Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2009

Appraising Critical Infrastructure Systems with Visualisation

Graeme Pye
Edith Cowan University

Matthew Warren

Originally published in the Proceedings of the 10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st-3rd December, 2009
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/2

Appraising Critical Infrastructure Systems with Visualisation

Graeme Pye and Matthew Warren
School of Information Systems
Deakin University
Victoria, Australia

Abstract

This paper explores the use of system modelling as an approach for appraising critical infrastructure systems. It reports on focus group findings with relation to the system modelling aspects of a critical infrastructure security analysis and modelling framework. Specifically, this discussion focuses on the interpretations of a focus group in terms of the likely benefits or otherwise of system visualisation. With the group focusing on its perceived value as an educational tool in terms of providing an abstract visualisation representation of a critical infrastructure system incident.

Keywords

Critical infrastructure, system, modelling, visualisation, security.

INTRODUCTION

The complexity and interconnection of modern critical infrastructure systems and their associated dependency issues raises a number of considerations with relation to undertaking security analysis and modelling of critical infrastructure systems. This research focuses specifically on the utilisation of system modelling as a means of producing a visualisation of the system structure, architecture, function and its perceived value or otherwise as an educational tool.

Initially, a discussion regarding modelling of critical infrastructure systems is undertaken to scope the issues of modelling such systems as a prelude to reviewing and reporting the findings of a focus group. In this research instance, Coloured Petri Nets (CPN) was the applied system modelling approach used to develop an abstract visualisation of the subject system utilising CPNTools (Jensen 2008) software.

Specifically, this paper reports on the outcomes and subsequent determinations of a focus group conducted to analyse and appraise a practical application utilising the security analysis and system modelling approach of the TARDIS framework (Pye & Warren 2009). The intention of the focus group was to examine and critique the CPN applied system modelling aspect of the TARDIS framework, as applied to a case study of a critical infrastructure system incident.

However, it is not the intention to discuss in detail the applied case study, but to report the merit of modelling a critical infrastructure system incident as a means of visualising the system status at various stages. Therefore, this paper is pursuant to reporting the focus group findings and the merit of utilising system visualisation via CPN modelling with CPNTools, of a critical infrastructure system incident.

MODELLING CRITICAL INFRASTRUCUTRE SYSTEMS

The functional complexity and interconnectedness of today's critical infrastructure systems and their structural information systems and communication networks, poses many challenges to modelling and analysing their security aspects. Particularly, in terms of interpreting the survivability, reliability and resilience characteristics of critical infrastructure systems and the services they provide to modern society. In essence it is the heterogeneous system environment and the interactive nature of these systems that presents several theoretical and practical challenges to modelling, predicting, simulating and analysing the causal behaviours and security factors. Additionally, the influence of external environmental factors and the potential impacts of interdependency relationships as infrastructures evolve and change in structure, or changing operational regulations governing critical infrastructure systems, are all important considerations (Brown *et al* 2004). As the interactions and responses are neither universally applicable nor transferable between independent, single critical infrastructure systems or interconnected multiple system configurations. The fact remains that critical infrastructure systems comprise a heterogeneous

mixture of dynamic, interactive, non-linear elements, unscheduled discontinuations and numerous other influential impositions and behaviours (Macdonald & Bologna 2003).

The challenges of analysing and modelling such large-scale systems, including their dependency relationships with other systems and their non-linear and time-dependent behaviour, remain largely undetermined or ill defined. According to McDonald and Bologna (*ibid*), mathematical models of critical infrastructure systems are vague and there are no applicable methodologies for assessing and comprehending the intricacies of critical infrastructure systems. Then add to this the effects of human interaction and the susceptibility to instigate failure or adaptively recover and manage wayward systems and it becomes self-evident, the difficulty of producing a concise system visualisation.

