Locating Risk through Modelling Critical Infrastructure Systems

G. Pye[1] and M.J Warren[2]

[1, 2]School of Information Systems, Deakin University, Geelong, Australia
Email: [1]graeme@deakin.edu.au, [2]mwarren@deakin.edu.au

Abstract

This paper introduces and discusses the research proposition of a link between the modelling of critical infrastructure system/s and risk identification and management. As a means of categorically identifying points of risk within a particular model of a critical infrastructure system/s for the purpose of solution creation and contingency development and testing in the modelling environment, prior to physical implementation. This research is at the preliminary stage of exploration and is an extension of current research into modelling critical infrastructure system/s and extends this research with regard to introducing risk perception and quantifying risk, along with establishing modelling guidelines for consistent model generation, as discussed.

Keywords

Risk management, perception, critical infrastructure, modelling.

1. Introduction

The essential services supplied to modern society by critical infrastructure systems are many and varied and traverse numerous sectors of society to reach a large number of diverse consumers. As a consequence of the high supply reliability of these systems, the delivery and availability of these services are predominately, taken for granted. For instance, when operating the light switch it is expect that the electricity will be available to energise the light globe and illuminate the room, but is there any contingency consideration given if this was not the case? For the most part, consumers expect these services to be there when needed and are not overly concerned with the threats and vulnerabilities that can put these systems at risk. Nor are they concerned with the potential inconvenience or the impact magnitude that losing any, some or all these services can potentially impose upon most facets of society's everyday function.

The consequence of society's reliance on critical infrastructure availability, technologies and the physical infrastructure supporting the delivery of their services,

necessitates the existence of a level of security to protect the availability and integrity of critical infrastructure systems. To achieve this requires identifying threat issues, the proactive mitigation of known risks, identifying new risks to prepare, develop and implement appropriate contingency plans. However, due to the diverse types of critical infrastructure, its physical size and scale, the management of security and identification of risks within the systems remains a difficult task.

One way to directly address these issues is to generate a model of targeted critical infrastructure system featuring its normal operation and use the model as a means of assessing the functional integrity and security of the system. This process would enable: an in-depth and scalable system security analysis of the system model; a broadening of system understanding, and provide a valuable tool and inexpensive means of identifying points of risk within the subject critical infrastructure system/s.

Therefore, with the advent of critical infrastructure modelling, the identification of risk and the subsequent solution creation to counter the risk are potentially testable with the incorporation of the solution back into the system model. This then encourages further assessment to theorise upon the various causal factors that are likely to impact upon system availability, integrity of security and deviations from the functional norm. Furthermore, this would lead to more accurate risk identification reflecting a common point of understanding and perspective, which would enable clear communication of the risk to the public, critical infrastructure owners, operators, governments and other stakeholders regarding system threats, vulnerabilities and risks.

Initially, this paper will briefly outline critical infrastructure from an Australian perspective and its system related characteristics to establish background knowledge, before proceeding to discuss the perception of risk in relation to critical infrastructures, its context and potential magnitude, along with discussing the various types of perceived risk. Next, is discussion that describes the potential that systems modelling offers, before going on to outline some fundamental guidelines applicable to modelling critical infrastructure systems to establish a guide for consistent model development. Finally, the conclusion will address and summarise the key research points identified to this time and any future research possibilities regarding the use of systems modelling as a means to enhance risk identification within critical infrastructure systems that may prove beneficial to key stakeholders.

2. Characteristics of Critical Infrastructure

In the Australian context, as with other technology-rich western societies, critical infrastructure systems deliver essential services across many differing sectors of the nation. Typically, critical infrastructure refers to those ‘physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period of time, would significantly impact upon the social or economic well-being of the nation or affect Australia’s ability to conduct national defence and ensure national security’ (AGD 2004 p1).

Therefore, the loss or interruption of critical infrastructure services would impact upon the normal functionality of the banking and finance sector, transport and distribution, energy, utilities, health, food supply, communications, government services and national icons, as identified in the Australian government's national strategy (TISN 2004).

