Revision Log

<table>
<thead>
<tr>
<th>Revision</th>
<th>Author</th>
<th>Date</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>355</td>
<td>tws</td>
<td>28/06/07</td>
<td>Added working paper cover.</td>
</tr>
<tr>
<td>353</td>
<td>tws</td>
<td>27/06/07</td>
<td></td>
</tr>
<tr>
<td>342</td>
<td>tws</td>
<td>18/06/07</td>
<td></td>
</tr>
<tr>
<td>340</td>
<td>tws</td>
<td>15/06/07</td>
<td>Added hacked logo. modified some contingency planning diagrams for workshop paper and slides in June.</td>
</tr>
<tr>
<td>338</td>
<td>rl</td>
<td>15/06/07</td>
<td>tweaking</td>
</tr>
<tr>
<td>337</td>
<td>tws</td>
<td>15/06/07</td>
<td></td>
</tr>
<tr>
<td>336</td>
<td>tws</td>
<td>15/06/07</td>
<td>finished first draft of slides for contingency planning.</td>
</tr>
<tr>
<td>331</td>
<td>tws</td>
<td>12/06/07</td>
<td></td>
</tr>
<tr>
<td>330</td>
<td>tws</td>
<td>12/06/07</td>
<td>typos</td>
</tr>
<tr>
<td>324</td>
<td>tws</td>
<td>07/06/07</td>
<td></td>
</tr>
<tr>
<td>245</td>
<td>rl</td>
<td>22/05/07</td>
<td>typos, paper should now be ready for circulation</td>
</tr>
<tr>
<td>241</td>
<td>tws</td>
<td>14/05/07</td>
<td></td>
</tr>
<tr>
<td>238</td>
<td>rl</td>
<td>11/05/07</td>
<td>re-ext cont plan sec</td>
</tr>
<tr>
<td>237</td>
<td>tws</td>
<td>10/05/07</td>
<td>Added citation on nuclear bunkers.</td>
</tr>
<tr>
<td>236</td>
<td>tws</td>
<td>10/05/07</td>
<td></td>
</tr>
<tr>
<td>235</td>
<td>rl</td>
<td>10/05/07</td>
<td></td>
</tr>
<tr>
<td>234</td>
<td>tws</td>
<td>09/05/07</td>
<td>First complete (ropey) draft complete. Needs a nuclear shelter quotation from RL.</td>
</tr>
<tr>
<td>233</td>
<td>rl</td>
<td>09/05/07</td>
<td>changed i* ref</td>
</tr>
<tr>
<td>232</td>
<td>tws</td>
<td>09/05/07</td>
<td></td>
</tr>
<tr>
<td>231</td>
<td>tws</td>
<td>09/05/07</td>
<td>Added figures for hazops section and alert section.</td>
</tr>
<tr>
<td>230</td>
<td>tws</td>
<td>09/05/07</td>
<td>Added hazops analysis section.</td>
</tr>
<tr>
<td>229</td>
<td>rl</td>
<td>09/05/07</td>
<td></td>
</tr>
<tr>
<td>228</td>
<td>tws</td>
<td>09/05/07</td>
<td></td>
</tr>
<tr>
<td>221</td>
<td>rl</td>
<td>08/05/07</td>
<td>typos</td>
</tr>
<tr>
<td>218</td>
<td>tws</td>
<td>01/05/07</td>
<td>Extended case study description. Some revisions to introduction.</td>
</tr>
<tr>
<td>217</td>
<td>rl</td>
<td>01/05/07</td>
<td>typos</td>
</tr>
<tr>
<td>213</td>
<td>tws</td>
<td>30/04/07</td>
<td>Added section describing conceptual model of responsibility (mostly).</td>
</tr>
<tr>
<td>212</td>
<td>tws</td>
<td>30/04/07</td>
<td>Merged with RL’s revision of introductory sections.</td>
</tr>
<tr>
<td>209</td>
<td>rl</td>
<td>27/04/07</td>
<td>chopped bit from overweight abstract</td>
</tr>
<tr>
<td>208</td>
<td>rl</td>
<td>27/04/07</td>
<td>sorted out the introduction, largely rewritten to make it slightly less pants...</td>
</tr>
<tr>
<td>207</td>
<td>rl</td>
<td>26/04/07</td>
<td></td>
</tr>
<tr>
<td>203</td>
<td>rl</td>
<td>26/04/07</td>
<td>changed labelling, end of intro</td>
</tr>
<tr>
<td>202</td>
<td>rl</td>
<td>26/04/07</td>
<td>rejigged intro</td>
</tr>
<tr>
<td>200</td>
<td>tws</td>
<td>26/04/07</td>
<td>Modified abstract, corrected citation entries.</td>
</tr>
<tr>
<td>199</td>
<td>tws</td>
<td>25/04/07</td>
<td></td>
</tr>
<tr>
<td>197</td>
<td>rl</td>
<td>25/04/07</td>
<td>added intro</td>
</tr>
<tr>
<td>196</td>
<td>rl</td>
<td>25/04/07</td>
<td></td>
</tr>
<tr>
<td>193</td>
<td>tws</td>
<td>25/04/07</td>
<td></td>
</tr>
<tr>
<td>192</td>
<td>tws</td>
<td>23/04/07</td>
<td>began case study description</td>
</tr>
<tr>
<td>191</td>
<td>rl</td>
<td>23/04/07</td>
<td></td>
</tr>
<tr>
<td>188</td>
<td>tws</td>
<td>23/04/07</td>
<td>Began constructing diagrams for case study on ambulance service. Added some scraps of text to introduction and motivation sections.</td>
</tr>
</tbody>
</table>
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.

