

System-of-Systems Security: A Survey

Michael Kennedy, David Llewellyn-Jones, Qi Shi, Madjid Merabti

School of Computing and Mathematical Sciences,
Liverpool John-Moores University, UK

Abstract – The area of System-of-Systems research is focused on using multiple complex and disparate systems to create a goal orientated solution that provides functionality greater than that of its component parts.

This paper describes the concepts of System-of-Systems through an exploration of recent definitions and characteristics, and presents some often cited examples. We will examine the composition of a System-of-Systems and discuss the security concerns surrounding these. We also highlight the generic components that compose a System-of-Systems and examine some of the concerns within these.

A selection of proposed approaches for providing security within System-of-Systems are considered; the papers examined look at general management frameworks to identify some of the challenges that exist for the provision of security within System-of-Systems.

I. INTRODUCTION

System-of-Systems (SoS) is a relatively new area of research that has applications across numerous disciplines. The SoS concepts are focused on improving efficiency and providing the means to address complicated issues that arise through the increased complexity in the information technology environment. This is being attempted through the combining of multiple systems with the goal of reducing the complexity that faces users of these systems and providing emergent behaviours, by creating systems that are formed from complex independent systems.

Current research attempts to address the many issues surrounding these multifaceted developments with the current focus on the creation of frameworks, methods and classifications. There are many challenges within the domain of SoS research and its related areas; one of these is that of the security available within the SoS. Due to the composition of these complex structures, in that they're created from working independent systems, they are subject to the usual security concerns and threats that affect all systems; however their increased complexity, dynamic nature, unique configuration and operation leads to additional security considerations that systems in isolation rarely have to consider.

The goal of this paper is to examine and discuss some of the security mechanisms and approaches that have been proposed for SoS. The following section will introduce the reader to the concept of a SoS and discuss some of their properties and characteristics, section III highlights some applications of SoS. Section IV provides a brief outline of the goals for providing IT security, followed by a discussion of some of the specific security concerns related to SoS. This is followed by an examination of some presented approaches to providing SoS security within

Section V. Section VI contains a brief summary of these approaches, and the paper is concluded in section VII.

II. SYSTEM-OF-SYSTEMS

There are a number of definitions available that have been presented in research publications with the aim of simplifying the concept of a SoS [1-2]. Geddes *et al.* [3] use the phrase "A system of systems is a collection of interacting systems embedded in a dynamic environment."

Jamshidi [4] uses a number of examples to describe a SoS, offering the practical definition that 'a SoS is a "super system" comprised of other elements which themselves are independent complex operational systems and interact among themselves to achieve a common goal'. However there exist many definitions that vary in semantics based on the context they've been formulated from. Therefore, currently there is no one agreed upon definition within the research fields exploring this domain.

The numerous definitions that are available to distinguish a SoS from a traditional complex system highlight the difficulty presented trying to define them. This has led to some authors attempting to define SoS through characteristics that can be reliably used to qualify whether a system can be termed a SoS. One of the first researchers to attempt this approach was Maier [5], who proposed five criteria that would allow the necessary distinction of these complex entities. These initial criteria consisted of managerial independence and operational independence of the components, evolutionary development, emergent behaviours, and geographical distribution. Following this initial approach a number of authors have adopted this idea and further evolved it. The most recent characteristics presented by Boardman and Sauser [6] are composed from various descriptions available in the literature. These are as follows

- *Autonomy*: The reason a system exists is to be free to pursue its purpose; this applies to both the whole SoS and constituent systems.
- *Belonging*: The component systems can choose to belong to the SoS based on their needs and enhance the value of the system's purpose.
- *Connectivity*: There has to be the means provided for the systems to communicate with each other for the exchange of information.
- *Diversity*: The SoS should be diverse and exhibit a variety of functions as a system compared to the limited functionality of the constituent systems.
- *Emergence*: The formation of new behaviours due to development or evolutionary processes.

These characteristics are groupings of the common themes from those sources and they provide a set of qualities that can assist with the distinguishing of SoS from traditional systems.

