Infrastructure Systems Interdependencies and Risk Informed Decision Making (RIDM):

Impact Scenario Analysis of Infrastructure Risks Induced by Natural, Technological and Intentional Hazards

Dr Rudolph Frederick Stapelberg [BscEng (Civil and Industrial); MBA (Exec); PhD (Eng); DBA; PrEng]
Adjunct Professor - Center for Infrastructure and Engineering Management
Griffith University, Gold Coast, Queensland Australia

ABSTRACT

Infrastructure can be defined as physical assets that are capable of an intended service delivery, comprising of rigid assets such as buildings, roads, bridges, and facilities, as well as flexible assets such as utilities and facilities related to water, sewage, power etc. including their systems and machinery. Infrastructure *systems* can be viewed as a structured network of interdependent mechanisms that enable the service delivery capability of physical assets predominantly inherent to infrastructure. Infrastructure systems are frequently connected at multiple points through a wide variety of mechanisms, such that a bi-directional relationship exists between the states of any given pair of infrastructures. Such bi-directional relationships or interdependencies among infrastructure systems dramatically increase the overall complexity of the "system of systems" of multiple infrastructures. This paper reviews current research into infrastructure systems interdependencies with regard to safety risks induced by natural, technological and intentional hazards. The paper further considers risk informed decision-making relating to questions such as:

- What analytic methods can capture, clarify, and predict the complex behaviours of infrastructure systems?
- Which measures of performance adequately describe systems complexity?
- How can risk and uncertainty be incorporated into the management of infrastructure systems?
- What are the safety risks induced by natural, technological, as well as intentional hazards?
- What would be the best approach to disaster management in view of multiple infrastructure systems interdependencies?
- Who are the principal decision makers and stakeholders, and what are their goals and objectives.
- What are the most appropriate response measures and adaptation strategies?
- What real contribution does scientific research have into hazards and risks of facilities, utilities, transport and services infrastructure?

Keywords: infrastructure systems interdependencies, risk informed decision-making, disaster management.

THE AUSTRALIAN CIPMA PROGRAM

Protecting critical infrastructure (CI) that underpins Australia's economic strength and social stability is a high priority for the Australian Federal and State Governments. The Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection (CIP), established in April 2003, forms the basis of a strong private sector and government partnership approach to this important national objective. The Attorney General's Department is the lead coordinating agency for CIP, and is sponsor and manager of the CIP Modelling and Analysis (CIPMA) Program, one of the priority initiatives already funded in the 2004–2005 and 2006-2006 Budgets [1].

Critical infrastructure is defined as critical physical facilities, utilities and defence infrastructure assets, critical industry assets and supply chains, as well as critical information and communication technology and networks, the destruction or degradation of which, or unavailability for an extended period, would significantly impact on the nation's social and economic well-being, or affect Australia's ability for national defence and security. Critical infrastructure extends across many sectors of the Australian economy, including State Treasuries and their agencies, local government authorities, banking and finance, transport, power, gas and water utilities, communications, built environment and facilities, manufacturing, mining and process industries, as well as national health and defence organisations. A fundamental characteristic of critical infrastructures is that they consist of complex, highly connected and highly interdependent systems. This is particularly evident in sectors such as power, gas and water utilities. The reliable continuity of the supply of electricity and water is critical to many other sectors of the community. A significant loss of supply for an extended period would have substantial negative impacts, both on the economy and the social well being of the population. Critical infrastructure can be damaged, destroyed or disrupted by natural disasters, negligence, accidents, computer hacking, criminal activity and malicious damage, as well as by deliberate acts of terrorism. The CIPMA Program will involve modelling, simulation and analysis of the primary dependencies and interdependencies of critical infrastructure.

The overall aim of the CIPMA Program is to develop the capability to answer questions posed by key decision makers in government and industry about critical infrastructure dependencies and interdependencies, and the flow-on consequences of a complex systems failure in one sector. Many physical infrastructure systems in the built environment, as well as facilities and utilities (transportation, water, power, and telecommunications) are complex adaptive systems with emergent systemic behaviour patterns that result from dynamic interactions among their inter-related components. Analysing physical infrastructure systems in terms of the ***dimensions of systems interdependencies***, namely infrastructure system characteristics, inter-system and intra-system causal relationships, environmental impact such as climate change, response behaviour, failure types, state of operation and interdependency risks, yields new insights into infrastructure systems behaviour and a consequent expanded thinking on risk informed decision making (RIDM) of critical infrastructure.

