Is the "System of Systems" a Useful Concept for Hazard Analysis?

A.J. Rae; University of York; Heslington, North Yorkshire, UNITED KINGDOM

R.D. Alexander; University of York; Heslington, North Yorkshire, UNITED KINGDOM

Keywords: System of Systems, Hazard Analysis

Abstract

Safety analysis is an activity governed by pragmatism and practicality rather than formal abstractions. Even the concept of a "hazard" has no universally-agreed definition, and there is no deterministic method for finding the set of hazards for a system. In this context, any claims about new challenges or methods must be tested according to their usefulness. In this paper we investigate the concept of a "system of systems". The rise of network-enhanced capability, particularly in the military domain, has led to differentiation between "large integrated systems" and "true systems of systems". This distinction has been rightly questioned by researchers who point out that all safety analysis should involve socio-technical considerations, and claim that there is no advantage in treating so-called systems of systems with separate methods.

We identify a range of circumstances where existing hazard identification techniques, including those explicitly designed for socio-technical analysis, are unreliable in finding certain types of hazard. We claim that distinguishing these circumstances will improve management of hazard identification and assessment in organizations with multiple interacting equipment programs. We support this claim with observations related to existing difficulties that organizations have with the "system of systems safety" issue.

The circumstances we identify are a sub-set of those commonly labeled as "system of systems". Broad application of new techniques without an understanding of where they are likely to be most effective will be counterproductive. We recommend a cautious investment in system of systems safety including a strong focus on measuring the costs and benefits of new modeling and hazard identification techniques.

Introduction

The intertwined concepts of "network enhanced capability" (NEC) and "systems of systems" (SoS) have been increasingly influential in design and acquisition of military equipment. This trend can be traced to U.S. military thinking after the 1st Gulf War, as exemplified by the writing of the then Vice-Chairman of the Joint Chiefs of Staff, Admiral William A. Owens (ref. 1). Owens was not proposing specific new equipment, but was promoting a way of thinking; a model for analyzing existing systems and planning new systems. As with all conceptual models, it is not meaningful to ask "Do systems of systems exist?" The relevant question is whether it is useful to apply the "system of systems" label to a set of situations. To a certain extent, this question can be answered in the positive by the wide adoption of "system of systems thinking" outside the safety community - if planners and designers are talking about systems of systems, then safety engineers perforce will need to communicate in these terms.

A more contentious issue is whether system of systems is just a new way of communicating existing concepts, or whether it is a better model for organizing and performing safety analysis in some circumstances. This issue cannot be resolved in isolation. Models are not ends in themselves – they have value as part of a sequence of activities employed to learn true and useful information about the real world. In this case we seek to learn about the hazards presented by a situation. A useful model will be one that supports efficient and reliable identification of hazards in that situation.

In the following sections of this paper we identify classes of hazard that cannot be reliably identified by single system procurement and in-service management programs. We consider ways in which this problem can be managed, and the implications of these alternatives for safety management.

Definition of System of Systems

SoS Concepts, Configurations and Instances: Although "systems-of-systems" (SoS) is a well established concept, the circumstances under which it is an appropriate or useful concept are not well defined. This is true for SoS engineering in general, but particularly for system safety engineering. One of the limitations has been the custom of demarking SoS from systems using characteristics of SoS. A consequence of this style of definition is that SoS have inherited many of the ambiguities inherent in the term "system".

The first ambiguity to be resolved is distinguishing between an *SoS Concept*, an *SoS Configuration*, and an *SoS Instance*. The precise definitions applied to these terms here are our own, applied to concepts which are commonly used implicitly in discussing SoS, but not always differentiated.

