Inf Syst E-Bus Manage (2008) 6:295–316
DOI 10.1007/s10257-008-0087-z

ORIGINAL ARTICLE

Decision support for emergency situations

Bartel Van de Walle · Murray Turoff

Published online: 26 March 2008

Abstract Emergency situations occur unpredictably and cause individuals and organizations to shift their focus and attention immediately to deal with the situation. When disasters become large scale, all the limitations resulting from a lack of integration and collaboration among all the involved organizations begin to be exposed and further compound the negative consequences of the event. Often in large-scale disasters the people who must work together have no history of doing so; they have not developed a trust or understanding of one another's abilities, and the totality of resources they each bring to bear have never before been exercised. As a result, the challenges for individual or group decision support systems (DSS) in emergency situations are diverse and immense. In this contribution, we present recent advances in this area and highlight important challenges that remain.

Keywords Emergency situations · Crisis management · Information systems · High reliability · Decision support

1 Introduction

Emergency situations, small or large, can enter our daily lives instantly. A morning routine at home all of a sudden turns into an emergency situation when our 5-year-old on her way to the school bus trips over a discarded toy, falls and hurts herself. At

This article is part of the "Handbook on Decision Support Systems" edited by Frada Burstein and Clyde W. Holsapple (2008) Springer.

B. Van de Walle (✉)
Department of Information Systems and Management, Tilburg University, Tilburg, The Netherlands
e-mail: bartel@uvt.nl

M. Turoff
Department of Information Systems, New Jersey Institute of Technology, Newark, NJ, USA

work, the atmosphere in the office turns grim when the news breaks that the company is not meeting its expected earnings for the second quarter in a row and, this time, the chief executive officer (CEO) has announced that hundreds of jobs are on the line. Emergency situations can be man-made, intentional, or accidental. Especially hard to plan for is the rare and violent twist of nature, such as the Sumatra–Andaman earthquake of 26 December 2004, with an undersea epicenter off the west coast of Sumatra, Indonesia, triggering a series of devastating tsunamis that spread throughout the Indian Ocean, killing approximately 230,000 people.

By definition, emergency situations are situations we are not familiar with—nor likely to be familiar with—and by their mere happening create acute feelings of stress, anxiety, and uncertainty. When confronted with emergency situations, one must not only cope with these feelings, but also make sense of the situation amidst conflicting or missing information during very intense time periods with very short-term deadlines. The threat-rigidity hypothesis, first developed by Staw et al. (1981) and further discussed by Rice (1990), states that individuals undergoing stress, anxiety, and psychological arousal tend to increase their reliance on internal hypotheses and focus on dominant cues to emit well-learnt responses. In other words, the potential decision response to a crisis situation is to go by the book, based on learned responses. However, if the response situation does not fit the original training, the resulting decision may be ineffective, and may even make the crisis situation worse (e. g., the 9/11 emergency operators telling World Trade Center occupants to stay where they were, unless ordered to evacuate). In order to counter this bias, crisis response teams must be encouraged and trained to make flexible and creative decisions. The attitude of those responding to the crisis and the cohesive nature of the teams involved is critical to the success of the effort (King 2002; Keil et al. 2002). In an emergency the individuals responding must feel they have all the relevant observations and information that is available in order to make a decision that reflects the reality of the given situation. Once they know they have whatever information they are going to get before the decision has to be made, they can move to sense-making to extrapolate or infer what they need as a guide to the strategic/planning decision, which allows them to create a response scenario, which is a series of integrated actions to be taken. It has also been well-documented in the literature that the chance of defective group decision making, such as groupthink (Janis 1982), is higher when the situation is very stressful and the group is very cohesive and socially isolated. Those involved in the decision are cognitively overloaded and the group fails to adequately determine its objectives and alternatives, fails to explore all the options, and also fails to assess the risks associated with the group's decision itself. Janis also introduced the concept of hypervigilance, an excessive alertness to signs of threats. Hypervigilance causes people to make "ill-considered decisions that are frequently followed by post-decisional conflict and frustration" (Janis 1982). As a result, the challenges for individual or group decision support systems (DSS) in emergency situations are diverse and immense. In contrast, individuals performing in emergency command and control roles who may have expertise in the roles they have undertaken, and who have feelings of trust for others performing related and supporting roles (such as delivering up-to-date information), are likely to be able to go into a state of cognitive absorption or flow that captures an

individual's subjective enjoyment of the interaction with the technology (Agarwal and Karahanna 2000), where they cope well with states of information overload over long periods of time and make good decisions, even with incomplete information. The knowledge that one is making decisions that involve the saving of lives appears to be a powerful motivator.

2 A model for emergency management processes

Many events in organizations are emergencies but are sometimes not recognized as such because they are considered normal problems: developing a new product, loss of a key employee, loss of a key customer, a possible recall on a product, the disruption of an outsourced supply chain, etc. Developing a new product is probably influenced by a belief that, if it is not done now, some competitor will do it and that will result in the obsolescence of the company's current product. Because the time delay in the effort for developing a new product is often much longer than what we think of as an emergency, we tend not to view many of these occurrences as emergency processes. This is unfortunate because it means that organizations, private or public, have many opportunities to exercise emergency processes and tools as part of their normal processes. One of the reoccurring problems in emergency preparedness is that tools not used on a regular basis during normal operations will probably not be used or not be used properly in a real emergency. The emergency telephone system established for all the power utility command centers to coordinate actions on preventing a wide-scale power failure was developed after the first Northeast blackout in the US. It was not used until after the power grid completely failed and resulted in the second failure almost a decade later, and then not until 11 h after the start of the failure process. Employees had forgotten it existed.

Sometimes our view of the emergency management effort is too simplified and farmed out in separate pieces to too many separate organizations or groups. In emergency management, the major processes and sub-processes are:

- Preparedness (analysis, planning, and evaluation):

  Analysis of the threats
  Analysis and evaluation of performance (and errors);
  Planning for mitigation;
  Planning for detection and intelligence;
  Planning for response;
  Planning for recovery and/or normalization.

- Training.
- Mitigation.
- Detection.
- Response.
- Recovery/normalization.

These segments of the process are cyclic, overlap, require integration, collaborative participation, involvement of diverse expertise and organizational units, as well as constant updating. These processes give us a structure for identifying and categorizing the various information and decision needs DSS must provide for in emergency situations.

