2007

Critical Infrastructure Systems Modelling: Benchmarking CPNTools

Graeme Pye
Deakin University,

Matthew J. Warren
Deakin University,

DOI: 10.4225/75/57a83951befa8
Originally published in the proceedings of the 8th Australian Information Warfare and Security Conference, Edith Cowan University, perth Western Australia, 3rd-4th December, 2007

Critical Infrastructure Systems Modelling: Benchmarking CPNTools

Graeme Pye and Matthew J. Warren
School of Information Systems,
Faculty of Business and Law,
Deakin University,
Geelong, Victoria, Australia, 3217
graeme@deakin.edu.au
mwarren@deakin.edu.au

Abstract

This paper reports on the application of systems modelling benchmarks to determine the viability of systems modelling software and its suitability for modelling critical infrastructure systems. This research applies the earlier research that related to developing benchmarks that when applied to systems modelling software will indicate its likely suitability to modelling critical infrastructure systems. In this context, the systems modelling benchmarks will assess the practicality of CPNTools to the task of modelling critical infrastructure systems.

Keywords

Critical infrastructure, modelling, system, dynamic and security.

INTRODUCTION

This research builds upon the earlier research of Pye and Warren (2007, 2006a, 2006b) into developing benchmarks. This research is the continuation of previous research undertaken to develop benchmarks to assess the potential suitability of systems modelling software for application to modelling critical infrastructure systems and reports on the application of these benchmarks based upon the software based modelling tool, CPNTools.

However, before venturing into the benchmark assessment the intention is to provide a brief history of the underpinning Petri Net research that has led to this particular point in time and is the heritage that underpins the research and development that has gone before arriving at CPNTools. Next the characteristics of critical infrastructure systems are reiterated to establish the primary characteristics that are important to the effective modelling critical infrastructure systems.

Additionally, a brief discussion will attempt to reconfirm the importance and necessity for modelling critical infrastructure systems and the possible benefits that such modelling can bring to service assurance analysis and analysis of the system security characteristics in maintaining the viability and integrity of these large and distributed systems that underpin our way of life and standard of living. After this the benchmarks will be measured against the claimed capabilities of CPNTools to determine its potential for modelling critical infrastructure systems.

Finally, conclusions are drawn as to the merit of this research and its indicative outcomes as to the potential practicalities of CPNTools for further application with the next steps in the continuing research project that will lay out the future application of Coloured Petri Net theory modelling via the use of CPNTools software to model critical infrastructure systems.

PETRI NETS

Petri nets are a tool used for the study of systems that enables a system to be modelled based on a mathematical representation of the system. Where a subsequent analysis of the petri net model will hopefully reveal important information about the structure and dynamic behaviour of the system and this information can then be used to evaluate the modelled system to derive strengths, weaknesses, improvements or changes (Peterson 1981).

A Brief History of Petri Nets

Petri Nets were originally developed from the early work of Carl Adam Petri whose 1962 doctoral thesis formulated the basis for a theory of communication between asynchronous components of a computer system that was particularly concerned with the casual relationships between events (Peterson 1981). However, with further research in the 1960's and '70's Petri Nets were soon recognised in theory as an adequate modelling

language for the analysis of synchronisation, communication and resource sharing between concurrent processes. Although, attempts to employ Petri Nets in practice revealed two serious flaws, first there were no data concepts and the models became excessively large and cumbersome because all the data manipulation had to be represented directly within the net structure itself. Secondly, there was no concept of hierarchy and therefore it was not possible to build a large model via a set of separate sub-models (CPN Group 1997a).

The resolution of these two issues came with the development of high-level Petri Nets in the 1970's and the hierarchical Petri Nets in the late 1980's, which removed these serious impediments to Petri Net modelling. The outcome was that Coloured Petri Nets (CPN or CP-nets) represents one of the better known dialects of high-level Petri Nets as it incorporates both the data structuring and hierarchical decomposition without compromising the original Petri Net qualities (CPN Group 1997a).