As society is ever more dependant on these services, this reliance necessitates the protection of such systems to maintain service availability, this requires a fundamental understanding of what characterises critical infrastructure systems. The principal characteristic of these critical infrastructures is that they are systems consisting of numerous sub-systems, all functioning seamlessly and cooperatively as one larger system to deliver their services. Additionally, they can also the existence with interconnections between seemingly autonomous critical infrastructure systems. The existence of these interconnections results in the formation of dependency relationships, where one critical infrastructure system can deliver or exchange services with another critical infrastructure system, which adds further complexity to the network structure of the critical infrastructure system as a whole (Pye and Warren 2006).

Therefore, critical infrastructure systems can be characterised as being complex, highly structured systems, interconnected with other highly cooperative networks to facilitate the supply of services. Scott (2005) noted this is particularly prevalent in the energy sector where the continuity of the electricity supply is essential to functionality of other critical infrastructures and their continued supply of services, particularly from the perspective of the national interest, business and social communities.

When considered from this perspective, the primary objective is maintaining infrastructure availability and the continued provision of critical infrastructure services to the community across all sectors (Pye and Warren 2005). However, the risks become apparent when considering that by their very nature critical infrastructure systems are vulnerable to damage, destruction, disruption, breakdowns, negligence, natural disasters, cyber incidents, illegal and criminal activity, vandalism and malicious damage (Pye and Warren 2006). The presumption that critical infrastructure services will always be readily available and there on demand is an expectation drawn from past experience where these services have nearly always remained available or have only been disrupted for relatively short intervals. This is particularly apparent when considering services such as electricity, information technology and telecommunications that have always maintained high levels of service availability.

The consequence of societal expectation is that critical infrastructure systems will always be available to deliver their services; therefore security of supply becomes a very important issue for owners, operators and users of critical infrastructure services. This means that they must identify their specific risk exposure at all levels, including sectors and sub-sectors of critical infrastructure such as depicted by Pye and Warren's (2005) overarching model of Australia's critical infrastructure. Hence

this research asserts that the use of targeted system modelling techniques would enable improved and faster identification of risk points, security threats and areas of vulnerability within the particular system's model. Thus enabling the development and testing of contingency plans in the model environment prior to physical implementation as a means to scope the impact of critical infrastructure service loss and engender a deeper appreciation of the risks to system security and availability.

3. A Perception of Critical Infrastructure Risk

It is apparent that some organisations within Australia utilising critical infrastructure services do not wholly understand where their particular organisation or infrastructure actually fits within the larger system arrangement of the wider critical infrastructure. Nor are they particularly self-aware of their own status or fully appreciate their potential obligations to the ongoing normal function and availability of the wider critical infrastructure system and its services (Pye and Warren 2006a).

For example, in the 2004 Australian Computer Crime and Security Survey participants were asked, 'Do you consider your organisation to be part of the critical national infrastructure?' (AusCERT 2004 p.5). This question focused on the National Information Infrastructure (NII) as a subset of critical infrastructure and related directly to the 'infrastructure which comprises the electronic systems that underpin critical services such as telecommunications, transport and distribution, energy and utilities, and banking and finance' (TISN 2004a p1). What was notable about the response was that of the total respondents, 84 (35%) considered that their organisation was part of the critical NII, while 123 respondents (51%) did not and most significantly was that the remaining (equating to 14%) respondent organisations were unsure or unaware of their status with regard to their criticality and the NII.

Subsequently, the same question was again put in the 2005 Australian Computer Crime and Security Survey; here 32% of the total respondents considered their organisation to be part of the critical NII, while 52% believed their organisation as not part of the critical NII. Significantly, in the 2004 survey, 14% of respondents were not sure of their actual positioning or status concerning the NII infrastructure and this level of uncertainty had increased to 16% of respondents in the 2005 survey (AusCERT 2005).