Emergency situations typically evolve during an incubation period in which the emergency (often unnoticed) builds up to ultimately lead to an acute crisis when the last defenses fall or when the circumstances are just right. For organizations, it is therefore crucial to focus on this phase and try to reduce the consequences or prevent the emergency from developing at all. During the *preparedness*, *mitigation*, and *detection* phases, it is important to prepare for the eventuality of an emergency by understanding the vulnerabilities of an organization, analyzing early warning signals which may point at threats to which the organization may already be or become exposed, and by taking precautionary measures to mitigate the possible effects of the threats. Developing emergency plans is one of the key activities in the *preparedness* phase. It should be clear that planning is critical and it is something that must go on all the time, especially since the analysis and evaluation processes must be a continuous processes in any organization that wants to be able to manage the unexpected in a reliable and responsive manner. *Mitigation* goes hand in hand in with *detection*, and what we do in mitigation is often influenced by the ability to detect the event with some window of opportunity prior to the event. The *response* phase is a very different phase during which the initial reaction to the emergency is carried out and the necessary resources are mobilized, requiring an intense effort from a small or large number of people dealing with numerous simultaneous emergencies of different scope and urgency. During the *recovery* phase, the pace of the action has slowed down from the hectic response phase, and there may be a need for complex planning support to relocate thousands of homeless families, to decide on loans for businesses to be rebuilt, or to start with the most urgent repairs of damaged public infrastructure. However, given a pandemic like the avian flu, the distinction between response and recovery becomes somewhat meaningless. Clearly the scale of the disaster can produce considerably complex and difficult situations for the recovery phases as evidenced by both 9/11 and Katrina.

The remainder of this chapter is structured according to the DSS needs for the various emergency management processes. In the following section, we introduce high-reliability organizations, a remarkable type of organization that seems to be well prepared and thrives well even though it deals with high-hazard or high-risk situations routinely. Concluding from this strand of research that mindfulness and resilience are key aspects of emergency preparedness, we discuss information security threats and indicate how DSS may help organizations to become more mindful and prepared. In Sect. 4, we focus on DSS for emergency response, and present a set of generic design premises for these DSS. As a case in point, we discuss a DSS for nuclear emergency response implemented in a large number of European countries. In Sect. 5, we focus on the recovery phase, and we highlight the role and importance of humanitarian information and decision support systems. We describe the example of Sahana, an open-source DSS developed since the 2004 tsunami disaster in Sri Lanka. We conclude in Sect. 6 by summarizing our main findings.

3 DSS for emergency preparedness and mitigation

3.1 Mitigation in high-reliability organizations

Some organizations seem to cope very well with errors (Wolf 2001). Moreover, they do so over a very long time period. Researchers from the University of California in Berkeley called this type of organization high-reliability organizations (HROs): "How often could this organization have failed with dramatic consequences? If the answer to the question is many thousands of times the organization is highly reliable" (Roberts 1990). Examples of HROs are nuclear power plants, aircraft carriers, and air-traffic control, all of which are organizations that continuously face risk because the context in which they operate is high hazard. This is so because of the nature of their undertaking, the characteristics of their technology, or the fear of the consequences of an accident for their socio-economic environment. The signature characteristic of an HRO, however, is not that it is error-free, but that errors do not disable it (Bigley and Roberts 2001). For this reason, HROs are forced to examine and learn from even the smallest errors they make.

Processes in HROs are distinctive because they focus on failure rather than success: inertia as well as change, tactics rather than strategy, the present moment rather than the future, and resilience as well as anticipation (Roberts 1990; Roberts and Bea 2001). Effective HROs are known by their capability to contain and recover from the errors they make and by their capability to have foresight into errors they might make. HROs avoid accidents because they have a certain state of mindfulness. Mindfulness is described as the capability for rich awareness of discriminatory detail that facilitates the discovery and correction of potential accidents (Weick 1987; Weick and Sutcliffe 2001). Mindfulness is less about decision making and more about inquiry and interpretation grounded in capabilities for action. Weick et al. (1999) mention five qualities that HROs possess to reach their state of mindfulness, also referred to as high-reliability theory (HRT) principles (Van Den Eede and Van de Walle 2005), and shown in Fig. 1. It is sometimes stated in a joking manner that long term survival of firms is more a function of those firms that make the smallest number of serious errors and not those that are good at optimization. Some of the recent disasters for companies in the outsourcing of supply chains may be a new example of this folklore being more wisdom than it is currently believed. The more efficient the supply chain (thereby providing no slack resources), the more disaster prone it is (Markillie 2006).

As Fig. 1 indicates, reliability derives from the organization's capabilities to discover as well as manage unexpected events. The discovery of unexpected events requires a mindful anticipation, which is based in part on the organization's preoccupation with failure. As an illustrative case of a discipline that is very concerned with the discovery of unexpected events and the risk of failure, we will next discuss how information security focuses on mindfulness in the organization.

3.2 Mindfulness and reliability in information security

Information security is a discipline that seeks to promote the proper and robust use of information in all forms and in all media. The objective of information security is

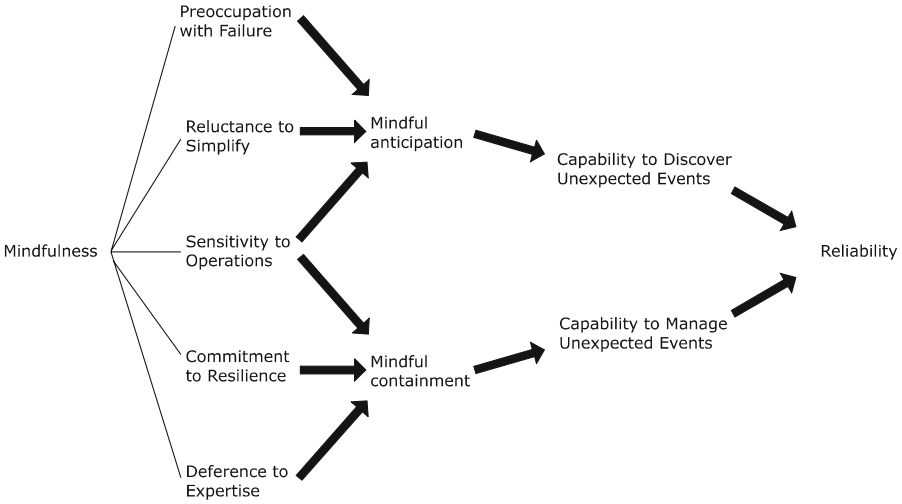

Fig. 1 A mindful infrastructure for high reliability (adapted from Weick et al. 1999)

to ensure an organization's continuity and minimize damage by preventing and minimizing the impact of security incidents (von Solms 1998; Ma and Pearson 2005). According to Parker, information security is the preservation of confidentiality and possession, integrity and validity, and the availability and utility of information (Parker 1998). While no standard definition of information security exists, one definition used is as follows: *Information security is a set of controls to minimize business damage by preventing and minimizing the impact of security incidents.* This definition is derived from the definition in the ISO 17799 standard (ISO 17799 2005) and accepted by many information security experts. The ISO 17799 is defined as a comprehensive set of controls comprising best practices in information security and its scope is to give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization. The ISO 17799 standard has been adopted for use in many countries around the world including the UK, Ireland, Germany, The Netherlands, Canada, Australia, New Zealand, India, Japan, Korea, Malaysia, Singapore, Taiwan, South Africa, and others.

