Benchmarks for Critical Infrastructure Systems Modelling

Graeme Pye and Matthew Warren
School of Information Systems, Deakin University, Geelong, Australia
graeme@deakin.edu.au
mwarren@deakin.edu.au

Abstract: This paper draws together previous security assessment research and builds upon the current systems modelling research investigation into the application of potential modelling styles that can be applied to model critical infrastructure systems, networks, their inter-relationships and functionality. The emphasis here is to develop appropriate benchmarks as a means of assessment to determine the appropriateness of various systems modelling styles and techniques and their suitability for modelling critical infrastructure systems. The benchmarks are applicable on a number of differing levels to determine the 'best fit' for modelling critical infrastructure systems, to aid in identifying potential system or inter-network vulnerabilities.

Keywords: Critical infrastructure, security, benchmark, systems modelling.

1. Introduction

The primary purpose of modelling is to produce a smaller scale abstract representation of the chosen system that closely exhibits or resembles the real world system in structure, functionality and behaviour (Pearsall 1998). There are numerous modelling approaches and modelling styles to choose from that can be applied to modelling dynamic systems, but the principle focus is determining the most appropriate modelling style; that when applied to a critical infrastructure system, will deliver a faithful representation of the existing real-world subject system or part thereof being modelled.

The task of selecting the appropriate modelling approach to use is a choice that at first may appear a relatively simple selection to make, but deeper consideration from the real-world perspective of what the model is to represent would suggest that this is not the case. Particularly with the existence of numerous modelling approaches that are quite capable of modelling across differing structures with similar characteristics. Therefore, the key issue is how to identify which is the most appropriate and workable modelling outcome to use? This requires clearly defined reference points against which to compare the various modelling styles prior to making a selection. This requirement is especially prevalent when considering that there is no 'one-size fits all' modelling approach, particularly in the greater context of this research where the overarching aim is related to modelling critical infrastructure systems from a security analysis perspective. Additionally, there is no time to apply a 'try it and see' plan to evaluate the merits of each particular modelling approach to only find that it is not workable. However, using a set of defined reference points delivers a method for comparing differing modelling approaches and styles to determine the most likely modelling style applicable to modelling the characteristics and features of targeted critical infrastructure systems.

To address this premise, this paper proposes the use of benchmarks applicable to determining the most appropriate modelling approach or style to apply to the modelling of critical infrastructure systems from a security analysis perspective. This paper will discuss and adapt an existing security-benchmarking framework, identify the common characteristics surrounding critical infrastructure systems, the preferable features a modelling style could deliver, before developing appropriate and relevant benchmarks with the adapted security-benchmarking framework. Then a justification explaining why it is necessary to determine and apply modelling styles and techniques to modelling critical infrastructure systems is undertaken, before conclusions are drawn and the future application of this benchmarking research are discussed.

2. Conceptual benchmarking framework

Benchmarking typically plays a central role in the assessment of business performance and in particular the analysis of the competitive performance of the business itself as a means to gauge performance against its rivals within its own business domain (McGaughey 2002). Benchmarking equates to setting evaluation standards against which comparative analyses of specific and

fundamental performance factors is undertaken that compare and measure against some established predetermined criterion (Koch & Robinson 2002). Likewise, this research proposes that benchmarking is a method that would be beneficial to informed judgement decisions regarding the selection of the appropriate modelling style applicable to the modelling of critical infrastructure systems. However, before identifying suitable benchmarks applicable to deriving such decisions, documentation capture of the comparative benchmarking results relating to the benchmarking assessment conducted against various modelling styles, requires a consistent documentation framework approach.

2.1 The framework

This particular benchmarking framework (see Table 1) is an adaptation of an online security-benchmarking framework developed previously by Pye and Warren (2006a), it has been adapted from a dedicated benchmark specific framework to one that is intended to support the application and documentation of generic benchmarks as identified.

Table 1: Generic Benchmaking Framework.

1	Benchmark Name:	Identifies the benchmark
2	Benchmarks:	States the various and acceptable benchmarks for measure
3	Benchmark Result:	States the result of the benchmark assessment (Pass/Fail/Analysis and Comment)
4	Benchmark Review:	Indicates future benchmark improvements

The generic benchmarking framework illustrated in Table 1 consists of a four sections. The initial section identifies the benchmark by name, the next section is where the various benchmarks for assessment are set and recorded, and section three pertains to the result of the benchmark comparison assessment and any pertinent comments with the final section relating to a review of the benchmark/s as it currently stands. This simple framework is a guide that enables the recording and documentation of the benchmarking process and delivers a framework that is readily adaptable to any benchmark development and assessment process.

