This is the published version:


Available from Deakin Research Online:

http://hdl.handle.net/10536/DRO/DU:30007036

Reproduced with the kind permissions of the copyright owner.

Copyright : 2007, Mindsystems Pty. Ltd.
Modelling Critical Infrastructure Systems

G. Pye and M. J. Warren
School of Information Systems
Deakin University, Australia,
Email: graeme@deakin.edu.au
Email: mwarren@deakin.edu.au

Abstract
This paper examines the basis of what constitutes a system/s and discusses the commonalities in relation to critical infrastructure system. It focuses on identifying, and discussing system characteristics, complexity, inter-relationships, dynamics and the importance of modelling as applied to critical infrastructure systems. It then considers four differing system-modelling styles with the view to assess and discuss their potential to model critical infrastructure systems, ahead of selecting the most promising and suitable for adoption to critical infrastructure system modelling.

Keywords: Critical infrastructure, dependency, system and modelling.

Introduction
The properties of critical infrastructure systems display the characteristics of highly structured, complex and interconnected networks that also have the added issues of dependency and interdependency relationships, which by necessity exist between infrastructure systems to facilitate the supply of services. This is particularly prevalent when considering the energy sector, where the continuity of the supply of electricity for example, is crucial to many other sectors of critical infrastructure and their systems, for the ongoing provision of services to the community at large (Scott, 2005).

Critical infrastructure systems are vulnerable and can be damaged, destroyed or disrupted by breakdowns, negligence, natural disasters, accidents, cyber incidents, illegal criminal activity, malicious damage or as the target of both conventional and information warfare to name a few. For these reasons and others, the continuity of supply requires protection against such hazards, threats, vulnerabilities and risks. Therefore the aim of government policy and, by association, that of infrastructure owners and operators, is to ensure continued supply availability through identifying and implementing improved protective safeguards and security analysis in response to the risks and threats posed (Scott, 2005).

The premise of this research is that as part of the wider security analysis process of critical infrastructure systems that part of this process should encourage the analyst to model such systems as a means to determine and identify system vulnerabilities. It is possible that such initial modelling of the system from a number of scalable levels within the infrastructure will not only enable the modelling of normal operations, but also enable the modelling of prognosticative outcomes resulting from deviations to normal function, whether they are internally or externally sourced influences or a combination thereof.
This paper begins with focusing on establishing the characteristics of what a system is essentially and discusses systems thinking and dynamics before proceeding to identify the characteristics of critical infrastructure systems. The next aspect focuses on the rationale behind the modelling of such systems and the issues surrounding the modelling of critical infrastructure systems, together with identifying the functional and relational dynamics at play both internally and externally to the system/s in general. Finally, a brief assessment of the potential value offered by various security system modelling and simulation development products will determine which modelling style is potentially adaptable to modelling critical infrastructure systems for further research.

What is a System?
What constitutes a system evokes different meanings, perceptions and conceptual visualisations to different individuals depending on their interpretation of the focal structure. This construct is generally derived from its functional characteristics, physical structure, its response behaviours and incorporates its inferred complexity of components that interact together to form a single functional system representation. Yet systems exist in numerous forms from the biological, ecological, social, to the mechanical and through to natural systems such as the solar system for example. In simple terms, systems exist to perform routine functions and are comprised of sub-systems, for instance a job can consist of a number of sub-systems relating particularly to human, economic, technical, legal and social systems that can act individually, be influential upon or interact with each other (Maani & Cavana, 2000).

In seeking an understanding of what commonalities are indicative of a system, it can be generally characterised that a system is a collection of smaller parts that cooperate with one another to function as a whole. However, a system is not only just the sum of its parts, but it is also a representation of its surrounding interactions, behaviours, influences and relationships with other systems, whereby a system can associate its own parts to itself and become a contributing part of an even larger system (Maani & Cavana, 2000).

The presence of some or all of these features will indicate the presence of a system, but to be able to develop a deeper understanding requires further investigation and analysis of the system itself. Therefore, to appreciate the complexity of how the internal sub-systems and their parts all interact and function collectively as a whole, requires the analyst to apply the paradigm of ‘systems’ thinking’ to develop an ability to comprehend the system as a whole, consisting of many parts, and its position within the wider system environment.

Systems’ Thinking
Systems’ thinking is a discipline dedicated to understanding the complexity that is intrinsic within all systems, irrespective of their size, nature, composition or influence exhibited upon the system. This is regardless of whether the system is located internally to a system or externally by association with other systems. As a paradigm, systems’ thinking is about describing the dynamics of relationships between the lessor parts within system and by extension the dynamics of relationships with other associated or neighbouring systems.