Security baselines have many advantages in the implementation of information security management in an organization, such as being simple to deploy and using baseline controls, easy to establish policies, maintain security consistency, etc. However, such a set of baseline controls addresses the full information systems environment, from physical security to personnel and network security. As a set of universal security baselines, one of the limitations is that it cannot take into account the local technological constraints or be present in a form that suits every potential user in the organization. There is no guidance on how to choose the applicable controls from the listed ones that will provide an acceptable level of security for a specific organization, which can create insecurity when an organization decides to ignore some controls that would actually have been crucial. Therefore, it is necessary to develop a comprehensive framework to ensure that the message of

commitment to information security is pervasive and implemented in policies, procedures and everyday behavior (Janczewski and Xinli Shi 2002) or, in other words, create organizational mindfulness. This framework should include an effective set of security controls that should be identified, introduced, and maintained (Barnard and von Solms 2000). Elements of those security controls are, respectively, a base-lines assessment, risk analysis, policy development, measuring implementation, and monitoring and reporting action.

One very good reason why emergency management has progressed very rapidly in the information field is that there is a continuous evolution of the threats and the technologies of both defense and offense in this area, coupled with the destruction of national boundaries for the applications that are the subject of the threats (Doughty 2002; Drew 2005; Stoneburner et al. 2001; Suh and Han 2003). Today we have auditors who specialize in determining just how well prepared a company is to protect its information systems against all manner of risks. Even individuals face the problem that their identities can be stolen by experts from another country, who then sell them to a marketer in yet another country, who then offers them to individuals at a price in almost any country in the world. In the general area of emergency management, maybe we need to all learn that it is time to evolve recognized measures of the degree of emergency preparedness for a total organization rather than just its information systems (Spillan and Hough 2003; Turoff et al. 2004a, b; Van Den Eede et al. 2006a).

3.3 Decision support systems for information security mindfulness

Group decision support systems (GDSS) have proven to efficiently facilitate preference and intellective tasks via anonymous exchange of information supported by electronic brainstorming and to reduce process losses in face-to-face meetings (Nunamaker et al. 1991), as well as distributed meetings (Hiltz and Turoff 1993; Hiltz et al. 2005). In a recent field study, a synchronous GDSS was used to support the exchange of information among senior managers of a large financial organization during a risk management workshop (Rutkowski et al. 2005; Rutkowski et al. 2006). This workshop was held to generate and identify an exhaustive set of risks related to information security. From the large number of risks generated in this first phase, a smaller number of risks was selected and assessed in terms of their expected utility (amount of damage), calculated from their expected impact and probability of occurrence. The most relevant risks were then discussed in the last phase of the workshop in order to build business preparedness scenarios to be activated should one of the identified risks actually materialize. The findings of this study indicated that the use of the GDSS increased the overall level of mindfulness among the participants on the importance of addressing risks in the organization. The anonymous input and exchange of information while using the GDSS encouraged participants to freely express their private opinion about very sensitive information in the organization. Overall, it was found that the managers involved in this study obtained a higher feeling of control and appropriation of the decision taken toward the business continuity scenarios to be built. Similarly, the fuzzy decision support system FURIA (fuzzy relational incident analysis) allows individual group members to compare their individual assessment of a decision

alternative or option (such as an information security risk) to the assessments of the other group members so that diverging risk assessments or threat remedies can be identified and discussed (Van de Walle and Rutkowski 2006). At the core of FURIA is an interactive graphical display visualizing group members' relative preference positions, based on mathematical preference and multi-criteria decision support models (Fodor and Roubens 1994; Van de Walle 2003; Van de Walle et al. 1998).

4 DSS for emergency response

4.1 Design principles for dynamic emergency response systems

Implicit in crises of varying scopes and proportions are communication and information needs that can be addressed by today's information and communication technologies (Bellardo et al. 1984; Fisher 1998; Turoff 2002). What is required is organizing the premises and concepts that can be mapped into a set of generic design principles, in turn providing a framework for the sensible development of flexible and dynamic emergency response information systems. Turoff et al. (2004a, b) systematically develop a set of general and supporting design principles and specifications for a dynamic emergency response management information system (DERMIS) by identifying design premises resulting from the use of the emergency management information system and reference index (EMISARI), a highly structured group communication process that followed basic concepts from the Delphi method (Linstone and Turoff 1975), and design concepts resulting from a comprehensive literature review. In their paper, Turoff et al. (2004a, b) present a framework for the system design and development that addresses the communication and information needs of first responders as well as the decision-making needs of command and control personnel. The framework also incorporates thinking about the value of insights and information from communities of geographically dispersed experts and suggests how that expertise can be brought to bear on crisis decision making. Historic experience is used to suggest nine design premises, listed in Table 1. These premises are complemented by a series of five design concepts based upon the review of pertinent and applicable research. The result is a set of general design principles and supporting design considerations that are recommended to be woven into the detailed specifications of a DERMIS. The resulting DERMIS design model graphically indicates the heuristic taken by this paper and suggests that the result will be an emergency response system flexible, robust, and dynamic enough to support the communication and information needs of emergency and crisis personnel on all levels. In addition it permits the development of dynamic emergency response information systems with tailored flexibility to support and be integrated across different sizes and types of organizations (Van Den Eede et al. 2006b).

4.2 Emergency response for industrial disasters: the Chernobyl nuclear disaster

Several large-scale industrial disasters causing considerable loss of human life and damage to the environment have occurred in the recent past. On 3 December 1984,

Table 1 DERMIS design premises (Turoff et al. 2004a, b)

P1 System training and simulation. Turoff et al. argue that finding functions in the emergency response system that can be used on a daily basis is actually much more effective than isolated training sessions. Indeed, if the system is used on a day-to-day basis, this will partly eliminate the need for training and simulation, as those who must operate the system gain extensive experience with the system just by using it
P2 Information focus. During a crisis, those who are dealing with the emergency risk are flooded with information. Therefore, the support system should carefully filter information that is directed towards actors. However, they must still be able to access all (contextual) information related to the crisis as information elements that are filtered out by the system may still be of vital importance under certain unpredictable circumstances
P3 Crisis memory. The system must be able to log the chain of events during a crisis, without imposing an extra workload on those involved in the crisis response. This information can be used to improve the system for use in future crises, but it can also be used to analyze the crisis itself
P4 Exceptions as norms. Due to the uniqueness of most crises, usually a planned response to the crisis cannot be followed in detail. Most actions are exceptions to the earlier defined norms. This implies that the support system must be flexible enough to allow reconfiguring and reallocation of resources during a crisis response
P5 Scope and nature of crisis. Depending on the scope and nature of the crisis, several response teams may have to be assembled with members providing the necessary knowledge and experience for the teams' tasks. Special care should also be given to the fact that teams may only operate for a limited amount of time and then transfer their tasks to other teams or actors. The same goes for individual team members who may, for example, become exhausted after many hours of effort, necessitating passing on the role to trusted replacements
P6 Role transferability. Individuals should be able to transfer their role to others when they cannot continue to deal with the emergency. For the support system, this means that clear descriptions of roles must be present and explicit in the software, as well as a description of the tasks, responsibilities, and information needs of each role
P7 Information validity and timeliness. As actions undertaken during crises are always based on incomplete information, it is of paramount importance that the emergency response system makes an effort to store all the available information in a centralized database which is open equally to all who are involved in reacting to the situation. Thus, those involved in the crisis response can rely on a broad base of information, helping them making decisions that are more effective and efficient in handling the crisis. When they suddenly need unexpected information (something that neither the system nor others predicted they would need) they need to be able to go after it and determine if it exists or not, and who can or should be supplying it
P8 Free exchange of information. During crisis response, it is important that a great amount of information can be exchanged between stakeholders, so that they can delegate authority and conduct oversight. This, however, induces a risk of information overload, which in turn can be detrimental to the crisis response effort. The response system should protect participants from information overload by assuming all the bookkeeping of communications and all the organization that has occurred
P9 Coordination. Due to the unpredictable nature of a crisis, the exact actions and responsibilities of individuals and teams cannot be pre-determined. Therefore, the system should be able to support the flow of authority directed towards where the action takes place (usually on a low hierarchical level), but also the reverse flow of accountability and status information upward and sideways through the organization

