Responsibility Modelling in Socio-technical Systems

Ian Sommerville
St Andrews University

System dependability

- General premise of our work is that a significant class of system 'failures' are due to inadequate consideration of social, organisational and cultural factors that affect the design and operation of a computer-based system
- Often manifested as a misfit between a system and the organisation using that system, resulting in:
  - User interaction 'errors'
  - Unreliable and inefficient processes
  - Provision of incorrect or inappropriate information to system users

Socio-technical systems

Socio-technical system failure

- Failures are not just catastrophic events but normal, everyday system behaviour that disrupts normal work and that mean that people have to spend more time on a task than necessary
- A system failure occurs when a direct or indirect user of a system has to carry out extra work, over and above that normally required to carry out some task, in response to some inappropriate system behaviour
- This extra work constitutes the cost of recovery from system failure

Research challenge

- What abstractions, methods and tools can be used in identifying socio-technical issues that significantly affect the operation of a system?
- How can these be used in practice to identify system vulnerabilities and to influence systems design practice.
- Our premise is that the notion of responsibility is a useful basis for investigating socio-technical issues and that modelling responsibilities provides useful insights.
- This is part of a wider programme of research in socio-technical systems engineering.

Responsibility definition

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

Why responsibility?

- System failures can result from misunderstandings about responsibilities and failures of people to discharge their responsibilities as expected
- Responsibilities are high-level abstractions that define (informally) what is expected of a human or automated agent. No assumptions are made about how an agent will discharge its responsibilities
- Responsibilities are natural abstractions that people can relate to and talk about
  - In system design, technical abstractions (such as objects) that are alien to system stakeholders are often used

Responsibility vulnerabilities

- Unassigned responsibility
- Duplicated responsibility
- Uncommunicated responsibility
- Misassigned responsibility
- Responsibility overload
- Responsibility fragility

What is a responsibility model?

- *A succinct definition of the responsibilities in a system, the agents who have been assigned these responsibilities and the resources that should be available to these agents in discharging their responsibilities.*