III. SYSTEM-OF-SYSTEMS APPLICATIONS

In order to further illustrate the ideas of a SoS a number of papers present examples that can be used to demonstrate the concepts. One of the most cited examples are those of military applications, exploring the collaboration of multiple systems for common goals, such as air defence and battle space awareness and management. Caffall and Michael [7] use the Ballistic Missile Defence System (BMDS) in their case study for an architectural framework, which is a system for protecting the country against the threat of a ballistic missile attack. This BMDS contains numerous independent systems that consist of sensors to track and detect a threat object and weapon systems that compute firing solutions and engage the threat object. These systems are managed by the battle management, that is defined as the decision making and actions executed to support the concept of precision engagement, to provide the general goal of protecting the country from attack via an airborne threat.

Jamshidi [4] also presents a number of examples of systems that could be classified as SoS. Some of the examples listed include critical infrastructure systems that provide essential services such as energy, communications and transport. The example of a wireless sensor network is also provided as well as that of a healthcare system. Another very popular example which appears in papers [8-9] is that of the aviation industry and the collaboration of all the different systems that are available within an airport such as check in desks, baggage handling, air traffic control, airplanes, and customs.

These examples demonstrate the diversity and complexity of SoS, and highlight the many differences that can be available between those systems classified as SoS. For example the component systems could be connected by either a physical network, such as the roads or air routes, a social network, such as people and organisations or an information network such as the Internet or telephone network. This implies that the provision for security as a generic framework for a complex SoS will be problematic and that the composition of the security framework will be highly dependent on those entities that compose the SoS.

IV. SYSTEM-OF-SYSTEMS SECURITY

Security within the SoS domain is a complicated task due to their complexity, dynamic nature, unique configuration and operation. Looking at a SoS from a bottom up approach, they are comprised of multiple complex systems collaborating in what could be a dynamic environment. In addition to the component system risks there are communication channels available to allow the systems to communicate with each other, these will expose additional security concerns. Finally there are many concerns relating to the management framework that will surround the SoS.

Examining these components that could potentially comprise any SoS further we see that these proposed generic components are as follows

The component systems within their own environment are all susceptible to failures and threats. These threats and risks can be increased when coupled with other components systems in a SoS. Furthermore once they become connected and begin operating with other systems they could be exposed to new threats and risks, which were not possible while operating in isolation.

Within the systems there is an additional security concern presented, by exposing an interface into the system for others to access system resources. The interfaces provide the functionality to allow a system to be part of a SoS and therefore act as a gateway into the SoS and the systems. It was these interfaces that were identified by Maier [5] as the architecture of the SoS and the area where the most risks are located to the SoS. The exposure of interfaces into the systems poses significant risks and provides extra possible attack vectors.

There are numerous threats and risks associated with network connectivity as detailed in Pfleeger [10]. The network is a critical component of the SoS and the enabling technology that allows the formation of a SoS. The difficulties presented in providing a secure and robust communication network are compounded by the fact that the nature of a SoS is at odds with one of the current approaches to network security. Typically networks are secured by providing a secure perimeter and controlling the access to the network via a managed gateway [11]. There could be problems due to the dynamic nature of the SoS making it difficult to define the boundaries of the SoS. By providing a secure perimeter and controlling the entrance and exit of all traffic into a system a reasonable amount of external robustness is provided. However in a SoS this perimeter may not be fixed and as easy to control as in traditional systems.

There are also the examinations of the data flows that exist within the network. There are risks presented as the data flows through the network and potentially through unknown systems [12]. There is the potential that system *A* could be communicating with system *E* through systems *B*, *C* and *D*. These conduit systems may be using or simply forwarding the data flow to another system that they have contact with. This possibility and many other unknown runtime configurations lend weight to the rationale that the data flows need to be considered and examined for their own security risks.

These areas identified above are the lower level concerns and cover the individual envisaged common components of the SoS, however there is also another important area that will need some consideration. From a top down approach there is the question of management and organisation of the SoS. This area presents many questions that will need answering.

While there are existing solutions to provide security for the low level components, there remain questions over the management frameworks and approaches to security. For example, there could be a firewall and IDS to protect the systems and networks, and a number of security policies

dealing with encryption and authentication schemes to protect the data flows and communication channels. These existing tried and tested solutions will perhaps remain suitable for their purpose after some minor changes and tweaks to adapt their use for a SoS context. The management framework presents many issues and is the focus of a majority of the research efforts.