in Bhopal a Union Carbide chemical plant leaked 40 tons of toxic methyl isocyanate gas, killing at least 15,000 people and injuring about 150,000 more. A lesser known example but with an even larger impact occurred in Henan Province in China, where the failing of the Banqiao and Shimantan reservoir dams during typhoon Nina in 1975 killed 26,000 people while another 145,000 died during subsequent epidemics

and famine. In that disaster, about six million buildings collapsed and in total more than 10 million residents were affected. However, of all industrial disasters in recent times, the 1986 Chernobyl nuclear disaster probably brings to mind the most apocalyptic visions of worldwide devastation.

The world's largest nuclear disaster occurred on 26 April 1986, at the Chernobyl nuclear power plant in Pripryat, Ukraine in the former Soviet Union. The cause of the disaster is believed to be a reactor experiment that went wrong, leading to an explosion of the reactor. As there was no reactor containment building, a radioactive plume was released into the atmosphere, contaminating large areas in the former Soviet Union (especially Ukraine, Belarus and Russia), Eastern and Western Europe, Scandinavia, and as far away as eastern North America, in the days and weeks following the accident. In the days following the accident, the evidence grew that a major release of nuclear material had occurred in the Soviet Union, and measures were taken by governments in the various affected countries to protect people and food stocks. In the Soviet Union, a huge operation was set up to bring the accident under control and extinguish the burning reactor, and about 135,000 people were evacuated from their homes. The number of confirmed deaths as a direct consequence of the Chernobyl disaster is only 56, most of these being fire and rescue workers who had worked at the burning power plant site, yet thousands of premature deaths are predicted in the coming years.

Nuclear power plants have been put forth as examples of what an HRO should be and yet we still see events like Chernobyl and Three-Mile Island. Some believe the root cause of Chernobyl was the lack of local authority of the professional operators of the plant to veto decisions by the higher ups that decided to take the plant operation outside the limits of the original performance specifications for the technology. Consider the comparison where a commercial airplane pilot in most countries has the right to veto the flight of the plane if he or she feels something is not right with respect to the readiness state of the aircraft. This was the case on 14 August 2006, shortly after the foiled airline terrorism plot in the UK, when British Airways flight BA179 from Heathrow Airport to New York turned back after an unattended and ringing cell phone was discovered on board. The pilot went against the advice of British Airways' own security team and decided "to err on the side of caution" (UK Airport News 2006). This example contrasts the lack in the Chernobyl power plant procedures of any clear process plan for the human roles in the plant when there is any uncertainty about decisions to be made, the accountability for those decisions, and the need for oversight. In emergencies with well laid out preparedness plans there is always the need for a command and control structure where those role functions have to be very clear to all who are involved.

4.3 RODOS, the real-time online decision support system for nuclear emergencies

The different and often conflicting responses by the different European countries following the Chernobyl disaster made it clear that a comprehensive response to nuclear emergencies was needed in the European Union. Funded by the European Commission through a number of 3-year research programs (so-called framework

programs), a consortium of European and formerly Soviet Union based universities and research institutions worked together to develop a real-time online decision support system (from which one can form with some creativity the acronym RODOS) that "could provide consistent and comprehensive support for off-site emergency management at local, regional and national levels at all times following a (nuclear) accident and that would be capable of finding broad application across Europe unperturbed by national boundaries" (Raskob et al. 2005; French et al. 2000; French and Niculae 2005; Ehrhardt and Weiss 2000). The objective was that RODOS would (Niculae 2005):

- provide a common platform or framework for incorporating the best features of existing DSS and future developments;
- provide greater transparency in the decision process as one input to improving public understanding and acceptance of off-site emergency measures;
- facilitate improved communication between countries of monitoring data, predictions of consequences, etc. in the event of any future accident; and
- promote, through the development and use of the system, a more coherent, consistent and harmonized response to any future accident that may affect Europe.

The overall RODOS DSS consists of three distinct subsystems, each containing a variety of modules:

- *Analyzing* subsystem (ASY) modules that process incoming data and forecast the location and quantity of contamination including temporal variation. These modules contain meteorological, atmospheric dispersion, hydrological dispersion, deposition and absorption, health effects, and other models. The ASY modules predict the evolution of the situation according to the best scientific understanding of the processes involved.
- *Countermeasure* subsystem (CSY) modules that suggest possible countermeasures, check them for feasibility, and calculate the expected benefit in terms of a number of criteria.
- *Evaluation* subsystem (ESY) modules that rank countermeasure strategies according to their potential benefit and preference judgments provided by the decision makers.

The interconnection of all program modules, the input, transfer and exchange of data, the display of the results and its modes of operation (interactive and automatic) are controlled by the RODOS *operating system* (OSY), a layer built upon the UNIX operating system of the host computer. Interaction with users and display of data takes place via a *graphical subsystem* (GSY), which includes a purpose-built geographical information system (RoGIS). This would display demographic, topographic, economic and agricultural data along with contours of measured or predicted radiological data. These displays seek to ensure that the output can be used and understood by a variety of users who may possess qualitatively different skills and perspectives (Marsden and Hollnagel 1996). In the early phases of an accident, local decisions are likely to be the responsibility of local plant management. However, regional emergency planning officers and senior officers in the emergency

services need to be immediately concerned with oversight, analyzing if there are sufficient resources to meet the demand, seeking out re-supply when necessary, and stepping into arrange maintenance and logistic support. In later phases, regional and national politicians would be involved depending on how serious the accident is.

RODOS is a real-time, online system connected to meteorological and radiological data networks; thus including several communication modules. Its database formats are defining the basis for data exchange on a European scale. All data required by the modules to process information are stored in databases, of which there are three main categories in RODOS:

- a database storing program data that include input and output data required by or produced by different modules, intermediate and final results, temporary data, etc.;
- a real-time database containing information coming from regional or national radiological and meteorological networks; and
- a geographical database containing geographical and statistical information for the whole of Europe.