Therefore, developing a representative system modelling that provides an acceptable visualisation of the subject system requires a deeper contextual understanding of the system, in order to effectively scope the system under investigation. This is not merely about just modelling the topology and dynamics of these large complex network systems, but incorporating the consequential rationality of human thinking, responses and reactions (Macdonald & Bologna 2003, Peters *et al* 2008). Moreover, there are additional complexity factors with network systems that are inherently difficult to comprehend (McDonald & Bologna 2003):

- Structural complexity – increasing number of nodes and links between nodes;
- Network evolution – the structural linkage which could change over time;
- Connection diversity – the links between nodes could have different weightings, directions or capacities;
- Dynamical complexity – the nodes could be non-linear dynamical systems;
- Node diversity – there could be many different node types; and
- Meta-complication – the various complications can influence other network nodes.

Additionally, critical infrastructures can be intractable systems that are difficult to manage, operate with consistency and maintain. They are typically large, physical and geographically distributed systems that are highly diverse and networked, consisting of system within system structures with respective performance variations. There are few system modelling tools that can characterise these infrastructures as whole or decompose the system structures (Schulman & Roe 2007).

Yet critical infrastructure analysis and modelling utilising simulation and optimisation-based techniques have played a part in examining potential interdiction options, through providing insights to mitigate facility loss and enable prioritisation of security strengthening efforts. Thereby system modelling simulation as an optimisation technique has proven invaluable in the analysing vulnerabilities through the examination of a range of applied impacts, with either implicit or explicit notions of optimising performance (Murray & Grubesic 2007).

Therefore, in the context of assessing system reliability and vulnerability through monitoring the simulation models of network nodes or links that are compromised, this enables corresponding changes in connectivity or performance to be visualised and documented. Although a final important consideration is the interdependency relationships that exist between differing critical infrastructure systems. Mussington (2002) identifies these relationships as a point at which a shortfall of knowledge for improving critical infrastructure security capabilities is incomplete and suggests that part of the problem is the complexity of relationships that is difficult to model. However, system modelling is a first step in analysing and answering persistent questions about the 'real' vulnerabilities of critical infrastructure systems (Brown *et al* 2004).

Therefore, it is the intention to seek to determine the merits of system modelling as a visualisation approach towards delivering discernable understanding and comprehension, with regard to analysing the security and functional aspects of critical infrastructure systems.

FOCUS GROUP RATIONALE

The principle rationale of the focus group was to validate the TARDIS framework and discover the suitability or otherwise of undertaking security analysis and modelling of the applied critical infrastructure system incident. The intent was to gather feedback in terms of incident response management, contingency planning and to elicit responses with regard to emergency management education and training approaches.

The composition of the focus group consisted of five invited participants who voluntarily consented to take part anonymously. The opinions, comments and interpretations captured in the moderated discussion undertaken during the focus group, consist of participant feedback from the perspective of an Australian federal government agency.

FOCUS GROUP OVERVIEW

The focus group comprised of two parts: the first consisted of presenting an explanation of the TARDIS framework system modelling intent and function, including a presentation of the critical infrastructure system incident case study. This was necessary to provide clarity and context along with enabling participants to ask any questions. The second part of the focus group was a moderated discussion inviting participants to review and critique system modelling aspect of the TARDIS framework, utilising CPNTools. The purpose of the moderated discussion was to capture and record participant comments and opinions with a view to examining the captured data to determine framework validation in this context.

FOCUS GROUP REVIEW FINDINGS

The review findings are the product of focus group responses to the TARDIS framework in consideration of the critical infrastructure incident case study. The data points relate directly to the following discussion themes:

1. Application of the TARDIS Framework;
2. TARDIS System Models;
3. Education and Training Factors; and
4. Strategic Management.

The collation of comments with regard to each theme forms the basis of the expanded discussions and determinations relating to each point and particular discussion theme.

Application of the TARDIS Framework

This moderated discussion theme focuses solely on the system modelling component of the TARDIS framework utilising CPNTools. It centres on the perceived value or otherwise of the system representation and visualisation approach used from an emergency management educational training perspective.

Initial interpretation

Participants were generally positive in their views regarding the system modelling, particularly in its suitability for systematically critiquing network-like critical infrastructure systems, in-depth case study development approaches and drill-down aspects including the decomposition of system models. Furthermore, the system visualisation offered an incident auditing approach suitable for investigating aspects of responsibility and decision-making, which would be invaluable for post-incident system analysis and as a critique for later educational and training purposes.

