Analysis and Modelling of Critical Infrastructure Systems

Graeme Pye and Matthew Warren
Deakin University, Geelong, Australia
grae@deakin.edu.au
mwarren@deakin.edu.au

Abstract: The increasing complexity and interconnectedness of critical infrastructure systems, including the information systems and communication networks that support their existence and functionality, poses questions and challenges. Particularly, in terms of modelling and analysis of the security, survivability and ultimately reliability and continued availability of critical infrastructure systems and the services they deliver to modern society. The focus of this research enquiry is with regard to critiquing and modelling critical infrastructure systems. There are numerous systems analyse and modelling approaches that outline any number of differing methodological approaches, each with their own characteristics, expertise, strengths and weaknesses. The intention of this research is to investigate the merit of applying a ‘softer’ approach to critical infrastructure system security analysis and modelling that broadly views the systems in holistic terms, including their relationships with other systems. The intention is not to discuss or criticise existing research applying quantitative approaches, but to discuss a ‘softer’ system analysis and modelling approach in a security context that is adaptable to analysis modelling of critical infrastructure systems.

Keywords: critical infrastructure, security analysis, systems modelling

1. Introduction

The interactive nature and characteristics of critical infrastructure systems presents several theoretical and practical challenges to modelling, prediction, simulation and analysis of the causal behaviours and security factors both within and between mixes of differing system types. Furthermore, understanding the potential impacts of interdependency relationships as infrastructures evolve and change in operational regulations governing critical infrastructure systems is an important consideration (Brown et al 2004). The interactions and responses are neither universally applicable nor transferable between independent, single critical infrastructure systems or interconnected multiple system configurations. 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). These configurations and behaviours present significant challenges to the security analysis and modelling of critical infrastructure systems.

2. System analysis and modelling considerations

Systems generally consist of a collection of lower level elements or subsystems that work together in a cooperative manner toward the greater overarching goal of the system. Furthermore, the characteristics of systems vary considerably and are largely the result of the type of system, open or closed, and the external environment that interacts and influences system functionality generally. Additionally, the relationships and influences exerted between subsystems also have a part to play in comprehending the subject system’s functionality and responses to differing circumstances.

2.1 System modelling themes

In general terms, applying the system security analysis or system modelling approaches to represent an interpretive conceptualisation of a real-world system (Berntsen et al nd) provides a means of viewing the important aspects or essence of the system at various levels, depending on the particular system modelling theme.

For example, other common system modelling and analysis themes are as follows (Avison 2003a):

- A three-level view, where the conceptual level is a descriptive high-level overview of the system domain, the logical level describing the system goals and intention, while the physical level describes the system itself including the technologies involved.
- Process modelling theme describes the logical analysis of the processes within the system and is a discipline that applies a basic technique of functional decomposition, which breaks down a complex problem into smaller, more manageable detail.
- Data analysis theme involves comprehending and documenting the data elements and their relationships within the system.

194
Graeme Pye and Matthew Warren

- Object-orientated theme models objects that represent elements of the system including people, data, processes and the interaction of these objects.

These themes are each applicable to general system analysis or modelling in the terms of their specific characteristics of application, however there is no singular theme directly applicable for critiquing and modelling critical infrastructure systems.

2.2 Blending methodological approaches

As Avison (2003b) outlines, methodologies provide a set detailed rules and guidelines to follow and work to that deliver a highly structured design approach to the specific task they are to address. Therefore, in the logical extension lies in utilising a number of individual themes or approaches in combination, to bring together characteristics of each specific method to provide specific expertise to meet the overall practical criteria and intention of critiquing and modelling of critical infrastructure systems (Wood-Harper et al 1985).

Therefore, a blended methodological approach utilising multiple system analysis and system modelling approaches in combination would conceivably bring together the characteristics of each that is applicable to achieving the overall goal of critiquing and modelling critical infrastructure systems.

2.3 System analysis modelling

Other modelling approaches related to information system analysis that Dennis et al (2009) discusses are as follows:

- Functional modelling is a description of the processes and the interaction of the system with its environment.
- Structural modelling is a conceptual description of the structure of the data supporting the processes and presents the logical organisation of data without focussing on the technical details of how the data is stored, created or manipulated.
- Behavioural modelling describes the internal dynamic aspects of a system that support the processes by describing the internal logic of the processes without specifying the process implementation.