The factors relating to the running and operation of the SoS are of major importance to them and will greatly affect the success or failure of the SoS. This could be broken down into the following areas that need consideration and provisions available for potential issues that may arise.

- *Ownership* – the ultimate ownership responsibility for the SoS and who will be responsible for dealing with issues arising from the SoS, for example if the system was used for malicious purposes, who would be legally culpable?
- *Auditing* – the tracking of transactions and use of the SoS, where will they be tracked and stored and who will be responsible for the generation and maintenance of logs?
- *Configuration* – the ability to manage and alter configuration settings associated with the SoS who will be responsible for investigating any configuration issues and performing changes?
- *Requirements* – the requirements that the SoS meets to ensure it's running as expected and functionally correct who will be responsible for testing and proving the system is running as expected?
- *Monitoring* – the monitoring for faults and issues within the SoS and ultimately who will be responsible for addressing any issues that may occur.
- *Authorisation* – the management and control of the authorisation schemes used and the ability to grant system authentication to interested parties.
- *Risk* – the management and control for the assessment, updating and mitigating of risks.
- *Environment* – the control and assessment of the operational environment and the creation and enforcing of policies to control environmental security related to the SoS.

This area is a large focus of many research papers and the majority of the papers focus on the creation and these management issues surrounding SoS.

In summary there are a large number of potential threats and attacks available against the computer systems within a SoS. Many failures, malfunctions or malicious actions that occur within a SoS appear of greater consequence than when they occur within an isolated system. In the case of an issue in a SoS all collaborating systems are at risk either directly via potential cascade vulnerability problems [13], where their assets are at risk, or indirectly, where the system is denied a resource it requires and then appears as a denial-of-service attack. This associative risk of potential vulnerabilities cascading to affect component systems is a serious risk both legally and monetarily.

V. STATE OF THE ART

This section aims to examine a selection of the papers available that contain ideas, frameworks, or schemes that can be considered to provide security for a SoS. Due to the nature of the SoS there are few concrete or typical examples to focus on and this leads to the security mechanisms being quite specific for the domain they're being developed for or utilised in. Due to the limited possibilities for discussion and the complicated nature we will focus on the management frameworks in particular.

A number of available papers focus on and discuss the approaches for a SoS framework, some of these include aspects of security. One example is a security engineering process as defined by Bodeau [14] that can be used to provide security for all aspects of SoS. This approach is planned to be integrated into the process of SoS engineering, referred to as S² engineering. The goal of S² engineering is to ensure that the SoS can function as a single integrated system to support its mission; this approach is primarily focused on military applications. The security issues highlighted within the paper are those of: how to identify and mitigate risks associated with connectivity, how to integrate security into the target architecture, how to approach constraints associated with legacy systems, and ensuring that there isn't an increased vulnerability to threats caused by transition to the target architecture.

The presented process is underpinned by some basic principles, as follows.

- Identify and mitigate risks associated with end-to-end flow of information and control. If possible, do not focus on risks internal to individual systems.
- Focus first on boundaries between security policies domains.
- Focus second on interfaces between individual systems
- Integrate security into target requirements and transition planning

The overall goal of the suggested process is to ensure that reliance on the SoS does not place sensitive information or mission readiness at risk. This is achieved by including some security specific processes in the processes that are defined for S² engineering, these processes include but are not limited to: information gathering, flow analysis, end-to-end testing, and target architecture and transition planning. The security processes are expected to be incorporated within these stages as they are occurring for the creation of the SoS, for example during the information gathering stage the paper highlights those areas that must be given extra consideration, such as a systems full and complete interface documentation so that they can be scrutinised by security engineers.

This proposed framework is a static approach that would occur during the planning and creation of a SoS or before the integration of a number of systems to create a SoS. The framework is realised in a manual way and heavily document-based requiring a solid and complete understanding of all the component systems that comprise the SoS. This approach has few if any automated steps The authors comment that as many stages as possible should be automated but with no

examination of which ones or how this would be achieved. This will require stakeholders to agree and collaborate on the various stages which would be time consuming and prohibitive in the case of a SoS the required quick deployment. This approach may also suffer under scalability issues. As the number of component systems and their configuration needs increases this framework could become prohibitive, expensive with regards to time and monetary costs and ultimately struggle to keep up with changes and evolution within the SoS. The documentation produced would also increase as the SoS evolves leading to the possibility that these documents become outdated and unmanageable when attempting to perform updates to these records.