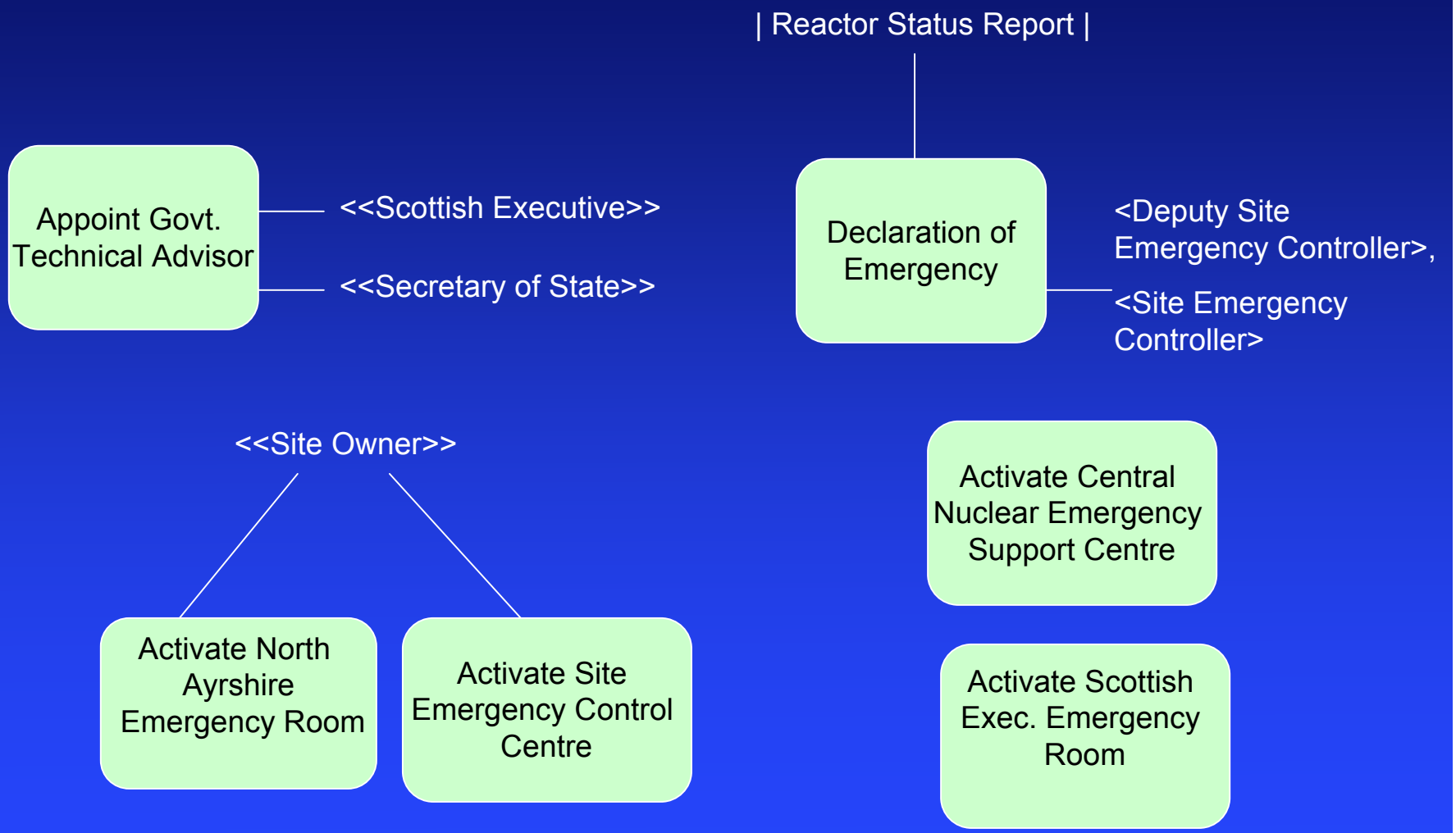
Responsibility models

- Simple graphical presentation that shows:
  - Responsibilities
  - Organisations/people/automated systems who are assigned specific responsibilities (agents)
  - Authority structures (where appropriate) i. e. information about accountability in an organisation
  - Responsibility dependencies
  - Information, and other resources required to discharge responsibilities

Types of responsibility models

- Planning models
  - Describe the intended allocation of responsibilities in some situation
  - Define the agents who should discharge the responsibility
  - Set out the resources that are normally required to discharge a responsibility
- Operational models
  - Planning models plus annotations that describe:
    - The agents that are actually assigned a responsibility
    - The resources that are actually used

Responsibility model notation



Contingency Planning

- Development of contingency scenarios and plans for coping with incidents
- Plans can be for a generic contingency, or specific scenarios (e.g. flooding)
- Single agency plans document resources, procedures etc to be utilised by the agency to discharge responsibilities
- Inter-organisational plans document the responsibilities that each organisation holds and can expect others to discharge
- Planning is evaluated through emergency exercises