In retrospect the increase in the number of organisations uncertain of their status in relation to NII critical infrastructure system highlights a disconcerting point that a significant number of organisations questioned in these surveys, did not necessarily appreciate or fully understand or were just not aware of their status within the NII system. This indicates a lack of risk liability awareness of these organisations within the NII critical infrastructure that could potentially and adversely impact service availability and functional security of other interconnected and dependent critical infrastructure systems (Pye & Warren 2006a).

This exemplifies a lack of circumstantial awareness and risk perception on the part of some organisations utilising a critical infrastructure system, whether this is a lack of understanding, education or awareness is unclear. Hence, this is where system modelling would clearly indicate where an organisation's own infrastructure fits within the schema of neighbouring or overall critical infrastructure system. Such modelling would enable organisations to undertake meaningful security and risk analysis to categorically determine an organisation's position, status, vulnerabilities and perhaps more importantly realise their infrastructure service availability and supply obligations to other interconnected and neighbouring critical infrastructure systems.

Therefore, this suggests that through applying systems modelling techniques, an organisation would be able to undertake further analysis to identify their own points of vulnerability within the scope of their own systems. The next step would be to extrapolate further through modelling, to see how these risks could potentially impact upon the organisation's own infrastructure and that of the wider critical infrastructure system itself. Thus, elaborating, identifying and comprehending the implications of identified risks through modelling will enable further action to categorise communicate and prioritise risk management for contingency plan development and implementation.

4. A Context of Risk

While there is an element of risk associated with any undertaking, the risk itself not only relates to the recognition of the specific threat or vulnerability, but also to determining a rating of the degree of each risk. This would involve apportioning a value or rating to each risk determining its potential to cause a deviation from normal function.

The awareness and subsequent management of risk involves identifying points of weakness within the system and determining to what extent an identified risk is acceptable and manageable. Assessing and rating the risk reflects a balance between opportunities for gains made, while minimising the potential for loss from an organisational perspective. Risk in this context is concerned with the impact and exposure to consequences of uncertainty or deviation from normal or expected function (Standards Australia 2004).

4.1 Risk and Critical Infrastructure Modelling

The modelling of a critical infrastructure system/s is an effective means of gaining an overview understanding and appreciation of system positioning and potential real-world influence within the larger critical infrastructure structure network. Of course there are other issues of system scalability, the variable dynamics within the system and supporting sub-systems along with the dependency relationships with other cooperating critical infrastructure systems; however these issues are presently outside the scope to this paper.

The primary consideration is to highlight the potential for risk identification through applying systems modelling techniques to targeted critical infrastructure system/s. The propose of this is that the modelling of critical infrastructure systems can further enhance risk detection and as a consequence, improve risk perception, appreciation and understanding across all sectors of critical infrastructure users, owners and operators to develop a common understanding of the degree of risk identified.

4.2 Degree of Risk?

The degree of risk itself incorporates a number of differing variables that when considered together can equate to a derived value of magnitude in relation to an individual risk being the possible cause of a hazardous or otherwise event occurring. Geoscience Australia (2004) applies the following risk formula to determine the degree or level of risk and likewise it can apply to critical infrastructure risk assessment where:

RISK = Hazard * Elements at Risk * Vulnerability.

This formula calculates the level of risk of an event occurring that depends on the magnitude of the hazard multiplied by identified number of elements at risk and the product of their vulnerability or susceptibility to damage or change.

This rudimentary formula provides an example of how to weight identified risk vulnerabilities within the model of a targeted critical infrastructure system and thus quantify potential risk differences within the jurisdiction of the model. Then by extrapolating this weighting value back to the actual physical infrastructure system itself, this enables risk prioritisation, investigation, analysis and communication to relevant stakeholders, together with solution development priorities to mitigate the risk. Additionally, any risk mitigation solutions implemented back into the critical infrastructure model, delivers a means of hypothesising the solution's potential effectiveness to mitigate the risk to an acceptable level.