OVERVIEW OF CONCEPTS

Infrastructure:
Infrastructure can be defined as physical assets that are capable of an intended service delivery, and which comprise of rigid assets such as the built environment including buildings, roads, bridges, and facilities, and assets that relate to community services such as public land and parks, and flexible assets such as utilities and facilities related to water, sewage, power etc. including their systems and machinery and computer hardware.

Infrastructure Systems:
Infrastructure systems can be defined as an integrated structured network of interdependent entities that enable the service delivery capability of rigid and flexible physical assets that are inherent to infrastructure.

Multiple Infrastructure Systems:
Multiple infrastructure systems are interlinked infrastructure systems that are connected at multiple points through a wide variety of mechanisms, such that a bi-directional relationship exists between the states of any given pair of infrastructures. Such bi-directional relationships (interdependencies) among infrastructure systems dramatically increase the overall complexity of multiple infrastructure systems.

Infrastructure System Interdependencies:
When examining the more general case of multiple infrastructures connected as a "system of systems", their interdependencies must be considered. Infrastructure interdependencies means a bi-directional relationship between multiple different infrastructures in a general system of systems through which the state of each infrastructure influences or is influenced by or correlated to the state of another.

Infrastructure Risk and Change Impact Adaptation:
Infrastructure risk is approached from the point of view that it is principally concerned with undesired events, and is tied to the prospect of being a threat. Defining infrastructure risk is complicated by the fact that it can be decomposed into two components: *likelihood* and *impact*. When a risk event is considered from the perspective of *likelihood*, the decision as to whether it will be construed to be a threat depends on how likely the occurrence of the event would be. However, even if the likelihood of the risk event is deemed to be low, the decision as to whether it will be construed to be a threat depends upon the resulting consequences of the *impact*. Infrastructure risk management however, requires a holistic approach to ***assessment of the vulnerability*** of critical infrastructure, and can be envisaged as an iterative process ranging from identification of internal and external sources of risk impacts, through to hazards and risk analysis, monitoring and diagnostics, modelling and prediction, knowledge management, risk response and risk mitigation, and consequence recovery. Such a holistic approach to a vulnerability assessment of critical infrastructure can be important, particularly in situations of significant impact such as climate stress on infrastructure interdependencies. In some cases joined systems subject to intense climate stress can be mutually supportive, in other cases failure of one may exacerbate the load placed upon another. Adaptive changes in one system can also imply significant effects for others. In this regard, "*climate change* is itself an adaptive response of the Earth's systems to enhanced global warming" [2].

Infrastructure Vulnerability to Natural Hazards:
Vulnerability analysis for ***disaster management*** of natural hazards can be broken down into components of:

- Exposure — the natural hazards or change impacts that will affect the system;
- Sensitivity — the reaction of the current system to those natural hazards or changes;
- Adaptive capacity — the scope for modifying the system to increase its capacity to cope with natural hazards or change impacts.

While these elements combine together to produce a net natural hazards effect or ***change impact vulnerability*** as indicated in Figure 1, it is possible to separate them and analyse them individually.

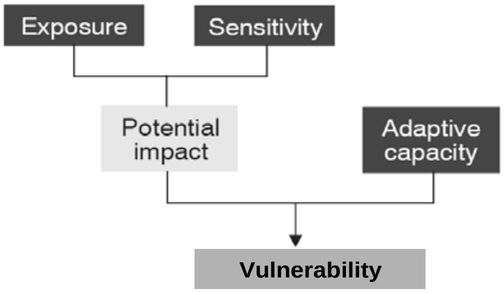

Figure 1: Infrastructure Vulnerability Analysis [2]

Climate Change Impact on Infrastructure Functions: Infrastructure dimensional functions (i.e. characteristics, inter-system and intra-system causal relationships, environmental impact, response behaviour, failure types, states of operation and interdependency risks) impacted by climate changes include [3]:

- Built environment infrastructure and building codes.
- Energy supply and distribution systems.
- Water and wastewater management systems.
- Transportation systems design and management.
- Public works operations and management.
- Public health care management services.
- Public safety and emergency preparedness.