The system is designed to be flexible in order to work equally well under various circumstances. Therefore, the content of the subsystems and the databases vary depending on the specific application of the system, i.e., the nature and characteristics of any potential nuclear accident, different monitoring data, national regulations, etc. The RODOS models and databases can be customized to different site and plant characteristics as well as to the geographical, climatic, and environmental variations across Europe. The current version of the RODOS system is installed in national emergency centers for use in Germany, Finland, Spain, Portugal, Austria, The Netherlands, Poland, Hungary, Slovakia, Ukraine, Slovenia, and the Czech Republic. Installation is under consideration in several other countries such as Romania, Bulgaria, Russia, Greece, and Switzerland. As a consequence, RODOS today is the virtually centralized resource for all relevant information that may be needed in any potential nuclear plant crisis in the European Union. Clearly, RODOS would be very useful in the event of a terrorist action to release a radioactive substance through a dirty bomb. However, there is no publicly stated mission of RODOS to provide this aid to those that would be most concerned with that type of event. We hope this is not an example of the lack of integration across governmental organizations responsible for this other problem.

5 DSS for emergency recovery

5.1 Emergency recovery

On 28 August 2005, hurricane Katrina hit the Gulf Coast, wreaking havoc in the states of Louisiana, Mississippi, and Alabama. Many areas of New Orleans were flooded and winds of more than 100 mph (160 km/h) tore off parts of the roof of the Superdome stadium where some 9,000 people who were unable or unwilling to

leave the city were taking refuge. Power lines were cut, trees felled, shops wrecked, and cars hurled across streets strewn with shattered glass. In the following days, the scale of the devastation caused by Hurricane Katrina and the subsequent flooding became clearer. About 80% of the low-lying city was under water. Helicopters and boats were picking up survivors stranded on rooftops across the area—many were to spend several more days there. On 1 September, with the lack of any local command and control facility, New Orleans appeared to descend into anarchy, with reports of looting, shootings, carjacking, and rapes. The local police force, reduced in number by 30%, was ordered to focus its efforts on tackling lawlessness. Anger mounted over the delay in getting aid to people in New Orleans and what was seen as an inadequate response from the federal government. In the following days, the relief effort was stepped up. Evacuations continued as military convoys arrived with supplies of food, medicine and water. Finally, on 3 September, more than 10,000 people were removed from New Orleans—the Superdome stadium and the city's convention center were cleared. The US appealed for international aid, requesting blankets, first aid kits, water trucks, and food. One year later, the scale and costs of the recovery efforts were impressive. FEMA (the Federal Emergency Management Agency) has paid out more than $13.2 billion under the National Flood Insurance Policy to policyholders in Louisiana. The US Small Business Administration (SBA) approved more than 13,000 disaster assistance loans to business owners totaling $1.3 billion and 78,237 loans to renters and homeowners totaling more than $5 billion. FEMA issued 1.6 million housing assistance checks totaling more than $3.6 billion to Louisiana victims, in the form of rental assistance and home repair or replacement grants (FEMA News release 1603-516 2006).

On the other side of the planet, aid was badly needed for those countries affected by the 2004 tsunami (mostly Indonesia, Sri Lanka, Thailand, and India) which had inflicted widespread damage to the infrastructure, leading to a shortage of water and food. Due to the high population density and the tropical climate of the region, epidemics were a special concern and bringing in sanitation facilities and fresh drinking water as soon as possible was an absolute priority. In the days and weeks following the tsunami, governments all over the world committed to more than $7 billion in aid for the affected countries, followed by donations from large companies and many smaller local private initiatives.

No matter how impressive the scope of the final efforts, Katrina demonstrated what happens when local command and control systems are lost and no realistic and workable plans exist for integration between the city, state, federal, and private sector response capabilities. The international response to the 2004 Indian Ocean Tsunami was nothing less than chaotic in the most crucial first days following the disaster. When disasters become large in scale all the limitations resulting from a lack of integration and collaboration among all the involved organizations begin to expose themselves and further compound the negative consequences of the event. Often in large-scale disasters the people who must work together have no history of doing so, they have not developed a trust or understanding of one another's abilities, and the totality of resources they each bring to bear were never before exercised. While a new organization is stumbling around trying to form itself into something that will work, the disaster does not wait for them.

5.2 Emergency recovery following major disasters: humanitarian information systems

In times of major disasters such as hurricane Katrina or the 2004 tsunami, the need for accurate and timely information is as crucial as is rapid and coherent coordination among the international humanitarian community (Bui and Sankaran 2001; Currion 2006). Effective humanitarian information systems that provide timely access to comprehensive, relevant, and reliable information are critical to humanitarian operations. The faster the humanitarian community is able to collect, analyze, disseminate and act on key information, the more effective the response will, the better needs will be met, and the greater the benefit to affected populations. In 2005 ECHO, the European Commission Directorate-General for Humanitarian Aid, announced its decision to approve a total amount of 4 million Euros to support and enhance humanitarian information systems essential to the coordination of humanitarian assistance (ECHO 2005). Specifically, it was decided to improve information management systems and services of the United Nations Office for the Coordination of Humanitarian Affairs (OCHA). OCHA was established in 1991 with a specific mandate to work with operational relief agencies to ensure that there are no gaps in the response and that duplication of effort is avoided. OCHA's information management extends from the gathering and collection of information and data, to its integration, analysis, synthesis, and dissemination via the Internet and other means.

To respond to information needs, OCHA has developed humanitarian information systems which include ReliefWeb, the regional information networks (IRIN), information management units (IMUs) and humanitarian information centers (HICs). These services have established solid reputations in the provision of quality information and are recognized as essential in the coordination of emergency response among partners in the humanitarian community. Common in the success of these systems, or information services, is that the information provided is based upon a solid information exchange network among all partners in the humanitarian community. ReliefWeb (http://www.reliefweb.int) is the world's leading online gateway to information on humanitarian emergencies and disasters. Through ReliefWeb, OCHA provides practitioners with information on both complex emergencies and natural disasters worldwide from over 1,000 sources, including UN, governments, nongovernmental organizations (NGOs), the academic community, and the media. ReliefWeb consolidates final reports, documents, and reports from humanitarian partners, providing a global repository one-stop shop for emergency response information. IRINs gather information from a range of humanitarian and other sources, providing context and reporting on emergencies and at-risk countries. IMUs and HICs collect, manage, and disseminate operational data and information at the field level, providing geographic information products and a range of operations databases and related content to decision makers in the field as well as headquarters. Other OCHA humanitarian information systems that provide complementary information services to meet the full range of information needs as described above include OCHA Online, the Financial Tracking System (FTS), and the Global Disaster Alert System (GDAS).