Summary findings

In terms of the usefulness of the system modelling, participants were of the belief that as a system diagnostic and network modelling tool, CPNTools was useful in providing an analysis and diagrammatical representation of an historical case study. Additionally, participants found they could appreciate the structure, functions and pinpoint the system problems, with one participant suggesting that the TARDIS framework had a possible business continuity planning application. Furthermore, participants thought the system modelling approach had a powerful ‘storytelling’ aspect in the context of visualising the system and its lower-level subsystems and components. In fact one of the aspects of the TARDIS framework system modelling approach that participants recognised as an important and valuable feature was the capability for decomposing the system in both the analysis and modelling phases. This enabled the examination of the system at differing levels of detail from an overall system perspective to an isolated view of the critical infrastructure system. Participants noted that system decomposition aspects of CPNTools within the TARDIS framework were a strength that had the potential to deliver valuable insights and understanding through its visual system representation.

Other strengths were that the system modelling delivered a means of auditing an incident that would enable scrutiny when reviewing decisions taken, to analyse their impact and consequences in response to the incident. As one participant explained, this was essential to investigating decision accountability and incident management responses, particularly with the private ownership of critical infrastructure systems and the responsibility for actions taken.

Therefore, reviewing incident response practices is important to improving the decision-making process and interpreting the appropriate responses and actions.

Additionally, participants were positive in their assessment of the system modelling capability to decompose the system to its lower-level structures and functions in terms of visualising aspects of security analysis, scenario development and system composition. Participants felt this feature delivered crucial insights into the architectural, structural, functional and incident location from a more visual and abstract perspective.

Furthermore, participants felt that system modelling aspect of the TARDIS framework would be very helpful for educational and training purposes in disaster response, contingency planning, emergency management and coordination. In terms of identifiable weaknesses, participants remarked that there was a lack of temporal feedback, particularly in the system model simulations. Event timings as an overlay, would illustrate the case study system changes over the timeframe of the critical infrastructure system incident, thus providing an appreciation of what happened and when. Participants felt this was a particularly important aspect, as time is a critical influence in incident response decisions in terms of the status of the system. Additionally, participants felt that the incorporation of incident timing would enhance the teaching and learning aspects for emergency management training purposes too. As mapping incident timeframes to changing system status dynamics is particularly valuable in comprehending what happened and when, especially while reviewing an incident. However, time was not a feature of this case study, but it remains a consideration for future incorporation in critical infrastructure system case studies.

Another weakness participants identified was that the CPN system modelling approach would not be particularly suited to analysing and modelling critical infrastructure incidents that were non-linear in nature. The problem is that the unpredictability of an evolving system incident consisting of multiple variables with multiple values would be difficult to interpret, than would otherwise be the case with a linear system event instance. Although, there is acknowledgement that there are interpretive compromises made in analysing and modelling with CPNTools to develop any visual representation of a critical infrastructure system incident.

An important aspect of the moderated discussion was the application of CPN system modelling within the TARDIS framework, was in the context of its suitability as a pre-incident or post-incident analysis tool. Participant views were diverse, with some believing there was merit in applying the system modelling approach in a pre-incident context to hypothetically ascertain, plan and develop appropriate future incident responses, based on the lessons learnt from past events. Other participants thought the approach was better suited to a direct post-incident analysis. Enabling the review of an incident as it unfolded to interpret or identify the effectiveness or otherwise of existing incident contingency plans. Either approach of the TARDIS framework's system modelling aspect had its advantages and disadvantages, although participants generally believed that it was better suited to looking at critical infrastructure system incidents from a historical perspective.