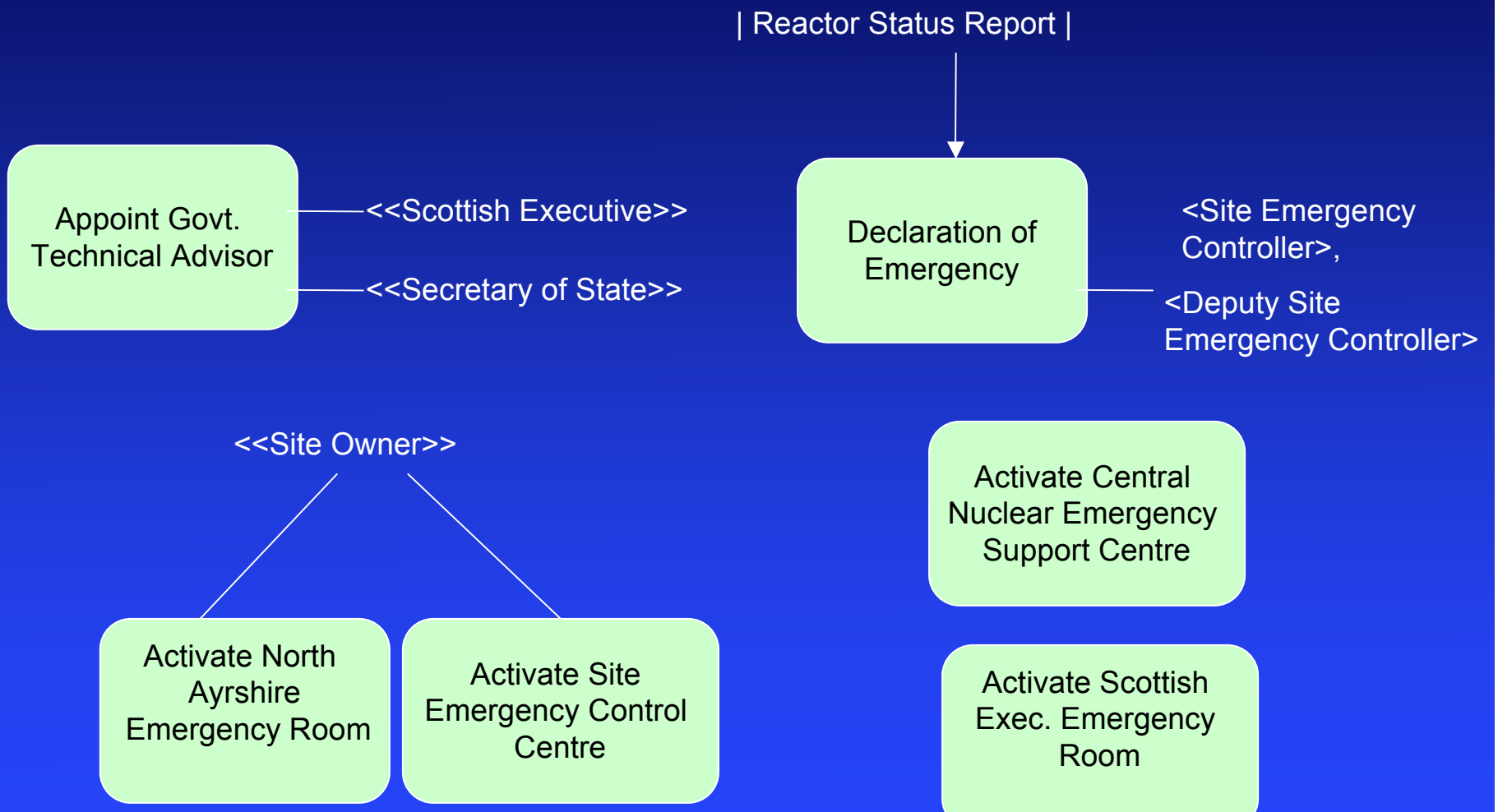
Problems in Contingency Planning

- Contingency *plans* are often verbose and rarely used during emergency responses
- Misunderstandings occur between organisations regarding:
  - Who holds particular responsibilities
  - How responsibilities are interpreted
- Circumstances may require unexpected agents to discharge responsibilities
- The appropriate information may not be available to an agent for a responsibility to be discharged
  - E.g. Communication infrastructure or process failures