An *SoS Concept* describes a set of configurations, and will ideally contain rules for determining and maintaining the safety of these configurations. An *SoS Configuration* includes:

- The number and type of agents which are present in the system
- The roles that are played by the agents
- The interfaces between the agents

Most non-SoS systems have tightly restricted configurations. Compare this to a battle-space where it cannot be determined a-priori:

- The numbers or types of platforms or personnel
- The missions that each platform or team will be performing
- Which other platforms or teams each team will need to communicate with, co-operate with or co-ordinate with

The distinction between *SoS Concept* and *SoS Configuration* recognizes that it is typical for an SoS to have a fluid configuration. By this we mean that there are many configurations which may arise that would be considered instances of the same SoS. Re-analysis of safety for each of these configurations is not feasible, so we need a management entity more abstract than a specific configuration. For example, the configuration of a wireless network changes every time a new device registers on the network; safety must be assured based on the concept and rules of the network, not on the details of each specific configuration.

A physical system may become part of an *SoS Instance* by joining a configuration. For example, when an armored vehicle attaches to the end of a convoy, the set of vehicles may be a valid *configuration* of the "Escorted Convoy" *SoS Concept*. Safety of the convoy participants will rely not just on individual vehicle design and behavior, but on the ability for the vehicles to safely co-operate and otherwise interact.

Demarcation of Integrated Systems and True SoS: The second ambiguity to be resolved arises from the concern that it is not appropriate to treat all integrated systems as SoS. Various heuristics have been devised to distinguish between "complex monolithic systems" and "true systems of systems". We discuss the various proposals here.

Hall-May and Kelly (ref. 2) refer to SoS as "systems whose constituent components are sufficiently complex and autonomous to be considered as systems in their own right and which operate collectively with a shared purpose". They claim that a property of such systems is that "the interactions between component systems are not constrained by physical design". As a method of demarcation, the initial definition is incomplete. It is a property of most systems that decomposition into smaller systems is possible, and these smaller systems will collectively share the purpose of the larger system. Autonomy of constituent components adds some depth to the definition, but is itself a loose concept (ref. 3). The observation about interactions which are not constrained by physical design is more interesting. It does not necessarily follow from the initial definition, but does distinguish a distinct class of systems. Even socio-technical systems often have interactions strongly constrained by design. If there is a class of systems for which configuration of the interactions between subsystems is very fluid, this may amenable to different forms of safety analysis, and therefore useful to distinguish as SoS.

Held (ref. 4) rightly criticises many existing definitions of SoS for focussing on *observations* about SoS properties rather than *definition* of an SoS. Held provides four defining criteria which he claims as necessary properties for something to be a SoS.

From reference 4:

1. **The system can be subdivided into independently operating systems.** The independent systems must themselves be systems.
2. **The system does not depend on all elements for survival.** For example, if the rudder on a 747 fails, the aircraft is very likely to crash destroying the rest of the nodes and ceasing to be a system as a whole. The 747 cannot be an SoS. The airport, however, will continue to operate. The airport can be an SoS.
3. **Systems in an SoS have some form of communication**. Communication is any form of information passing, regardless of intent. For example a deer showing a white tail while running is passing the information of danger to any other observing deer. The intent of the deer was to run in fear, not to communicate the danger.
4. **Elements have a common mission.** A mission can be described which encapsulates the behavior of the group.

Criteria 1, 3 and 4 can be satisfied by almost any system. Criterion 2 can be satisfied by any system incorporating redundant components. Even using the example given, a 747 will survive the loss of one engine whilst an airport is unlikely to operate correctly in the absence of the electrical power system. The 747 and the airport cannot be differentiated using this criterion. Contrary to Held's emphasis on properties rather than observations, Criterion 2 may be a weakly generalizable observation arising from the more important property of component systems with separate management and lifecycles.

Periorellis and Dobson (ref. 5) identify the key feature of SoS as co-operation between autonomous component systems. This definition is compatible with that of Hall-May and Kelly (ref. 2) above if co-operation between autonomous agents is seen as a driver for fluid configurations.

All of these definitions attempt to differentiate systems and SoS without first acknowledging that SoS as a concept only has utility insofar as SoS should be treated differently from other systems. The strength of any definition of SoS comes not from any objective correctness but from its ability to aid in the selection of appropriate safety management methods. It is likely that there is not a single dividing line between "conventional system" and "System of Systems". At the very least, there is almost certainly a class of systems that require socio-technical analysis extending beyond a single equipment platform, but do not have the fluid configuration and fragmented management typical of Systems of Systems.