While these approaches may not necessarily be directly applicable to this research, in terms of critiquing and modelling critical infrastructure systems there are elements of these approaches that are complimentary to system analysis and the principles of system modelling.

The principle intention of system security analysis is to determine an intricate understanding of the focal systems to identify and monitor potential system vulnerabilities and develop solutions. An additional approach to enhance the insights gained from system analysis into the functional characteristics, security and structural features of systems is to develop a model of the subject system that conceptually represents the focal, real-world system of interest for further investigation.

3. Analysis and modelling: The challenges

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. According to McDonald and Bologna (2003), mathematical models of critical infrastructure systems are vague and there are no applicable methodologies for assessing and comprehending the intricacies of critical infrastructure systems. Add to this the effects of human interaction, from both the perspective of a susceptibility to instigate failure and adaptability to manage and recover wayward systems. This requires that modelling these networked critical infrastructure systems is not only about modelling the subject system itself, but incorporating consequential rationality of actual human thinking, responses and reactions, including the topology and dynamics of these large complex network systems (Macdonald & Bologna Ibid, Peters et al 2008).

Furthermore, 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;
Graeme Pye and Matthew Warren

- 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.

Add to this the fact that critical infrastructures can be intractable systems that are difficult to manage, operate and maintain with large, physical and geographically distributed systems that are highly diverse. Typically consisting of networked components or ‘systems within systems’ structures and various performance variations; there are few modelling mediums that can characterise these infrastructures as whole systems (Schulman & Roe 2007).

However, critical infrastructure analysis and modelling utilising simulation and optimisation-based techniques have played a significant part in examining potential interdiction impacts, recognising the insights they provide for mitigating facility loss and prioritising security strengthening efforts. Thus proposing that simulation as an optimisation technique, has generally proven valuable in the analysis of vulnerabilities in critical infrastructure networks, system simulations can enable the examination of a range of impacts, with either implicit or explicit notions of optimising performance (Murray & Grubesic 2007). Therefore, in the context of assessing system potentiality, reliability and vulnerability through monitoring the simulation models of networks as nodes or links that are compromised, enables corresponding changes in connectivity or performance to be documented.

A final important consideration for modelling critical infrastructure systems 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, Brown et al (2004) recognises that modelling is a first step in analysing, identifying and answering persistent questions about the potential of ‘real’ critical infrastructure system vulnerabilities.

For example, modelling critical infrastructure systems and the dependent and interdependent relationships or influences between infrastructures can deliver structural insight. Pederson et al (2006) provides a representation of differing infrastructures and their interdependent relationships and likely response connections based on a flooding event scenario that draws a parallel with Hurricane Katrina in New Orleans. In Figure 1 the individual infrastructure networks are represented on a single plane and the parallel lines within each plane represent sectors and sub sectors within that particular infrastructure. The spheres or nodes represent key infrastructure components within that sector; for instance, the energy sector contains electricity generation and distribution and natural gas production and distribution. Dependencies can exist within each infrastructure and between differing internal sectors. The solid lines crossing sectors within a specific infrastructure represent internal dependencies and the broken lines between different infrastructures represent dependencies that can also exist between different infrastructures or infrastructure interdependencies.

Figure 1 illustrates where the dependencies and interdependencies exist within the greater infrastructure system and highlights where dependency relationships exist and the inherent and potential complexity these relationships bring to infrastructures. Additionally, a model of this nature enables those attempting to manage the chaotic environments of disasters and emergency response during catastrophic events to gain a clear appreciation for where these relationships exist both within and between critical infrastructure systems. Understanding this is important for emergency response decision-makers and agencies responsible for recovery, rescue and restoration purposes because a failure to understand these dynamics would result in poor coordination and an ineffective response. Thereby, resulting in the mismanagement of resources, including supplies, rescue personnel and security teams that may generate a loss of public confidence or trust and at worst, loss of human life (Brown et al 2004, Pederson et al 2006).

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 such as telecommunications and electricity grids, this immediacy of resource consumption can lead to potentially instantaneous cascading failures that impact across interdependent critical infrastructure systems. Alternatively, other infrastructures that exhibit buffering characteristics similar to fuel and gas production and distribution infrastructures that supply physical resources have a level of reserve within these systems where any failure would not necessarily be instantaneous in its effect, but the effects would exacerbate over time (Svendsen & Wolthusen 2007). These differences in scenario circumstances and the characteristics of the critical infrastructure systems involved would by necessity require careful consideration in a modelling context. Particularly, when seeking to identify, predict and even quantify the effects of cascading incidents among interdependent infrastructure systems. This would add informative value with regard to developing public policies that aim to address critical infrastructure vulnerabilities and especially those that relate to critical infrastructure system security (Zimmerman & Restrepo 2006).