Extended Abstract

Responsibility Modelling for Contingency Planning

Ian Sommerville, Tim Storer and Russell Lock

September 17, 2007
Responsibility Modelling for Contingency Planning

Ian Sommerville, Tim Storer and Russell Lock

September 17, 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 ................................................. 3

2 Contingency Planning ................................... 3

3 Responsibility Modelling ................................ 5

4 Model of Responsibility .................................. 6

5 Case Study .................................................. 7
   5.1 Background ............................................. 8
   5.2 Responsibilities in Different Environments .......... 9
   5.3 Evacuation ............................................... 11
   5.4 Cascade Alert System .................................. 14
   5.5 Discussion: Uses of Responsibility Modelling for Contingency Planning .... 15

6 Conclusions and Future Work ............................ 15
1 Introduction

The process of contingency planning supports a variety of different processes in the wider activity of civil defense. These include risk assessment, business continuity management, inter-organisational cooperation, coordination and communication, as well as communicating with the wider public. The activities are undertaken by a wide variety of organisations, including, for example, police forces and charities. The purpose of contingency planning 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.

The process of contingency planning involves multiple organisations, each with 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 emergency response 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 permits 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 may also be applied to identify other vulnerabilities in the contingency plan. HAZOPS was designed to analyse industrial processes, predominantly in the chemical industry; however it has also been employed for the analysis of information systems [4, 14], in order to establish the consequences of failure of particular information flows for a system. Some HAZOPS-type analysis is provided as part of the case study examples within this paper, to illustrate the potential of this approach.

The paper is structured as follows. Section 2 provides background information on the process of contingency planning. Section 3 provides an insight into the development of more dependable systems through the use of responsibility modelling techniques. Section 5 illustrates through use of real world examples how responsibility modelling can be applied to the domain of contingency planning. Section 4 provides information on the model of responsibility used in the case studies. Section 6 provides information on the future progression of the research in line with our use of real world case ethnographic case studies, 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
Figure 1: The emergency planning cycle, extracted from [13]. The cycle consists of two major processes; consultation and implementation.

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 United Kingdom, response organisations are coordinated by Civil Resilience 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 wholly 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 sufficiently high level abstraction of system dependability requirements [16]. Whilst technical measures can contribute to the dependability of a system, they generally fail to provide dependability of large complete systems because they do not account for human behaviour. A broader view of how human users interact with technical components of a system is necessary in order to understand how human, social and technical measures can contribute to an overall system.

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 a software system. 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]. However, it is common for different types of agent in a system to contribute to overall dependability in different ways. For example, technical components provide a reliable means of performing repetitive tasks or routines, whilst human operators provide for the handling of unexpected exceptions which cause a technical agent to fail. 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. In addition, an analysis of this form allows for consideration of both the constraints on, and resources available to an agent with respect to the responsibilities it may be required to discharge.

