THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 10 NUMBER 2

AUGUST 2011

INTERDEPENDENCIES

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

In this issue of *The CIP Report*, we highlight interdependencies between critical infrastructures. While the USA PATRIOT Act definition of critical infrastructure does not explicitly refer to interdependencies, it is generally understood that numerous critical infrastructures depend on other infrastructure systems. Therefore, it is important to understand how damage to one system can impact other systems. However, identifying interdependencies between critical infrastructures is merely the first step. The next step involves implementing solutions to protect interdependent systems. Unfortunately, many of these systems are regulated by different authorities, thus further complicating the analysis and protection of interdependent infrastructures systems. This issue addresses these challenges.

First, the Director of the Pacific Northwest Center for Regional Disaster Resilience, Pacific NorthWest Economic Region (PNWER) discusses the importance of developing and participating in regional interdependencies tabletop exercises to identify infrastructure interdependencies. Then, academicians from the National Central University and the National Science and Technology Center for Disaster Reduction in Taiwan explain their research on designing corresponding tools for disclosing critical infrastructure interdependencies. Next, researchers from City University London describe their approach to interdependency analysis through Preliminary Interdependency Analysis (PIA). Finally, we summarize the recent U.S. Government Accountability Office (GAO) report that addressed the efforts of the U.S. Department of Homeland Security (DHS) to address overlaps and gaps in their approach towards critical infrastructure protection (CIP).

This month's *Legal Insights* examines the challenges involved with overlapping jurisdictions and regulations in critical infrastructure protection.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

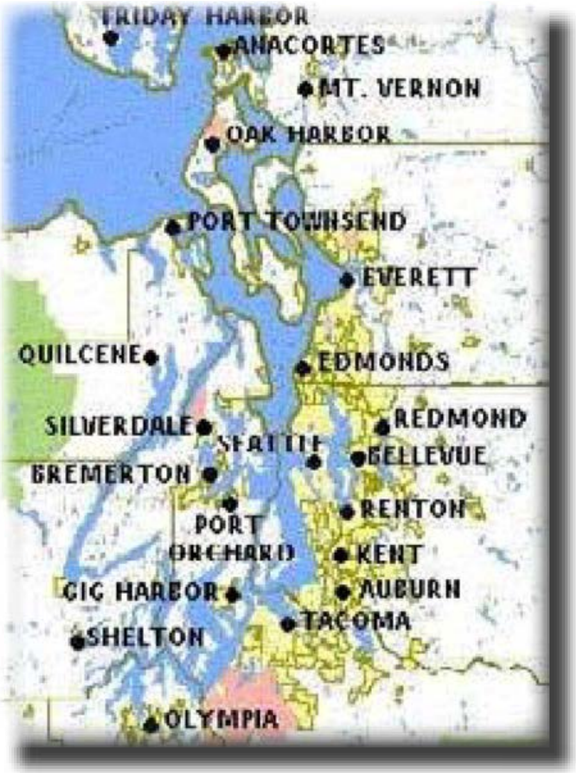
Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Regional Interdependencies Tabletop Exercises: Essential Tool to Improve All-Hazards Security and Resilience

by Paula Scalingi, Ph.D., Director
Pacific Northwest Center for Regional Disaster Resilience,
Pacific NorthWest Economic Region (PNWER)

Since the mid-1990s, an increasing number of practitioners and experts have come to recognize that understanding potential impacts of interconnections among regional infrastructures and essential service providers is fundamental in assuring security and resilience.

Government and business leaders in regions across the Nation and in Canada have developed, or are contemplating, creating public-private partnerships with interdependencies as a primary driver. At the same time, development of capabilities to address interdependencies has been slow at best, hampered by scarcity of available data, constraints on sharing sensitive and proprietary information, and limited assessment tools that can be utilized at the local level for all-hazards planning, situational awareness, and informed decision-making for preparedness, mitigation, response, and recovery.



The Puget Sound region includes the Puget Sound, Puget Sound lowlands, and the surrounding region roughly west of the Cascade Range and east of the Olympic Mountains. It includes nine counties, among them King County, the Nation's 11th largest, which encompasses the Greater Seattle Area.

Decade of Stakeholder Collaboration

The oldest of these interdependency-focused partnerships is in the Puget Sound Region of Washington State. It is facilitated by the Pacific NorthWest Economic Region (PNWER), a cross-border consortium comprised of the states of Washington, Oregon, Idaho, Montana, and Alaska, and the Canadian provinces and territories of British Columbia, Alberta, Saskatchewan, Yukon, and the Northwest Territories. Since late 2001, PNWER, through its Pacific Northwest Center for Regional Disaster Resilience (CRDR), has worked with private, non-profit, and local government organizations and State and Federal partners in an ongoing process to raise awareness of interdependencies, associated preparedness gaps, and prevention and mitigation activities to improve regional preparedness and resilience.