In the US, the Humanitarian Information Unit (HIU) was created in 2002 by Secretary of State Powell as "a U.S. Government interagency nucleus to identify, collect, analyze and disseminate unclassified information critical to USG preparations for and responses to humanitarian emergencies worldwide." In 2004, the task "to promote best practices for humanitarian information management" was added to the HIU's mission statement. The role of the HIU is to provide critical and reliable information quickly and efficiently to US government organizations involved in providing humanitarian assistance in response to disasters and emergencies overseas. The HIU has developed products for the Secretary of State, the administrator of the US Agency for International Development (USAID) and the National Security Council. These products are almost always created to be unclassified, so that they can be shared easily with other audiences within the international humanitarian community: the UN, NGOs, the media, the public, etc. Another role of the HIU is to develop, test, and promote new technologies for better humanitarian information management. The HIU has been in the forefront of using and promoting geographic information systems (GISw) and satellite imagery, both for strategic and operational uses and applications. In addition, the HIU has tested and promoted the use of personal digital assistants (PDAs), global positioning systems (GPSs), and digital cameras on humanitarian field assessments. The HIU has also used collaboration tools and content management software to improve interagency collaboration and information sharing. VISTA is an example of a new web-based visualization tool that not only provides situational awareness, but facilitates humanitarian situational analysis as well (King 2006).

5.3 The Sahana open-source humanitarian information and decision support system

Sahana is a web-based collaboration tool that addresses the common coordination problems during a disaster from finding missing people, managing aid, managing volunteers, tracking relocation sites, etc. between government groups, the civil society (NGOs), and the victims themselves. Sahana is an integrated set of pluggable, web-based disaster management applications that provide solutions to large-scale humanitarian problems in the aftermath of a disaster. The main applications and problems they address are as follows:

- *Missing person registry*: helping to reduce trauma by effectively finding missing persons;
- *Organization registry*: coordinating and balancing the distribution of relief organizations in the affected areas and connecting relief groups, allowing them to operate as one;
- *Request management system*: registering and tracking all incoming requests for support and relief up to fulfillment and helping donors connect to relief requirements;
- *Camp registry*: tracking the location and numbers of victims in the various camps and temporary shelters set up all around the affected area.

The development of Sahana, a free and open-source disaster management system distributed under terms of the GNU lesser general public license, was triggered by the tsunami disaster in 2004 to help coordinate the relief effort in Sri Lanka (Sahana Wiki Community 2006). It was initially built by a group of volunteers from the Sri Lankan information technology (IT) industry and spearheaded by the Lanka Software Foundation. An implementation of Sahana was authorized and deployed by CNO (the main government body in Sri Lanka coordinating the relief effort) to help coordinate all the data being captured. Development of Sahana continues today to make the system applicable for global use and to be able to handle any large-scale disaster. Sahana has been deployed successfully in the aftermath of several large natural disasters, for instance following the large earthquake in Pakistan in 2005, and the mudslide disaster in the Philippines and the Yogjakarta earthquake, both in 2006. The long term objectives of Sahana are to grow into a complete disaster management system, including functionality for mitigation, preparation, relief, and recovery. The current status, ongoing development, and future goals are intensively discussed in two web-based communities, the Sahana Wiki pages (Sahana Wiki Community 2006) and the Humanitarian-ICT Yahoo! Group (Humanitarian-ICT 2006).

6 Conclusion

Using standard emergency management terminology, we have in this chapter categorized DSS for emergency situations according to the different phases of crisis preparedness, response and recovery. We have presented DSS that have been developed or implemented in response to some of the worst emergency situations our society has been confronted with in recent times, such as the Chernobyl, Indian Ocean tsunami, and hurricane Katrina disasters. Serving as a foundation for this overview, we started by introducing high-reliability organizations, as these seem to be dealing remarkably well with emergency situations on a daily basis. In this conclusion, we stress once again the need for such organizations to support and sustain efficient emergency response and recovery efforts, and summarize some of the key aspects of DSS we believe are crucial for high-reliability emergency management.

6.1 Role multiplicity

In any emergency effort to allocate a particular resource, there are many specific roles involved and it must be clear to everyone involved who is the person that is performing a specific role at a specific time. These fundamental role functions are:

- *Requesting*: individuals who are requesting the resource and are trusted by the others to know that this request is a valid one.
- *Observing or reporting*: those trained to be able to make observations about the situation and report information that will be useful to others in carrying out their tasks.

- *Allocating*: The persons allocating the resource to meet the requests being made must make judgmental decisions on the priority of each request.
- *Local oversight*: persons in other areas who know something would interfere with an allocation must make the others aware of the occurrence of such interference (mudslides, traffic jams, flooded roads, etc.).
- *Maintaining and servicing*: making sure that a resource is adequately maintained and re-supplied with associated items or people.
- *Situation analysis and awareness*: what is the overall consumption rate of this resource and what more is occurring in the way of threats that might increase demand?
- *Global re-supply*: someone must be seeking other sources for increasing the availability of the resources.

For any large-scale disaster, at least these seven roles need to be explicitly known to everyone involved as the response takes place. In cases of explicit toxic and biological substances an added role function of the expert in the hazard type needs to be added. Since no one should work 24 h a day, roles have to be backed up but at any moment there must be a person performing in each of these roles or we can easily go into situations of overload. The people involved have to be trained in multiple roles and have to trust one another enough to be willing to hand over their role to someone else when they are too exhausted to continue. They also need to know that when they come back to reassume their role that what has occurred and what they need to know at that moment will be waiting for them as a part of the system tracking the events associated with each role. Automated systems cannot work even for local oversight without very extensive sensor networks to input all possible local conditions while the disaster is in progress.

6.2 Planning and analysis

The planning and analysis functions of emergency preparedness are core to any overall emergency management operation. They need to directly involve those who will actually execute the command and control functions as well as some of the on-site operations. They must focus on the processes and roles involved and should be tailorable with respect to the definitions of roles and events that are triggered by or reacted to the various roles. This means any local group should be able to tailor the content of the operational system they will be using. By assessing the risks and designing roles and event structures necessary to counter those risks, those who will use the system should be able to build templates that can be inserted into the command and control system to guide the actual response process. Since we cannot take all those who should be involved and afford to make them part of a single organization dedicated to this purpose of planning and analysis, the challenge is to turn this function into an HRO-style operation. It must be one we can have confidence in for large-scale disasters of any type, including those in corporations as well as those faced by government at all levels. A basic flaw of current emergence planning and response is the lack of a permanence in a core disaster response organization that can engage continuously in being an HRO organization,

develop the plans, recommend the mitigation policies and actions, oversee the training, be the coordination, command, and control core, and integrate functions over all the organizations engaged in any large-scale response no matter what the societal relationships are among the responding parties. Any large-scale emergency is in effect a situation that demands complete control of the situation by one unified team for the duration of the situation. That core does not have to be large given today's technology and even in 1960s it never exceeded 400 for the federal government.