As well as identifying the vulnerabilities in a system, an analysis of responsibilities may also identify changes to the responsibility relationships or constituent agents of a system that
provide an increased assurance of system dependability. The analysis may, for example, show how only allocating a 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 complex nature of agent capabilities, the nature of resources and the meaning of a particular responsibility require the analysis to be a part of the dialogue between system analyst and the various stakeholders in a system (i.e. it is domain specific), and may 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 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].

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 inter-connection 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 illustrate the different views of the responsibility model.

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]. Intuitively, the model of responsibility presented in this paper is as follows. An agent (either human or automated) 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. 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 limita-
tion is defined within the model. When an agent decomposes a responsibility target, they are considered to be the creator of the new targets and (initially, at least) responsible for them. 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.

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 are defined by a user, which indicate one process must be completed, before another may be executed. Further, follows in sequence relationships may be associated with messages, indicating the information that a process requires before it may be executed.

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

Figure 2 gives a conceptual overview of the model of responsibility model adopted here. The figure shows the hierarchies of basic entities in the model of responsibility; the relationships between entities and the functions which may be used to alter the model. 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 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

This section provides a selection of responsibility views of a responsibility model constructed from a case study of a particular civil contingency. The diagrams are derived from the debriefing report for the Carlisle storms in January 2005 [9]; and the Cumbria County Council General Emergency Plan[7], which provided the initial basis for the response to the flooding. The diagram presented illustrate particular examples from the debrief report where the misunderstanding or mis-assignment of responsibilities caused difficulties during the response. The purpose of the case study is to demonstrate how a responsibility modelling approach can be used to illustrate, analyse and support the discussion of vulnerabilities in a contingency plan. The case study does not demonstrate by itself that the use of the responsibility modelling notation would be sufficient to identify vulnerabilities in a contingency plan prior
Figure 2: Summary of concepts in the model of responsibility. An instance of the model consists of sets of the entities and relationships illustrated. The state of the model can be altered by the operation.

to an emergency, since the model in this case was constructed “after the fact”. Successful identification of vulnerabilities during the construction of a plan would require an appropriate methodology which employs the graphical notation. In addition, modelling and analysis needs to be undertaken by domain experts (in this case, emergency response and flooding events), to be effective; the work presented in this case study represents analyses constructed on the basis of written documents and would be of primary use as a basis for initiating discussions, rather than an end-product. Rather, the case study demonstrates the potential for responsibility modelling to express vulnerabilities graphically, providing a basis for clearer identification and discussion of vulnerabilities during planning.

5.1 Background

Between 7th and 8th of January 2005, the north west of England and, in particular, the city of Carlisle suffered substantial flooding due to heavy rainfall. The flooding was a combination of the heavy rainfall and the blocking of drainage channels by debris caused by the storms. In addition to the flooding, the severe storms caused structural damage to buildings and caused 24 large vehicles to be blown over, blocking major access roads. The flood was worsened by the increased flow of water down the river Eden from further up-stream, causing the river to burst its banks.

An early consequence of the flooding was the loss of several premises significant to the emergency response, including the police headquarters, the fire service headquarters in Carlisle
and the city’s Civic Centre, which would otherwise have been used as a reception centre for evacuees. The loss of the police HQ meant the loss of a number of IT systems that would otherwise have been employed in the command and control of the response. In addition, by the morning of the 8th, electrical power throughout Carlisle had been lost due to the flooding of a critical substation. Mobile phone communications were also affected. By late afternoon on the same day, the UHF radio transmitter on the civic centre began to fail as its batteries exhausted.

As a consequence, the Cumbria General Emergency plan was invoked by the Deputy Chief Constable of Cumbria, and a major incident was declared. Gold and Silver commands were established at Penrith police station, and at Carlisle Castle respectively. The transfer of command and control functions to these alternate premises caused immediate difficulties, since the new IT suite at Penrith had not yet been completed, and gold command did not have access to relevant local information (maps of Carlisle etc) at their new location. In addition, the move between premises resulted in a degrading of the communications between Gold and Silver commands.

To respond to the emergency, the police established a mobile police station in the city centre and initiated a search and rescue operation in conjunction with the Fire Service in the areas affected by flooding. This included the establishment of rendezvous locations near to the flooded areas. The local Ambulance Service Trust were responsible for transportation of evacuated residents from rendezvous locations to reception centres, as well as supporting medical care in the centres. Boats and RAF helicopters were used to assist in the evacuations. Three reception centres were established for evacuees and provisioned with essentials, including food and emergency generators. In addition to the immediate response, Gold command also coordinated communications with the media in order to distribute information, including advice to evacuate areas of Carlisle where possible.