Multi-Step Process

This model approach, which has been customized for other regions in the Nation and in Canada, involves developing an interdependency-focused Regional Resilience Initiative through a multi-step process. This process entails: (1) convening government, private sector, and other organizations and associations with roles and responsibilities or significant interests in disaster

(Continued on Page 3)

Exercises *(Cont. from 2)*

preparedness and continuity; (2) enlisting a "core" group of these organizations to plan and conduct a regional interdependencies workshop; (3) collecting additional lessons learned from sector and other focus groups, interviews, and a stakeholder survey; (4) holding a stakeholder-designed regional infrastructure interdependencies exercise; (5) producing a baseline assessment of current regional capabilities and gaps; (6) integrating outcomes from steps 1 through 5 into an action plan of needs and recommended short (low-hanging fruit), medium, and long-term activities to address these needs; (7) prioritizing the action plan activities and validating it in a final regional workshop; and (8) establishing work groups to develop requirements and identify project lead organizations and resources (funds and expertise) for action plan implementation.

The *Blue Cascades* Exercise Series

Regional interdependency tabletop exercises have been an integral element of this multi-step process since PNWER began its infrastructure security and disaster resilience activities. Regional tabletops are not used to test plans, but are scenario-focused, intensive, and highly-interactive workshops that enable diverse stakeholders to share information in a trusted environment and explore first-level, and in some cases, second and third-level interdependencies. It is not uncommon for participants in developing these exercises to uncover unknown key linkages that could cause significant challenges under certain conditions.

The first of PNWER's interdependency exercises, called *Blue Cascades*, was modeled directly on an innovative stakeholder-designed regional tabletop — *Black Ice* — developed by the U.S. Department of Energy's (DOE) Office of Critical Infrastructure Protection with Salt Lake City area infrastructures examining potential disruptions from a severe blizzard impacting the 2002 Winter Olympics. *Blue Cascades I*, held in September 2002, focused on a physical terrorist attack on energy systems and other infrastructures. Subsequent *Blue Cascades* tabletops focused, respectively, on cyber and critical information technology (IT) systems security (*Blue Cascades II*, 2004); a 9.0 subduction zone earthquake (*Blue Cascades III*, 2006); pandemic preparedness (*Blue Cascades IV*, 2007); post-disaster supply chain resilience (*Blue Cascades V*, 2008); and health and safety impacts from combined catastrophic flooding during a pandemic (*Blue Cascades VI*, 2010).

For each of these exercises, a stakeholder Scenario Design Team of 30 to 40 utilities, businesses, non-profits, and local, State, and Federal agencies met in person and through bi-weekly conference calls crafted a multi-faceted narrative covering a broad array of interdependencies disruptions and health and safety, economic, environmental, and societal impacts. The Scenario Design Team developed the timeline based on their organization's greatest continuity or security concerns, providing "injects" (scenario events) concerning assets, systems, operations, and business practices. The Team developed questions to illuminate issues associated with assessing interdependencies; cyber

(Continued on Page 4)

In Blue Cascades VI, held March 2010, stakeholders convened in Seattle to examine interdependencies impacts of a major flood during a pandemic.

Exercises *(Cont. from 3)*

Center for REGIONAL DISASTER RESILIENCE

threats and incidents; risk assessment and mitigation; cooperation and coordination; information sharing and alert and warning; reliable, resilient interoperable communications and IT systems; roles and responsibilities; recovery and reconstitution; business continuity and continuity of operations; logistics and supply chain resilience; human factors and at risk populations; public information and risk communications; exercises, training and education; and post-disaster assistance. The Scenario Design Team members reviewed all scenario drafts, provided background materials, and in some cases, facilitated their own injects during the exercise. Lessons learned and recommended improvement activities from each of the six regional tabletops were successively compiled in stakeholder-validated action plans, which in turn were incorporated into an updated *Integrated Action Plan*. In effect, this *Integrated Action Plan* is a compendium of stakeholder recommended mitigation activities spanning the last ten years and a regional resilience status report that charts progress made in terms of activities completed, underway, or yet to be initiated.

Addressing Interdependency-Related Needs

Through this ongoing, multi-step process that has regional interdependency exercises as an integral element, Puget Sound stakeholders have been able to complete just under a third of the 115 recommended activities from all six *Blue Cascades* exercises. Some of these activities have been supported by State agencies and King County, the City of Seattle, and other localities with private sector funds or in-kind contributions. Several projects have been sponsored by Federal agencies, including various components of DOE, DHS, Defense Threat Reduction Agency (DTRA) , U.S. Department of the Navy, and U.S. Army Corps of Engineers.

PNWER's Center for Regional Disaster Resilience has had a lead role in many of these implementation activities, including development with the Washington State Fusion Center of a cross-sector information sharing and analysis capability; an interdependencies identification template for use by regional stakeholders; a regional risk mitigation strategy for the Tri-Cities Area of Washington State focusing on dam and levee resilience; a Northwest Warning and Alert Network (NWWARN) for public and private real-time sharing of situational information; creation of a regional public-private information security consortium — the Northwest Alliance for Cyber Security; regional energy assurance and resilience planning; a comprehensive Community Bio-Event Resilience Pilot Project to examine stakeholder needs in major health-related events; and facilitation of a Pacific Northwest Critical Infrastructure Protection (CIP) Task Force of CIP managers from the PNWER member jurisdiction states and provinces.