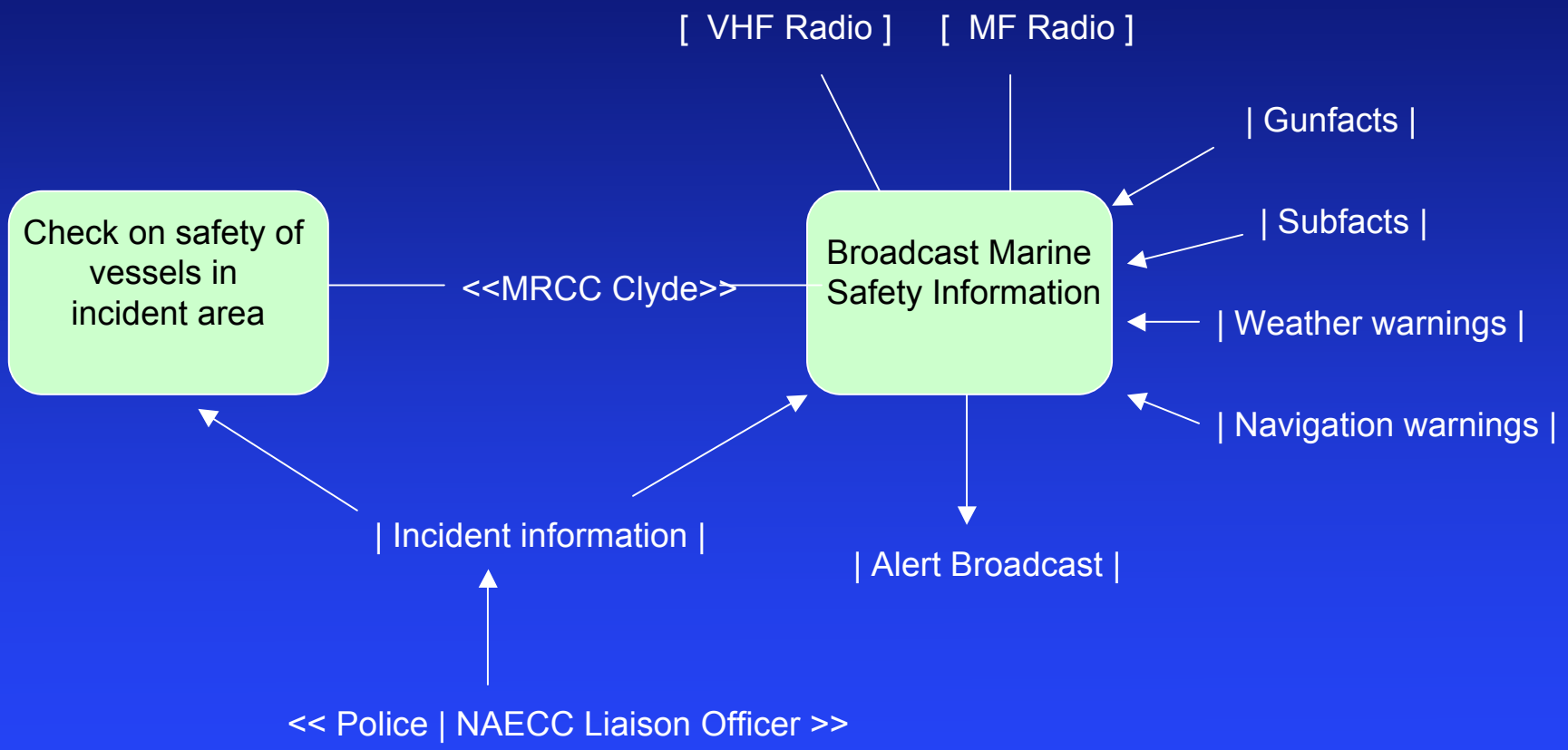
Coordination system for CP

- Scenarios from a (socio-technical) coordination system for contingency management are used as the driver for our work
- Each agency involved has its own C & C system and does not wish to invest in a shared C & C system for managing emergencies
- System has to support
  - Joint planning
  - Sharing of information from different systems
  - Audit trail of actions taken during an emergency
  - Provision of information to managers in the field

Responsibility planning model



Information resources



Responsibility modelling benefits

- They are a way of facilitating the analysis of responsibilities and discussing responsibilities across organisations
- They support risk analysis and the identification of a class of potential vulnerabilities in a system
- They serve as a means of identifying *information requirements* and help identify redundancy and diversity that should be planned for in a system
- They may be useful as a means of documenting responsibilities and learning from experience

Information requirements

- Requirements for information to be provided to agents to help them do their work, requirements for information sharing and access control and requirements for information that is to be generated
- When systems are created by the configuration of existing systems, their behaviour is constrained. There is limited scope for defining the functionality of a system
- We argue that a behavioural approach to requirements specification should be replaced by a focus on the information produced, consumed and shared by the agents in the system