Infrastructure Vulnerability to Technology Hazards: In the case of the vulnerability of infrastructure to technological hazards, vulnerability analysis can be broken down into components of interdependency, similar to the taxonomies developed by Rinaldi, Peerenboom, and Kelly [4] and Dudenhoeffer, Permann and Manic [5]. This ***categorization of interdependencies*** can also be used to classify vulnerability by relationships:

- Physical – a physical reliance on material flow from one infrastructure to another and engineering reliance between components.
- Informational – reliance on transfer of information between infrastructure and informational or control requirement between components.
- Geospatial – a relationship that exists entirely because of the physical proximity of components.
- Logical –dependencies that exist between components even if no physical linkage or relationship exists.

Be it through direct physical connectivity, transfer of control information, geospatial proximity, or logical dependency, most critical integrated infrastructure systems interact and are therefore vulnerable to technological hazards. These interactions often create complex relationships, component dependencies, as well as interdependencies that cross infrastructure boundaries. The modelling and analysis of technological interdependencies between critical infrastructures is a relatively new and important field of study.

Infrastructure Vulnerability to Intentional Hazards: With ***critical infrastructure protection (CIP)*** against vulnerability to intentional hazards, only criteria affecting vitally necessary systems are taken into consideration [6]:

- Survivability – the capability of a system to fulfil its mission in the presence of intentional hazards.
- Dependability – reliance on the services that a system delivers when vulnerable to intentional hazards.
- Complexity – induced cascading failures in complex networks triggered by intentional hazards.
- Uncertainty – lack of knowledge about unknown and unidentified options for intentional hazards.
- CIP strategies – management policies and involvement in protection against intentional hazards.

Survivability and Dependability in CIP: Survivability is defined as the capability of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents and at the same time its ability to evolve to meet continual changes in an organisation and its environment. A survivable system has the ability to continue to provide service (possibly degraded or different) in a given operating environment even when various events cause major damage to the system or its operating environment. Ultimately, critical infrastructure protection focuses on vitally necessary systems where the mission of a system's functionality must *survive*, and not necessarily on any particular component of the system or the system itself. The challenge is to identify essential processes within infrastructures, which are vital for the survivability of large integrated systems. Only critical processes should be considered in determining critical infrastructure systems survivability. In contrast, systems dependability should be referred to for overall functioning of the components of a system under any circumstance.

Dependability is a property that is usually stated as a set of requirements with which a system has to comply. Dependability in critical infrastructure protection includes attributes and methods, as indicated in Figure 2 below [6]:

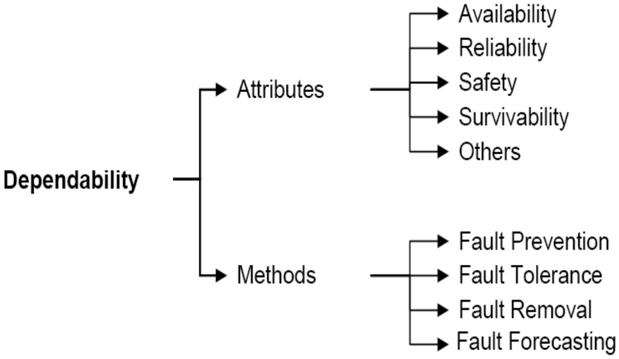

Figure 2: Attributes and Methods of Dependability [6]

Attributes: The availability of a system is defined as the probability that the system will be functional at any required time. The reliability of a system is defined as the probability that the system will meet its requirements over a period of time when operating in a prescribed environment. The integrity of the system is a measure of the combination of attributes such as system availability, reliability, safety, survivability and maintainability.

Methods: The notion of an event that causes damage is informally referred to as a 'fault'. Dependability relates to such faults from the perspective of; fault prevention - how to prevent the occurrence or introduction of faults; fault avoidance - the process of building a system in such a way that certain faults do not arise; fault tolerance - building systems that are able to react in a requisite way to prescribed faults; fault removal - how to reduce the presence (number, severity) of faults; fault forecasting - estimating the occurrence and consequences of faults.