In the area of training and exercises, the CRDR with stakeholders, in addition to the *Blue Cascades Series*, has conducted several dozen seminars, workshops, and targeted tabletop exercises on all-hazards threats and interdependencies and related specialized topics. These topics include National Incident Management System (NIMS) for private sector organizations; cybersecurity and process control systems; catastrophic bridge collapse issues and transportation resilience; post- catastrophic flood recovery; business and manufacturing supply chain resilience; communications and information sharing; cross-border health resilience; agriculture and livestock response and recovery issues; and bio-attack restoration needs.

Value Added of Interdependency Exercises

Based on the above positive outcomes for Puget Sound Partnership members, regional interdependency exercises clearly

(Continued on Page 19)

Disclosing Interdependencies between Critical Infrastructure: Steps, Tools, and Examples

by Ssu-Min Tseng, Graduate Research Assistant, Department of Civil Engineering, National Central University, Taiwan; Ting-Wu Ho, Graduate Research Assistant, Department of Civil Engineering, National Central University, Taiwan; Cheng-Ting Chiang, Graduate Research Assistant, Department of Civil Engineering, National Central University, Taiwan; Jau-Lang Su, Head of Technology and Manmade Disasters Reduction Division, National Science and Technology Center for Disaster Reduction, Taiwan; and Chien-Cheng Chou, Associate Professor, Department of Civil Engineering, National Central University, Taiwan

Introduction

Critical infrastructure (CI) is broadly defined as a set of important assets for producing or distributing a continuous flow of essential goods or services of a country (Rinaldi et al., 2001). Since operating a CI system usually requires support from other CI systems, these interactions often create complex relationships or so-called interdependencies that cross system boundaries (Haimes, 2005). For example, in a water supply system, adding a new water pump station can serve more nearby communities but also creates a dependent relationship with the power system. Research has shown that in order to actively reduce the impact of a disaster, disaster management officials should focus more on the damage caused during and after the disaster (Laefer et al., 2006). Given that most of the damage during and after a disaster can be attributed to CI interdependencies, disclosing interdependencies between CI systems is the topic that needs more comprehensive and systematical studies.

Recent research has designed several modeling approaches to describing CI interdependencies; however, these models cannot precisely render actual relationships between CI systems and/or their components in accordance with the interdependency types and attributes (Chou and Tseng, 2010).

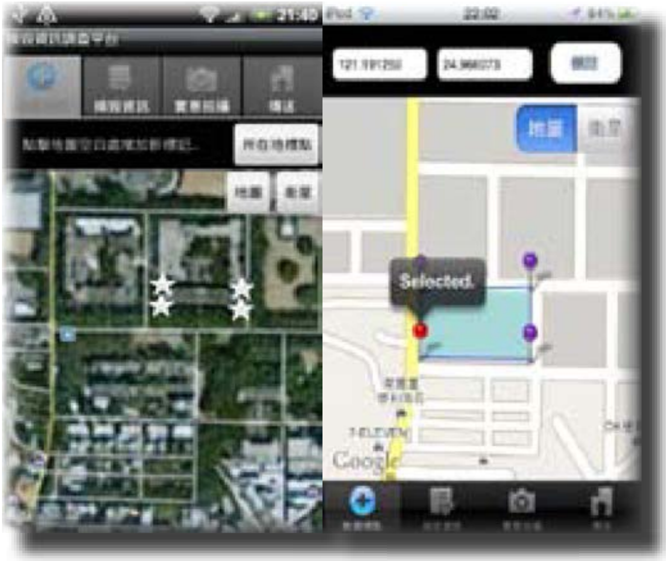


Figure 1: Using CIFC to mark the boundary of a failed CI system. (Left): on Android platform; (Right): on iPhone platform.

In addition, after one CI system stops, it may take some time to let another system cease to function. The spatial dimension has been incorporated into many CI interdependency models; nevertheless, the time dimension is required to record every event during and after a disaster but currently does not exist in such models. This research aims to propose a process and to design corresponding tools for disclosing CI interdependencies. The authors believe that a comprehensive understanding of how networked CI systems work and interact with respect to time can provide the means to better evaluate vulnerabilities related to hazards.

Steps and Tools for Disclosing CI Interdependencies

Detailed explanation of the steps for disclosing CI interdependencies can be found in CI paper published by the American Society of Civil Engineers (Chou and Tseng, 2010). The basic strategy is that historical CI failure records should be collected, synthesized, and analyzed. Patterns of CI interdependencies then can be disclosed using a data mining algorithm, namely Generalized Sequential Pattern (GSP) discovery. A post-

(Continued on Page 6)

Interdependencies Models *(Cont. from 5)*

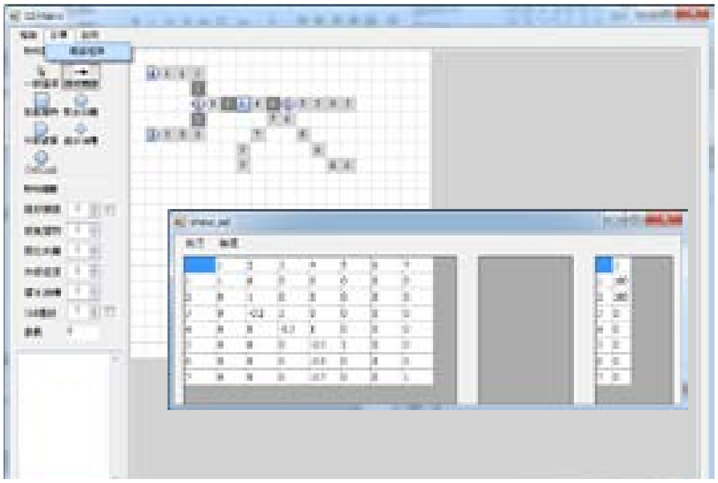
process tool was developed to help efficiently and effectively identify interesting patterns in accordance with the parameters specified by users. Currently, an integrated decision framework, consisting of several computerized tools for ease of the aforementioned tasks, is being developed. The following paragraphs describe each tool developed for this research.