Ultimately, the choice of whether to treat a given situation as an SoS for safety purposes should be guided by the likelihood that treatment as an SoS will improve the management of hazards. It is definitely not plausible that this would be the case where there is a single configuration or a small number of well defined configurations which change slowly, if at all. (Even though the system is complex, networked and geographically distributed). In such situations there is no prospect that SoS treatment would result in anything other than application of unnecessary or even inappropriate modeling techniques.

In the next section we will argue that there are situations with emergent hazards that cannot be reliably identified with techniques based on analysis of individual component systems. We will return to the question of definition as a way of distinguishing these situations as candidates for SoS hazard analysis.

Types of Hazard

A *system* is a collection of interacting components. For any system, there may be smaller collections of interacting components that are also systems, and larger systems that the system is part of (ref. 6).

A *hazard* is a condition or event which will lead to harm in certain circumstances (ref. 7). Hazards may typically be decomposed into a source of harm, a target of harm, and a means for allowing them to be connected.

In order to identify the hazards of a system, it may be necessary to model conditions and events outside of the system. Those things that are part of a model but not part of the system under investigation are the *environment*. It follows from the definitions of system and environment that the environment may itself comprise a system or systems other than the one under investigation.

For the purpose of safety analysis, the concept of "correct" system behavior has little significance. Even the designed, specified and intended behaviors of a system can result in hazards. Except in the case of internal hazards (dealt with below) it is the environment of a system which determines whether any particular behavior may lead to a hazard, not the design or specification of the system. Therefore, a large part of system safety is ensuring that a system's behavior is safe in all the environments and situations it will encounter. This is particularly true for mobile or distributed systems, but is still important for monolithic static systems (e.g. a chemical plant that has been vandalized or struck by lightning).

On the understanding that hazard identification is not a deterministic activity, and that any hazard may be identified by any process, we will talk about "reliable identification", meaning that a competent practitioner with good knowledge of the system could be reasonably expected to identify both the hazard and the causal mechanisms which may generate the hazard. The underlying concept, familiar in systems engineering: human performance in engineering tasks is variable, but may be shaped by the circumstances of the task.

Classes of hazards can be distinguished based on the relationship between the hazard and the environment. Note that even in cases where the environment is not necessary for *identification* of a hazard, consideration of the environment may be useful for *assessing* consequent risk of a hazard. Hazard risk assessment is beyond the scope of this discussion. The taxonomy presented here is newly developed to show how characteristics of a situation may change the nature of hazards. It measures only one dimension of hazards (the relationship between the hazard and the system environment) and is not intended as a complete hazard taxonomy. A complementary taxonomy presented by Cruickshank and Redmond (ref. 8) illustrates the different types of interactions between component systems within an SoS.

1. **Internal (material or component) hazard:** The system contains a source of harm, a target of harm, and means to allow them to be connected. No knowledge of the environment is necessary to reliably identify the hazard and its causes.

   Example: A vehicle contains a human operator and toxic substances. No knowledge of the environment is necessary to identify the hazard of operator exposure to the substances. Whilst the environment might provide an initiating event in an accident sequence, most of the causal nexus leading to the hazard can be identified within the system.

2. **System-on-environment hazard:** The system contains a source of harm, but potential targets of that harm are outside the system. Knowledge of the environment is necessary to distinguish between safe states of the system and unsafe states of the system.

   Example: A naval point-defense system determines whether targets are hostile, and fires a weapon at them. With no knowledge of the environment it is possible to recognize that there may be unsafe circumstances in which to fire the weapon, but not to further analyze those circumstances.

3. **Environment-on-system hazard:** The system contains targets of harm, but the sources of that harm may be outside the system. Knowledge of the environment is necessary to classify those sources.