Other issues are present within the framework relating to the identification of security risks and threats which require mitigation measures and resolution steps. It is a difficult operation to discern all threats and risks that isolated systems encounter during their operational lifetime. The inclusion in a SoS will only increase the risks and complicate this process making it a very daunting prospect. Furthermore during the stages of the assessment there is little consideration afforded to those emergent behaviours that may occur and how to distinguish and handle them. Failure to identify these emergent behaviours would result in the plans and framework being inaccurate and provide difficulties in discerning the actions to be taken when an unpredicted behaviour occurs.

The process may work for a centrally managed and controlled SoS within the military domain. However if these processes were applied to other domains there are questions about the practicality, cost and scalability that would need to be addressed. Overall the framework presents principles that provide a sound basis for assessment of a SoS and its features, the basic principles offered are very applicable to any SoS framework.

A framework for the management of SoS is presented by Gorod *et al.* [15], based on the characteristics presented by Boardman and Sauser [6]. The proposed framework is built on the International Organisation for Standardisation (ISO) Network Management model. They highlight the numerous comparisons within research papers of a SoS with a network and postulate that a SoS can benefit from being represented as a network. They map the network management model of Fault management, Configuration management, Accounting management, Performance management and Security management (FCAPS) to some SoS management conceptual areas, such that:

- Fault management maps to Risk management
- Accounting management maps to Resource management
- Security management maps to Policy management

They use these mappings and the characteristics of a SoS to produce a SoS Operational Management Matrix (SoSOMM) that is intended to reduce the complexity and assist the management of the SoS.

This is a theoretical approach that defines ways that a SoS could be managed, but has not been tested in any practical implementations or simulations. This framework provides some interesting features and ideas; it's based on a model that

is currently in use and has a solid history being created and managed by the ISO. There are a number of issues related to how some of the activities associated with the framework could be implemented within the SoS domain. For example, under performance management the ability to monitor and measure the performance of individual systems in a consistent and thorough manner during operation will need addressing.

With the arrangement of this proposed process being high level abstract goals, there are many questions about how to implement the processes to perform the required actions within the SoS. The authors themselves provide the possible next step of using SoSOMM to evaluate a real-world SoS. They suggest the Internet as a possible real world example to consider.

Agrawal [16] examines security in the SoS domain and offers a new approach to providing a security schema. Moreover the paper hypothesises that the traditional security approach of forward static security is insufficient for the dynamic uncertain environment that is associated with SoS. The author suggests the use of macroscopic schemata for security that will allow the system to monitor the environment and feed the results back into the system to allow it to adapt and alter its security position. The schemata must account for local risks within the systems and the aggregated global risks to the SoS as a whole. Agrawal presents an example of a schema for an access control system, and uses the examples of two recent studies mapped to the example schema.

The proposal is only theoretical but implies that this approach will be feasible when the technologies are available. The question of adaptable security raises the issues that if an attacker compromises the security system they could exploit the system wide control and gain access to all aspects of the SoS. There are other potential issues with the use of adaptable control mechanisms for security systems when considering defects within the security system. With a powerful controlling system any defects within the program could have far reaching issues that go undetected due its automated nature.

Keromytis *et al.* [17] present a holistic approach to security in their paper; their architecture is not specifically intended for a SoS and is rather directed at protecting a single service or system. However this architecture is distributed in nature and modular and the concepts could be utilised to offer a security architectures for SoS.

This architecture - termed SABER - is intended to provide a complete integrated security solution as an alternative to the typical security mechanisms. They suggest using automated survivability architecture to block, evade and react to attacks. A typical security solution is constructed from isolated independent systems such as firewalls and Intrusion Detection Systems. SABER provides a unified framework by integrating several such technologies and is designed to be deployed across a distributed system. This architecture uses a multi layered approach to defend against attacks and uses a coordinated response to survive security breaches. The intention is that SABER provides this coordinated defence and response in an automated fashion, by monitoring and reacting

to events and actions. It then utilised this knowledge to operate the modular components and provide multiple approaches to defending against different attacks. By lessening the need for human intervention when an attack is detected the system can respond quicker and minimise any potential damage or loss.