Briefly, the process of disclosing CI interdependencies begins with collection and integration of historical failure records of CI systems in the study area. A tool, called CI Failure Information Collector (CFIC), has been developed using the Android and iPhone platforms (see Figure 1 on Page 5).

Users can utilize CFIC to mark the boundary of a CI system that triggered a failure event. The event time and associated attributes information can be entered in the subsequent forms of the Android or iPhone platforms. The authors assume that if an external disruption occurs and directly damages one component of CI, it may further trigger a series of failure events pertaining to several CI systems. After proper collection of the external disruption information and all of the consequent failure records, a sequence with an ordered list of events can be automatically produced using CFIC. Once a sufficient number of such sequences has been collected, use of GSP can generate CI interdependency patterns that serve as an important role in disaster mitigation.

Then, a modeling tool called CI Interdependency Modeler (CIIM), which is currently being developed, can help map the patterns generated to the corresponding interdependency model (see Figure 2).

Figure 2: Using CIIM to map the patterns generated to the corresponding CI interdependency model



It should be noted that the CI inoperability input-output model proposed by Haimes (2005) and the Infrastructures Interdependencies Simulation (I2Sim) model proposed by the research team at the University of British Columbia require a matrix structure denoting interdependencies between CI systems. Hence, our CIIM is designed to help users build the matrix. Ideally, if an external disruption has only one-time impact on a CI, and if interdependencies between CI systems do not change over time, the final state of each CI system due to interdependencies can be computed directly. More sophisticated features such as the dynamic state and matrix of CIIM are being developed in order to best describe CI interdependency relationships over time.

Finally, a Post-process CI interdependency Patterns Discovery (PCPD) tool was developed to efficiently and effectively identify interesting patterns (see Figure 3 on Page 16).

The authors assume that disaster mitigation officials should know current failure events and would like to see what future events will occur, based on historical failure information analyzed. This tool can provide a better classification of the patterns so that the officials can retrieve relevant information on demand. In addition, the sequential patterns generated could be used to analyze the possibility of breaking the failure chain for CI interdependency-related disaster mitigation. Since related failure events occur sequentially, a mechanism similar to the firewall concept could be employed to limit the spread of CI interdependency failures. For instance, if a water pump station is very important for nearby communities, an alternative power source should be established for it, as long as its original power supply component is identified as the firewall component.

Conclusions

With the ever-increasing demand

(Continued on Page 18)

Preliminary Interdependency Analysis (PIA): Summary of the Method and Tool Support

by Robin Bloomfield, Nick Chozos, and Peter Popov,
Adelard LLP, London, UK
Centre for Software Reliability, City University London

Introduction

One of the greatest challenges in enhancing the protection of CIs against accidents, natural disasters, and acts of terrorism is establishing and maintaining an understanding of the interdependencies between infrastructures and the dynamic nature of these interdependencies. Interdependency can be a source of "unforeseen" threat when failure in one infrastructure may cascade to other infrastructures, or it may be a source of resilience in times of crisis; e.g., by re-allocating resources from one infrastructure to another.

Understanding interdependencies is a challenge both for governments and for infrastructure owners and operators. Both, to a different extent, have an interest in services and tools that can enhance their risk assessment and management to mitigate large failures that may propagate across infrastructures. However, cost of investment in infrastructure modelling and interdependency analysis tools and methods, including the supporting technology, may reach millions of pounds, depending on the size of the system to be modelled, on the level of detail, and on the mode of modelling (real-time or off-line). These factors will determine the software, hardware, data, and personnel requirements.
It is therefore very important to understand what the scope and the overall requirements of an interdependency analysis service are going to be before proceeding with such an investment. However, the decision on what modelling and visualisation capabilities are needed is far from simple. Detailed requirements may not be understood until some modelling and simulation has already been conducted, in order to identify critical dependencies and decide what level of fidelity is required to investigate them further.

This article presents an approach to interdependency analysis that attempts to address these challenges; the approach — Preliminary Interdependency Analysis (PIA) — starts off at a high-level of abstraction, supporting a cyclic, systematic thought process that can direct the analysis towards identifying lower-level dependencies between components of CIs. Dependencies can then be analysed with probabilistic models, which would allow one to conduct studies focused on identifying different measures of interests, e.g., to establish the likelihood of cascade failure for a given set of assumptions, the weakest link in the modelled system, etc. If a high-fidelity analysis is required, PIA can assist in making an informed decision of what to model in more detail. The method is applicable as both:

1) A lightweight method and accessible to Small-to-Medium Enterprises (SMEs) in support of their business continuity planning (e.g., to model information infrastructure dependencies, or dependencies on external services such as postal services, couriers, and subcontractors); and

2) A heavyweight method of studying with an increasing level of detail the complex, regional, and nationwide CIs combining probabilistic and deterministic models of CIs.