Instead of forming committees that meet only once in a while and hand down finished plans to others who must somehow execute them, we need in the future to set up virtual organizations (Mowshowich 1997, 2002) of those that would be involved in the command and control functions as well as the response functions. They should operate as virtual teams no matter where they are, using the same command and control system to create templates for roles and events based upon scenarios of offense threats and defense plans. This system would allow them to act out roles using the real system and in essence engage in training games that they and others have designed (Turoff et al. 2006). Over a week one would expect that they would spend 4–8 h individually, at a time of their choosing, doing this, much as one might play a multi-player recreational game.

In order to be an HRO, an organization has to exist and operate on a continuous basis. We cannot have emergency management teams for wide scale disasters that only exist when the disaster occurs or they will never be able to work as effectively as an HRO. Since we will always be faced with the limit that physical resources for most disasters do not come together until the disaster occurs, our only effective recourse is to set up a continuous ongoing virtual preparedness organization that uses the same command and control software as its ongoing virtual operational capability. This would appear to be the only feasible way to be able to bring together the people from different organizations (or different units of a single organization) and turn the emergency management function into a continuous operation for those that need to be involved. It has the added benefit of the resulting command and control function becoming a virtual command and control center. Given that we had lost the local command and control centers in both 9/11 and hurricane Katrina for the initial 48 h or longer, this becomes an obvious direction to take. The need to allow people in different dispersed locations to get to know one another and work regularly together is another important element of developing the trust necessary for those collaborating in an emergency response environment (Hiltz et al. 2005).

6.3 Emergency management

The endeavors of emergency management and business continuity need to become recognized professions in both industry and government. Today we face threats of great sophistication and wide-scale complexity that will demand a high quality of societal performance and commitment for our civilization to survive. As our society increasingly rests upon a foundation of information and

communications systems, the so-called hacking threat of the past has given way to information warfare and international processes for identity theft and fraud. Where we once contended with nature as the source of major disasters we are increasingly faced with man-made disasters of both a short-term and long-term nature. The hundred-year disasters are becoming much more frequent and Mother Nature seems to be reacting to some of the abuses we have practiced upon her. In the US the age of critical infrastructure (roads, sewers, power grids, bridges, etc.) are now older than they have ever been in recent history (since the late 1940s) and growing older still with the lack of adequate replacement and maintenance budgets resulting from the short-term planning horizons and the pressures for budget cutbacks that are easier to politically make in the area of maintenance and replacement.

Instead of focusing on discovering our mistakes and correcting them, our current pressures in both the public and private sector focus on concerns for liability and political fallout, which tend to force the obfuscation of problems and mistakes in all sectors of the society (Baumgartner and Jones 1993). We still find infighting for political control of the emergency management function between different application areas (fire, police, medical) and the resulting segmentation of the problem rather than the recognized need for high-quality professionals in the field to be given control for integrated approaches for preparedness and response (Van de Walle and Turoff 2006). Our responses to major disasters still seem to be short term spasms of response that are not integrated into long term plans of mitigation and recovery that would smooth out the difficulties in the recovery process years after the event. The fact that the FEMA maps for who should need flood insurance and who would not were thirty years out of date left large numbers of people with no funds to rebuild their homes and massive numbers of court cases now trying to determine if Katrina destroyed homes by wind or water! This is hardly a situation that gives confidence to the public in the ability of a government to protect them in future disasters.

In conclusion, we need a major commitment as a society to treat emergency management as a process that involves integrated planning by all the segments of the society so that mitigation and recovery, for example, are treated as two sides of the same coin. The tools for decision support need to be encompassing in that emergency management is a true multicriteria problem not easily reduced to smaller problems like models of the impact of weather on clouds of toxic substances. We have many such models in the literature, and not one that allows examination of the life cycle of a disaster impacting on a given location or organization that treats the balance between mitigation and recovery years before and years after the event, and integrates the requirements for resources to treat the event for the totality of the given location or the given organization.

Acknowledgments We wish to thank Starr Roxanne Hiltz for her review of this document and Gerd Van Den Eede for sharing many insights on high-reliability organizations and the importance of mindfulness. The first author gratefully acknowledges funding support by the European Commission under the Sixth Framework Programme through a Marie Curie Intra-European Fellowship and by the Interactive Collaborative Information Systems (ICIS) project on complex decision making, supported by the Dutch Ministry of Economic Affairs, grant nr: BSIK03024.

References

Agarwal R, Karahanna E (2000) Time flies when you're having fun: cognitive absorption and beliefs about information technology usage. MISS Q 24(4):665–694

Barnard L, Von Solms R (2000) A formalized approach to the effective selection and evaluation of information security controls. Comput Secur 8(3):185–194

Baumgartner FR, Jones BD (1993) Agendas and instability in American politics. University of Chicago Press, Chicago

Bellardo S, Karwan KR, Wallace WA (1984) Managing the response to disasters using microcomputers. Interfaces 14(2):29–39

Bigley G, Roberts K (2001) The incident command system: high reliability organizing for complex and volatile task environments. Acad Manage J 44(6):1281–2000

Bui TX, Sankaran SR (2001) Design considerations for a virtual information center for humanitarian assistance/disaster relief using workflow modeling. Decis Support Syst 31:165–179

Currion P, Keynote address at the 3rd international conference on information systems for crisis response and management ISCRAM2006, Newark, New Jersey

Doughty K (2002) Business continuity: a business survival strategy. Inform Syst Contr J 1:28–36

Drew S (2005) Reducing Enterprise Risk with Effective Threat Management. Inf Sec Manage, January/February 37–42

ECHO Humanitarian Aid Decision 230201 (2005) Decision Reference ECHO/THM/BUD/2005/02000

Ehrhardt J, Weiss A (2000) RODOS: Decision support for off-site nuclear emergency management in Europe, EUR19144EN, Luxemburg, European Community

FEMA News release 1603–516 (2006) By the numbers: hurricanes katrina and rita disaster assistance update, 31 July. Accessed via http://www.fema.gov/news/newsrelease.fema?id=28379

Fisher HW (1998) The role of new information technologies in emergency mitigation, planning, response and recovery. Disast Prev *Manage* 7(1):28–37

Fodor J, Roubens M (1994) Fuzzy preference modeling and multicriteria decision support. Kluwer, Dordrecht

French S, Niculae C (2005) Believe in the model: mishandle the emergency. J Home Sec Emergen Manage, 2(1)

French S, Bartzis J, Ehrhardt J, Lochard J, Morrey M, Papamichail N, Sinkko K, Sohier A (2000) RODOS: Decision support for nuclear emergencies. In: Zanakis SH, Doukidis G, Zopounidis G (eds) Recent Developments and Applications in Decision Making. Kluwer, Dordrecht, pp 379–394

Hiltz SR, Turoff M (1993) The Network Nation, Revised Edition, MIT Press

Hiltz SR, Fjermestad J, Ocker R, Turoff M (2005) Asynchronous virtual teams: can software tools and structuring of social processes enhance performance? In: Galleta D, Zhang P, Sharpe ME (eds) Human–computer interaction in management information systems: applications, vol II

Humanitarian ICT Yahoo! Group. Accessed via http://groups.yahoo.com/group/humanitarian-ict/