Recovery from the emergency began on the 10th, with flood waters beginning to subside and forecasts indicating reduced rain-fall. The focus of the emergency response began to move to planning for the hand over of control to the local authority, although systematic house-to-house searches continued. Pumps began to be deployed throughout Carlisle, but in particular at the sub-station responsible for supplying electrical power to much of the city. During the day partial rail and bus services were restored, although schools remained closed. Power, telephone and cable services were gradually restored throughout the week, with complete restoration achieved on the 12th. Handover to the city council occurred on the morning of the 13th.

The remainder of this section presents a selection of responsibility models based on aspects of the emergency described above, but also with reference to the emergency plan initially used to coordinate the response where appropriate.

5.2 Responsibilities in Different Environments

A significant factor within emergency response is that the responsibilities assigned to an agent are dynamic and dependent on environmental conditions. The environment in which a responsibility is held refers to the set of circumstances which influence how an agent chooses to discharge that responsibility, e.g. through delegation of responsibilities to different agents. In the modelling approach we have adopted, the different conditions are presented as alternative diagrams for comparison.

Figure 3 illustrates some of the different responsibilities held by the Ambulance Service
Trust responsibilities in typical operating conditions.

(b) Trust responsibilities during the flooding.

Figure 3: Ambulance Service Trust Responsibilities in two different environments. Figure 3(a) illustrates the responsibilities allocated to the Trust in typical operating circumstance. Figure 3(b) illustrate the additional responsibilities allocated to the Trust during the flooding. The implication from the two different environments is that the resources allocated to the Trust during an emergency should be reviewed.

Trust agent during normal and exceptional conditions due to flooding. During normal operation, the Trust is responsible for responding to emergency calls which require a medical response, but is also responsible for monitoring for major incidents. Figure 3(a) illustrates these two responsibility relationships (the authority relationships are omitted). Objective targets of responsibility are denoted as cloud like objects. Agents are denoted by text enclosed by angle brackets. Responsibility relationships are denoted by edges drawn between the agent (the Trust) and the target of responsibility, terminated by a filled square.

Once an emergency incident has been invoked, the environment in which the Trust operates has changed, as it has been delegated two new responsibilities, and considered to have discharged its responsibility to monitor for a major incident. The two new responsibilities assigned to the Trust in the figure are to assist in evacuation (by transporting evacuees from rendezvous locations to reception centres) and to provide medical assistance at the newly opened reception centres. In the former case, the responsibility to assist in the evacuation of residents from rendezvous points was not documented in the emergency plan used during the response, although the plan does list a general responsibility for the trust to make Trust resources available as required by the nature of the emergency:

“Deploy ambulance resources, as required, to the scene of an incident...coordinate the deployment of ambulance resources at the scene.” [7]

This figure captures the responsibility of the Trust to provide ambulances in a variety of roles, dependent on the environment, i.e. the nature of the emergency. However, the responsibility to evacuate residents from rendezvous locations to reception centres requires specific information resources, which the ambulance service did not initially receive - a requirement discussed in greater detail in Section 5.3. In the latter case, the responsibility to provide medical assistance at reception centres is documented in the Emergency Plan [7, s1, pp6], and the Trust were able to discharge this responsibility once they had been notified that a major incident had been declared (See Section 5.4). Figure 4 illustrates the transformation on
(a) Prior to delegation.  (b) Delegated responsibility relationship.

Figure 4: Delegation of a responsibility to an allocated agent-resource. The Ambulance Service Trust delegates responsibility for providing medical care at reception centres to the St Johns Ambulance. Note that the Trust retains a responsibility relationship to Gold command for providing the medical centres, which is distinct from the relationship between the Trust and the St Johns Ambulance.

the model of responsibility used to illustrate how the Trust delegates responsibility for medical care at reception centres to a resource it has been allocated; the St Johns Ambulance, a voluntary organisation. Figure , illustrates the responsibility relationship for the medical centres between the Trust (the holder of the responsibility) and Gold command (the Authority). The authority relationship is denoted by an edge drawn from the responsibility target to the authority agent, with the line terminated by a cross. In addition, the St Johns Ambulance is illustrated as a resource allocated to the Ambulance Service. In Figure 4(b), the model of responsibility has been transformed by the creation and delegation of a new responsibility relationship. The Trust creates a new responsibility for providing medical assistance to the reception centres as a means of discharging its responsibility to Gold command. The new relationship is then delegated to the St Johns Ambulance, so that the Trust is now the authority for the responsibility relationship. Note the emphasis on responsibility relationships for the same objectives in the model. The St Johns Ambulance is responsible to the Trust for providing medical care in the reception centres, whilst the Trust is responsible to Gold command for the same objective.