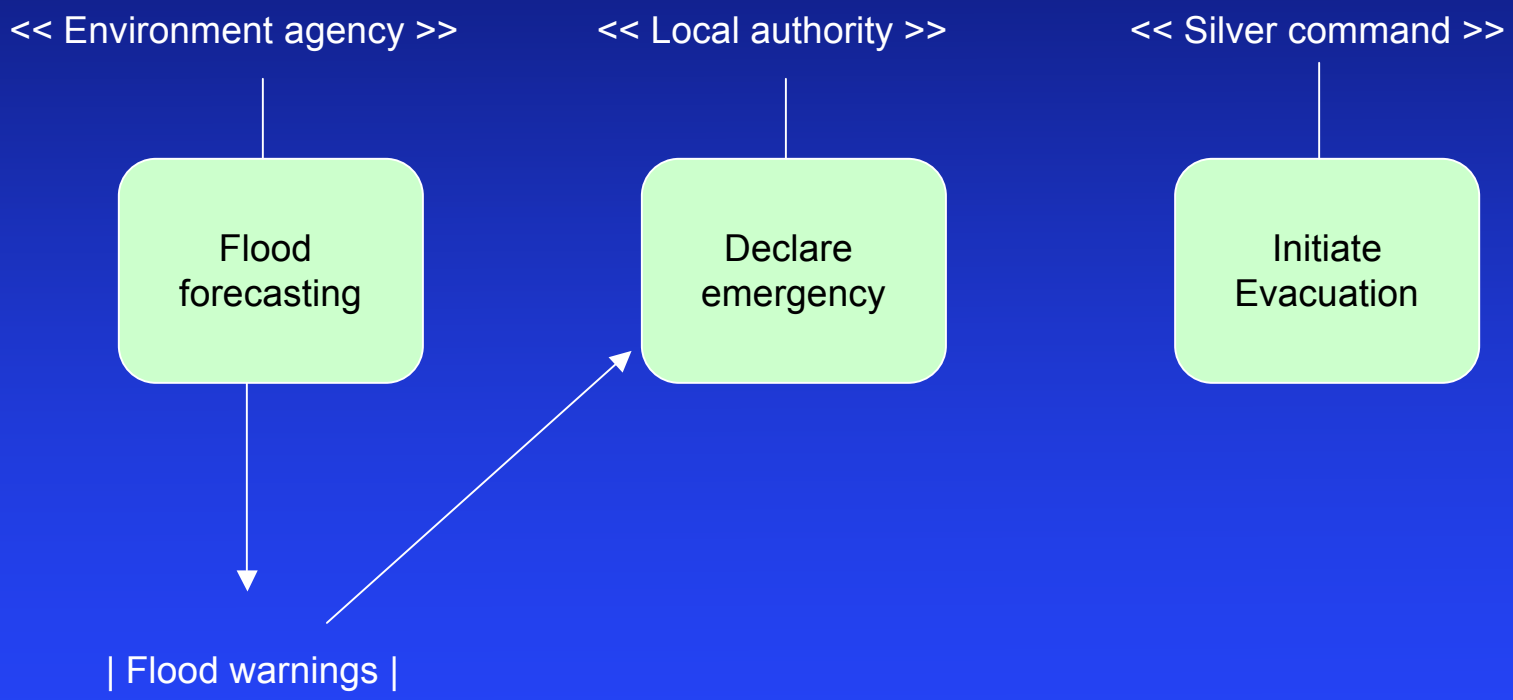
Information analysis

- We assume that the holder of a responsibility needs some information to discharge that responsibility
- Information requirements are concerned with:
  - What: The information required
  - Where: The source of that information
  - How: The channel (or channels) through which that information is delivered
  - Structure: How the information is organised/should be organised
  - Presentation: How the information should be presented to a user of that information

Deriving information requirements

- What information is required to discharge a responsibility?
- Where does the information come from?
- What channels are used to communicate this information?
- What information is recorded in the discharge of this responsibility?
- What channels are used to communicate the recorded information?
- What are the consequences if the information is unavailable, inaccurate, incomplete, late, early, etc.?