PIA is supported by a toolkit; the PIA Toolkit is based on two, 3rd party software applications:

PIA Designer: This allows a modeller to define a model of interdependent CIs and define the parameters needed for any quantitative study. For visual representation, the tool uses a proprietary tool *Asce* (http://www.csr.city.ac.uk/projects/cetifs.html); and

Execution Engine: This allows for executing a model developed with the PIA Designer, i.e., a simulation study based on the model to be conducted and the measures of

(Continued on Page 8)

Preliminary Analysis *(Cont. from 7)*

interest to be collected. The Execution Engine uses *Möbius* (http://www.mobius.illinois.edu/), customised extensively with a bespoke proprietary development.

The current version of the toolkit allows for two main categories of models:

- Model of interdependent CIs at a fairly high level of abstraction (i.e., without detailed modelling of the networks used by the respective services). The model can be parameterised and then the simulation executable can be deployed on the Execution Engine.

- As above, but adding any degree of detail that the modeller may consider necessary, including high fidelity deterministic models available as 3rd party software modules.

The method supported by the toolkit was successfully applied to a range of case studies — from a relatively simple IT infrastructure of an SME (a couple of dozens of modelled elements) to a regional system of two CIs, namely the power grid and telecommunication network around Rome, Italy (with 800+ modelled elements).

Method: Preliminary Interdependency Analysis

PIA is an analysis activity that seeks to understand the range of possible interdependencies and provide a justified basis for further modelling and analysis. Given a collection of CIs, the objectives of PIA are to develop, through a continuous, cyclical process of refinement, an appropriate *service model* for the infrastructures, and to document assumptions about resources, environmental impact, threats, and other factors.

PIA has several benefits. In particular, PIA can:

- Help one to discover and better understand dependencies which may be considered as "obvious" and as such are often overlooked (e.g. telecommunications need power);

- Support the need for agile and time-efficient analyses (one cannot always wait for the high fidelity simulation); and

- Be used by SMEs, not just infrastructure owners and government.

PIA allows for the creation and refinement of interdependency models, in a focused manner, by revisiting earlier stages in the PIA process in the light of the outcomes of latter stages. For example, an initial application of PIA should result in a sufficiently concrete and clearly defined model of CIs (and their dependencies). However, following the first design iteration, an analysis of the model could cause one to question the assumptions made earlier in the design process. As a consequence, the model may be revised and refined; as we shall see later on, revisiting previous phases of the development process is a key aspect of the PIA method and philosophy overall.

PIA is broadly broken up in two parts:

Qualitative Analysis: The modelling exercise begins with a definition of the boundaries of the system to be studied and its components. Starting off at a high-level, the analyst may go through a cyclical process of definitions, but may also be focused on a particular service; therefore, the level of detail may vary between the different parts of the overall model. The identification of dependencies (service-based or geographical) will start at this point.

Quantitative Analysis: The models created during the qualitative PIA are now used to construct an executable, i.e. a simulator of the model behaviour in the presence of failures of the modelled entities for the chosen model parameterisation. The model parameterisation may be based either on expert judgement or on analysis of incident data. Examples of such data analyses and fitting the available data to plausible probabilistic data models was presented in the recent WP1 deliverable.[1]

The PIA Toolkit provides support for both the qualitative and quantitative analyses. Figure 1 (on Page 9) illustrates an overview of the method and the toolkit.

(Continued on Page 9)

[1] PIA: FARA Project, WP1 Deliverable, "Industrial Sector-Based Modelling of 1337 Critical Infrastructure Incidents in the European Union," Adelard document reference D/496/12102/1, Issue 1, April 2010.