Introducing Coloured Petri Nets (CPN)

Coloured Petri Nets (CPN) is a modelling language tool developed for systems where communication, synchronisation and resource sharing play an important part in the functioning of the system and it is here that CPN combines the strengths of the ordinary Petri Nets with the strengths of a high-level programming language. Petri Nets provide the primitives for process interaction, while the programming language provides the primitives for the definition of data types and the manipulation of data values (CPN Group 2003).

In the context of systems modelling, CPN have three primary purposes. Firstly, a CPN model is a description of a particular system model that can represent a system specification of a system yet to exist or as a presentation of a current real-world system for explanation to other people. The obvious advantage here is that by creating the a model an investigation can be undertaken to analyse the system before construction begins, which is particularly relevant where design errors may jeopardise security, functionality or expensive to correct. Secondly, the behaviour of the model can be analysed by simulation, which is similar to program execution and debugging or by applying a formal means of analysis as in program verification. Thirdly, it is recognisable that the process of creating the system description and undertaking the analysis should give the modeller an in-depth understanding of the modelled system (CPN Group 1997b).

There are further qualities that CPN bring to modelling systems such as their graphical representation is intuitively very easy to grasp and understand, they have well defined semantics that unambiguously defines the behaviour of each CPN and they can be used to describe a large variety of different systems. CPN offer hierarchical system descriptions containing explicit description of both state and actions that is built on the semantics of true concurrency (CPN Group 1997b).

Therefore, in terms of modelling critical infrastructure systems, CPN offers a mathematically defined technique for the specification, analysis, verification and performance of concurrent distributed systems that requires further investigation and benchmarking to ascertain its viability for modelling the 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 p1 2004a).

Furthermore, 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 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. Consequently, critical infrastructure systems can be further characterised as dynamic systems because they are highly reliant on each other and by necessity must function together in a cooperative manner so that the system as a whole, can function and supply the services normally expected (Pye & Warren 2006b).

Another intrinsic characteristic of critical infrastructure systems as a whole is the 'unboundedness' of the component systems that are related or networked together to form a larger functioning system. This is characterised by the distributed nature of the cooperating systems and 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, hierarchical system structures, dependency relationships existing between and within infrastructure systems and they exhibit network connection characteristics that are subject to both internal or external change and influences. Furthermore, the exchange of services between co-operating infrastructure systems and sub-systems requires a level of synchronisation and concurrency of operation in order for services to progress from their source to their intended destination. These characteristics necessitates that in the national interest critical infrastructure systems do need to be modelled as part of the overall security analysis process and assessed to determine points of weakness or areas of vulnerability. The modelling and functional computer simulation of critical infrastructure systems is potentially the most appropriate and perhaps cost effective way to manage this process, along with solution development and testing of solution models prior to physical implementation into critical infrastructure systems.

Why Critical Infrastructure Modelling is Important

From a systems dynamics perspective there is a strong logic that offers potential improvements in the analysis, security, functional understanding and strategic management perspectives of critical infrastructure systems that will assist in understanding the performance of the system and variations over time (Warren 2005). Since performance reflects the state of resources or service provision, steering strategies can be developed and tested with system modelling, prior to developing policies, physical implementation and taking security decisions that address variations from normal functionality in the face of unexpected challenges.

With this in mind it is then quite feasible to develop adverse scenarios that could be applied to critical infrastructure models to represent such threats and vulnerabilities that would impinge upon 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 and the identification and protection of offshore and maritime assets, accident management, cyber incidents to name a few scenarios that could reasonably be developed and applied to models of critical infrastructure (AGD 2004b).

Therefore, by applying modelling techniques to the critical infrastructure systems that everyone takes for granted such as: communication networks; banking; energy; water and food supplies; health services; emergency services and transport networks (DPMC 2004) for example: this provides the opportunity to actually model adverse situations as applied to the critical infrastructure system, without necessarily testing this same adverse scenario situation in the physical realm of the infrastructure itself.