The architecture that composes SABER consists of the following components.

- A network denial-of-service (DoS) resistant architecture.
- Intrusion and anomaly detection tools, placed within service contexts to detect both malicious activity as well as stealthy “scans and probes”.
- A process migration system that can be used to move a service to a new location that is not (currently) targeted by an attacker.
- An automated software-patching system that dynamically fixes certain classes of software-based vulnerabilities, such as buffer overflows.

These components are tied together in a distributed infrastructure that operates a publish-and-subscribe event architecture. This infrastructure is the critical component and provides the command and control structure, including a monitoring solution for problem detection and an event distiller to find the cause of problems and perform the appropriate action. This was implemented via a system that has full awareness of the network to allow it to reconfigure its topology.

This proposed system is a step towards automation and providing dynamic security that can adjust its posture based on the feedback from the system and operational conditions. Some interesting features presented in the work are those of automatic service migration and automatic patching. Examples are provided for a number of scenarios, which are detailed within the paper using the example of a bank system. The example of service migration actions are locking down and moving a database to a secure separate server to protect loss of data. The patching mechanism is capable of patching known vulnerabilities and possibly being able to identify attack vectors in a mirrored sandbox and provide source-code transformations for the live system for exposed vulnerabilities.

The goal of this architecture is to allow a system to survive and continue to operate unaffected in the event of an attack or malfunction, which would be a hugely beneficial approach in a SoS framework. This would provide a web of security across the SoS, providing a complete security solution.

One potential issue with this approach is that of having to introduce additional systems to secure in the SABRE architecture: each module that is added would be another potential attack vector and raises questions about the security of the architecture. Any compromise of the architecture also presents the potential risk of the dynamic security being used maliciously and actually locking down access to the system for legitimate users and owners. Effectively using a SoS to protect a SoS. The proposed system is currently in the prototyping stage.

Dagali and Kilcay [18] approach SoS through the exploration of Multi Agent Systems (MAS) as a possible way

of understanding the behaviour and controlling the SoS through computational intelligence. Their approach is to use loosely coupled agents to provide monitoring and control of the SoS similar in concept to that of biological systems such as ants or wasps. Such systems exhibit the ability to cope with the diverse and changeable environment in which they exist.

They highlight the fact that within the SoS domain the requirements are affected by the architecture of the existing systems that will limit the capabilities and technologies that are available to provide the solution to the requirements. This contrast with a traditional isolated system where these constraints aren't as strict and often the designers are largely free to choose the architecture that provides the best solution to the requirements.

The paper explores some computational intelligence techniques that could be used for modelling and monitoring the SoS. Proposing that swarm intelligence could focus on the system behaviour and analysis, while a MAS and distributed artificial intelligence could be focused on system design. They present some methodologies that can be applied to the analysis and design stages of a SoS that will allow the production of robustness, reliability, scalability and flexibility within SoS.

While the authors fail to address security issues directly they offer a possible way to monitor and model a SoS so that the security framework will have the access to a quantifiable way of viewing the SoS. The work is a theoretical proposal that identifies an issue with the current analysis techniques available for SoS and provides a possible approach to solve this issue.

According to Tervo and Wiander [19] one of the biggest contributions to IT related problems occurs from what they classify as the system surroundings and community. Based on their study of critical infrastructure systems problems reported in the Finnish media, they found that the majority of identifiable issues were related to updates and new system installations. This is followed by incompatibility as the second biggest cause of problems within the classification. They conclude that environmental problems overrule system internal technical and people related problems. This work highlights that large systems and nets of systems become complicated combinations of different systems, having considerable vulnerabilities that are mostly based on the complex interconnections in the system's surroundings. These vulnerabilities are exposed due to inadequate management of updates and system management when systems are collaborating. This presents a need to examine the interfaces and interdependencies within the systems more thoroughly before updates and collaborations occur.