Therefore, systems’ thinking requires the investigator or analyst to look at the dynamics of the system by considering it from the following three perspectives (Maani & Cavana, 2000):
- Dynamic thinking is appreciating that the world is not static and that things are changing constantly;
- Operational thinking is the cognitive condition of understanding the physics of operations and how things really work;
- Closed-loop thinking is recognising that cause and effect are not always linear and that the end (effect) can influence the means (cause).

This is not as easy as it may first appear when considering the implications of larger systems interacting with other large systems and that each in themselves contain numerous sub-systems all interacting within the boundaries of their own system. Additionally, this complexity exacerbates further when considering the influential relationships that can potentially exist between large systems as well as within the sub-systems making up these larger systems too. All this information is at best difficult for humans to comprehend and process in relatively small and simple systems, let alone when contemplating large, complex, multiple systems and their functional behaviour.

To address this issue the application of systems modelling techniques delivers an ability to represent the system from an overview perspective that enables scalable modelling of the system’s components and its internal structures through to the greater external system environment in which the system resides and functions.

**Systems Modelling**

To analyse and comprehend the magnitude, functional behaviour, influence and physical structure of any system, at any level of scale, it is beneficial to our ultimate comprehension to model it. Modelling enables the analyst to depict and scope the system of interest in such a fashion as to enable the analyst to gain a high-level and expansive view of the system. By modelling the system, we can develop an appreciation of the structure of the system itself and the interconnection between its internal elements or components. In addition, modelling also delivers potentially powerful insights into the relational influences of neighbouring or associated systems that can affect the system and how localised change can affect the whole system including the resources that the system provides to or utilises from other systems. In achieving a model reflective of a system understanding and functionality as such, then it should enable model manipulation to an extent where it becomes possible to predict and measure possible system behaviour in response to the manipulation based on attempts to imitate the precursor influences that lead to eventual system change (Maani & Cavana, 2000).

In considering the modelling of the system from this perspective as such, is essentially modelling a system that exhibits change and thereby the influence of ‘cause and effect’. This requires applied system thinking in relation to and consideration of, modelling the dynamic characteristics inherent within the system or external to the system, where a cause (system influence) has a potentially different effect each time on the means of how the system responds, changes or reacts. Hence, in this context, the overriding characteristic is that the system is not behaviourally constant in necessarily reproducing the same repeatable result or outcome, but dynamic in the sense that the result can be infinitely variable and therefore modelled with this consideration in mind.

Similarly, critical infrastructure systems also exhibit the aforementioned dynamic behaviour and characteristics of multiple variables that can potentially coerce differing outcomes and system responses. Therefore, the modelling of such systems requires that particular
consideration to the type of modelling method employed, must by necessity, represent the dynamics characterised by the system. Such modelling methods must be capable of precise application to represent authentically a theoretical account that is truly representative of the dynamic characteristics inherent in the physical critical infrastructure system at that time and its subsequent behavioural responses.

Modelling Systems Dynamics
While modelling gives us the ‘big picture’ representation of the system, the modelling of systems that exhibit dynamic behaviour requires the careful consideration of a number of issues. For instance, a dynamic system is adaptable and its parts are interrelated in such a manner that a change in part of the system, by consequence affects other parts of the system and therefore the overall system and its performance. Furthermore, not only can the system be functionality influenced by internal changes, it is also susceptible to influence from external changes in environmental factors surrounding the system or from other existing systems, via feedback.

Feedback and System Dynamics
This premise of system dynamics reflects the description provided by the System Dynamics Society (2006) that describes the term ‘system dynamics’ as a method of studying and modelling complex response systems that are apparent in any sort of feedback-equipped system. Feedback is the situation where via a chain of ‘cause and effect’, A influences B, which in-turn influences A and therefore the study of the link A and B cannot be undertaken independently, as it is the link between A and B that predicts how the system will behave. With this in mind, only the study of the whole system as a feedback system will lead to the appropriate systematic conclusions for modelling purposes.

Therefore, to construct a useful interpretation or model of a dynamic system as described requires an analysis of the system to develop a useful understanding of the system situation through elaboration, exploitation and interpretation of a simulation model, which is heavily reliant on the mental interpretation of the developer. Here a useful interpretation refers to a given understanding of the system situation at a given moment together with the perceived mental structure of the whole system (Schaffernicht, 2006).