Complexity in Infrastructure System Networks:
Complex networks are inherent in infrastructure systems (e.g. computer networks, energy distribution networks, transport networks). Characterising structural properties of networks is of fundamental importance to understanding the complex dynamics of these systems. Networks are inherently difficult to understand, as the following list of possible complexities illustrates [7]:

- Structural complexity – Increasing the number of component nodes and links between the nodes.
- Network evolution – Changing links between network nodes over time.
- Connection diversity – Links between nodes could have different weights, directions and signs.
- Dynamical complexity – In a network the state of each node can vary in time in multiple ways.
- Component diversity – Components within a network may be of very different nature.
- Meta-complication – Various meta-systems or outside network complications can influence each other.

Complexity theory implies that different components of a system are interdependent to the extent where changes in one component may affect another, or result in failure of interconnected systems. A unifying framework is thus needed to develop a solid theoretical understanding of the physical processes underlying the formation of complex infrastructure system networks.

Uncertainty, Knowledge and CIP Strategies:
The analysis of vulnerability in infrastructure systems is a major input to the risk assessment that must be performed to establish critical infrastructure protection priorities. Comparison of protection options is complicated because of uncertainty, as the vulnerabilities of infrastructure systems are not necessarily constant. The susceptibility of the electric power grid to disruption continually changes as loads ebb and flow and as generation resources come on line, are utilized, or made unavailable. There are also persistent vulnerabilities in both hardware and software. For example, computers controlling electric power grids are accessible and subject to manipulation by anyone with software hacking knowledge. Dealing in uncertainty requires using probability estimates. If probabilities are used (e.g., the probability of a given type of intentional hazard, or attack on an installation’s vulnerability), they typically cannot be obtained from empirical frequency distributions as events are uncommon or hypothetical. Instead, the probabilities must be derived using a combination of modelling, gaming, and analysis; all with a good deal of subjectivity. Further, the probabilities should change over time as knowledge of infrastructure systems interdependencies and their related vulnerability to risks induced by natural, technological, as well as intentional hazards improves. The likelihood of an increase in vulnerability increases as the number of components increases. Modelling techniques are only now emerging for the analysis of vulnerability in infrastructure systems [8].

MODELLING INFRASTRUCTURE SYSTEMS

The complexity and interconnectedness of critical infrastructure poses challenges for the modelling and analysis of infrastructure systems interdependencies. While it may appear straightforward to apply GIS to determine the geospatial proximity of site-specific physical critical infrastructure, it is much more difficult to model and analyse the dynamics of their systems. Crucial to the modelling process is the capture and analysis of infrastructure system dependencies through models that incorporate integrated processes with infrastructure systems functionality to determine the criticality or vulnerability of these infrastructure systems. While the dependencies within an infrastructure network are often well understood, the region of interest in interdependency modelling is the risk impact that one infrastructure can impart upon another. The key effects to model, and gain an understanding of, are the ***chains of influence*** that cross multiple infrastructure systems and induce potentially unforeseen effects. These chains, potentially composed of multiple interdependency types, constitute the physical connectivity paths between network nodes of infrastructure system components. The network paths represent cascading consequences of a risk event, or the derived dependency of one component from another [9].

The various chains of influence of infrastructure networks present numerous theoretical and practical challenges in modelling, prediction, simulation, and analysis of cause and effect relationships in interdependent systems. These systems comprise a heterogeneous mixture of dynamic, interactive, and often non-linear entities, unscheduled discontinuities, and numerous other significant effects. Modelling and analysis of these systems requires consideration of their non-linear and time-dependent behaviour based on certain knowledge of empirical facts and uncertain knowledge based on hypothetical data as indicated in Figure 3. Existing mathematical models of such systems are too vague and there are very few methodologies for understanding the complex behaviour of integrated critical infrastructure systems [10].