VI. DISCUSSION

Looking at the body of work on the area of SoS so far, they are diverse entities with a number of definitions available, and characteristics used to distinguish them from traditional systems. There are few typical examples of a SoS and currently the approach is to look for those systems that exhibit the properties associated with a SoS and examine these to identify transferable methods.

The subject of security within the SoS domain, as highlighted above, is approached in a largely theoretical manner and in a number of cases considered within the greater scope of the management frameworks. While this is an advantageous approach to ensure that the security concerns are addressed from the beginning of the SoS the approaches are mainly manual and static in nature. As highlighted by Agrawal [16] in the domain of SoS this approach alone may not be suitable and the systems will need a method to alter their security position. Such as that proposed by Keromytis *et al.* [17] to provide a coordinated security approach that can monitor the environment and respond appropriately. These theoretical approaches could also encounter issues with scalability and maintenance, if the number of systems collaborating increases these processes explored above can become prohibitive in terms of time and financial costs. Moreover any changes in the environment or systems could invalidate or reduce the effectiveness of any process or procedures that have been incorporated into the frameworks. As highlighted by Tervo and Wiander [19], some of the big IT issues come from the changes to systems or operating environments. This is due to the rigidity in these methods and a need for them to be performed before the system is in use. Furthermore the methods described above are aimed at the management level of SoS and approach them from a top down view, implying that to provide a robust SoS needs a complete SoS wide view and understanding of it. This approach could be acceptable within the domains that are centrally controlled such as the military applications. However when looking at other domains where a SoS can be observed such as Web services or a major public event such as a sporting or entertainment event. There are difficulties presented in discerning all the entities involved in any transactions let alone being able to obtain a SoS level view through manual methods.

The evolution of SCADA systems presents an interesting problem space as their progression leads to their availability over the internet. These present highly attractive targets to malicious intentions via the anonymity of the Internet and large scale, high publicity impact their disruption can cause. These targets are susceptible due to their attachment to common platforms that have known vulnerabilities. Furthermore their existing frameworks that have been developed in isolation with little need to consider the dangers of access from possible unauthorised sources present further issues. The field of security around SCADA systems is an active research area [20] [21] [22].

In order to provide the security methods discussed above within SoS an number of the methods described could be attempted in an automated approach. Some of the candidates for automation within the above frameworks could be the following

- Monitoring of the parties involved
- Assurance of the functionalities and correctness of any involved systems
- Establishing a level of trust for systems and managing this trust

- Testing of SoS as a complete entity.
 - Providing a logging and auditing method for the SoS
- Using an automated approach would speed up the deployments and integration into a SoS as well as reducing the complexity that can be encountered while attempting to manage and control multiple different systems.

VII. CONCLUSION

In this paper we have explored some of the areas relating to SoS security. Having approached this from the view of defining a SoS and presenting the characteristics that are common to one. We briefly looked at some examples and discussed some of the security concerns surrounding a SoS. This was followed by an examination of some of the proposed approaches for providing security for a SoS.

The subject of SoS security is a complicated undertaking and presents many unique challenges that will be difficult to resolve. There are many questions about security within the SoS domain and one of the big challenges in this area is the diversity that can exist between different SoS compositions and the lack of a typical example. This makes providing an all encompassing solution that can be used for all SoS a wicked problem. However the selection of a strong example and creation of a robust security mechanism and approach for this area could provide a solution that is transferable to other SoS. The proposals examined above contain some good ideas that could act as starting points however they are largely theoretical with few demonstrated examples of them working.

REFERENCES

- [1] V. Kotov, "Systems of systems as communicating structures," *Hewlett Packard Computer Systems Laboratory Paper*, 1997.
- [2] P. Periorellis and J. Dobson, "Organisational failures in dependable collaborative enterprise systems," *Journal of Object Technology*, vol. 1, 2002, pp. 107–117.
- [3] N. Geddes, D. Smith, and C. Lizza, "Fostering collaboration in systems of systems," *SMC'98 Conference Proceedings. 1998 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No.98CH36218)*, 1998, pp. 950-954.
- [4] M. Jamshidi, "System of Systems Engineering—New Challenges for the 21st Century," *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, 2008, pp. 4–19.
- [5] M.W. Maier, "Architecting principles for systems-of-systems," *Systems Engineering*, vol. 1, 1998, pp. 267-284.
- [6] J. Boardman and B. Sauser, "System of Systems - the meaning of of," *2006 IEEE/SMC International Conference on System of Systems Engineering*, 2006, pp. 118-123.
- [7] D. Caffall and J. Michael, "Architectural Framework for a System-of-Systems," *2005 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, 2005, pp. 1876 - 1881 Vol. 2.
- [8] M. Hosking and F. Sahin, "An XML based system of systems agent-in-the-loop simulation framework using discrete event