It is the interpretation of these system characteristics and modelling issues that when applied to critical infrastructure systems reflect the similarities of system constructs, components and dynamic behavioural characteristics of critical infrastructure systems.

Critical Infrastructure System Characteristics
According to Australia’s national strategy, critical infrastructure is defined as “those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, 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, 2004a, p1).

Moreover, by its very structure critical infrastructure systems are interconnected and networked together as necessary for the supply and demand of services to and from each other
and consumers in varying degrees. It is this structural inter-relationship between critical infrastructure systems and the internal components within them, which characterises critical infrastructure as a dynamic system made up of smaller independent or reliant systems. Therefore, critical infrastructure systems can be further characterised, as dynamic systems because they are highly reliant on each other, susceptible to influence and interrelated by necessity to function together in a cooperative and dynamic manner so that the system can remain adaptable to function and supply the services as normally expected (Pye & Warren, 2006b).

Another intrinsic characteristic of critical infrastructure systems is the ‘unboundedness’ of the component systems that are interrelated or networked together to form a larger functioning system. This is characterised by the distributed nature of local system administrative control that exists without any central governing authority. An unbounded environment cannot be partitioned into a number of finite bounded environments because of the lack of global perspective given to the associated cooperating systems beyond the boundary of their local system, consequently there is a lack of the ‘big picture’ information represented locally, in regard to feedback from the system as a whole (Ellison et al., 1999).

From this we can draw the inference that indeed critical infrastructure systems do display similar characteristics to that of dynamic systems because they consist of multiple variables with dynamically changing values, dependency relationships existing between and within interrelated infrastructure systems and they exhibit network connection characteristics that are subject to both internal or external change and influences. This necessitates that in the national interest critical infrastructure systems do need to be modelled as part of the overall security analysis process to assess, identify and determine points of weakness or areas of vulnerability.

The modelling of critical infrastructure systems offers an alternative and possibly cost effective and timely way to manage the security analysis process by reducing the task to a manageable size. Particularly, when considering the sheer size and magnitude of these systems, modelling presents a means of collating data and undertaking security system analysis to derive security solutions, test and further analyse the refined models prior to implementation into the physical critical infrastructure system.

**Why Critical Infrastructure Modelling is Important**

From a systems dynamics perspective there is strong logic that offers potential improvements in the analysis, security, functional understanding and strategic management perspectives of critical infrastructure systems, along with insights into understanding variations in system performance (Warren, 2005). Since performance is an indicator of the state of resources or service provision, strategies can be developed and tested through system modelling to enhance policy development and review physical implementation prior to taking security decisions that physically address performance variation and deviations from normal functionality in the face of unexpected challenges.

Therefore, by further extending modelling in this manner it is quite feasible to develop adverse scenarios that could be applied to critical infrastructure system models, thereby representing security threats and vulnerabilities that can impinge upon the system. This would enable analysts to predict the resultant system response/s and its potential affect on the following (AGD, 2004b):
• Business continuity;
• Incident and consequence management;
• Information system attacks and vulnerabilities;
• Electronic crime;
• Protection of key sites from attack or sabotage;
• Chemical, biological and radiological threats to water and food supplies;
• Accident management;
• Cyber incidents.

These are just a few possible scenarios that will possibly be developed for testing on models of critical infrastructure systems once the modelling method that is deemed appropriate has been chosen for the focus of ongoing research. Thus enabling the potential scalable modelling of critical infrastructure systems such as (DPMC, 2004):

• Communication networks;
• Banking;
• Energy;
• Water and food supplies;
• Health services;
• Emergency services;
• Transport networks.

Fundamentally, this provides the opportunity to model adverse situations as applied to the critical infrastructure systems, without necessarily testing this same adverse scenario situation in the physical realm of the infrastructure itself.

This will inevitably assist those confronted with undertaking and exercising control over the security of critical infrastructures systems to better manage and cope with unexpected decisions. Jensen and Brehmer (2003) describe these as ‘dynamic decision issues’ that characterise a series of related decisions where invariably the system’s situation will change both in itself and in the response to the actions taken. Therefore, the modelling and analysis of the security dynamics at play within the system not only enables observation of the normal functionality, but also the functionality of an adverse change and its effect upon the critical infrastructure system. Thus to a degree removing the element of surprise, for without this prior knowledge owners and operators of critical infrastructure systems will remain severely handicapped and ill prepared for whatever may potentially eventuate (Warren, 2005).