   Example: A hostile-environment vehicle contains human passengers. Knowledge of the environment is necessary to know what the vehicle must protect passengers from.

4. **Facilitator hazard:** The source of harm and target of harm are outside the system, and the system is a means of allowing the source and target to be connected. The environment must be known in enough detail

to be able to distinguish between behaviors of the system which allow source and target to be connected and behaviors which do not.

Example: A system provides data communication. Knowledge that the system is used to communicate friendly and enemy position data used in firing decisions is necessary to identify the hazards of the system.

5. **Interaction hazards:** The environment contains other systems. Knowledge of the interactions between the system under analysis and these other systems is sufficient to identify the hazards.

   Example: A sensor system supplies data to other systems. Hazard identification requires knowing all of the ways in which the data can be dangerously wrong.

6. **Teamwork hazards:** The environment contains other managed systems which may also interact. Knowledge of the interactions between these other systems in the environment is necessary to identify the hazards.

   Example: An air traffic control system sends instructions to aircraft to avoid collisions. These aircraft may also communicate directly (for example through the Traffic Collision Avoidance System (TCAS)) or indirectly (by observation).

Internal hazards (type 1 above) can be reliably identified using models that contain no detail of the environment.

System-on-environment and Environment-on-system hazards (types 2 and 3 above) can be reliably identified using models that represent the environment as an interface with the system under investigation.

Facilitator and Interaction hazards (types 4 and 5 above) may be identified by models of the interface between the system and its environment, but this requires implicit understanding of how other agents interpret information across the interface. As with teamwork hazards (type 6 above), facilitator and interaction hazards can only be reliably identified when the model of the environment includes internal states of other agents.

The environment may comprise multiple systems, and the internal state of all of these systems may be relevant. Any model capable of reliably identifying type 4, 5 and 6 hazards must include, as a bare minimum:

1. A set of agents with internal state.
2. A mechanism (communication) for the agents to affect the internal state of other agents.

Communication here is used in its broadest sense – it covers any co-operative or asynchronous mechanism (including collisions and weapons fire) for changing the state of another agent. A particularly insidious case is communication through observation – an agent may correctly or incorrectly infer the state of another agent based on its visible behavior.

Non-SoS Solutions

The existence of facilitator, interaction and teamwork hazards does not lead inevitably to a need for SoS hazard analysis. There are other solutions to the difficulties which these hazards present for single-system hazard analysis.

One of the more intuitive solutions is to expand the boundary of what is considered as a single “system”. For example, “Systems-Theoretic Accident Modeling and Processes” (STAMP) (ref. 9) uses socio-technical system models to capture hazards which cannot be reliably identified by considering only equipment elements within a system. Such solutions can be effective for accident investigation where there is a specific configuration to assess. The approach has not been demonstrated for systems with fluid configurations.

Fluid configuration is not the only challenge to simply expanding the boundary of a single system. If the boundary is to include other systems, sufficient detail about these systems must be available. This is not necessarily the case where those systems are managed as separate programs with lifecycles which are not synchronized with the system

under investigation. For example, a military communication system must work safely not just with current equipment, but with equipment not yet designed.

A further difficulty is that this approach is not practicable to apply to every component system in a SoS, as it would involve considerable duplication of effort. Lack of a single organizational owner for the SoS would make it difficult to avoid such duplication.

An alternate approach is to assign responsibility for facilitator, interaction and teamwork hazards to a single component system within a SoS. This approach is promising even for fluid configurations, so long as all configurations contain a role for a directive element, typically a "command and control", "backbone", or "hub" component system. For this approach to be effective, other component systems must only communicate with each other through the directive component system, and that system must have a high level of awareness of the behavior of other component systems.

In practice it is difficult to ensure that both of these requirements hold. Component systems may communicate through implicit channels (such as visual observation) as well as formal channels. They may also gain new ability to communicate through addition of new functions.