- simulation," *2009 IEEE International Conference on Systems, Man and Cybernetics*, 2009, pp. 3293-3298.
- [9] A. Khosravi, S. Nahavandi, and D. Creighton, "Interpreting and modeling baggage handling system as a System of Systems," *2009 IEEE International Conference on Industrial Technology*, 2009, pp. 1-6.
- [10] C.P. Pfleeger and S.L. Pfleeger, *Security in Computing, 4th Edition*, Prentice Hall, 2006.
- [11] S. Northcutt, L. Zeltser, S. Winters, K. Kent, and R.W. Ritchey, *Inside Network Perimeter Security (2nd Edition) (Inside)*, Sams, 2005.
- [12] B. Zhou, A. Arabo, O. Drew, D. Llewellyn-Jones, M. Merabti, Q. Shi, A. Waller, R. Craddock, G. Jones, and A. Yau, "Data Flow Security Analysis for System-of-Systems in a Public Security Incident," *3rd Conference on Advances in Computer Security and Forensics. Liverpool John-Moores University*, 2008.
- [13] C. Servin, M. Ceberio, E. Freudenthal, and S. Bistarelli, "An Optimization Approach using Soft Constraints for the Cascade Vulnerability Problem," *NAFIPS 2007 - 2007 Annual Meeting of the North American Fuzzy Information Processing Society*, 2007, pp. 372-377.
- [14] D. Bodeau, "System-of-systems security engineering," *Computer Security Applications Conference, 1994. Proceedings., 10th Annual*, 1994, p p. 228-235.
- [15] A. Gorod, R. Gove, B. Sauser, and J. Boardman, "System of systems management: A network management approach," *Conference on System of Systems*, 2007.
- [16] D. Agrawal, "A new schema for security in dynamic uncertain environments," *2009 IEEE Sarnoff Symposium*, Ieee, 2009, pp. 1-5.
- [17] A.D. Keromytis, J. Parekh, P.N. Gross, G. Kaiser, V. Misra, A. Nieh, D. Rubenstein, and S. Stolfo, "A Holistic Approach to Service Survivability," *In Proceedings of the 1st ACM Workshop on Survivable and Self-Regenerative Systems (SSRS)*, 2003, pp. 11-22.
- [18] C. Dagli and N. Kilicay, "Understanding Behavior of System of Systems Through Computational Intelligence Techniques," *2007 1st Annual IEEE Systems Conference*, 2007, pp. 1-7.
- [19] H. Tervo and T. Wiander, "Sweet Dreams and Rude Awakening - Critical Infrastructure's Focal IT-Related Incidents," *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1-8.
- [20] G.M. Coates, K.M. Hopkinson, S.R. Graham, and S.H. Kurkowski, "A Trust System Architecture for SCADA Network Security," *IEEE Transactions on Power Delivery*, vol. 25, 2010, pp. 158-169.
- [21] N. Cai, J. Wang, and X. Yu, "SCADA system security: Complexity, history and new developments," *Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on*, 2008, pp. 569-574.
- [22] P. Capodiecì, S. Diblasi, E. Ciancamerla, M. Minichino, C. Foglietta, D. Lefevre, G. Oliva, S. Panziera, R. Setola, S.D. Porcellinis, F.D. Priscoli, M. Castrucci, V. Suraci, L. Lev, Y. Shneck, D. Khadraoui, J. Aubert, S. Iassinovski, J. Jiang, P. Simoes, F. Caldeira, A. Spronska, C. Harpes, and M. Aubigny, "Improving Resilience of Interdependent Critical Infrastructures via an On-Line Alerting System," *2010 Complexity in Engineering*, 2010, pp. 88-90.