**Modelling Critical Infrastructure Systems**

The effective modelling of critical infrastructure systems would enable both the government and critical infrastructure owners, operators and customers to analyse, identify and effectively manage and maintain the security, stability and availability of their particular critical infrastructure through the development of solutions and contingencies against unexpected challenges to the system’s stability (Pye & Warren, 2006a).

To this end, the authors briefly examine four different modelling methods and their potential to address the primary issues of effectively representing the modelling of critical infrastructure systems, to represent the existing physical properties of the infrastructure system within the modelling scope. Also with a view of incorporating its dependency
relationships to other associated infrastructures, within the boundaries set by the model developer and whether such modelling techniques as applied, justifiably represent the dynamics of the system being modelled and if it is applicable, adaptable or transferable to critical infrastructure modelling.

The EASEL Way

EASEL (Emergent Algorithm Simulation Environment and Language) is a beta version software program designed for the ‘simulating, depicting, and gathering information about networks, software agents, and other active entities of the physical, electronic and software worlds, about their interactions, and about their collective global effects’ (Fisher, 1999, p1) of the real-world systems upon which the EASEL simulation is modelled.

EASEL is a script language that utilises property-based types to define the various entities (actors) that can be created by the language and its strength lays in its capability to depict and model, unbounded systems to simulate the complex interactions that take place between the various types of entities within the system (Redman et al, 2005). The software package remains freely available online for download from the Software Engineering Institute at Carnegie Mellon, but current support and development of the EASEL software itself seems to have lapsed (SEI, 2006).

Redman’s (2003) research into system survivability noted that the use of EASEL as a simulation development tool had some performance limitations that impinged upon the design and development of this network survivability, simulation research project. Principally the software was only available for the Apple Macintosh operating system platform and because the software was still in the ‘beta’ development, there was a lack of resources to support the developer or instructions to aid simulation production using the EASEL software. Therefore, the simulation development was a time consuming process due to ‘trial and error’ development method employed, the lack of support and the taxing resource load imposed by EASEL on the operating system, this made testing and running of the simulations difficult due to the resource demand and program instability. Likewise, Marasea’s (2003) research utilised EASEL to develop a simulation model representing an attack upon a critical infrastructure system, here again Marasea (2003) noted similar design, development, support and operational issues that impinged upon this research project too.

EASEL is not particularly conducive to rapid model development or systems analysis of dynamic and unbounded systems modelled utilising the EASEL environment. This is due largely to the long development lead-time necessary to develop a functional simulation, the essentially non-existent user support for EASEL development and the issue of heavy computer resource use. Even in the review of these previously functioning simulations, there still a major issue that more often than not led to the computer devoting 100% resources to running the EASEL software, to the extent that the simulation program cannot load and run therefore making analysis of the simulation impractical.

EASEL presents one alternative to the question of modelling critical infrastructure systems however, the time consuming model development process and the lack of ongoing development of the EASEL software package itself, has now ceased (SEI, 2006). This indicates that there is a need to model critical infrastructure systems quickly so that important analysis of the system can be undertaken to identify normal operation, vulnerabilities and the effect of adverse incidents upon normal system functionality.
Stock and Flow Diagrams

A form of dynamic system modelling that is growing in popularity within business particularly, is the Stock and Flow diagram whose notation consists of three of three different types of elements, namely, stocks, flows and information. The three elements together in a diagram graphically represent any dynamic process that may be apparent in any business and therefore can be utilised to represent the characteristics of such processes and illustrates the relationship among variables that have the potential to change over time (Kirkwood, 2005).

Figure 1 illustrates an example of a very simple stock and flow diagram with the three elements Casual Staff, sales and Permanent Staff and models the structure of the business process concerning the rate at which Casual Staff numbers reduce to zero, as the numbers of Permanent Staff required, is dictated by the flow of sales.

![Figure 1: Stock and Flow Diagram.](image)

The two different types of variables illustrated inside the rectangles are variables called a stock, level or accumulation. The variable sales is shown next to the ‘butterfly valve’ or ‘bow tie’ symbol and this type of variable is known as a flow or rate, thus the two lines through the butterfly valve looks like a pipe with the valve controlling the flow. The premise of Figure 1 is that this represents the flow of Casual Staff towards Permanent Staff with the rate of flow controlled by the sales valve; this is the key idea behind the difference between stock and flow. Therefore, a stock represents an accumulation of something and a flow is the movement of something from one stock to another (Kirkwood, 2005).