2.2 The benchmarking process

The methodical application if the benchmarking process as it pertains to the benchmarking of critical infrastructure modelling style follows the structure of the framework and provides a guide for the consistent application of a particular benchmark/s in its comparison to differing modelling styles. The process is as follows:

1. Initially a check should ensure that the appropriate and applicable benchmark is utilised in comparison against the specific aspect of the modelling style as intended.
2. Next, the process of benchmark assessment comparison establishes whether the specific aspect of the modelling style passes or fails the level of measure relating to the specific benchmark, but if this is unclear or uncertain then a further and deeper analysis is required to establish benchmark suitability.
3. During this Step, the resultant outcome of the benchmark comparison process during Step 2 records whether the benchmark was passed or failed or is unclear requiring further analysis and comment regarding any reasons why the result is so, this also provides a documented and auditable record trail.
4. The final Step of the benchmarking process is a review of the existing benchmark/s to consider appropriateness of application, level of measure and relevance going forward.

While this benchmarking framework is somewhat generic in nature, it was adapted in such a manner with the view to enable a degree of flexibility with the identification, selection and establishment of such benchmarks and their subsequent application. The intention is that this framework will form the basis for the management of the benchmarks and act as a guide for applying the benchmarking process for judging the merits of particular system modelling style or technique. Although, before any benchmarks pertaining to systems modelling are developed and

applied, it is necessary to determine the general characteristics of critical infrastructure systems as this will enhance the development of targeted and applicable benchmarks. The intention is that from this analysis, these benchmarks will become the basis upon which to assess the merits of a particular modelling style and its potential to deliver a representative model of a critical infrastructure system.

3. Critical infrastructure system characteristics

The characteristics and nature of critical infrastructure systems are in themselves the result of increased technological interconnectedness and complexity as well as the incorporation of heterogeneous, dynamic and interactive components that form these physically large and geographically dispersed systems (Macdonald & Bologna 2003). However, in this paper's context the characteristics identified remain general in terms of moving towards the goal of establishing worthwhile benchmarks for comparatively determining the most appropriate modelling style. This is managed through utilising a consistent benchmarking process to compare and judge potential modelling styles for their suitability and adaptability to model critical infrastructure systems. To this end, it is important to identify and understand the particular characteristics and features that are indicative of critical infrastructure systems for the development of suitable and practical benchmarks, which would additionally identify desirable modelling attributes suitable to modelling critical infrastructure systems. From this investigation can be derived the key benchmarks applicable to the determination of the appropriateness and suitability of a specific modelling style application to modelling the features and characteristics of critical infrastructure systems.

3.1 Critical Infrastructure features

The critical infrastructure systems themselves are many and varied, yet they possess characteristics that exhibit a commonality across most critical infrastructure systems that should form the basis of any benchmark development. The following is a short list of the principle characteristics:

- Spatial Scalability of Structure;
- Time Dynamics;
- Dependency and Interdependency Relationships;
- Operational Factors.

Although this list is not an exhaustive catalogue of the key characteristics of critical infrastructure systems, they do form the basis of the wider benchmark development aspects as these characteristics warrant consideration in undertaking analysis, modelling and simulations of critical infrastructure systems.

3.1.1 Spatial scalability of structure

The spatial scale of critical infrastructure systems and the scalability of the physical structures will vary widely between infrastructures and depends on the fineness of focus applied to the analysis of the particular infrastructure. For example, Rinaldi et al (2001) noted that this listed hierarchy of elements could represent the scalability of an infrastructure:

- Part, being the smallest component of a system that can be identified in an analysis;
- Unit, refers to the functionality of a related set of parts;
- Subsystem, as an array of units;
- System, is the grouping of subsystems;
- Infrastructure, the complete collection of systems with a common focus;
- Interdependent Infrastructures are the interconnected network of infrastructures and the environment.

The fineness of scale listing here attributed to critical infrastructure system scalability in this manner resembles the notion of geographical scales when considering that infrastructures can physically span cities, regions, nations and internationally (Rinaldi et al 2001). This notion of

scalability of critical infrastructure systems is further supported by the research of Pye and Warren (2006b) pertaining to the critical infrastructure model created, where hierarchical rankings were developed to represent the various levels of critical infrastructure, existing in the Australian context.

3.1.2 Operational time dynamics

Another common characteristic apparent across and within critical infrastructure systems is the functionality and dynamics of time and the vast functional range of time that can exist between differing infrastructures. For example, the relevant time scales of operational infrastructures can vary from milliseconds (e.g., electricity system operation) to hours (e.g., gas, water, and transportation systems) to years (e.g., the upgrade construction of infrastructure for additional capacity), furthermore the dynamics of time also has a central implication within dependency relationships between infrastructures (Rinaldi et al 2001).