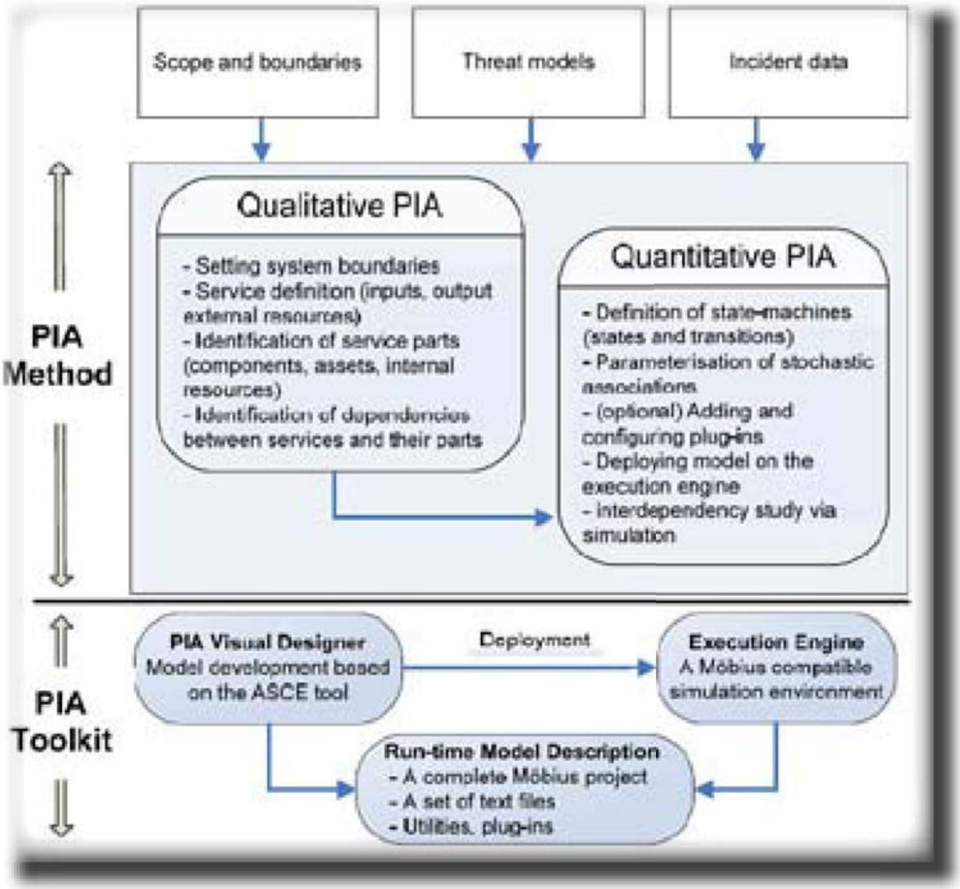
Preliminary Analysis *(Cont. from 8)*

The interdependency models, of course, have to be related to a purpose and this should be captured in terms of a scenario and related requirements. The narrative aspect of the scenario is enormously important as it provides the basis for asking questions and discovering interdependencies as the starting point for more formal models. Typically the systems of interdependent CIs of interest are complex. They include many services, which in turn consist of many parts. Given the complexity and size of the analysed systems, tool support is essential.

PIA Model Architecture: Two Levels of Abstraction

PIA models broadly operate at two distinct levels of abstraction.

Figure 1: Overview of PIA Method and Toolkit


Scope and boundaries
Threat models
Incident data
PIA Method
Qualitative PIA
- Setting system boundaries
- Service definition (inputs, output external resources)
- Identification of service parts (components, assets, internal resources)
- Identification of dependencies between services and their parts
Quantitative PIA
- Definition of state-machines (states and transitions)
- Parameterisation of stochastic associations
- (optional) Adding and configuring plug-ins
- Deploying model on the execution engine
- interdependency study via simulation
PIA Toolkit
PIA Visual Designer
Model development based on the ASCE tool
Deployment
Execution Engine
A Möbius compatible simulation environment
Run-time Model Description
- A complete Möbius project
- A set of text files
- Utilities, plug-ins

Model of Interacting Services (service-level model): The modelled CIs are represented by a set of interdependent services. Here, the view is purposefully abstract so we can reason about dependencies among the services (i.e., data centre X depends on power plant Y). Service-level dependencies are elicited by the defined lower-level dependencies among each service's constituent entities (physical components, resources, etc.). These associations among components are referred to within PIA as *coupling points*. The coupling points *incoming* to a service can be associated with the resources that the service requires (e.g., a telecommunication service consumes "commodities" supplied by a power service). The resources consumed by a service can be obtained from the organisation's reserves (*internal resources*) or provided by another organisation (*external resources*). The *outgoing* coupling points instead define how the outputs from a service get consumed by other services (as either inputs or resources).

Detailed Service Behaviour Model (DSBM): Implementation details are provided for an *individual service*, e.g. the networks upon which a particular service relies. For instance, a GSM telecommunication operator typically relies on a network of devices deployed to cover a particular area (e.g. masts, etc.). Via DSBM, we can choose the level of detail used to model these networks.

In the example above, DSBM may range from a connectivity graph — which cells of the network are connected with each other to a high-fidelity model of the protocols used in the GSM network. We tend to think of DSBM as the networks owned (at least partially) and/or maintained by the respective service operator, i.e., an organisation. Although such a view is not necessary, it allows one to model, via DSBM, several important aspects. For instance, the level of investment and the culture (strong emphasis on engineering vs. outsourcing the maintenance) within the organisation will affect how well the network is maintained (i.e., frequency of outages and speed of recovery). Thus, the process of

(Continued on Page 10)

Preliminary Analysis *(Cont. from 9)*

recovery (a parameter used in DSBM) can be a useful proxy of the level of investment. Through DSBM, one can study scenarios which at first may seem outside the scope of PIA. An example of such a scenario would be comparing the deregulation vs. tight regulation in critical CIs.