Inevitably, people confronted with the undertaking of exercising control over dynamic systems, be they business production systems, the economy, global warming and in this case critical infrastructure management for example. They are still required to deal with what Jensen and Berndt (2003) describe as ‘dynamic decision issues’ *[sic]* that characterise a series of related decisions where invariably the systems/s situation will change both in itself and in the response to the actions taken. Modelling of the dynamics at play within the system enables not only the normal functionality to be observed, but also the functionality of an adverse change and its effect upon the critical infrastructure system as a whole, for without this knowledge owners and operators of the critical infrastructure will remain severely handicapped and ill prepared for whatever may potentially eventuate (Warren 2005).

Therefore by modelling critical infrastructures in a manner that indicates the hierarchical scalability of the underlaying systems and the concurrent transfer of services across the greater system structure itself, this will enable exploration of the structures, to characterise the functionality and describe the dynamic behaviour of the focal critical infrastructure system from the perspectives of service assurance availability and system security characteristics and their assessment.

MODELLING BENCHMARKS

The following Tables consist of the individual benchmarks grouped together and identified as applicable to the various modelling benchmark criteria as listed (Pye and Warren 2007):

- Modelling Scalability of System Structure;
- Modelling System Architecture;
- Modelling System Analysis Techniques;

- Modelling System Behaviour;
- Modelling System Operations;
- Model Development and Creation;
- Model Simulation Adaptation.

Under each of these modelling criteria are a number of relevant benchmarks that will give a comparative indication of the differing capabilities and features between modelling styles and techniques as benchmarked.

1	**Benchmark Name:**	**Modelling Scalability of System Structure**
2	**Benchmarks:**	- Model multiple systems. - Model large single systems. - Model localised smaller systems. - Model partial systems.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 1 Modelling Scalability Benchmarks.

The aim of these benchmarks are to assess the scaling capability of the modelling style and whether it is capable of supporting and producing models representing multiple critical infrastructure systems, both large and small single systems as well as delivering partial representations of critical infrastructure systems.

1	**Benchmark Name:**	**Modelling System Architecture**
2	**Benchmarks:**	- Distributed systems. - Closed systems. - Network-centric systems. - Unbounded systems.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 2 Architecture Modelling Benchmarks.

These benchmarks are to assess whether the modelling style is capable of modelling differing system architectures and arrangements of critical infrastructure systems and interconnecting networks.

1	**Benchmark Name:**	**Modelling System Analysis Techniques**
2	**Benchmarks:**	- Reflect dynamic systems thinking. - Reflect operational systems thinking. - Reflect closed-loop systems thinking. - Apply other systems analysis techniques.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 3 System Analysis Benchmarks.

The intention of the benchmarks for assessing modelling system analysis techniques is to assess the capability of the particular modelling style to represent and deliver models of systems that have been analysed using these techniques that highlight the system analysis characteristics.

1	**Benchmark Name:**	**Modelling System Behaviour**
2	**Benchmarks:**	- Model dependency relationships. - Model interdependency relationships. - Model inter-system interactions. - Model intra-system interactions. - Model linear and non-linear behaviour. - Model service load and system load fluctuations.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 4 System Behaviour Benchmarks.

In order to better understand and comprehend just what is happening within the system and the influences and effects of relationships with other systems, it is important that the modelling style is capable of meeting these modelling benchmarks by adequately modelling the behavioural reactions and responses of the target system, particularly from a dependency relationship perspective.

1	**Benchmark Name:**	**Modelling System Operations**
2	**Benchmarks:**	- Model normal system function. - Model abnormal incident function response. - Model communication operations. - Model protective security measures and security responses. - Model redundant system responses. - Model to identify critical system pathways/pinch points. - Model potential scenario and solution impact.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 5 System Operation Benchmarks.

To enable modelling to be utilised as an effective means of analysing the functionality of critical infrastructure systems, it is necessary for it to be able to depict the operations and responses of the system itself at a number of differing levels. Through this, it is then possible to see just what is happening within the systems and subsystems from an operational perspective.

1	**Benchmark Name:**	**Model Development and Creation**
2	**Benchmarks:**	- Development Timeframe to completed model. - Systematic model development process. - Interpretability of the model.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 6 Model Creation Benchmarks.