Although there was scope for the predictive use of the TARDIS approach, the consensus was that its main strength lay in the analysis and modelling of critical infrastructure system incidents using historical case studies. The reasoning was that the TARDIS approach offered a means of formally undertaking numerous historical, complex system analyses that could determine likely decisions and courses of action taken. This would then enable contingency and disaster planners to appraise and reconfirm the decisions and actions taken during the event. This approach would identify weaknesses within the contingency response procedures and the actions taken during the incident. The outcome would enable the implementation of incremental changes to improve response measures and actions including decision-making processes, to establish better emergency response systems in the future. This is not to say that the TARDIS approach is not applicable to developing predictive outcomes as applied to hypothetical system incidents. However, it was felt that its strength lay in using system visualisations from a storytelling, educational and training perspective to analyse and model critical infrastructure system incidents after their occurrence.

The feature of system decomposition within the modelling representations of the case study incident was a powerful feature of the CPNTools system modelling software. This provided clarity and comprehension to the focus group participants in terms of system architecture, structure, functionality, causal location and the consequential aspect of the incident. However, as participants suggested, the incorporation of temporal aspects as an overlay would demonstrate the changing characteristics of the system that would further enhance the visual practicality of system modelling and the subsequent simulation aspects. As an aside to the incorporation of time into the system models, there is a capability within CPN modelling for the incorporation of time into system model representations. In this instance, the consideration and inclusion of specific event timings within CPN system models was beyond the scope of this case study.

TARDIS System Models

This part of the moderated focus group discussion focused exclusively on the system modelling aspects and the visual representations developed in CPNTools utilising the principles of CPN system modelling.

Initial interpretation

The participant's responses to the system modelling capabilities (CPNTools) were very positive in terms of comprehending the system models, their structure and the capability to apply a system simulation to provide a deeper comprehension of system interactions and service delivery. Participants suggested that this system modelling approach also had further applications for producing meaningful visualisations related to modelling organisational contingencies. Particularly, human communication networks, decision-making structures and disaster management communication, particularly in educational and training terms for business organisations, local government, and state and federal government agencies.

Summary findings

The participants generally found CPN system models (using CPNTools) easy to follow and were able to comprehend what was happening within the system simulations and, more importantly could see the location of the causal system incident failure including the consequences. Additionally, participants felt the decomposition of system models into subsystem layers and components particularly helpful for comprehending complex structures and functions of the system, and enabling an enhanced explanation that was easy to follow and appreciate. Furthermore, a participant suggested that depending on the target audience and information required, the modelling aspect could offer managers an illustration of what can go wrong and the consequences. Additionally, it may provide system designers with information and feedback about the proposed system prior to construction and implementation, or to enhance training and educational exercises for emergency response management and contingency planning.

Participants thought the system simulation feature of CPNTools system modelling was a very powerful aspect of the TARDIS framework, as it enabled them to appreciate visually the broader impacts and consequences to the community and business organisations. This coupled with the ability to drill-down and decompose the system to observe and isolate the system model at the subsystem and component level, was a valuable feature that assisted in enhancing their understanding and appreciation of the case study. Especially from the perspective of describing the interconnections with other associated systems and that the implementation of changes to model simulations enables users to see other speculative consequential outcomes of the system model. Participants expressed the opinion that these simulations offered valuable outcomes in the education and training environment, as students could see and speculate upon appropriate emergency responses and decision-making within the CPN system modelling environment.

In summary, the focus group was positive in response to the system modelling approach and capabilities of the TARDIS framework, utilising CPNTools software as the system modelling environment. Furthermore, participants suggested extending this approach to modelling and mapping communication networks within organisations or businesses would prove useful for emergency management planning. Finally, they felt the system modelling approach was especially powerful in a visual sense for education and training purposes.

Education and Training Factors

The focus group were further asked to express opinions regarding the potential educational and training factors related to producing abstract visualisations of critical infrastructure system models.

Initial interpretation

The initial interpretation of the suitability of the system modelling visualisation approach utilised in the TARDIS framework is that it offers potential, in terms of security analysis and system modelling suitability for case study based training and instructional exercises. Participants thought this would prove useful for aiding the educational and training aspects of contingency planning and disaster recovery management. However, just where the focus lies requires further specifically targeted research and investigation to determine the application and likely benefits of using abstract visualisations of critical infrastructure systems in an educational context.