3.1.3 Dependency and Interdependency Relationships

Although not prevalent in all critical infrastructure systems, there exists to some degree a dependency or interdependent relationship between and within most critical infrastructures that pertains to the supply/exchange of services between infrastructure systems. These relationships can exist in a number of forms, as listed (Pye & Warren 2006b):

- TCID (Total Critical Infrastructure Dependency);
- MCID (Multiple Critical Infrastructure Dependency);
- BCID (Bridging Critical Infrastructure Dependency).

As Pye and Warren (2006b) defined, a dependency relationship is based on the premise that there exists a reliance or influence between infrastructures or multiples thereof that is a heavily biased or one-sided relationship. Alternatively, if the infrastructures are mutually reliant on each other for the supply/exchange of services and the dependency influence has greater equity of distribution between infrastructures, then this is an interdependent relationship. Additionally, Rinaldi et al (2001) also identified that depending on the looseness or tightness of these dependency relationships and the time dynamics involved, this will have an impact on the operational characteristics of the critical infrastructure systems involved too.

3.1.4 Operational factors

The operational characteristics of critical infrastructure systems will also change depending on the load imposed on the systems involved and how stressed they are or become in response to fluctuations in system stability. These factors relate closely to the security and risk contingencies within the system and the operating procedures, continuity plans, operator education, backup, redundant systems, existing workarounds and even the decisions taken in emergencies that play a crucial role in crisis management and mitigation of infrastructure operation (Rinaldi et al 2001).

Another operational characteristic of some critical infrastructure systems is the unboundedness of the component systems that are interrelated or networked together cooperatively to form a larger system. System unboundedness is characterised by the distribution of local system administrative control that exists within the component systems, but the system as a whole is without a central governing authority (Ellison et al 1999). In summary, these systems are large, complex and increasingly interconnected with their network of supporting information systems, subsystems, relationships and other identified characteristics and factors. These all play key roles in determining the operational characteristics of critical infrastructure systems that have key implications for the security and risk management of critical infrastructures. Additionally, they also predominantly represent the more common characteristics that are apparent across most critical infrastructure systems, which require consideration as to how they are modelled, simulated or analysed. Furthermore and alternatively from the modelling perspective, there are modelling attributes that are preferable from the perspective of modelling dynamic systems that may also value-add to the process of modelling critical infrastructure systems.

3.2 Preferable modelling attributes

The preferable modelling attributes are those features that a modelling style or technique can potentially deliver to the analyst that in some cases goes directly to the deliverables of a particular modelling style, particularly in relation to what the critical infrastructure system model should be capable of depicting and representing to the modeller and analyst. The modelling of critical infrastructure systems has the potential to deliver some desirable insights from the analyst perspective and differing modelling styles will naturally exhibit differing modelling capabilities. Consequently, the following list represents those capabilities that would be ideal for depicting and modelling functional critical infrastructure systems. Although one single modelling style is unlikely to meet all these capability criterion, they will however form the basis for developing benchmarks to assess the modelling capabilities of various modelling styles and ultimately the selection of the 'best fit' for modelling critical infrastructure systems:

Modelling capabilities:

- Centralised, distributed, network-centric, unbounded and closed systems;
- Scalability of large, local and partial systems;
- System's physical attributes including critical pathways and system redundancy;
- Internal and external system security features;
- Highly connected and interconnected complex systems;
- Mapping system communications and exchange of services;
- Dependency relationships with other associated systems;
- Functional system time considerations;
- Normal and adverse system operations and responses;
- Scenario and solution outcomes.

Other aptitudes:

- Systematic model development process;
- Systems analysis, depicting 'cause and effect';
- Adaptation to a computer simulation;
- Learning the modelling language for application;
- Pace of model development in time.

The modelling attributes listed, although not conclusive do indicate the preferable aspects of what a modelling style or technique might be capable of delivering to the analyst attempting to model a critical infrastructure system. This now forms the starting point of the benchmark development where a particular critical infrastructure system characteristic are matched to the most appropriate modelling preference, to develop an applicable benchmark.

4. Modelling benchmarks

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

- 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.

Table 2: Modelling scalability benchmarks

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

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.

Table 3: Architecture modelling benchmarks

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

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.

Table 4: System analysis benchmarks

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

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.

Table 5 System behaviour benchmarks

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

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.

Table 6 System operation benchmarks

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

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.