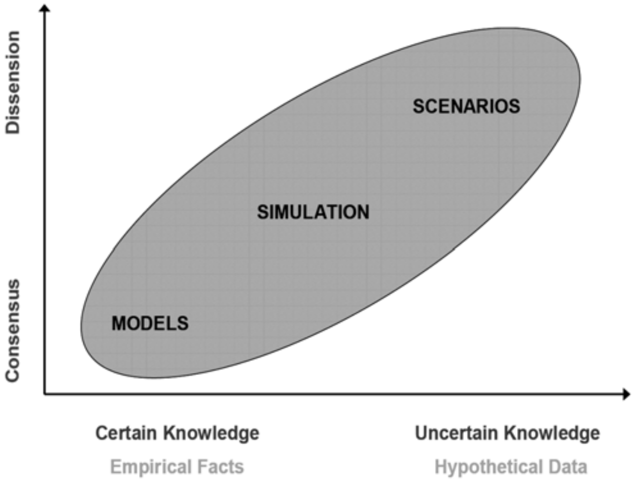

Figure 3: Application Areas of CIP-Methodologies [10]

Critical Infrastructure Modelling Requirements: Various innovative modelling approaches have been developed for infrastructure systems, including agent based modelling; effects-based operations (EBO) modelling; input-output (IO) modelling; models based on game theory; models based on risk; operations research models; dynamic simulation models; as well as systems dynamics modelling. Despite this wide diversity, the modelling of critical infrastructure is complicated by the quality and availability of data, intricacy of systems hierarchical organisational structures, complexity of interactions between infrastructures, and implications and sensitivity of results. Critical infrastructure modelling requires representation of its structural complexity and inherent systems behaviour. The abstraction process will result in a selection of relevant parameters to be used for the description of the selected system, which will assist the ***scalability*** of the model.

Infrastructures can be represented by their hierarchical, organisational structure, starting at the system-of-systems level and moving down to the levels of single infrastructures, systems, subsystems, assemblies, units/components and parts. In looking at the different levels, each level is composed of several elements. Each element contributes to the output of its level, while relying upon components of other levels. These elements are characterised by physical representations and processes, data-based functions and processes, human control and management functions and relations, as well as strategic management functions and external constraints. All these representations have an impact on the capabilities and behaviour of infrastructures. In a hierarchical description of critical infrastructures, different sets of relevant parameters have to be considered for each level according to the operational functions of the level. Flows, time responses etc. have to be studied in each hierarchical level. Whatever level has to be considered, ranging from a set of functional entities to integration of critical infrastructures, there is a limited set of system architectures and behaviour patterns that have certain intrinsic properties. These behaviour patterns have to be studied precisely and care must be taken of not masking their level-intrinsic properties by shifting perspectives from one level to another. A careful level mapping of integrated infrastructures is needed which will assist the ***functionality*** of the models [10].

Furthermore, in many complex networks, the human participant is the most susceptible to failure and the most adaptable in management and recovery. Thus, modelling these networks will need to include modelling the bounded rationality of human thinking and intervention. Modelling will therefore need to be carried out at different resolutions and the various analytical models, simulations and scenarios should differentiate their differences as tools for assessment and prediction in their degrees of certainty and acceptance. This poses significant requirements for the selection and application of appropriate modelling tools and techniques.

Modelling Critical Infrastructure Interdependencies: Although there are many models available for the analysis of individual critical infrastructures, analytical models for their interdependencies are not common. One modelling framework treats interdependent infrastructures as a complex adaptive system (CAS). A CAS is a complex system, such as a critical infrastructure (CI) system, characterized by the following properties [11]:

- The system is constructed of heterogeneous, autonomous, decentralised agents;
- The system is dynamic, because of feedback (learning);
- System agents are self-organising;
- The system is emergent (the whole is greater than the sum of its parts).

Agent-based modelling, dynamic simulation, and social network modelling (including human participation), are techniques that can be employed under this framework. Another method presents a mathematical framework in which infrastructures are modelled as networks with demand for their services, capacity to satisfy their demands, and uncertainty in the supply, demand, and system failure [12].

The illustration in Figure 4 is a simple modification of a structure presented by the U.S. Government National Science Foundation of interdependencies between multiple infrastructure systems. The structure portrays the complexity of infrastructure interdependencies that can exist between critical infrastructure systems [13].