Flood emergencies



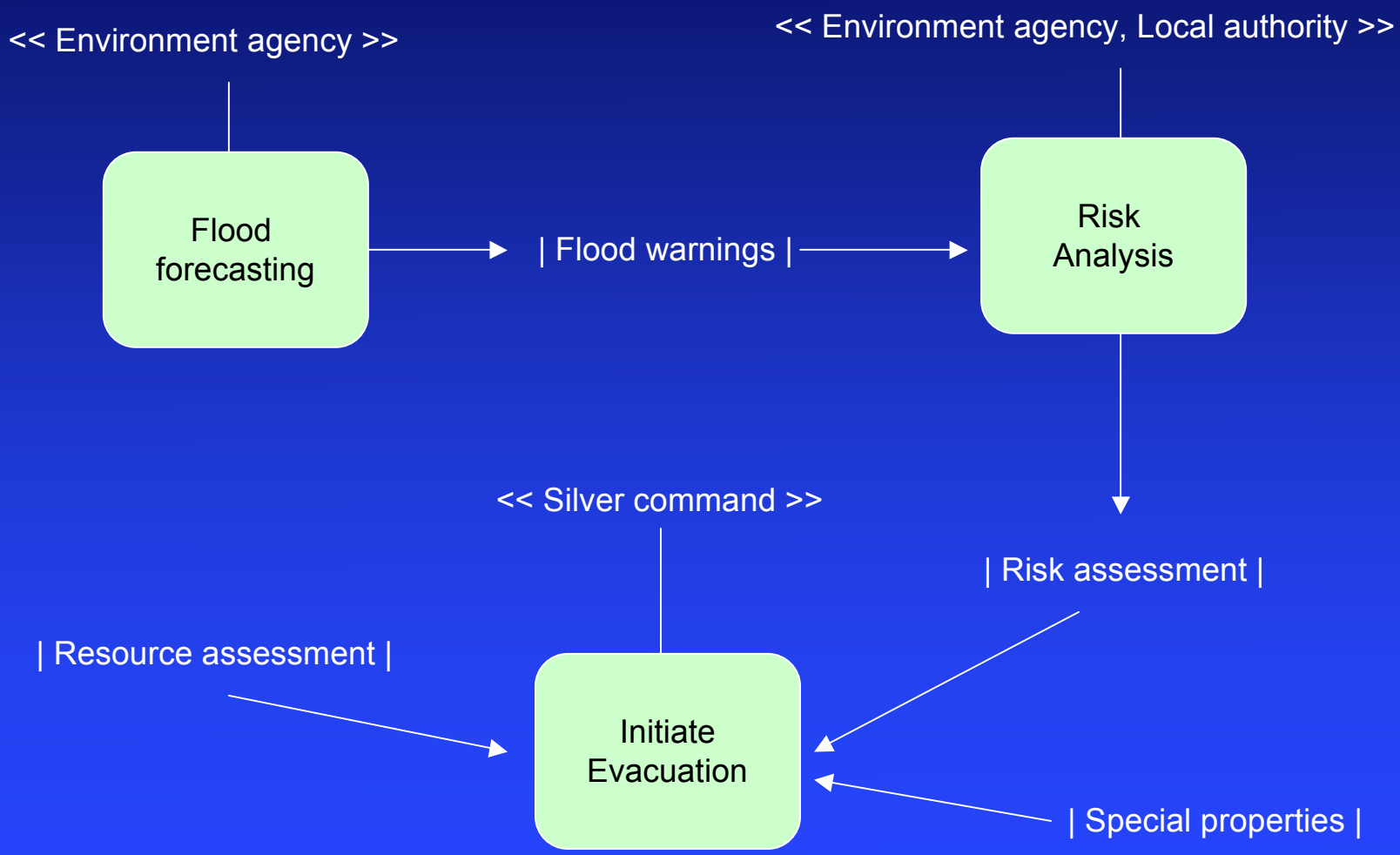
Initiate Evacuation

- Information requirements
  - Risk assessment showing properties at risk from predicted flooding, predicted times of flooding and the likelihood of flooding in specific areas (Environment agency, local authority)
  - Information about 'special properties' e.g. hospitals, care homes, schools, where the residents will require help to be evacuated (Local authority)
  - Availability of resources from emergency services and other agencies (Emergency services liaison officers)

Information analysis

- Risk assessment
  - An assessment of the areas that are of risk from the flood and the probabilities of flooding in these areas (What info)
  - Based on flood warnings from environment agency and local knowledge (Where from)
  - Telephone, web, meetings (Channels)
  - Areas at risk and imminence of risk; Who made decision and what local knowledge used (What recorded)
  - Fax to silver command or meeting
  - Vulnerabilities - discussed later

Initiate evacuation



Vulnerability analysis

- The responsibility model reflects the understanding of an organisation about who is responsible for what and what that responsibility entails
- Where multiple agencies are involved, there are likely to be discrepancies between their understanding of responsibility
- Examining and comparing models allows us to identify:
  - Responsibility omissions - responsibilities that each organisation assumes are assigned to some other organisation or which are simply not assigned to any organisation
  - Responsibility misunderstandings - situations where different organisations understand a responsibility in different ways