Summary findings

The intent of this discussion theme was to elicit comments regarding various impressions of the potential educational and training aspects of visually modelling critical infrastructure system incidents. Particularly, as the focus group participants' expertise lay in education and training within the area of emergency management and contingency planning, it was therefore important to investigate its potential as an educational and training tool. A number of diverse views were expressed with regard to the potential usefulness of system modelling visualisation via CPNTools as an educational and training tool. This was from their expert perspective of educational trainers of emergency management and contingency planning and thus applied to analysing and modelling critical infrastructure system incidents. However, it was the consensus that further investigation and research to establish the TARDIS framework's applicability as a tool for system modelling visualisation for education and training purposes, was required.

Strategic Management

In an additional consideration, the focus group was asked to consider the system modelling and visualisation aspects of the TARDIS framework in terms of the strategic management from their perspective of emergency management education and training.

Initial interpretation

The intention was to seek participant thoughts on the extendibility of the TARDIS framework and its potential for delivering strategic management outcomes. Participants felt that the TARDIS approach would value-add to the development of strategic contingency plans for business organisations, through visualisation modelling and analysis of their crucial systems. However, it was deemed that this requires further research to assess this definitively.

Summary findings

One participant thought that although this was not the primary focus, its application did offer potential for identifying strategic management options in an operational context. This opinion was in the context of an operational team undertaking a review of the sequence of events that occurred within a particular critical infrastructure system incident to determine their significance. Additionally, another participant suggested that this would enable the operational team to appreciate the relationship between what they do and the system, particularly in consideration of action timeframes and how their communication structures and systems function under stress. The outcome of this type of assessment would enable operational teams to identify model and implement strategic management initiatives for improved cooperation, coordination and streamlining of their operational approach for the future.

Further to the potential for identifying strategic management initiatives through system visualisation modelling via the TARDIS framework. The focus group felt that the approach would simplify system complexity through decomposition that to an extent may 'demystify' what actually occurs during an event and enhance incident appreciation. Strategically, this may be used as a teaching and learning resource tool to augment the development of individual decision-making skills, communication structures and incident management procedures necessary for delivering strategic and measured responses to future unexpected incidents. At this point, a participant highlighted that through the applied system modelling approach, it was visually obvious from a reliance perspective as to which of the geographically distant communities were directly impacted by the incident. The participants felt this would be very useful strategically in explaining and illustrating to system managers, owners and operators the importance of system availability and service provision to the wider community.

Participants also felt that the visualisation of the system would value-add to the development of strategic contingency plans for business organisations through analysing and modelling their crucial systems. This would therefore enable businesses or government agencies to prioritise and strategically allocate resources to minimise the impact of an unexpected incident. Thereby potentially reducing any system downtime, loss of data or information and perhaps reduce the economic affects to governments, business, staff and community.

Finally, in terms of governmental recovery management, participants thought the TARDIS approach would be an especially useful tool for undertaking reflective analysis after the event. Particularly utilising visualisation through system modelling to investigate and map the strategic communication pathways from government to individuals within affected communities. Especially, in terms of communicating essential information to community members before or after a significant emergency event to effectively manage the response and recovery processes to get the resources to where they are needed.

This discussion theme elicited views and interpretations of the extensibility of the TARDIS framework system modelling approach in terms of identifying its possible adaptability to identifying, visualising and determining strategic management indicators that would be applicable to critical infrastructure system managers, owners and operators. Although, this was a digression for participants, away from considering the TARDIS framework as a security analysis and modelling tool for critical infrastructure system incidents. Focus group participants felt there was scope for extending and applying the TARDIS framework system modelling in relation to strategic management approaches that would be applicable to a number of levels. These included reviewing system managerial and incident response management and planning, through to strategically managing the processes and structures of communication with the community, in both pre-incident planning and post-incident recovery management contexts.

FOCUS GROUP CONCLUSIONS

The comments and opinions were constructive and reflected favourably on the benefits and outcomes of the system modelling aspect of the TARDIS framework as an approach for visualising and modelling of a critical infrastructure system incident. This was primarily evident in the favourable responses of the initial moderated discussion theme and further evidenced in subsequent themes in terms of system modelling, the decomposition feature of CPNTools and the added diagrammatical dimensions of the system simulation aspects.