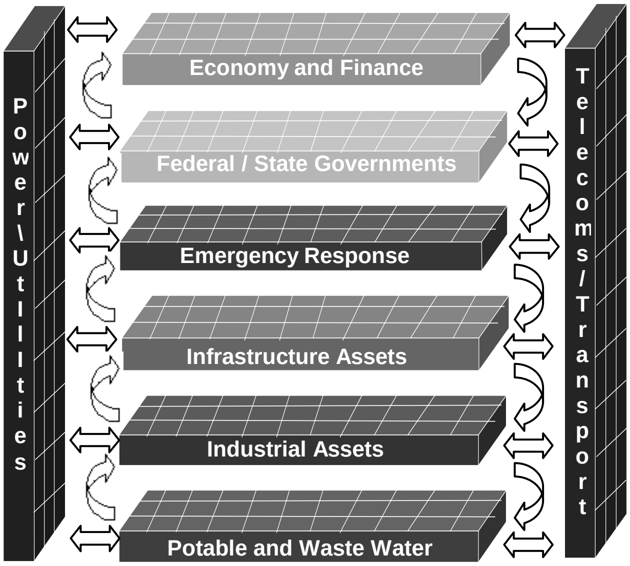

Figure 4: Infrastructure Interdependencies [13]

Modelling complex infrastructure interdependencies that can exist between critical infrastructure systems requires a modelling approach that uses a workbench-toolbox design that combines the simplicity of visual models with easy access to simulation and analysis modelling tools for decision-making. Such modelling also must include impact scenario analysis (ISA) of infrastructure risks induced by natural, technological and intentional hazards. Such a modelling tool is System Dynamics modelling.

SYSTEM DYNAMICS MODELLING

System Dynamics is a methodology for complex problem solving, with simulation and analysis development. System Dynamics was first formulated in the 1960s by Jay Forrester professor in MIT’s Sloan School of Management [14]. Originally, System Dynamics was applied to modelling and problem solving in industrial corporations, but the most famous application of System Dynamics modelling was that of the Club of Rome, contained in its book “Limits to Growth”. Published in 1972, it sold twelve million copies in 37 languages [15]. Whilst the book did not precisely predict infrastructure vulnerabilities, it stated that if the world's consumption patterns and population growth continued at the same high rates of the time, the earth would strike its limits of growth within a century. However, the message was that the predicted outcome was not inevitable and that nations could change their policies - the sooner the better.

System Dynamics can similarly be applied to modelling complex infrastructure interdependencies of critical infrastructure systems, considering various impact scenarios. As an example, the structure presented by the U.S. Government National Science Foundation illustrated in Figure 4 can be simplified to the integrated nodal framework in Figure 5 of the dynamic interrelationships underlying CI systems interdependencies [9].

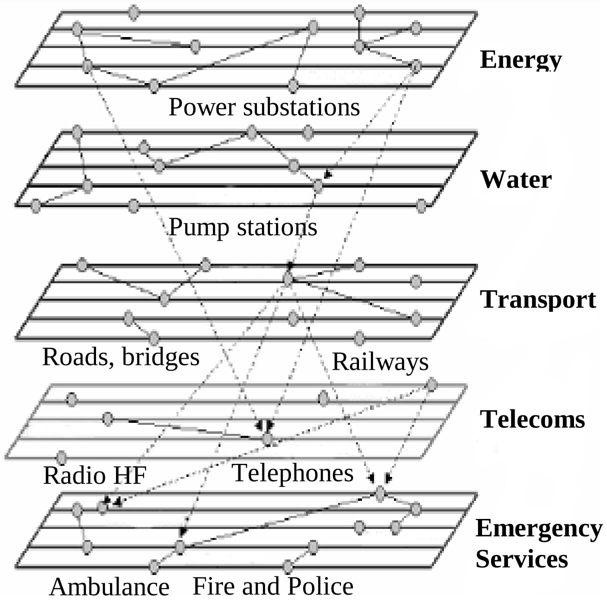

Figure 5: Relationships of CI Interdependencies [9]

Considering the detail interrelationships of the critical infrastructure systems of Figure 4, and the integrated nodal framework of the critical infrastructure systems interdependencies of Figure 5, System Dynamics models of the interrelated nodes and their links can now be modelled taking into account the complexity of these relationships and impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards.

Modelling Construct of System Dynamics:

The System Dynamics approach to complex problems focuses on feedback processes. It takes the philosophical position that feedback structures are responsible for changes over time. The premise is that dynamic behaviour is a consequence of system structure. Figure 6 depicts a System Dynamics construct that begins with an understanding of the system and its inherent dependencies then problem definition, system conceptualization and model formulation, with update feedback loops to a further understanding of the system. From the model formulation of, for example, a critical infrastructure system, the system is then simulated with consideration of infrastructure dependencies and interdependencies [16].