These benchmarks refer to the length of the timeframe required adequately develop and produce a finished model representation of the critical infrastructure system and whether the modelling style is governed by rules of application and what impact these would have on the model development process. The final benchmark listed relating to the interpretability of the model, relates to the non-professional perspective and whether it is easy to understand and logical in presentation.

1	**Benchmark Name:**	**Model Simulation Adaptation**
2	**Benchmarks:**	- Readily adaptable to computer simulation software. - Simulation development timeframe. - Mapping system responses and accuracy. - Implement scenario and solution testing.
3	**Benchmark Result:**	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	**Benchmark Review:**	Indicates future benchmark improvements

Table 7 Simulation Adaptation Benchmarks.

This final set of benchmarks are aimed towards determining the practicality of whether the model can be easily converted to a computer simulation and how adaptable the particular modelling style is to the development of computer simulations of the modelled critical infrastructure system. These benchmarks also address issues of development timeframe and the accuracy of mapping system responses and the simulation's ability to reflect scenario changes and solution testing quickly.

The intended outcome is that by applying these benchmarks against modelling styles applicable to modelling dynamic and complex systems that a particular modelling style would emerge as meeting more of the benchmark capabilities and therefore become justified as the likely 'best fit' modelling style suitable for further application to modelling critical infrastructure systems.

CPNTOOLS BENCHMARK ASSESSMENT

CPNTools is a CPN modelling software package that is the result of over twenty years of research and development by the CPN Group led by Professor Kurt Jensen at the University of Aarhus in Denmark. The CPN Group are held in high regard as world-leaders in the industrial application of high-level Petri Nets and their tools. CPNTools is the latest generation software support tool for modelling Coloured Petri Nets.

Modelling Scalability of System Structure Benchmarks

CPNTools meets all benchmarks and is capable of both modelling partial or whole systems of a hierarchal nature and can represent multiple systems and sub-systems in a scalable manner and is achievable in a relatively short timeframe.

Modelling System Architecture Benchmarks

CPNTools is particularly suited to and was developed specifically to model distributed systems and is capable of modelling closed and network-centric systems too. However, what remains unclear and yet to be determined is the capability to model unbounded systems, this will require further investigation. However, in regard to the characteristics of critical infrastructure systems then CPNTools is capable of modelling each the respective benchmark system architectures.

Modelling System Analysis Techniques

CPNTools is capable of representing the dynamics changes of systems via its ability to simulate the behavioural properties of systems and is therefore capable of enabling the application of system analysis based on the dynamics, operations and feedback loop effects as applied to analysing a system, additionally it enables an analysis of a system to be made in regard to assessing service availability.

Modelling System Behaviour Benchmarks

CPNTools is capable of demonstrating system behaviour as per the modellers' interpretation of the system and the relationships and interconnections between the relevant sub-systems. System behaviour in this context relates to the operations and dynamic behaviour displayed by the systems and would be observable within the system simulation process supported by CPNTools.

Modelling System Operations Benchmarks

CPNTools is capable of demonstrating system operations as per the modellers' interpretation of the systems' normal functionality, response to adverse system events, the hierarchical system structure and operations and dynamic behaviour of the system. This is one of the primary qualities of CPNTools is that it is capable of modelling concurrent behaviour in distributed systems and through the graphical representation interface it is possible to identify and ascertain the security characteristics of the system.

Model Development and Creation Benchmarks

Model development via the CPNTools interface is a relative quick developmental process that allows a systematic process to be applied to the development and specification or description of systems yet to be built. This capability permits the modeller to assess and test the system design and the intuitive presentation of the system via the CPNTools interface enables easy system interpretation, explanations and discussion regarding the system without requiring high-level CPN knowledge or a detailed understanding of the modelling process.

Model Simulation Adaptation Benchmarks

The clear advantage of using CPNTools is it capability to simulation the modelled system and the interface of the program enables the implementation of subtle or major system changes to happen in a short timeframe that does not require laborious data collection or redesign. The CPNTool's interface enables system changes to be effected quickly to test potential system solutions and assess operational scenario responses.