![Diagram of infrastructure interdependencies](image)

**Figure 1:** Infrastructure interdependencies (Pederson et al 2006)

As an alternative approach, Little (2003) suggests that applying analysis and modelling techniques to historical critical infrastructure incidents and events would enable incremental improvements in prediction, forecasting and preparedness for future events and allows the instigation of new engineering approaches to design and construction. Thus, enabling critical infrastructure systems to become more robust and better able to withstand and cope with 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, community expansion plans. This would reduce costs, enhance critical system redundancy, improve traffic flow, secure data and information protection and better prepare for and respond 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 subject critical infrastructure systems' relevant environment.
4. Critical infrastructure system modelling considerations

In briefly discussing and identifying the generic characteristics of Australian critical infrastructure systems, the following outlines the specific modelling considerations required for representational modelling of critical infrastructure systems, circumstances and their attributes (Pye & Warren 2008):

- Systematic scoping perspective of the system to be modelled or part thereof and granularity detail of hierarchical levels within the subject system;
- Identifying system criticalness and points of criticalness with the subject system;
- Systems are generally transitional (services move from source to destination);
- Systems are distributed in character;
- Systems operate autonomously or semi-autonomous (typically no central control for cooperating subsystems);
- Deadlocking issues (transport, communication);
- System scalability (systems made up of subsystems) and complexity;
- Network connected systems (stand-alone) systems and the relationships (dependency and interdependency);
- Operational factors and environmental influences (internal and external);
- System redundancy and backup systems;
- Control and communication (critical pathways, internet);
- Time (temporal) scale dynamics within and around systems;
- Depict 'cause and effect' and possible dynamic changes within system/s; and
- System concurrency issues.

The ability to model these systems (incorporating the considerations above) in a relevant context is important to assessing system security, understanding functionality and dynamic behaviours in order to develop strategies that address and maintain the continuity of service. This in part relies upon identifying and protecting key points of infrastructure system concentration, pinch or choke points and remote exposures in order to maintain high-levels of service assurance, continuity, system availability and short system restoration times.

5. System modelling principles

The overarching principle applied to system 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 the system model must remain representative of the system to enable security points within the system to become visible. To achieve this and 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 (Pye & Warren 2007).

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 system models, as follows (ibid):

- 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 conceptual 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 system model.
- 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 becomes necessary. However this does require continued refinement and revision to avoid adding unnecessary complexity to the model.
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 by decomposition of the system into manageable component parts that apply the previous principle to develop the system model.

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.

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 to (Pye & Warren 2007):

- Categorise and develop an understanding of the problem context for modelling;
- Decide on the model structure based on analysing the available data;
- Determine model realisation of where the parameters of the model have been established;
- Identify a model assessment as the point at which the model is deemed acceptable, valid and usable as a system model that reflects normal functionality; and
- Apply model implementation, by utilising the model to gain valuable predictive data and likely system scenario responses.

These system modelling principles offer common sense guidelines that are applicable to modelling critical infrastructure systems and dealing with the complexities of the characteristics incumbent of critical infrastructure systems.

6. Conceptual system modelling objectives

Furthermore in conceptually modelling critical infrastructure systems, there are system modelling objectives that provide deliverable insights into critical infrastructure systems through their modelling. This should strive to deliver from the perspective of system functionality, security characteristics and dynamic behaviour, but not limited to the following (CIPMA 2007):

- Identify system scope, interconnections between systems both within and across critical infrastructure sectors incorporating levels of scale and future system scalability;
- Deliver insights into the system behaviours and responses of complex networks and their communication, control and service provision dynamics;
- Identify and analyse the extent and influential magnitude of relationships between cooperating systems, particularly from the aspect of dependency and interdependency relationships;
- Observe through applied modelling, normal system functionality and predict the potential flow-on effects of critical infrastructure system failure and likely cascading impacts;
- Identify potential system choke points, single points of failure and other likely security vulnerabilities;
- Model assessments of potential security measures for systems prior to their physical implementation;
- Apply risk and security mitigation strategies to test and evaluate the beneficial or otherwise outcomes for continuity planning and development; and
- Models must be conceptually representative of the physically distributed nature and functionality characteristics of the subject infrastructure systems.