ISO 17799, 2005. Information technology—security techniques—code of practice for information security management. http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html. Accessed August 2005

Janczewski L, Xinli Shi F (2002) Development of Information security baselines for healthcare information systems in New Zealand. Comput Secur 21(2):172–192

Janis IL (1982) Groupthink: psychological studies of policy decisions and fiascoes. Houghton-Mifflin, Boston

Keil M, Tiwana A, Bush A (2002) Reconciling user and project manager perceptions of IT project risk: a Delphi study. Inf Syst J 12:103–119

King G (2002) Crisis management and team effectiveness: a closer examination. J Bus Ethics 41(3):235–249

King D (2006) VISTA, a visualization analysis tool for humanitarian situational awareness. In: Van de Walle B, Turoff M (eds) Proceedings of the 3rd international conference on information systems for crisis response and management ISCRAM, pp 11–16
Linstone H, Turoff M (eds.) (1975) The Delphi method: techniques and applications. Addison Wesley Advanced Book Program. Now online via http://is.njit.edu/turoff
Ma Q, Pearson M (2005) ISO 17799: 'Best practices' in information security management? Commun ACM 15:577–591
Markillie P (2006) When the supply chain breaks: being too lean and mean is a dangerous things. Economist 17:16–28. In a special section on "The Physical Internet: a survey of logistics. pp 3–18
Marsden P, Hollnagel E (1996) Human interaction with technology: the accidental user. Acta Psychol 91:345–358
Mowshowitz A (1997) On the theory of virtual organization. Syst Res Behav Sci 14(6):373–384
Mowshowitz A (2002) Virtual organization: toward a theory of societal transformation stimulated by information technology. Quorum, Westport
Niculae C (2005) A socio-technical perspective on the use of RODOS in nuclear emergency management. Ph. D. dissertation, Manchester Business School
Nunamaker JF Jr, Dennis AR, Valacich JS, Vogel DR, George JF, (1991) Electronic meeting systems to support group work: theory and practice at Arizona. Commun ACM 34(7):40–61
Parker DB (1998) Fighting computer crime, a new framework for protecting information. Wiley, New York
Raskob W, Bertsch V, Geldermann J, Baig S, Gering F (2005) Demands to and experience with the decision support system RODOS for off-site emergency management in the decision making process in Germany. In: Van de Walle B, Carle B (eds) Proceedings of the Second International ISCRAM Conference ISCRAM2005
Rice RE (1990) From adversity to diversity: applications of communication technology to crisis management. Adv Telecommun Manage 3:91–112
Roberts KH (1990) Managing high reliability organizations. Calif Manage Rev (Summer):101–113
Roberts K, Bea R (2001) Must accidents happen?: lessons from high reliability organizations. Acad Manage Exec 15(3):70–79
Rutkowski A-F, Van de Walle B, van Groenendaal W, Pol J (2005) When stakeholders perceive threats and risks differently: the use of group support systems to develop a common understanding and a shared response. J Home Sec Emergen Manage 2(1):17
Rutkowski A-F, Van de Walle B, Van Den Eede G (2006) The effect of GSS on the emergence of unique information in a risk management process: a field study. In: Proceedings of HICSS40, p 9
Sahana Wiki Community (2006) Accessed via http://www.reliefsource.org/foss/index.php/Sahana
Spillan JE, Hough M (2003) Crisis planning in small businesses: importance, impetus and indifference. Eur Manage J 21(3):389–407
Staw B, Sandelands I, Dutton J (1981) Threat-rigidity effects in organizational behavior: a multilevel analysis. Admin Sci Quart 26:501–524
Stoneburner G, Goguen A, Feringa A (2001) Risk management guide for information technology systems. In: Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, NIST Special Publication, October, pp 800–830
Suh B, Han I (2003) The risk analysis based on a business model. Inf Manage 1–9
Turoff M (2002) Past and future emergency response information systems. Commun ACM 45(4):29–32
Turoff M, Chumer M, Hiltz R, Klashner R, Alles M, Vasarhelyi M, Kogan A (2004a) Assuring homeland security: continuous monitoring, control, and assurance of emergency preparedness. J Inf Technol Theor Appl 6(3):1–24
Turoff M, Chumer M, Van de Walle B, Yao X (2004b) The design of a dynamic emergency response management information system. J Inf Tech Theor Appl 5(4):1–36
Turoff M, Chumer M, Hiltz SR, (2006) Emergency planning as a continuous game. In: Proceedings of ISCRAM2006 (The third international conference on information systems for crisis response and management), NJIT, Newark NJ, May, pp 477–488
U.K. Airport News 2006. Accessed via http://www.uk-airport-news.info/heathrow-airport-news-140806b.htm
Van de Walle B (2003) A relational analysis of decision makers' preferences. Int J Intell 18:775–791
Van de Walle B, Rutkowski A-F (2006) A fuzzy decision support system for IT service continuity threat assessment. Decis Support Syst 43(3):1931–1943

Van de Walle B, Turoff M (2006) ISCRAM: growing a global R&D community in information systems for crisis response and management. Int J Emerg Manage (forthcoming)
Van de Walle B, De Baets B, Kerre EE (1998) Characterizable fuzzy preference structures. Ann Oper Res 80:105–136
Van Den Eede G, Van de Walle B (2005) Operational risk in incident management: a cross-fertilisation between ISCRAM and IT governance. In: Van de Walle B, Carle B (eds) Proceedings of the 2nd international conference on information systems for crisis response and management ISCRAM2005, pp 53–60
Van Den Eede G, Van de Walle B, Rutkowski A-F (2006a) Dealing with risk in incident management: an application of high reliability theory. In: Proceedings of HICSS40, p 10
Van Den Eede G, Muhren W, Smals R, Van de Walle B (2006b) Incident response information systems capability: the role of the DERMIS design premises. In: Van de Walle B, Turoff M (eds) Proceedings of the 3rd international conference on information systems for crisis response and management ISCRAM2006, pp 251–261
Vogus TJ, Welbourne TM (2003) Structuring for high reliability: HR practices and mindful processes in reliability-seeking organizations. J Organ Behav 24:877–903
Von Solms R (1998) Information security management (3): the code of practice for information security management (BS 7799). Inform Manage Comput Sec 6(5):224–225
Weick K (1987) Organizational culture as a source of high reliability. Calif Manage Rev 29(2):112–127
Weick KE, Sutcliffe KM (2001) Managing the unexpected: assuring high performance in an age of complexity. Wiley, San Francisco
Weick KE, Sutcliffe KM, Obstfeld D (1999) Organizing for high reliability: processes of collective mindfulness. Res Organ Behav 21:81–123
Williams TM, Ackermann F, Eden C (1997) Project risk: systemicity, cause mapping and a scenario approach. In: Kahkonen K, Artoo KA (eds) Managing risks in projects. E&FN Spon, London, pp 343–352
Wolf F (2001) Operationalizing and testing normal accidents in petrochemical plants and refineries. Prod Oper Manage 10(3):292–305