The final element of the Figure 1 diagram is the information link represented as a curved arrow and this notation represents that the value of Casual Staff influencing the value of sales. Additionally, and of equal importance is the lack of an information arrow from Permanent Staff to sales, which illustrates that information regarding the value of Permanent Staff has no influence over the value of sales (Kirkwood, 2005).

Hence, the purpose of the stock and flow diagram is to depict the process changes and how the elements and the structure of the process interact together to bring about change. This form of modelling focuses on the elements that make up the process (sometimes likened to the components of the system) and how the performance of the process changes over time and forms the basis of studying the dynamics of a simple process using stock and flow diagrams.

The underlying weakness of stock and flow diagrams is that they can only deliver a simplistic representation within a defined process boundary of a simple process. Unfortunately, from the perspective of modelling critical infrastructure systems stock and flow diagrams are not readily applicable to this type of system modelling due to the size and complexity of the systems. The other important issue is the scalability potential of stock and flow diagrams in regard to these systems as they tend to become difficult to interpret due to
the diagrams added complexity in depicting the logical interconnection, processes and dependency relationships of critical infrastructure systems. It appears that stock and flow diagrams are better suited to modelling less complex system processes with clearly defined boundaries and is not necessarily well suited to modelling multiple interconnected and large complex critical infrastructure systems from a security analysis perspective.

**Viable Systems Modelling**

The Viable System Model (VSM) represents a framework for managing the security of large multi-level organisational information systems as a means of detecting, checking and identifying threats and vulnerabilities as they appear. VSM utilises local sub-system monitoring that can distinguish between threatening and non-threatening behaviours and adjusts the whole system as a consequence (Hutchinson & Warren, 2002).

From the research perspective of Hutchinson and Warren (2002), VSM provides a framework to manage the security and normal function of organisational information systems that are cooperating as a larger overall information system, to deliver ongoing system security that takes into consideration all levels within the greater system.

The disruption or destruction of information systems can cause serious loss of service to customers and increasingly information systems are under threat from both internal and external sources and there is a need to establish a robust and dynamic response to protect information assets (Gokhale & Banks, 2004). In view of the structure of critical infrastructures and their reliance upon information systems, there is obviously a need to establish ways to protect such systems and VSM may offer benefits for this perspective.

However, from the aspect of modelling the activity of a critical infrastructure system with a view to analysing the critical infrastructure system as a whole, its internal system components and the dependency relationships between critical infrastructure systems, VSM may not be applicable due to the sheer scope, size and diversity of function. Therefore, while it may be applicable at the organisational level, the magnitude and scale necessary for modelling critical infrastructure systems across the state or national level would be well beyond VSM’s capabilities and difficult for an analyst to implement and manage with any ongoing effectiveness at this scale. VSM remains useful as a framework for organisations, but is simply not adaptable to critical infrastructure system modelling.

**Coloured Petri Nets**

Jensen (1998) indicates that CPN’s as a modelling language, is theoretically well founded and adaptable for application to systems of the size and complexity that characterise typical industrial projects, which is not unlike the characteristics inherent in critical infrastructure systems. Coloured Petri Nets (CPN) offer a systematic method of modelling highly interconnected, cooperating networked systems in a scalable manner that depicts diverse function and their logical interconnection based on the physical representation of the critical infrastructure systems modelled.

Furthermore, the CPN model enables an analysis of the physical and operational structure of the critical infrastructure system to be analytically scrutinised by means of simulations and state spaces that incorporate time. Thus lending the use of CPN’s to performance evaluation
to evaluate how fast the system functions. Additionally, it is a relatively simple task to
develop a computer simulation representation of the critical infrastructure system from the
initial model. Therefore, a CPN model can potentially represent the normal functionality of
the system and the normal functional relationships between cooperating critical infrastructure
systems. From this perspective, the CPN notation would represent the following within the
model (Jensen, 1998):

- Place - represents a particular infrastructure;
- Transition – is the exchange of services between cooperating infrastructures;
- Token – has a value, but must exist at the input place to enable the transition to fire;
- Arcs – represent the connections between infrastructures.

When a critical infrastructure system model is developed that satisfactorily reflects normal
functionality, it seems a relatively easy and quick task to redevelop another CPN model to
indicate, incorporate and represent a potential threat to the system to deduce a possible system
response observation. Thus, the central focus of this system modelling research is to predict
and map the potential security impact upon the critical infrastructure system/s modelled and
the associated critical infrastructures via their dependency relationships. From this viewpoint,
it is possible to identify the probable outcomes of threats and vulnerabilities and potential
solution scenarios responses. In this way, it enables the testing of proposed security solutions
within the modelling environment on the system, before potentially progressing towards
actual implementation in the physical critical infrastructure system itself.