The outcome of the benchmarking process indicates that CPNTools software based on the theory of Coloured Petri Net modelling is capable of modelling critical infrastructure systems. The CPNTools software appears to be able to take into consideration the main characteristics of critical infrastructure systems and in all likelihood is capable of delivering a suitable medium for modelling these large systems.

CONCLUSIONS

The benchmarking analysis undertaken within this paper indicates the CPNTools software meets the majority of the fundamental benchmarks, which indicates that CPNTools is a suitable choice for modelling critical infrastructure systems. This suggests that CPNTools has the capabilities necessary to model the primary characteristics and behaviours pertinent to critical infrastructure systems and therefore it follows that the next step in this research is to test the validity of CPNTools by modelling and assessing the CPNTools outcome.

It is important that a systematic validation of the CPNTools modelling premise is assessed to ensure that under the scrutiny of security experts that CPNTools does hold the potential for successfully modelling critical infrastructure systems as this research indicates. Hence, the next step in this research is the validation assessment of this research that would take the form of a 'pilot' assessment of a small critical infrastructure system model that best illustrates and challenges the capabilities of CPNTools for modelling such systems.

Depending on the validation assessment outcome, CPNTools will then model a larger scale critical infrastructure system to illustrate the systematic, hierarchical and scalable interconnections and cooperation of systems as a subset of the larger critical infrastructure system. This would represent the model description of the chosen critical infrastructure system to illustrate the detailed structure of the system, to characterise the system's functionality and the dynamic behaviour of the system, from the system analysis perspective of service assurance and system security characteristics.

REFERENCES

AGD (2004a) Critical Infrastructure Protection National Strategy, TISN, URL: http://www.nationalsecurity.gov.au/ , Accessed: November 2004.

AGD (2004b) Protecting Australia's Critical Infrastructure [Online Media Release], Attorney-General's Department, URL: http://www.ag.gov.au/ , Accessed: May 2005.

CPN Group (1997a) History of Petri Nets, [Online], University of Aarhus CPN Group, URL: http://www.daimi.au.dk/CPnets/intro/history.html, Assessed: September 2007.

CPN Group (1997b) Why use CP-nets? [Online], University of Aarhus CPN Group, URL: http://www.daimi.au.dk/CPnets/intro/why_cpn.html, Assessed: September 2007.

DPMC (2004) Protecting Australia Against Terrorism, Department of the Prime Minister and Cabinet, URL: http://www.dpmc.gov.au/publications/protecting_australia/docs/protecting_australia.pdf, Accessed: October 2004.

Ellison R.J. et al (1999) 'Survivability: Protecting Your Critical Systems', IEEE Internet Computing, no. Nov/Dec.

Jensen E. & Brehmer B. (2003) 'Understanding and Control of a Simple Dynamic System', System Dynamics Review, vol.19, no.2, pp. 119-137.

Peterson J.L. (1981) Petri Net Theory and the Modeling of Systems, Prentice-Hall Inc., Englewood Cliffs, NJ, USA.

Pye G. & Warren M.J. (2007) Benchmarks for Critical Infrastructure Systems Modelling. 6th European Conference on Information Warfare and Security (ECIW), Academic Conferences International (ACL). Shrivenham UK, pp. 2007-216.

Pye, G. and Warren, M. (2006a) Conceptual Modelling: Choosing a Critical Infrastructure Modelling Methodology, in Dr Craig Valli & Dr Andrew Woodward (eds), Proceedings of the 7th Australian Information Warfare and Security Conference, pp. 103-113, Edith Cowan University, Perth, Western Australia

.Pye G. & Warren M.J. (2006b) 'Security Management: Modelling Critical Infrastructure', Journal of Information Warfare, vol.5, no.1, pp. 46-61.

Warren K. (2005) 'Improving Strategic Management with the Fundamental Principles of System Dynamics', System Dynamics Review, vol.21, no.4, pp. 329-350.

COPYRIGHT