PIA Stages

PIA is carried out in seven stages (see Figure 2):

Qualitative Stages:

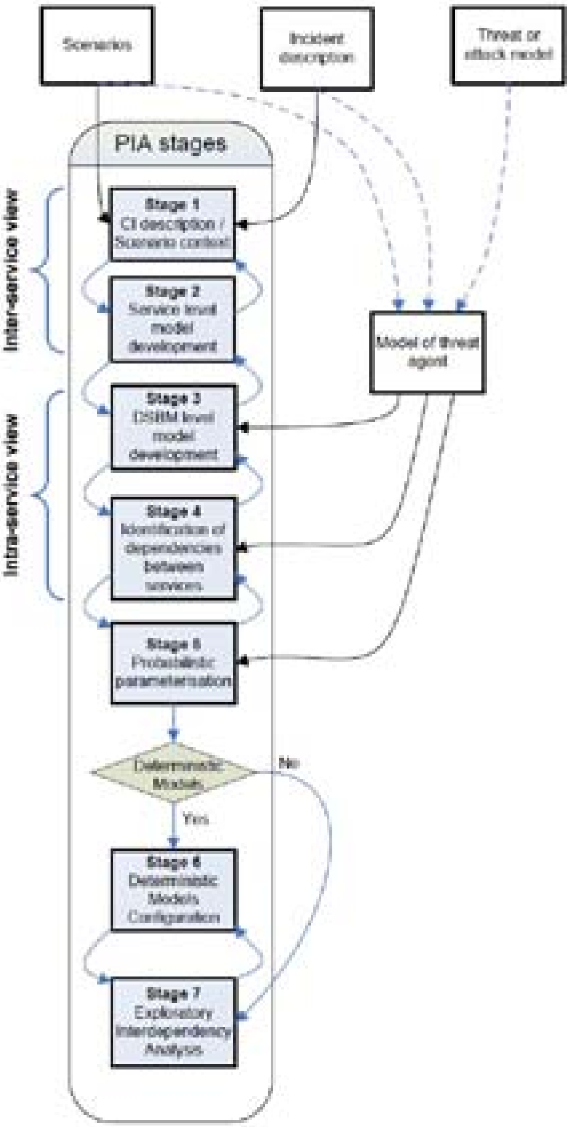
Stage 1: CI Description and Scenario Context: A CI description provides a concrete context and concept of operation. This is the first level of scoping for the analysis task; the CI description provides the first indications of analysis boundaries. DSBM entities are identified and recorded.

Stage 2: Model Development: A model of the services (resources, inputs, outputs, system's, and states) and the operational environment and system boundaries are developed, based on the CI description. Model boundary definitions are used at this stage to further restrict the scope of the analysis. Dependencies between the services are identified and the coupling points are defined: these refer, on the one hand, to the inputs and resources required by each of the services and, on the other hand, to the outputs that each of the services produces.

Stage 3: DSBM Model Development: DSBMs are defined by selecting the right level of abstraction for the services: some of the services may be treated as black-boxes. In this case, their representation in the DSBM will require no refinement in comparison with Stage 2. For those services, which are modelled in more detail, one starts by defining explicitly their components and the assets, including using existing models of the underlying physical networks used by the services. A level of consistency is achieved between the service model and DSBM: the coupling points appear in both views.

Stage 4: Initial Dependency and Interdependency Identification: While some of the service dependencies have already been identified and recorded in Stage 2 (via input/output/resource identification), at this stage, the modeller looks for additional sources of dependence (e.g., common components/assets). This may make several services vulnerable to common faults or threats. These can be derived by examining the service-level model, taking into account other contextual information (e.g., scenarios, threat models, and attacker profile). The captured dependencies are modelled as stochastic association between the services or components thereof. Each stochastic association is seen as a relationship between a parent and a child: the state of the parent affects the modelled behaviour of the child.

Figure 2: PIA Method Stages


Scenarios
Incident description
Threat or attack model
PIA stages
Inter-service view
Intra-service view
Stage 1
CI description / Scenario context
Stage 2
Service level model development
Stage 3
DSBM level model development
Stage 4
Identification of dependencies between services
Stage 5
Probabilistic parameterisation
Model of threat agent
Deterministic Models
No
Yes
Stage 6
Deterministic Models Configuration
Stage 7
Exploratory Interdependency Analysis

Stage 5: Probabilistic Model Development: Since we are dealing with risk, we take the view that, given the state space formed by the modelled entities (MEs), a

(Continued on Page 17)

DHS Addresses Overlaps and Gaps in CIP

This May, the U.S. Government Accountability Office (GAO) responded to an inquiry from the House Committee on Homeland Security by briefing the committee on existing DHS efforts to address overlaps and gaps in their CIP efforts.[1] The briefing contains overviews of both CIP in general and DHS programs specifically, as well as the methodology GAO used for this inquiry and their main findings. Generally, GAO found that DHS is leveraging existing CIP coordination mechanisms to identify overlaps and gaps. In addition, DHS is addressing overlaps and gaps by further clarifying the different roles of the various Federal agencies with regulatory authority by using existing coordination mechanisms, including memoranda of understanding (MOUs) and working groups.

GAO arrived at these conclusions after a multi-faceted investigation, including review of existing planning and review documents, a nine month performance audit, and discussion with a broad range of stakeholders. GAO engaged these stakeholders to solicit their views on DHS efforts to identify and address the overlaps and gaps that they experience in regulation and operation of critical infrastructure. These stakeholders included representatives from 9 of the 18 critical infrastructure sectors; officials at DHS, the Federal Energy Regulatory Commission (FERC), and the Nuclear Regulatory Commission (NRC); homeland security officials from three states; and officials from a private sector company and an industry association.