CPN modelling offers an interesting approach to modelling critical infrastructure systems that
requires deeper investigation, as it takes into consideration the dynamic nature of the systems
involved, the dependency relationships that exist between cooperating infrastructure systems
as well as mapping service delivery or failure within the critical infrastructure system model
too.

**Modelling Assessment Overview**

Of the four modelling styles discussed, they all address the modelling issues in some part
from their own specialised perspective and are all potentially beneficial and capable for the
analysis of system security issues relating to critical infrastructure systems, however there is
no single perfect solution. What is required is to choose the modelling method that is
adaptable and potentially delivers the ‘best fit’ modelling capability to enable the effective
modelling of critical infrastructure systems. It must take into consideration, system scalability
and scope, interdependency relationships, incorporate systems dynamics, and enable rapid
model development for security scenario testing, analysis and security solution development.

While, EASEL was specifically designed to model unbounded and dynamic systems it was
found that the simulation software was unstable and computer processor greedy, operating
system specific (Apple only), still in the software development stage although this has now
cesed, along with negligible user support. Indeed the overriding issue was the extended
design and development lead-time needed to develop a model simulation that means the
timeframe required to develop and model security solutions quickly makes EASEL
impractical for this task.
Stock and flow diagrams are currently very popular within the field of modelling dynamic systems and processes in business and they lend themselves to rapid model development. Unfortunately, from a critical infrastructure modelling aspect, stock and flow diagrams are not very scalable as the diagrams do become unsuitably complex to be of any real value when dealing with the relationships between multiple processes within a system or representing external system influences. While there is a need to understand the modelling notation used, it does not necessarily translate well to the non-professional perspective concerning an appreciation of the system being modelled. Additionally, the modelling methodology itself seems more appropriate to modelling smaller, less complex and isolated processes that represent system dynamics.

VSM represents system modelling from the information security management perspective of an organisation, which by it very nature requires close and trusting cooperation between the infrastructures exchanging services and VSM displays a highly level of complexity that impacts upon the security management coordination required. Unfortunately, the VSM security management framework is not a modelling tool applicable to modelling the systems for security analysis from the critical infrastructure system perspective, although it would have a part to play in the management of security within the organisation supporting the critical infrastructure owners and operators.

Finally, CPN’s offer a potential modelling instrument that is network centric, scalable, which resembles the logical structure and physical representation of critical infrastructure systems and is very quick and easily to develop. It also has the added benefit that enables the building of a computer-generated simulation based directly off the initial model, depending on what modelling package used. Much of CPN modelling research literature currently relates to process modelling because CPN modelling enables rapid model development and computer simulation development in very short timeframes. This feature would greatly assist in developing and testing security solutions that are also easy to manipulate and change if modelled utilising CPN’s.

**Conclusion**

This research has led to identifying the system characteristics and properties inherent in critical infrastructure systems and investigated the issues incumbent in modelling systems generally, and those of critical infrastructure systems. Several commonalities regarding system analysis, systems thinking, and system modelling are also consistent and applicable to critical infrastructure systems from a systems modelling development perspective.

Additionally, the importance of modelling critical infrastructure systems provides a process whereby normal functionality of a particular critical infrastructure or associated dependent critical infrastructure systems offers opportunities for the identification of threats, vulnerabilities and risks. Furthermore, this also presents the opportunity to model potential security solutions for analysis and assessment prior to the physical implementation.

This investigation also represents an initial comparison of modelling methods that have been previously applied to analysis and simulation of unbounded networks (Easel), organisational security (VSM), system dynamics modelling (Stock and Flow Diagrams) and network analysis (CPN) and their potential application to modelling critical infrastructure systems.
As critical infrastructure systems were found to be highly networked, complex, and dynamic in nature and subject to the influence of dependency relationships, it appears that CPN’s offer the best possibilities for addressing the modelling of critical infrastructure systems for security analysis purposes. Although, further stepwise research will continue to more deeply assess the capability of applying CPN’s to the task of the effective modelling and computer simulation development of physical critical infrastructure systems. This research now forms the foundation for the next step in the ongoing research investigation into the application of CPN’s to modelling scaleable of critical infrastructure systems and their associated internal and external system network connections and relationships.

References