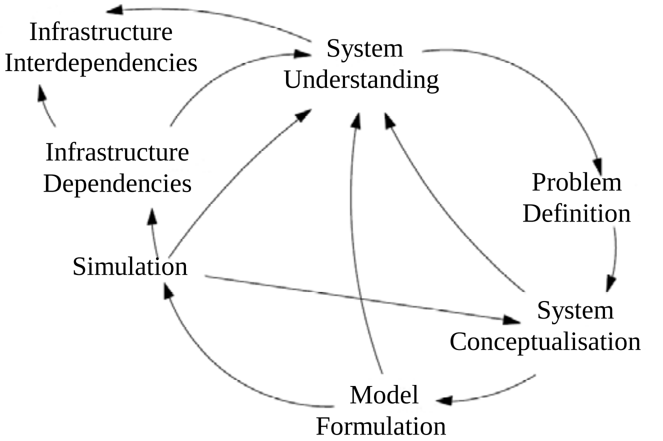

Figure 6: The System Dynamics Construct [16]

Consider the System Dynamics model of Potable and Waste Water critical infrastructure indicated in Figure 4 and illustrated in Figure 7 [17], with *dependencies* of potable water resources inherent to this sector, as well as *interdependencies* with other infrastructure sectors.

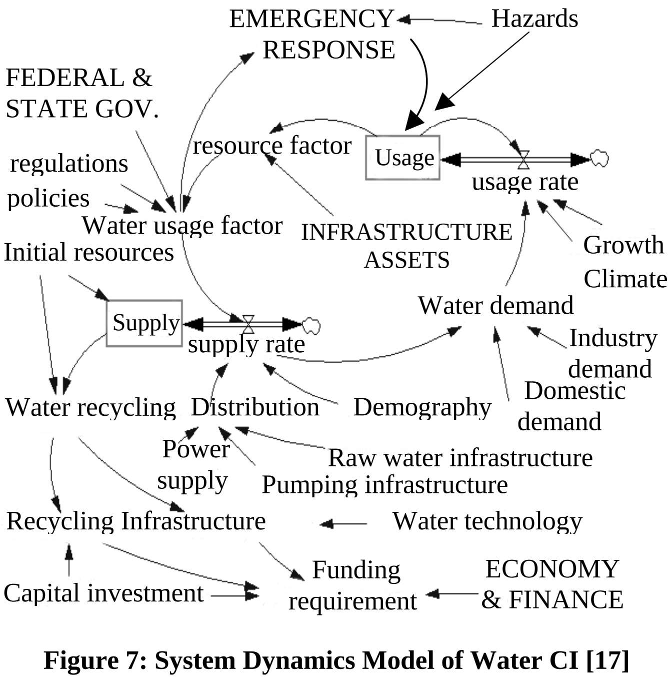

Figure 7: System Dynamics Model of Water CI [17]

Although this modelling approach has merit if attempted on a relatively uncomplicated scale with generalised concepts of complexity, System Dynamics models need to consider the overall comprehensive impact of risks induced by natural, technological and intentional hazards for integrated critical infrastructure systems as depicted in Figure 4, and require greater construct and computing capability than the simplistic examples presented here.

The Australian CIPMA Program is thus being designed to assess complex and critical infrastructure networks. CIPMA was launched in 2006 by the Attorney-General's Department, with a budget of $19 million. The program is being designed to identify the areas of highest risk in Australia's infrastructure and related systems, and to gauge the flow‑on affects if the infrastructure fails or is compromised. The CIPMA initiative is being driven by the CIPMA Development Team, which comprises the Attorney-General's Department, Geoscience Australia and CSIRO. The overall objectives are to [18]:

- Identify connections between and across infrastructure.
- Better understand the behaviour of complex networks.
- Analyse the relationships that exist between critical infrastructure sectors and their interdependencies.
- Examine the cascade effects of infrastructure failure.
- Identify potential points of failure, choke points and other vulnerabilities.
- Assess options for investment in improved security.
- Test mitigation strategies and business plans.