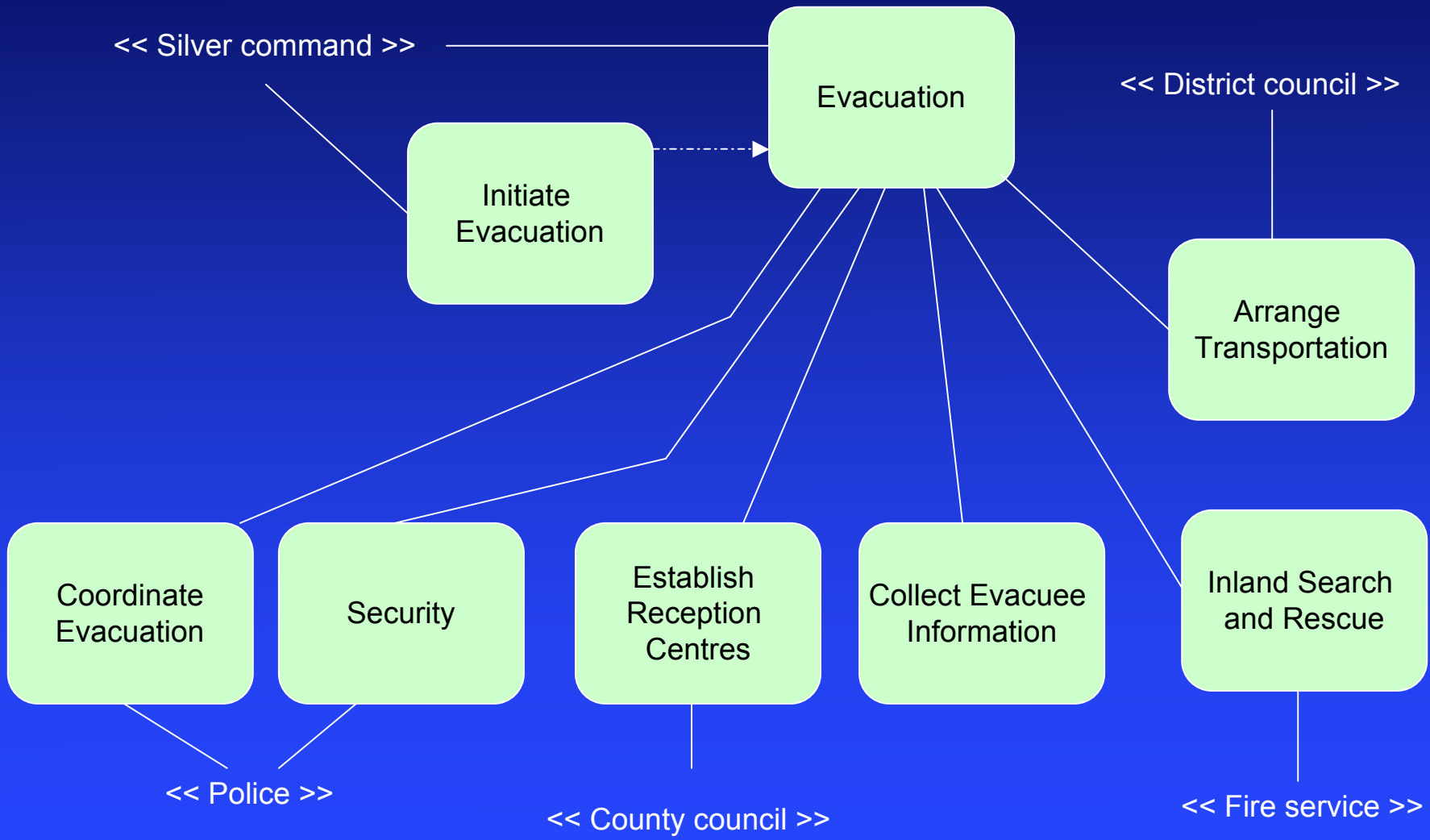
HAZOPS

- A HAZOPs-style 'what if' analysis can be applied to the information requirements for each responsibility
  - Analyses the robustness of the contingency plan in failure circumstances
- Guide words were selected to query information channel failure:
  - Early
  - Late
  - Never
  - Inaccurate