5.3 Evacuation

As described in the background to the case study, as part of the planned response to the flooding, the Police Force were responsible to Silver Command for evacuation of residents from flooded premises, whilst the Fire Service were responsible for search and rescue operations. The state of responsibilities anticipated in the construction of the Emergency Plan is illustrated in Figure 5(a). In addition, the figure illustrates the informational resources required by the Police Force in order to discharge their responsibility:

**Priority List** The list of residences that should be evacuated as a priority. These include, for example, nursing homes and residential care homes.
Evacuated List A list of residences that have already been evacuated, either by the police, or by the residents themselves. This list allows the police to avoid visiting every residence and concentrate resources on priorities.

Rendezvous Locations A list of locations where the Fire Service are able to leave rescued residents so that they can be evacuated to reception centres by the police.

During the response to the flooding, it became apparent that the Police Force required assistance in evacuating residents from rendezvous locations to reception centres. To provide for the extra capacity, the Police Force delegated responsibility for assisting in evacuation to the Ambulance Service Trust. Figure 5(b) illustrates the responsibilities regarding evacuation after the delegation. The Trust has been assigned a new responsibility created by the Police Force to “Assist Evacuation” (with the Police Force as authority). In addition, the figure illustrates the allocation of the Rendezvous Locations information resource to the Trust. The
Table 1: HAZOPS analysis of the Rendevous Locations list.

<table>
<thead>
<tr>
<th>Responsibility: Assist Evacuation</th>
<th>Information</th>
<th>Guide Word</th>
<th>Consequence</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rendevous Locations</td>
<td>Never</td>
<td>Ambulances are unusable for evacuation of rendevous locations</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Late</td>
<td>Ambulances are only usable later during the response once correct rendevous locations are established</td>
<td>medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Early</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Inaccurate</td>
<td>Resources are wasted because some ambulances are sent to incorrect rendevous locations.</td>
<td>medium</td>
<td></td>
</tr>
</tbody>
</table>

Trust needs the information for the same reason as the Police Force. The need for rendevous locations to be agreed and shared is noted here, since the debrief report from the Trust describes how:

“The Trust was requested to supply vehicles to assist in the movement of people from the affected areas although there was confusion regarding a rendezvous point (RVP). Fire and Police requests for vehicles to assist with the evacuation were to addresses that were inaccessible and not to a predetermined RVP.” [9, pp68]

The Trust’s debrief report suggests that rendezvous locations agreed prior to the flooding were changed, and that alternative locations also became unavailable during the course of the flooding. The report is of interest, since it describes how an agent was delegated a responsibility for an objective, but lacked the associated information resources in order to effectively discharge that responsibility. Figure 5(b) illustrates the information required by the Trust to discharge its responsibility, but does not provide an analysis of the consequences if that information is unavailable or inaccurate. For this purpose, a HAZOPS analysis of information resources can be employed [4, 14].

For a HAZOPS analysis, risks associated with information resources are identified using context relevant guide words (late, unavailable, inaccurate, early etc). The risks are then assessed for consequences for the system should they occur. Applying HAZOPS analysis to models of responsibility provides a means of analysing the information requirements associated with the effective discharge of a responsibility; that is, what does an agent need to know in order to discharge their assigned responsibility? For contingency planning, the analysis provides a means of assessing potential vulnerabilities in planning documents, if for example, an agent has been assigned a responsibility it lacks the relevant information for.

Table 1 shows a HAZOPS description of the risks associated with the Rendevous Location Information Resource. The guide words employed in the analysis are never arrives, arrives late, arrives early, and arrives inaccurate. In each case, the probability and consequences of the risk occurring are stated. For example, the risk that the Trust receives inaccurate information results in ambulances being sent to the wrong locations, wasting resources that could be deployed elsewhere. This reflects the situation in which the Trust is not updated on new locations being used by other agents. Note also that the “early” guide word is included in the HAZOPS analysis for completeness. The guide word is useful because in some circumstances it
may be preferred to not give certain information to some agents too soon; the Silver command may not wish to distribute the fact that a road has been cleared to the public for example, if the road is needed for priority traffic.