Another important conclusion was the reaffirmation of applying the TARDIS framework to historical case study incidents, although it was recognised that the framework was potentially applicable to hypothetical situations and predictive outcomes. Focus group participants felt the real strength and value lay in system modelling after the incident had occurred from a 'lessons learnt' perspective. In the context of an education and training tool, the opinion was that the system visualisation aspect of the TARDIS framework would value-add in the environment of education and training. This would be achieved by presenting alternative interpretations of incidents to develop analysis skills, understanding, comprehension and intuition of the potential consequences for critical infrastructure system failures.

Participants identified the TARDIS framework's relevance and suitability for case study system modelling depiction and suggested that it would also be suitable for analysing and visually modelling communication networks. Furthermore, the identification of strategic management issues had potential benefits for areas including: business contingency planning; emergency management response planning; emergency services; communication analysis and disaster recovery management of critical infrastructure systems in the Australian context.

SYSTEM VISUALISATION OUTCOMES

The primary outcome of this focus group investigation was that the visualisation of critical infrastructure system incident through system modelling offers an insight into developing greater understanding of the situation for system security and other analysis purposes.

The analysis and modelling of critical infrastructure systems also offers the potential to determine interdependencies that are susceptible to cascading failures and identifying the divergent systems characteristics likely to exacerbate such interconnected infrastructure failures. Particularly, where the consumption of services is virtually immediate and no buffering or reserve of resources exists within infrastructures. This is particularly evident in telecommunications and electricity grids, where the immediacy of resource consumption can lead to potentially instantaneous cascading failures that impact other interdependent critical infrastructure systems. Alternatively, other infrastructures exhibit buffering characteristics similar to fuel and gas production and distribution infrastructures where physical supply resources have a level of reserve. Within these systems failure would not necessarily be instantaneous, but the effects would exacerbate over time (Svendsen & Wolthusen 2007).

The differences in scenario characteristics and the characteristics of the critical infrastructure systems involved would by necessity require careful consideration in any modelling context. Particularly, when seeking to identify, predict and even quantify the effects of cascading incidents among interdependent infrastructure systems with regard to public policies that aim to address critical infrastructure vulnerabilities and especially that relate to critical infrastructure system security (Zimmerman & Restrepo 2006).

According to Little (2003), applying analysis and modelling techniques to historical critical infrastructure incidents and events enables incremental improvements in prediction, forecasting and preparedness for future events and allows the instigation of new engineering approaches to design and construction. This enables critical infrastructure

systems to become more robust to withstand the rigours of natural hazards, crippling failures, accidents and incidents as they occur in the future.

Due to the increasing importance of secure critical infrastructure systems, there is an effort to develop analysis and modelling approaches that can accurately model critical infrastructure system behaviour, identify interdependencies and vulnerabilities to various threats. Some of the potential outcomes of analysis and modelling simulation approaches to assessing critical infrastructure systems may prove beneficial to governments, government agencies, military planning and defence and community expansion plans. This may reduce costs, enhance critical system redundancy, improve traffic flow, secure data and information protection and enable better preparation for and response to emergencies (Pederson *et al* 2006).

Although in the context of Australian critical infrastructure system characteristics, there are modelling considerations that are particular to the visualisation of critical infrastructure systems. However, the ability to model these systems utilising a visual medium such as CPNTools, does offer another alternative that may provide invaluable insights into the security assessment and analysis of critical infrastructure system incidents.

CONCLUSION

The private and public owners in the infrastructure industry now have heightened security obligations with regard to the Australian national security status. This includes maintaining critical infrastructure system availability and supply of services to industry, business and the wider community, who are increasingly dependent and reliant on critical infrastructure systems. Further compounding this is the increasing interconnectedness between infrastructures via the information communication technologies that are increasingly pervading into these systems and therefore creating new interactions, interdependencies and dependency relationships. These technological innovations have thus introduced new risks and vulnerabilities enabling decentralised utility supply, distributed, autonomous control of network operations and information sharing provided by multifunctional information and communication infrastructures.