The Überlingen mid-air collision (ref. 10) demonstrated how an initially directed SoS (air traffic with a single controller) can become more complex due to the addition of new communication functions (the Traffic Collision Avoidance System TCAS). In this accident the air traffic controller gave instructions to two aircraft in order to avoid a conflict. These instructions were opposite to those generated by the TCAS system. One aircraft obeyed the instructions of the controller and the other obeyed the instructions of TCAS, cancelling the effect of both attempts to avert the collision.

E-Health initiatives have demonstrated the difficulty entailed in a central communications system being fully aware of hazards related to traffic between other component systems. This is a problem with respect to facilitator hazards – the communications system can ensure that data is delivered reliably and faithfully, but cannot prevent data being inaccurate at the time it is provided, or misinterpreted by a recipient.

Organizational Issues for SoS Hazard Management

Hazard identification and management is itself a socio-technical process: it involves interacting people, processes and tools, with success being dependent on appropriate management of these interactions. There are a number of organizational characteristics which are frequently associated with situations labeled as System of Systems.

Firstly, there are typically separate "system owners" for each component system. These may change over the life of a system (a typical example being an acquisition or development owner, and an in-service owner). If the component systems are being deliberately designed to work together, the interface between them may be formally managed through bilateral agreements.

Secondly, there is a temporal offset between the lifecycles of component systems. Some component systems may have completed design before the SoS is formed, and will join the SoS as "legacy" systems. Other component systems may not even be envisaged when the SoS is first formed, and may have a lifecycle extending beyond that of the SoS.

Thirdly, there are demands on component system design and behavior external to the combined system. The sources of these demands may include other combined systems of which the component system is also a member.

These characteristics combine to create uncertainty of boundaries and responsibilities for hazard analysis. At best this is likely to lead to duplication of effort between component system projects. At worst, there will be hazards that are not acknowledged to be anyone's responsibility.

Even if there were no technical argument for distinguishing SoS from other systems, there is a strong organizational argument to appoint a single owner for each SoS Concept (as defined earlier in this paper). This owner will need to

be equipped with suitable tools for hazard identification. In particular these tools should be good at identifying interaction, facilitator and teamwork hazards without duplicating the work of individual system analysis.

Revisiting SoS Definition

In the previous sections we have discussed three properties that systems may have:

1. Fluid configurations of autonomous elements.
2. Interaction, facilitator and teamwork hazards.
3. Component systems which will be expected to operate co-operatively or in physical proximity, where each component system is owned and managed separately.

The first property characterizes a subset of those systems which are currently viewed as SoS. The second and third properties present challenges for current hazard identification and management. Any safety critical system which has the first property will also have the second property, and many real life instances of systems with the first property also have the third property.

This does not provide a perfect way of demarking System of Systems. As suggested earlier, there may be multiple classes of collaborative systems which could benefit from bespoke hazard management methods. We particularly point to large socio-technical systems with moderately stable configurations as an example of a class which some definitions would class as "System of Systems", but which present different challenges to hazard identification than do our "fluid configurations of autonomous elements". An example of such a socio-technical system would be the regulatory structure surrounding the Walkerton water contamination accident (ref. 11).

The three properties are useful in determining where SoS approaches are likely to have a good return on investment. Whether any given SoS approach is worthwhile is still an open empirical question. The value of SoS hazard identification can be measured by the number and severity of *new* hazards and hazard causes that are identified by SoS hazard identification after component system hazard identification has already been conducted. The cost effectiveness can be measured by comparing this value to the effort required.

Relating SoS to Real-World Accidents and Incidents

Whilst accidents provide useful real-world case studies for illustrating concepts and techniques, these illustrations must be viewed with the understanding that hazard analysis is an imperfect human endeavor which may be significantly easier in hindsight. This is particularly true of SoS accidents, where a large number of possible configurations have been reduced to one actual configuration, and a large state space describing system behavior has been reduced to one trace of actual states and events. Additionally, we can never be sure whether an adverse outcome is a result of a general shortcoming in the methods applied, or in the specific application of those methods

Accordingly, it would not be appropriate to discuss accidents and to claim that different hazard analysis techniques could or would have prevented those accidents. Through examples, we seek to illustrate that whilst not all accidents that have been labeled as "system of systems accidents" exhibit the characteristics that we have discussed above, there are situations which both match our characteristics and can result in accidents unless appropriately managed.

In each of the following examples, the accident has been previously described as a "system of systems accident".

In 1982, Air Florida Flight 90 crashed into a bridge over the Potomac river in Washington DC. The crash site attracted emergency responders from multiple local, state and federal agencies. Responders from different agencies were unable to communicate due to both procedural and technical interface issues, reducing the effectiveness of the response (ref. 12). This situation meets all three of our properties. Each agency is an autonomous element, and the configuration was ad-hoc (whilst it may seem possible to design a permanent configuration for the region, in practice jurisdictional relationships depend on the exact location of any incident). The hazards included pair-wise interaction hazards (unable to communicate) as well as teamwork hazards (conflicting mental models resulting from different organizational information paths). The solution adopted in response was to retain the fluid configuration of agencies, but to create a regional co-ordination element, filling the role of SoS Concept Owner.

Rasmussen (ref. 13) discusses the Herald of Free Enterprise capsize at the Port of Zeebrugge as emerging from multiple decision makers acting independently to optimize their own operation. Whilst the autonomous agents in this case did give rise to interaction hazards, they operated as a fixed configuration within a single organization. This suggests that the Zeebrugge situation would have been better treated as a large socio-technical system rather than a SoS.

The Überlingen mid-air collision (ref. 10) is frequently cited as a System of Systems accident. This scenario involved three autonomous agents, in one of many hundreds of possible configurations of aircraft and controllers, with each agent guided by a different mental picture and under separate management and regulation.

Another air-traffic accident commonly discussed as SoS related is the fratricidal shoot-down of two Black Hawk helicopters during Operation Provide Comfort in 1994 (ref. 14). The no-fly zone above Iraq met all of the characteristics discussed above. Autonomous agents (helicopters, AWACS and F-15s) were operating in an unpredicted configuration where there was no Identify Friend-or-Foe (IFF) or voice radio interface between the helicopters and the F-15s. The different management structures of the United States Army and United States Air Force contributed to both to lack of an interface and the lack of mitigation for the emergent teamwork hazard.

The Flight 90 emergency response, Überlingen collision and the Black Hawk fratricide involved all three of the properties we have discussed above, and so fall into our subcategory of System-of-Systems. The Herald of Free Enterprise capsize is not in this same category, but may be in a separate subcategory of complex socio-technical systems with relatively static configurations.

Conclusions

System of Systems (SoS) has become established as a concept independent of system safety engineering. Some response is required from the safety engineering discipline to ensure that SoS are treated appropriately. This does not mean that there is necessarily any advantage in treating all situations labeled as SoS with bespoke hazard identification and assessment techniques. The SoS label is too widely applied to be useful in differentiating systems for SoS-specific safety analysis.

There are, however, two subcategories of SoS where it is highly plausible that advances on existing practice will be necessary for thorough treatment of hazards. The first sub-category contains large complex socio-technical systems with relatively static configurations. Techniques such as those based on STAMP (ref. 11) show promise in addressing this sub-category.

We have identified a second sub-category with the characteristics:

1. Fluid configurations of autonomous elements.
2. Interaction, facilitator and teamwork hazards.
3. Component systems which will be expected to operate co-operatively or in physical proximity, where each component system is owned and managed separately.

Examples of SoS within this sub-category are air traffic control, battle-spaces and ad-hoc communications infrastructure such as emergency response co-ordination or autonomous vehicle operation. It is within this sub-category that we believe application of new hazard identification methods bespoke to SoS are most likely to yield value. The value of any particular approach with respect to the number and severity of *new* hazards and hazard causes that are identified by SoS hazard identification after component system hazard identification has already been conducted is an open empirical question.

Practical application of new SoS hazard identification and assessment methods should initially focus on those systems we have identified as most likely to yield value, and should include mechanisms to monitor the cost and benefit of the new techniques.