As it stands currently, the quantifying of identified risks is an aside to this paper and will be the subject of ongoing and detailed research, but it does deliver a means of quantifying comparative risks for risk prioritisation within the model environment. However, this brief investigation does provide a starting point into its application and will assist in determining a common understanding regarding potential risk magnitude within the physical system. This would form part of the overall system analysis process as applied to the security and risk analysis of critical infrastructure system models.

4.3 Perceptions of Risk

In the context of modelling critical infrastructure and identifying points of risk, the perception of the risk itself varies depending on the perspective of those considering the risk. For instance the research of Gardner and Gould (1989) noted some common phraseology that describes technological risk from differing perspectives. For

example, the phase *'speaking different languages'* referred to the different risk definitions applied by scientific community and the general public and what constitutes a *'socially acceptable'* technology. This reflects the difference in values and philosophies regarding risk as most professional risk managers, engineers, scientists and experts tend to express risk quantitatively in terms of money lost. While, the general public is more inclined to regard risk qualitatively in terms of who is impacted and the acceptability of risk from a societal perspective rather then assigning a cost that is acceptable.

In between these two broad groups is the government who must determine national policies, expenditure and resources on risk mitigation from a national perspective. Sjöberg (2001) notes that while this is part of the democratic process it is not perfect, sometimes decisions on risk policy and resource distribution means that not all stakeholders are satisfied with the outcome. Similarly from the Australian perspective, in response to the high levels of private ownership of critical infrastructure, the government initiated the Trusted Information Sharing Network (TISN) as a committee structure for managing, coordinating and sharing of restricted security information with infrastructure owners and operators. This also provides a means of managing risk in the national interest to deliver credible information (AGD 2004a), but this process has some drawbacks too.

The crux of this style of risk perception management is the gathering of credible information from a number of sources for consideration to determine a consensus viewpoint or single risk perception. However, in reality depending on one's circumstance this can potentially lead to differing interpretations and misunderstandings of the magnitude of the risks identified and communicated. In view of this situation the development of a consensus or single view of perceived risk/s is imperative to the overall management of security and risk in the critical infrastructure system/s.

Therefore, the modelling of critical infrastructure systems provides a potential avenue for determining, identifying and investigating the risks inherent in critical infrastructure systems and a means to develop a recognised point of reference for acceptable understanding and magnitude of the risk. The potential benefit to risk management and detection that modelling brings is that it enables clients to see where the risk exists within their critical infrastructure systems, the analysis of risk, its assessment and the contingency plans developed to negate the potential effects if the risk comes to fruition. This is why modelling should be an integral part of any security or risk analysis process of critical infrastructure systems because the use of models in the discipline of information systems bodes well both as a user-analyst communication tool and is a well recognised means of communicating common understandings and conceptual ideas related to real-world systems.

5. Why Modelling?

The primary aim of modelling a critical infrastructure system is to give the viewer a perspective of not only the external environment, but the internal characteristics of the system's environment and to map the targeted system boundaries to visualise its place within these surroundings. From this the modeller can begin to see and understand what influences contribute to characterising the functioning systems and its potential interactions and connections with neighbouring systems, thereby developing an appreciation of the system's status within the greater critical infrastructure schema (Pye & Warren 2006).

Maani & Cavana (2000) suggest that in order to fully comprehend the functional behaviour of any system, at any level, that modelling the system is the easiest method to generate an overview of the system and its points of connection and interactions. Modelling enables the analyst to cope with system complexity, scalability, understand the system structure, the interaction points between the system components and sub-systems, the relational influences with other neighbouring systems and theorise about potential system responses.

From this modelling perspective the system is essentially one that exhibits change and is dynamic in nature and thereby under the influence of *'cause and effect'*. With this in mind the modeller can being to manipulate the model to theorise how the actual system could potentially react to similar changes made in the physical system itself. Likewise, this principle behaviour is also a characteristic of critical infrastructure systems that also exhibit dynamic behaviour, thus enabling the analyst to model such systems to theorise and predict the potential system responses to change. Thereby enabling by extension the opportunity through *'cause and effect'* principles, to apply and model various *'what if'* scenarios. Additionally, such system modelling enhances the ability to also identify points of risk within the model that are likely to be evident within the physical system itself (Pye & Warren 2006).

Therefore, it is important to consider that the modelling process applied to critical infrastructure systems remains consistent to deliver a fair and equitable approach to modelling the target system and for the determination of security and risk points within the system. Underpinning this approach is the requirement to adopt a consistent approach to the model development thus requiring the application of fundamental guidelines with regard to the consistent development of critical infrastructure models.

6. General Fundamentals of Modelling

The overarching principle applied to critical infrastructure modelling should incorporate a keep it simple approach for the development of such system models. This is important because of the highly complex nature of critical infrastructure systems, and yet the endpoint model must also remain representative of the subject system to enable risk points within the system to become visible. To achieve this and

yet remain consistent in application, the following fundamental modelling principles represent an attempt to focus on the consistent application of modelling techniques as applied to critical infrastructure systems.

The research of Pidd (1996) developed five desirable and simple principles to apply to the development of discrete computer simulations or in the use of programming language, similarly these same principles can also be adapted and utilised as guides to the development of critical infrastructure models, as follows (Pidd 1996):

1. Model Simple, Think Complicated.
   This identifies that the modeller must keep in mind that the model itself is a tool to support and extend the thinking, impressions and conceptional understanding of the physical system as a model. Therefore the avoidance of additional complexity and need for clear physical system boundaries are established for the subject system model.

2. Be Parsimonious, Start Simple and Add.
   The problem with the previous principle is identifying where the balance lies between simplicity and complexity. There is no general answer to this problem, but a solution lays in adopting a *'prototyping approach'* where the gradual development of the model starts out with simple assumptions and by only adding further complexity as it become necessary. However this does require continued refinement and revision in order to avoid adding anything unnecessary to the model.

3. Divide and Conquer, Avoid Mega-models.
   This is common advice given to those dealing with a complex problem, the aim being to breakdown the problem or in this case, decomposition the system into manageable component parts that applies the previous principle to develop the system model.

4. Do Not Fall in Love With Data.
   The model should drive the data collection, not the other way round and this requires the modeller to develop ideas for the model and its parameters from a selective perspective of what data types are collected, analysed, interpreted and implemented into the model together with a feedback testing regime to test the model developed.

5. Model Building May Feel Like Modelling Through.
   As the model is an attempt to represent part of reality or an action taken or to increase understanding, the consideration remains that the model at some point becomes the best representation it can be and continued *'muddling'* with the model can be detrimental to assumptions based on the completed model.

These modelling guides adapted from Pidd's (1996) work illustrate some key points of reference that attempt to maintain consistency when developing, analysing, and

implementing models within the realm of modelling of critical infrastructure systems. This will assist the modeller in: (1) categorising and developing an understanding of the problem context for modelling: (2) deciding the model structure based on analysing the available data: (3) model realisation where the parameters of the model have been established; (4) the model assessment is the decision point at which the model is deemed acceptable, valid and usable as a model of the subject system and reflects normal functionality; and, (5) the model implementation where working with the model to gain valuable predictive data and likely responses to scenario testing.

7. Conclusion

The primary assertion of this research is that a model of a critical infrastructure system/s can provide a means to identifying and locating points of risk within the model and by extension the physical critical infrastructure system too.

This research into risk identification takes advantage of the benefits that modelling brings in establishing an overview of the subject system and its environment and presents a means of depicting a conceptual *'big picture'* view. Utilising this modelling approach lends itself to incorporation into the security analysis of critical infrastructure systems that would potentially lead to the development of a common perception and definition of risk and vulnerability, thereby narrowing the sematic gap of the identified risk/s across differing sectors of the wider critical infrastructure realm. The advantage of utilising modelling in this manner would encourage a consensus outcome of the level and exposure to the risk/s identified in the model and by association the physical critical infrastructure system itself.