The collection of interactive change processes in the Australian infrastructure industry is creating a new generation of critical infrastructures. These systems are so interwoven with new technologies that traditional approaches to managing spatial planning, policy making, regulation, technological, information and communication, physical and cyber security require rethinking. Similarly, governments and owners and operators must consider their interactions and connections with other critical and non-critical infrastructure systems. This is particularly relevant in terms of capacity allocation, service provision, system availability, planning and security as a function of changing economic, environmental and regulatory conditions.

Therefore, understanding critical infrastructure system behaviour and security implications, vulnerabilities and mitigating identified security risks is a current concern of many nations, including Australia. In terms of a system thinking perspective, comprehending the design, operation, management and ultimately the security of any critical infrastructure system is important to conceptualising the system, its goals and performance. This applies equally to all differing levels of the greater system structure including the behaviour of the identified subsystems. Hence the ability to visualise the system through applied modelling techniques as discussed here, offers one approach to appraising critical infrastructure systems with visualisation.

As Bentley (2006) intimates, critical infrastructure systems tend to be interdependent and even interconnected and systems failure – be it through natural disaster, accident or poor management – can bring entire communities and their industries and utilities to a grinding halt. Just imagine, for example, a major electricity failure, which these days can bring just about everything to a stop, from transport to workplaces, water supplies, telecommunications and transport hubs that would cause widespread disruption and damage. Therefore, the ability to analyse and critique the security aspects of critical infrastructure systems, together with modelling these systems visually, offers an avenue for assessing critical infrastructure system security and identifying vulnerabilities. Through locating these inherent weaknesses, appropriate solutions and remedial actions can be appraised and implemented to mitigate security risks to system availability and service supply.

REFERENCES

Bentley A. (2006) *Infrastructure: Critical Mass*, CSIRO Solve, No.7.

Brown T., Beyeler W. & Barton D. (2004) Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems, *International Journal of Critical Infrastructures, 1*(1), 108-117.

Jensen K. (2008) Special section on coloured Petri nets, *International Journal on Software Tools for Technology Transfer, 10* (1), 1-3.

Little R.G. (2003) Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, in *36th Hawaii International Conference on System Sciences (HICSS'03)* IEEE Computer Society.

Macdonald R. & Bologna S. (2003) Advanced Modelling and Simulation Methods and Tools for Critical Infrastructure Protection, Retrieved March, 2007 from http://www.iabg.de/acip/doc/wp4/D4_5_v0_1_RM.pdf

Murray A.T. & Grubesic T.H. (2007) Overview of Reliability and Vulnerability in Critical Infrastructure, in *Critical Infrastructure*, Springer Berlin, Heidelberg, Berlin, pp. 1-8.

Mussington D. (2002) *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*, RAND, Santa Monica, CA, USA.

Pederson P., Dudenhoeffer D., Hartley S. & Permann M. (2006) *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory (INL), Idaho Falls.

Peters K., Buzna L. & Helbing D. (2008), 'Modelling of cascading effects and efficient response to disaster spreading in complex networks', *International Journal of Critical Infrastructures, 4* (1/2), 46-62.

Pye G. & Warren M.J. (2009) Security Analysis and Modelling Framework for Critical Infrastructure Systems, in *8th European Conference on Information Warfare and Security*, Academic Publishing Limited, Lisbon, Portugal, pp. 198-207.

Schulman P.R. & Roe E. (2007) Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures, *Journal of Contingencies and Crisis Management, 15* (1), 42-49.

Svendsen N.K. & Wolthusen S.D. (2007) Connectivity models of interdependency in mixed-up critical infrastructure networks, *Information Security Technical Report, 12* (1), 44-55.

Zimmerman R. & Restrepo C.E. (2006) The next step: quantifying infrastructure interdependencies to improve security, *International Journal of Critical Infrastructures, 2* (2/3), 201-214.

COPYRIGHT

Pye and Warren ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors