Chapter 13

Responsibility Modelling

Russell Lock, Loughborough University; Ian Sommerville, University of St Andrews and Tim Storer, University of Glasgow

Summary

Responsibility Modelling (RM) is a graphical modelling and analysis technique designed to help people record and analyse responsibilities within organisations, to explore the structure and dependability of socio-technical systems. RM uses 'Responsibility' as a unifying concept to explore the relationships between personnel, technical systems and information resources, within a systems' organisational structure. Associated with responsibilities are agents, who discharge the responsibility, and resources, which are used by agents. The graphical notation is accompanied by a risk analysis technique designed to improve dependability and resilience within the socio-technical system.

Background

Our work on responsibility modelling has been based on our socio-technical view of system dependability where we believe that the best way to improve dependability is to consider how people work with computers to achieve dependability. We were looking for a unified way to model socio-technical systems that could relate the human and automated agents in the system to their working environment.

Technical components are ideally suited towards consistent undertaking of repetitive tasks. Human operators, with their greater flexibility, can often adapt to unplanned situations before failures manifest themselves. The notion that human agents in a system, employed appropriately, can contribute positively to the dependability of technical systems is one that is often missed in discussions of software dependability.

For our purposes, we define a responsibility as:

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' in this context refers to both the undertaking of activities, and accountability for those activities. The phrase organisational, social and cultural norms relates to the inherent nature of responsibilities; that systems are adapted to fit the organisational culture they operate in, and that processes are subject to both social and legal compliance. RM was first proposed during the development of the ORDIT methodology in 1993. ORDIT defined a graphical notation to describe the responsibilities held between human agents within socio-technical systems. The ideas were developed in the DIRC project and documented in a book entitled Responsibility and Dependable Systems. Further development has taken place since then at the universities of St Andrews, Loughborough, York and Glasgow.

RM is designed to model responsibilities across complex organisations, which could be real organisations or 'virtual organisations' that encompass several organisations working together on a shared problem. An example of a virtual organisation is the team that is created to cope with civil emergencies where several emergency services work with local authorities to cope with emergencies such as flooding, terrorist attacks, major accidents, etc. Contingency plans are drawn up in advance of an incident, but such plans are wordy documents that are often inconsistent and incomplete. We have investigated how to use responsibility modelling to represent these plans with a view to making them more accessible (and hence easier to analyse by experts) and to discover potential vulnerabilities that could result in system failures.

By exploring the dependencies between responsibilities and human, technical and information resources, a number of areas can be explored. For example:

1. Who is responsible for updating a given information resource?
2. Who uses that resource?
3. What training people require to access that resource?

Responsibility modelling provides a modelling technique that helps ensure that, for example, the contradictory views of agents, and unallocated responsibilities / resources are identified and discussed. The research at St Andrews extended this by allowing end users to explore the risks associated with deviation from the expected within a given system. By doing so the dependability and resilience of the system can be explored with reference to: Analysing the current configuration of a system to determine what improvements can / should be made on an ongoing, periodic basis.

In the event of evolution or unanticipated change, examining 'before' and 'after' analysis to determine what effect this has had on the ongoing dependability and resilience of a system. Effectively measuring the dependability and resilience of a socio-technical system itself is complex. The distinction between failure and success is unlikely to be clear within a socio-technical system. As such reliability metrics and such as MTTF (Mean Time To Failure), MTTR (Mean Time To Recovery) etc, are of limited use.

In these situations it is more appropriate to apply vulnerability analysis techniques similar to those used in dependability and safety cases to illustrate the strength of the system from the perspective of its processes, training and management. Whilst applicable to both technical and socio-technical systems, dependability / safety Cases require expert construction, an often unreasonable approach outside the safety critical domain, where resources are limited, and such techniques are not mandatory.

HAZOPS (Hazard and Operability Study) is an approach to vulnerability analysis originally developed by ICI in the 1970s, for use in the chemical industry which has been applied to wider domains, including work on socio-technical systems. HAZOPS focuses on the identification of potential vulnerabilities using keywords and associated risks through in-depth descriptions of the system in question, with a focus on technical operability and efficiency. HAZOPS keywords are used to construct tables examining the effect of deviation from the norm for a given process. For example: given a specific deviation for a given process, (something occurring early, late, never, in reverse, too much etc); what are the consequences; what actions could be taken to mitigate the consequences; what safeguards could be put in place; what is the risk of occurrence etc.

RM applies an adapted HAZOPS approach designed to achieve much of the assurance provided by standard HAZOPS whilst being less sensitive to incomplete information, and through the use of more limited generic categories of hazard, which have been tailored towards the concerns of system evolution.