In addition to analysing plan vulnerabilities, the analysis may provide guidance to coordinators during an on-going emergency response in which responsibilities are assigned dynamically. In such circumstances it is desirable to identify what information resources should be allocated to an agent when it is assigned a responsibility. The RM/HAZOPS analysis provides this guidance by identifying the information resources required to discharge generic responsibilities, allowing a coordinator to consider which of the information resources are required to discharge the new responsibility. In the example given by Figure 3, the model of responsibility illustrates the information resources employed by the Police Force to discharge responsibility for evacuation. When responsibility to assist in the evacuation is delegated to the Trust, the analysis suggests that some of the information resources employed by the Police Force will also be required by the Trust; the HAZOPS analysis also provides a description of the consequences if the Trust does not obtain the information it requires - its ability to evacuate residents from rendezvous locations will be degraded.

5.4 Cascade Alert System

An early stage in the response to an incident is the notification of relevant organisations of the need to initiate their internal response procedures. The Cumbria Emergency Plan describes the manner in which the multiple agencies required to coordinate a response will be informed that a major incident has been declared through the use of a “Cascade Alert System.” In principle, the alert system is invoked by the Police Force, who are responsible for contacting other major responders, such as the Local Authority, the Fire Service and the local Ambulance Service Trust. The debrief document states that the alert process was invoked at 0800 on the 8th of January. However, the Ambulance Service Trust debrief report describes the Trust’s decision to declare a major incident in isolation from other agencies:

“At approximately 0945 hours the decision was made by the Trust to declare a major incident...At no time prior to the Trust declaring a major incident at 0945 hours, had any of the other agencies contacted the Trust with regards to declaring a major incident or to the activation of the contingencies within the Cumbria County Council General Emergency Plan (CCC GEP). Had the incident been declared as a major incident prior to 0945 hours and the alerting cascade as per CCC GEP carried out, the provision of supporting agencies would have been realised at an earlier time.”[9, pp66]

Figure 6(a) illustrates the expected mechanism for declaring a major incident from the perspective of the Trust. The Control Duty Manager (CDM), an employee of the Trust is responsible for monitoring for a declaration of a major incident. Monitoring is modelled as a process, since it is considered a well defined procedure. On receiving an alert the CDM is then responsible for initiating the Trust’s own cascade alert system, including notifying senior managers via the pager system, recalling staff and notifying the St John’s Ambulance (as discussed in Section 5.1). However, by 9:45, the Trust had not received notification via the alert system as expected, despite circumstances that suggested that a major incident declaration was appropriate. Rather than wait further for an alert via the County alert system, the
Trust instead declared a major incident based on the information available, including number of emergency calls, the loss of several ambulances due to the flooding, and the decreasing ability of the Trust to respond effectively to emergency calls due to reduced access. As a consequence, the Trust’s cascade system is initiated, although rather later than desirable.

5.5 Discussion: Uses of Responsibility Modelling for Contingency Planning

The preceding sections have presented three example views of a model of responsibility based on a general contingency plan and flooding incident debrief report. The views presented demonstrate three different applications of responsibility modelling to the management of civil contingencies. Responsibility modelling may be used to document, disseminate and analyse the responsibilities assigned to different organisations in a contingency plan. Figure 3 gives a simple example of this, illustrating the responsibilities of the Ambulance Service Trust in both normal and emergency incident environments. Modelling responsibilities also provides an analysis of the information required by an agent in order to discharge a responsibility; with the potential that the model be used in an operational context to determine information requirements of newly assigned responsibilities; Section 5.3 discusses this application. Finally, responsibility models may be used to document the assignment of responsibilities during an emergency incident or exercise and compare these with the assignments anticipated during the contingency planning process. Figure 6 illustrates how a planned assignment of responsibilities failed during the emergency response in the case study, and describes how the Trust recovered (locally) from external failures. In each of these applications, the same model of responsibility is employed, but analysed using different approaches and views.

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 com-
munication 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, cur-
rently 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 early 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**

Technical Report CS-TR-819, School of Computing Science, Newcastle upon Tyne, Clare-
mont 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

complex socio-technical systems. Technical Report YCS-2005-390, University of York,
2005.