References

1. Owens, William A. *The Emerging U.S. System-of-Systems*. TR-0039. Defense Technical Information Centre, February 1996.

2. Hall-May, Martin, and Tim Kelly. "Defining and Decomposing Safety Policy for Systems of Systems." In *Computer Safety, Reliability, and Security*, edited by Rune Winther, Bjørn Gran, and Gustav Dahll. Lecture Notes in Computer Science 3688. Springer, 2005.

3. Clough, Bruce T. "Metrics, Schmetrics! How The Heck Do You Determine A UAV's Autonomy Anyway?" In *AIAA 1st Technical Conference and Workshop on Unmanned Aerospace Vehicles, Systems, Technologies, and Operations*, 2002.

4. Held, J.M. "Systems of Systems: Principles, Performance and Modelling". PhD Thesis, The University of Sydney, 2008.

5. Periorellis, P., Dr. Panayiotis Periorellis, Prof John, and E. Dobson. "Organisational Failures in Dependable Collaborative Enterprise Systems." *Journal of Object Technology* 1 (2002).

6. UK Ministry of Defence. *Safety Management Requirements for Defence Systems*. 4th ed., 2007.

7. Leveson, Nancy. *Engineering a Safer World*. MIT Press, 2011.

8. Michael, J.B., Man-Tak Shing, K.J. Cruickshank, and P.J. Redmond. "Hazard Analysis and Validation Metrics Framework for System of Systems Software Safety." *IEEE Systems Journal* 4, no. 2 (2010).

9. Leveson, Nancy, and Nicolas Dulac. "Safety and Risk-Driven Design in Complex Systems-of-Systems." In *1st Space Exploration Conference: Continuing the Voyage of Discovery*. Orlando, FL, 2005.

10. German Federal Bureau of Aircraft Accidents Investigation. *Investigation Report (Ueberlingen)*. AX001-1-2/02, May 2004.

11. Leveson, Nancy, Mirna Daouk, Nicolas Dulac, and Karen Marais. *Applying STAMP in Accident Analysis*. Technical Report http://sunnyday.mit.edu/walkerton.pdf, 2003.

12. Department of Homeland Security. "The System of Systems Approach for Interoperable Communications", 2008.

13. Rasmussen, Jens. "Risk Management in a Dynamic Society: a Modelling Problem." *Safety Science* 27, no. 2-3 (1997).

14. Office of Special Investigations. *Review of U.S. Air Force Investigation of Black Hawk Fratricide Incident*. GAO/OSI-98-4. United States General Accounting Office, 1997.

Biography

Dr Andrew Rae, Ph.D. Department of Computer Science, University of York, Deramore Lane, York YO10 5GH, Uk. Telephone - +44 7783 446 814, facsimile - +44 1904 325 599, e-mail – andrew.rae@cs.york.ac.uk
Dr Rae is a Research and Teaching Fellow in the High Integrity Systems Engineering (HISE) group in the Department of Computer Science at the University of York. His research focuses on improving the evidence base for safety engineering practices. Drew has broad experience as a safety practitioner in the rail, aerospace and defence sectors. Drew holds a PhD and a BE (Computer Systems) both from the University of Queensland.

Dr Rob Alexander, Ph.D., Department of Computer Science, University of York, Deramore Lane, York, YO10 5GH, UK, telephone – +44 1904 325474, facsimile – +44 1904 325599, e-mail – robert.alexander@cs.york.ac.uk

Dr Alexander is a Lecturer in the High Integrity Systems Engineering (HISE) group in the Department of Computer Science at the University of York. Since October 2002 he has been working on methods of safety analysis for systems of systems and autonomous systems, with a particular emphasis on simulation and automated analysis. He is currently supervising research projects on certification of autonomous systems, dynamic risk assessment for systems of systems, and automated hazard analysis using simulation and metaheuristic search. Rob graduated from Keele University in 2001 with first class honours in Computer Science, and was awarded his doctorate in 2008 by the University of York.