The key components of a responsibility model are:

1. Responsibilities, indicated by a round-edged rectangle.

2. Agents (named in pointy brackets) who are assigned responsibilities and who take actions to 'discharge' these responsibilities. Agents may be individuals, roles or organisations.

3. Resources which are used in the discharge of a responsibility (named within straight brackets). These may be shared information or may be physical resources such as tools or vehicles.

Figure 1 is an example RM diagram based on an analysis of a flood contingency plan for Carlisle in northern England. Notice that the responsibility 'Collect Evacuee Information' does not have an agent associated with it. Drawing up the responsibility model revealed this vulnerability in the emergency plan, since it did not define which agency should collect this information.

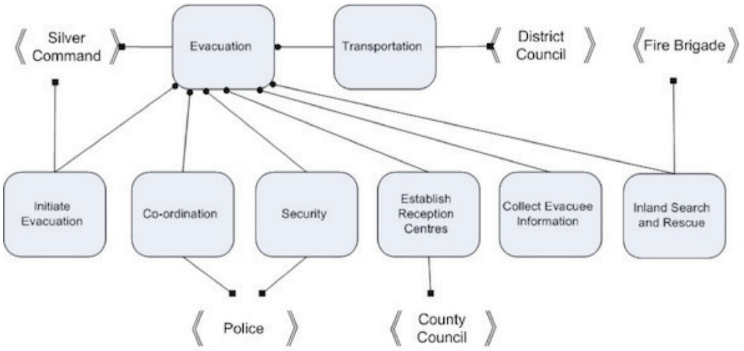

Figure 1: Example RM diagram for flooding evacuation

Resources can also be associated with responsibilities as shown in Figure 2. In this case, the responsibility 'Initiate Evacuation' requires information resources (information about risk assessments and flood warnings) to discharge the responsibility.

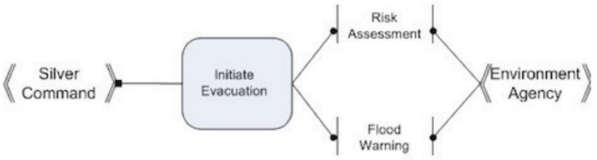

Figure 2: Example RM diagram for resource association

Risk Analysis

Responsibility modelling uses a modified HAZOPS approach to facilitate end user exploration of the vulnerabilities and associated risks of system configurations. Clauses are used, as in HAZOPS, to outline the risks associated with events/potential events. Clauses can then be grouped into tables exploring similar situations. The discursive analysis of clauses can be used to promote:

Risk Avoidance (determining how to eliminate a given hazard) Risk Minimisation (reducing the risk of hazard occurrence) Risk Mitigation (determining how to deal with the consequences of hazard occurrence effectively)

Each clause contains the following information:

Target: The entity to which the clause refers, for example, a responsibility or physical resource.

Context: What is occurring, for example, has there been a flood?

Hazard: A restricted set of hazard keywords designed for generic use within RM models:

Early: The availability of resources before they are required

Late: The availability of resources after they were required

Never: By exploring the effect of permanent failure system resilience can be explored.

Insufficient: Occurrence at an inappropriate rate / level. The types of potential issue are broad and include: Insufficient management; Insufficient maintenance; Insufficient training; Insufficient process capacity; Insufficient physical resources within a given system; Insufficient information flow (in terms of depth and/or frequency)

Incorrect: The effect of incorrect information within SoS can be far reaching and potentially even life threatening. For example, during investigations into contingency flood plans within Cumbria it was discovered that lists used by multiple organisations, of people to be evacuated from flood risk areas in the event of serious flooding, did not take into account transitory residents using caravan parks, effectively designating them locations with no population.

Risk: Risk is defined as a combination of the probability of the hazard and the severity of the hazard occurring. While probabilistic measurement would give the best basis for comparison and analysis, it is likely to be beyond the capabilities of untrained users to either generate consistently or reason about. Instead, qualitative statements are preferable, as categories specific to a given domain can be formulated and applied in a more consistent manner.

Consequences: The potential effects of the hazard manifesting itself in the wider system.

Recommended Actions: The cause(s) of action, either mitigation or avoidance, that could be taken to deal with the situation in question. Whether a given course of action should be taken is tempered by economic, organisational and political factors.

Responsibility model use

RM has been applied to a number of domains ranging from contingency planning to system procurement. There are a number of promising avenues for future research, including those of system simulation and SoS (System of System) modelling. RM is a technique backed up by tools constructed over a number of years to support those developing and discussing models, with the added benefits of semi automated analysis for potential problems. Responsibility models have also been used as a basis for understanding the requirements for the information that is required by agents in discharging a responsibility. A set of standard questions is used to derive some of the requirements for systems that may be used to support agents who have been assigned responsibilities.