Understanding and appreciating the characteristics and idiosyncrasies of critical infrastructure systems and the specific considerations are the foundations upon which the conceptual modelling of these systems can deliver the modelling objectives as listed previously. The modelling of such systems demands of the modeller an intimate understanding and appreciation of the complexities of subject systems, to deliver a representative and well-scoped model, for without the knowledge gleaned from analysing system models, any subsequent critical infrastructure system model produced cannot be a representative model.
Graeme Pye and Matthew Warren

7. Australia's critical infrastructure: Discussion and context

Critical infrastructure systems are vitally important to the economy and the community. Particularly with the proliferation of telecommunication and information infrastructures, it is apparent the profound influence those critical infrastructures and the services they deliver to all levels, structures and functionality of the economy and society. As history has shown, infrastructure innovation has boosted economic growth, contributed to improved public health, changed the mobility of society and improved information networks and brought comfort to the community.

In many aspects, present-day critical infrastructures were laid out to service the development of an industrial economy and to an extent seemed inadequate and ill-prepared as the backbone of the new modern economic structure relating to information and knowledge-based services. The service-based economy expects highly reliable, flexible and quality services rather than cheap utilities and commodity-based services. There is continuing public consternation with the performance of some critical infrastructures particularly where users have tailor-made quality-of-service and service-on-demand expectations that have been plagued with problems of road congestion, power outages, stressed public transport systems, viruses and denial of service attacks on the internet.

It seems that many of the traditional critical infrastructures were slow in adapting to societal demands. This is in part due to the deep 'embeddedness' in spatial and economic structure including the large, long-term capital investment in the physical basis of critical infrastructure systems, which remain barriers to the adoption of timely innovations and their adaptation to changing requirements of users and system security and service availability requirements. However, in contrast to the resistance of physical infrastructures to change, profound and ongoing change has been unleashed in the Australian context with public ownership, organisation and market structure of critical infrastructure sectors resulting from de-regulation and privatisation of critical infrastructure systems. Additionally, the convergence of markets and the contraction of ownership into multi-utility organisations will greatly increase the complexity of infrastructure industries and the regulation of infrastructure bound markets.

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 situation is the increasing interconnectedness between infrastructures via the information communication technologies that are increasingly pervading 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 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 have to take into account their interactions and connections with other critical and non-critical infrastructure systems, particularly in terms of capacity allocation, service provision, system availability planning and security as a function of changing economic and regulatory conditions. Furthermore, 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 and comprehending the design, operation, management and ultimately the security of any critical infrastructure system, it is important to be able to conceptualise the system goals, performance at differing levels of the greater system structure and the behavioural aspects of subsystems. Structurally, critical infrastructures are large integrated systems, which are comprised of subsystems linked together into a network organised system. The result is a 'cause and effect' influenced system with integrated subsystems and interfaces enabling interactive effects. Particularly where an interface represents: the contact area between one system and another system element; or the system and the human; or its environment. For example, such interactions across an interface may relate to energy and material flows, information exchanges, personal communications, and propagation of cause and effect influences, operational decisions and control manipulations.
8. Conclusion

As Bentley (2006) intimates, critical infrastructure systems tend to be interdependent and even interconnected and systems failure – be it through natural disaster, terrorism or poor management – can bring entire communities and their industries and utilities to a grinding halt. Therefore, the ability to analyse and critique the security aspects of critical infrastructure systems, together with modelling these systems offers an avenue for assessing critical infrastructure system security, identifying vulnerabilities and locating inherent weaknesses, so appropriate solutions and remedial action can be implemented to mitigate such security risks to system availability and service supply. To address this directly and return to the focus of this research with regard to how to critique and model critical infrastructure systems, the previous system analyse and modelling descriptions have outlined a number of differing methodological approaches and their characteristics. Additionally, descriptions of a number of potential system modelling approaches applicable in a security context were characterised and are potentially both adaptable and suitable to modelling critical infrastructure systems. While each system security analysis approach and system modelling approach reviewed is capable on their own terms, they remain limited and narrow in focus for analysis and modelling of critical infrastructure systems. Therefore, it is proposed that a possible solution to critique and model critical infrastructure systems may lay in the development of a generic multifaceted or blended methodology that outlines the adoption of multiple system analysis and modelling approaches. This would represent a hybrid methodology that in turn would form the basis for combining multiple approaches as a single multifaceted practical framework application for security analysis and modelling of a critical infrastructure system.

References