Furthermore, modelling risk solutions back into the model enables further analysis and testing to determine the likely outcomes before physical implementation of the solution into the system itself. Additionally, the development of a critical infrastructure system model also provides the opportunity to apply various adverse scenarios and conditions to predict system responses to assist further in contingency plan development and testing to support the adoption of pre-emptive security measures into the physical system.

The successful enhancement of risk identification and risk perception understanding relies heavily on the comprehension and interpretation of the modelling process used to represent a particular critical infrastructure system. Therefore, the application of the general modelling guidelines outlined delivers a loose structure for the development of critical infrastructure models that will lessen the possibility of modelling and risk perception biases introduced by the modeller. Furthermore, the simple formula for quantifying risk in relation to its magnitude of hazard, the number of risks and value of the vulnerability was touched on briefly and delivers a means of prioritising risk. Additionally, this now provides a starting point for more in-depth future research into applying a value of magnitude to the risk/s and system vulnerabilities.

This paper seeks to delineate an area of future research that may prove fruitful after the initial critical infrastructure system modelling research matures. The intention is for future research to progress towards creating computer simulations of the critical infrastructure system/s modelled to further enhance the modelling, analysis process and understanding of system functionality and response. Once achieved, this will then enable analysts to closely replicate the physical system's response in a simulation and then test the system simulation with various adverse scenario tests to observe the simulated system's responses and reactions. Data and information gathered from this analysis process could then be analysed and applied to strengthen the physical critical infrastructure system's security and to mitigate risks as identified.

References

AGD Web Site (2004), "Critical Infrastructure Protection National Strategy", www.nationalsecurity.gov.au/, (Accessed 11 November 2004).

AGD Web Site (2004a), "Protecting Australia's Critical Infrastructure", www.ag.gov.au/, (Accessed 12 May 2005).

AusCERT (2004), Australian Computer Crime and Security Survey, AusCERT, Brisbane, Australia.

AusCERT (2005), Australian Computer Crime and Security Survey, AusCERT, Brisbane, Australia.

Gardner G.T. & Gould L.C. (1989), "Public Perceptions of the Risks and Benefits of Technology", *Risk Analysis*, Vol. 9, No. 2, pp. 225-242.

Geoscience Australia Web Site (2004), "What is risk?", www.ga.gov.au/urban/factsheets/risk_modelling.jsp, (Accessed 8 January 2007).

Maani K.E. & Cavana R.Y. (2000), *Systems Thinking and Modelling. Understanding Change and Complexity*, Prentice Hall, Auckland, NZ.

Pidd M. (1996), "Five Simple Principles of Modelling", in *Proceedings of the 1996 Winter Simulation Conference*, ACM, pp. 721-728.

Pye G. & Warren M.J. (2005), "Australian Commercial-Critical Infrastructure Management Protection", in *4th European Conference on Information Warfare and Security*, Academic Conference Limited (ACL), Wales, UK, pp. 249-259.

Pye G. & Warren M.J. (2006), "Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology", in *7th Australian Information Warfare and Security Conferenc*e, School of Computer and Information Science, Edith Cowan University, Perth, WA, pp.103-113.

Pye G. & Warren M.J. (2006a), "Security Management: Modelling Critical Infrastructure", J*ournal of Information Warfare*, Vol. 5, No. 1, pp. 46-61.

Scott G. (2005), "Protecting the Nation", *AUSGEO News*, No.79.

Sjöberg L. (2001), "Political decisions and public risk perception", *Reliability Engineering and System Safety*, Vol. 72, pp.115-123.

Standards Australia (2004), *Risk Management, AS/NZS 4360:2004*, Standards Australia/Standards New Zealand, Sydney/Wellington.

TISN Web Site (2004), "Critical Infrastructure Protection National Strategy", www.tisn.gov.au/, (Accessed 10 October 2004).

TISN Web Site (2004a), "Protection of the National Information Infrastructure (NII)", www.tisn.gov.au/, (Accessed 25 May 2005).