Table 7: Model creation benchmarks

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

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 nonprofessional perspective and whether it is easy to understand and logical in presentation.

Table 8 Simulation adaptation benchmarks

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

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.

5. Justification for modelling the critical infrastructure systems

There are numerous styles of modelling that purport to be suitable to modelling dynamic systems, yet the challenge remains in determining, selecting and applying the most suitable modelling style for modelling critical infrastructure systems. Through the application of benchmarking, it is possible to assess quickly the relevance and usefulness of modelling styles to determine their suitability for modelling these systems and their analysis.

Macdonald and Bologna (2003) noted the structure and aspects of numerous interactive infrastructure systems present many practical challenges for modelling, prediction, simulation, and 'cause and effect' analysis along with the relationships issues of coupled systems. From this perspective, being able to model the system provides the analyst with the capability to see and deal with the system within the modelling environment, as opposed to conducting an initial analysis in the field, although a physical inspection would confirm the outcomes and findings of the modelling analysis.

Additionally, as Fleckner (2004) noted, Australia though its geographical isolation and perhaps good fortune has largely remained immune from the political threat issues and attacks aimed directly at the nation's critical infrastructure systems. Although in the current political climate, failure by the infrastructure owners and government to analyse, prepare and protect Australia's critical infrastructure systems would expose these companies to legal liability, ridicule and blame for not having foreseen the risk and prepared contingency plans accordingly.

Therefore, modelling critical infrastructure systems presents a practical way of dealing with the consequences of physical size and the geographic magnitude of distribution of these systems. Furthermore, with the increasing complexity and interconnectedness of these systems and the resultant influences of dependency relationships and operational characteristics, this highlights applied modelling as a highly practical method of analysing, not only the operations and

contingency plans in place, but more importantly a means of analysing the very security of these critical infrastructure systems.

6. Conclusion

In moving forward from here with the benchmarks identified and established is the practical application of these comparative benchmarks against various systems modelling styles, techniques and applications to analyse, critique and ascertain their capability and suitability for modelling critical infrastructure systems.

The modelling benchmarks developed and detailed here establishes a number of criteria that convey comparative standards for the review of the capabilities of various modelling styles and techniques, to enable the application of a consistent and comparative measure that is repeatable. The benchmarking process outlined is consist in application and focused upon attempting to match the common characteristics of critical infrastructure systems to the desirable features that modelling styles can bring to modelling similar dynamic and complex systems. Through benchmarking, this now delivers a means of tailored and repeatable assessment as applied by benchmarks that are applicable to determining the appropriate modelling style based on the 'best fit' for presenting and representing the key characteristics and behaviours exhibited by critical infrastructure systems.

With the active application of the benchmarking process as applied to various modelling styles, this will address the current situation where existing modelling attempts have resulted in vague or ambiguous outcomes previously. While this proposed benchmarking solution is not definitive, it attempts to address the current situation where there is still a lack of any practical and definitive solution dedicated to the modelling of critical infrastructure systems. Therefore it remains that due to a current lack of formal methodologies for understanding the behaviour, influences and complexity of these systems (Macdonald & Bologna 2003), benchmarking presents an opportunity to suitably identify a modelling style that is potentially acceptable as a 'best fit' for ongoing modelling and security research into the analysis of critical infrastructure systems.

References:

Ellison R.J. Fisher D.A. Linger R.C. Lipson H.F. Longstaff T.A. and Mead N.R. (1999) "Survivability: Protecting Your Critical Systems", *IEEE Internet Computing*, no. Nov/Dec.

Fleckner A. (2004) "Critical Infrastructure Protection and the Terrorist Threat", *Information Age*, no. Oct/Nov, pp. 17-18.

Koch H. & Robinson P.E. (2002) Evaluating Electronic Commerce Initiatives with Benchmarks: Insights from Three Case Studies, in Eighth Americas Conference on Information Systems, Dallas, TX, USA, pp. 1251-1258.

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

McGaughey, R. E. (2002) "Benchmarking business-to-business electronic commerce", *Benchmarking: An International Journal*, vol.**9**, no.5, pp. 471 - 484.

Pearsall J. (Ed) (1998) *The New Oxford Dictionary of English*, Clarendon Press, Oxford.

Pye G. & Warren M.J. (2006a) A Conceptual Model of and Framework for Benchmarking Online Security', in IADIS International Conference e-society 2006, International Association for Development of the Information Society (IADIS), Dublin, Ireland, pp. 501-508.

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

Rinaldi S.M. Peerenboom J.P. Kelly T.K. (2001) "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *Control Systems Magazine, IEEE*, vol.**21**, no.6, pp. 11-25.