The standard questions are:

1. What information is required to discharge this responsibility?
2. What channels are used to communicate this information?
3. Where does this information come from?
4. What information is recorded in the discharge of this responsibility and why?
5. What channels are used to communicate this recorded information?
6. What are the consequences if the information required is unavailable, inaccurate, incomplete, late, early?

The notation used in responsibility models

RM uses a number of key entities and relationships. Figure 3 illustrates the entities and relationships, with further information on each provided below.

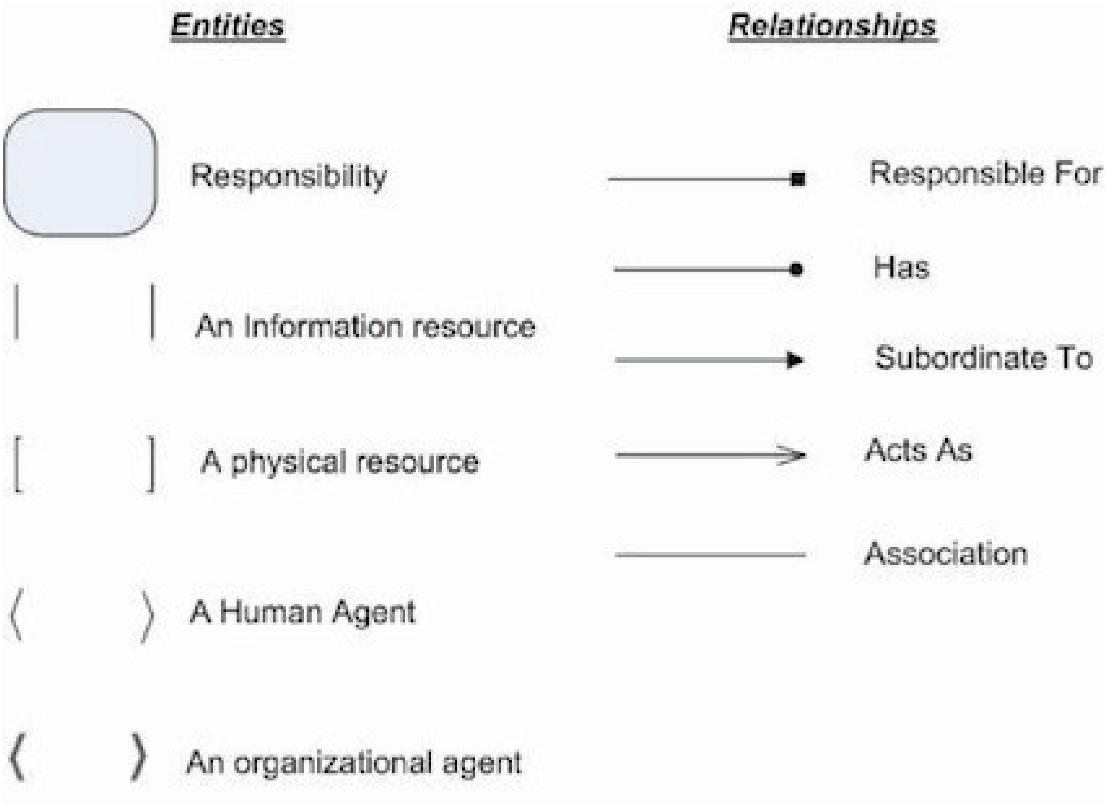

Figure 3: The entity and relationship types within RM

Key **Responsibility**: A stated activity or abstract concept. For example, raising an alarm.

Information Resource: For example, a report or database.

Physical Resource: For example, a piece of equipment such as a PC.

Human Agent: For example, an administrator Organisational Agent: For example, the government, the NHS etc. **Responsible For**: The allocation of an agent to a responsibility.

Has: The allocation of resources to agents or responsibilities.

Subordinate To: To model organisational hierarchies.

Acts As: For example, Bob acts as an administrator.

Association: Used to annotate models with relationships of a domain specific type not covered explicitly by the notation.

Retrospective

Responsibility modelling is a relative recent development and it is still evolving as a practical approach to modelling organisations. Our experiments so far suggest that the notion of responsibility is practical and intuitively understandable and the responsibility modelling can be applied in a range of different domains. So far, the approach has proved to be most useful as a tool for analysing responsibilities and further work is required on how it can be used constructively to help in the organisational change process where new responsibilities are planned.