REFERENCES

[1] Australian Government Attorney General's Department (AGD) (2006) "Critical Infrastructure Protection Modelling and Analysis Program", Trusted Information Sharing Network for Critical Infrastructure Protection, Australian Government.

[2] Allen Consulting Group (2005), "Climate Change Risk and Vulnerability", final report, level 11, 77 Eagle St Riverside Centre, Brisbane QLD 4001.

[3] Department of the Environment and Heritage (2005), "Climate Change Risk and Vulnerability: Promoting an Efficient Adaptation Response in Australia", Communications Director, Australian Greenhouse Office, Department of the Environment and Heritage, Canberra ACT 2601.

[4] Rinaldi S., Peerenboom J., and Kelly T., (2001), "Identifying, Understanding, and Analysing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, IEEE, December 2001.

[5] Dudenhoeffer D., Permann M., and Manic M., (2006) "CIMS: A Framework for Infrastructure Interdependency Modelling and Analysis." Proceedings of the 2006 Winter Simulation Conference 2006, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers.

[6] Schmitz W. (2003), "Summary of the Cross Connections Between WP1-WP6 Deliverables [Work packages to provide a roadmap to support development and application of modelling and simulation, gaming and further adequate methodologies and tools for critical infrastructures and their interdependencies]", Work Package ACIP IST-2001-37257, ACIP D6.1 Comprehensive Roadmap, European Commission and Information Society Technology Programme with IABG mbH Einsteinstrasse 20 85521 Ottobrunn Germany.

[7] Strogatz Steven H. (2001) "Exploring Complex Networks", Department of Theoretical and Applied Mechanics and Center for Applied Mathematics, Cornell University, Ithaca, New York 14853-1503.

[8] US National Research Council (2002) "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism", Committee on Science and Technology for Countering Terrorism, The National Academies Press, ISBN: 0309084814.

[9] Pederson P., Dudenhoeffer D., Hartley S., and Permann M. (2006) "Critical Infrastructure Interdependency Modelling: A Survey of U.S. and International Research", Idaho National Laboratory Critical Infrastructure Protection Division Idaho Falls, Idaho 83415

[10] Schmitz W. (2003), "Analysis and Assessment for Critical Infrastructure Protection", Work Package ACIP IST-2001-37257, ACIP D6.4 Comprehensive Roadmap, European Commission and Information Society Technology Programme with IABG mbH Einsteinstrasse 20 85521 Ottobrunn Germany.

[11] Kim H., Biehl M., and Buzacott J., (2005), "Modelling Cyber Interdependencies between Critical Infrastructures", Proceedings of Third IEEE Conference on Industrial Informatics, Australia.

[12] Nozick L., Turnquist M., Jones D., Davis .J., and Lawton C., (2004), "Assessing the Performance of Interdependent Infrastructures and Optimising Investments", 37th Annual International Conference on System Sciences, Big Island, HI.

[13] US Government National Science Foundation (2002), "An Integrated View of the National Science Foundation and Infrastructure Systems Research", authored by Heller M., Program Director, Infrastructure & Information Systems, NSF, 4201 Wilson Boulevard, Arlington, Virginia USA.

[14] Forrester J. W. (1961), "Industrial Dynamics", New York: John Wiley & Sons, Inc. (1968), "Principles of Systems", (second preliminary edition) Cambridge, MA: Wright-Allen Press, Inc. (1969), "Urban Dynamics", Cambridge, MA: The M.I.T. Press. (1971), "World Dynamics", Cambridge, MA: Wright-Allen Press, Inc.

[15] Meadows D.H., Meadows D.H., Randers J., and Behrens W., (1972), "Limits to Growth", report for the Club of Rome's project on the predicament of mankind. Published by arrangement with Universe Books (New York) Potomac Associates, Inc. Washington DC and the Club of Rome, ISBN 0 330 24169 9.

[16] Richardson, G., and. Pugh A., (1996), "Introduction to System Dynamics Modelling", Productivity Press, Portland, Oregon.

[17] Ventana Systems, (2006) "Adaptation of VENSIM System Dynamic Modelling for Examples in Water Provision Critical Infrastructure", www.vensim.com

[18] Bentley A., (2006), "Infrastructure: Critical Mass", CSIRO, Clayton South Victoria 3169, Australia.