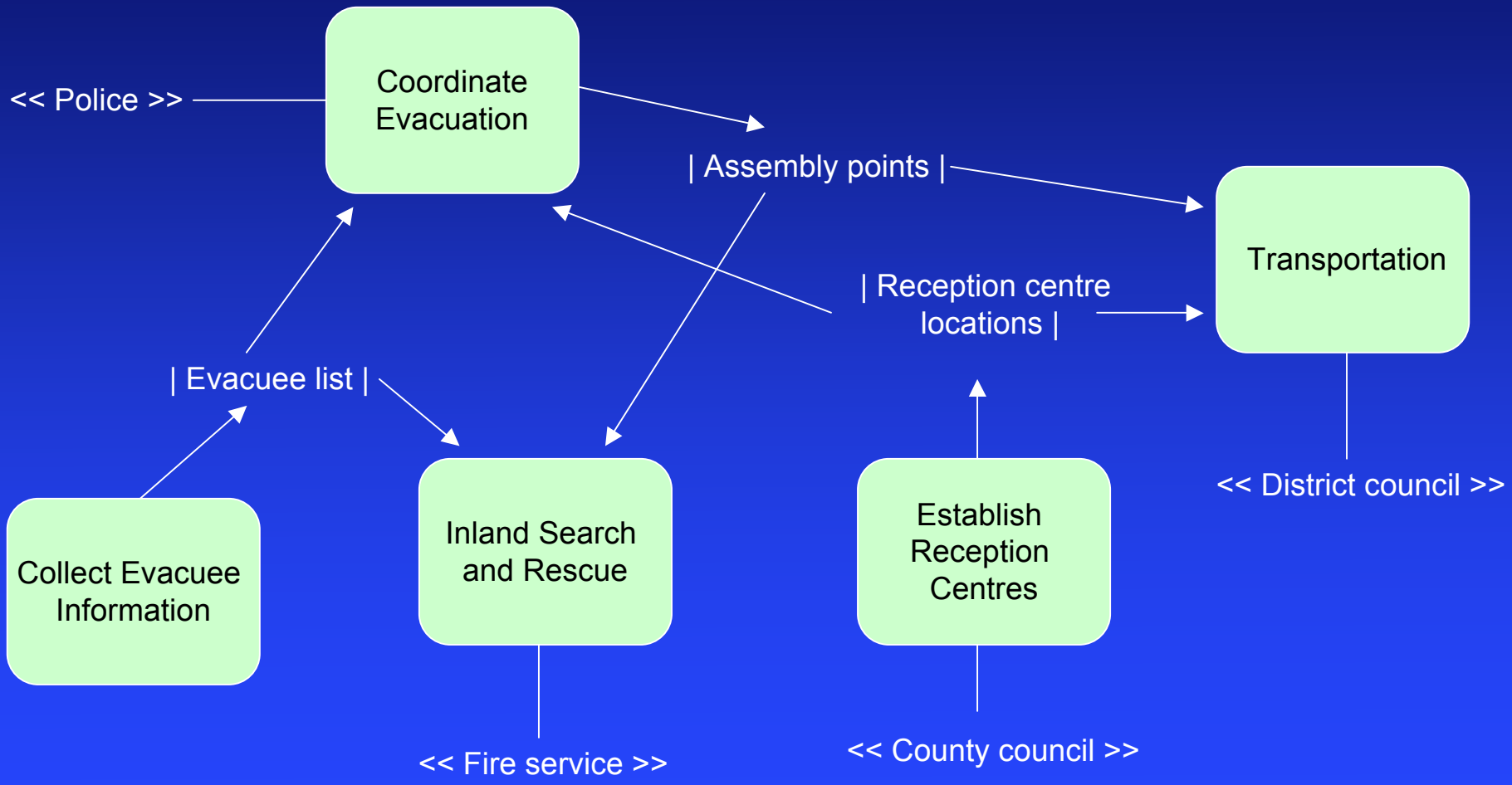
HAZOPS Analysis

Responsibility: Initiate Evacuation			
Information	**Guide word**	**Consequence**	**Probability**
Flood Warning	Never	No preparation is made for evacuation	Low
	Late	Preparation occurs later than optimal	Medium
	Early	Prediction later proves inaccurate	Low
	Inaccurate	Incorrect areas are evacuated	Low
Risk Assessment	Never	Decision on evacuation is less informed	Low
	Late	Initiation of evacuation occurs late	Low
	Early	-	-
	Inaccurate	Incorrect decision on evacuation is made	Medium

Evacuation responsibilities



Evacuation coordination



HAZOPS Analysis

Responsibility: Coordinate Evacuation			
Information	**Guide word**	**Consequence**	**Probability**
Evacuee List	Never	Evacuation is hard to plan – operation becomes "ad-hoc" as residents are evacuated as they are discovered.	Low
	Late	Initial evacuation is "ad hoc" until information is available.	Low
	Early	-	-
	Incorrect	Inappropriate resources are allocated to evacuation – causes inefficiencies	Medium
Assembly Point locations	Never	Organisations responsible for Search & Rescue and Transport cannot be directed to assembly points. Evacuees potentially do not reach reception centres	Low
	Late	Initial build up of evacuees at ad-hoc assembly points selected by Search & Rescue organisations.	Medium
	Early	Assembly points may need to be changed (due to flooding) so information is incorrect.	Medium
	Incorrect	Organisations responsible for Search & Rescue and Transport, are unable to rendezvous at a common assembly point	Medium

Conclusions/Current work

- Responsibility models appear to be useful in supporting some kinds of analysis of socio-technical systems, particularly the analysis of information requirements and system vulnerabilities
- The models serve to faciliate debate amongst the agencies involved in procuring and using these systems
- Current work
  - Development of tool support allowing web based access to responsibility models on fixed and mobile devices
  - Development of approaches to annotating planning models to describe operational responsibilities