DHS coordination with critical infrastructure partners to identify gaps and overlaps occurs within several existing coordination mechanisms, including direct correspondence between DHS as a Sector Specific Agency and relevant Federal regulators, communication with State officials with critical infrastructure responsibilities, and meetings between the many entities explicitly purposed to identify relationships between sectors, such as the Government Cross-Sector Council and the sector Government Coordinating Councils. To address the gaps and overlaps once they have been identified, DHS leverages relationships with Federal regulators with potential overlapping jurisdictions to clarify and harmonize differing roles and responsibilities. To illustrate this process in action, DHS identified the Chemical Facility Anti-Terrorism Standards (CFATS) as a significant source of potential duplicative effort and has therefore sought out coordination with the U.S. Coast Guard to clarify where and how both CFATS and the Maritime Transportation Security Act (MTSA), the USCG's purview, would regulate any given facility. To that effect, a MOU and working groups has increased coordination and reduced duplicative efforts. DHS has also identified possible overlaps related to CFATS with the NRC, the U.S. Environmental Protection Agency, and the Bureau of Alcohol, Tobacco, and Firearms and is pursuing similar outreach and coordination to clearly establish the different regulatory jurisdictions.

Gaps in CIP can only be filled with more information. Therefore, DHS also engages in several activities designed to reveal what gaps exist in the current state of CIP. These activities include developing and distributing tailored security tools (e.g., a tool specific to the needs of NASCAR), conducting training and exercises, and conducting vulnerability and security assessments that lead to specific remediation procedures for owners and operators.

In conclusion, the GAO report highlighted the efforts of DHS to avoid confusion and redundancies, especially with regards to overlapping sectors and interdependent infrastructures. ❖

[1] GAO-11-537R, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*, (May 19, 2011), http://www.gao.gov/new.items/d11537r.pdf.

Legal Insights

Interdependent Infrastructure and Overlapping Jurisdiction

The identification of interdependencies among critical infrastructure is one of the most important and challenging tasks that faces the critical infrastructure community. This task is both important and challenging given the potential for cascading events among infrastructure systems. The cascading effects of interdependency was demonstrated in 1998, when the loss of a single telecommunications satellite "led to an outage of nearly 90% of pagers nationwide" and effected the banking, financial services, and emergency services networks.[1] The cascading events scenario has been increasingly complicated by the recent technological advances that have made cascading interdependency situations even more dangerous. Furthermore, once the challenges are recognized, it is often even more difficult to implement solutions since critical infrastructure interdependency are complex systems that involve multiple regulatory authorities. Critical infrastructure interdependency are difficult to understand,[2] and even once vulnerabilities are identified, addressing them is a difficult task in its own right. As discussed in the previous article, GAO illustrated this in a recent report by analyzing potential regulatory overlaps with CFATS. The GAO report discussed how a facility that falls under CFATS could also be regulated by MTSA — which could result in "maritime facilities where part of the facility is subject to MTSA regulations while another part of the facility is subject to CFATS."[3] There is ongoing work to identify potential overlaps with CFATS and cybersecurity regulations and NRC authority. As is evident, interdependencies among critical infrastructures can create a morass of regulations which is difficult for regulators to execute and for owners and operators to understand and effectively navigate.

The response to overlapping jurisdictional problems and the underlying potential for cascading effects has been the development of partnerships that span sectors and span the private – public divide. The *National Infrastructure Protection Plan* (NIPP) provides a legal framework for coordination to address interdependency issues via the Critical Infrastructure Partnership Advisory Council (CIPAC).[4] A variety of partnerships were created that "fosters relationships and facilitates coordination within and across CIKR sectors" and importantly across public and private lines. These partnerships include private owners and operators, and officials from all levels of government. Although most of the actual work of these partnerships is not released to the public due to security concerns, an overview of their form will provide an informative look into the problems they were created to solve.

The private sector cross-sector

(Continued on Page 13)

[1] Steven Rinaldi, James Peerenboom, and Terrence Kelly, *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, (2001).

[2] See *National Infrastructure Protection Plan* (NIPP) (2009), noting that "[i]nterdependency analysis is often so complex that modeling and simulation capabilities must be brought to bear," 19.

[3] GAO Letter to the Honorable Bennie G. Thompson and the Honorable Sheila Jackson-Lee, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlap sand Gaps in Critical Infrastructure Security Activities* (2011).

[4] *National Infrastructure Protection Plan* (NIPP) (2009), available at http://www.dhs.gov/xlibrary/assets/NIPP_SectorPartnership.pdf.

[5] Available at http://www.dhs.gov/xlibrary/assets/NIPP_SectorPartnership.pdf.

[6] Testimony of Kenneth C. Watson, Vice Chairmen, Partnership for Critical Infrastructure Security, Inc. (PCIS) before the Senate Homeland Security and Government Affairs Committee, July 12, 2007, available at (http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=5fbc72dd-3dc6-4f21-9119-e49cca0d9fc6).

Legal Insights *(Cont. from 12)*

coordinating council,[6] whose active body is the Partnership for Critical Infrastructure Security (PCIS), "serves as a forum where cross-sector issues and interdependencies are addressed."[7] The cross sector coordinating council is composed of leadership from each of the Sector Coordinating Councils (SCCs), which are "self-organized, self-run, and self-governed" and composed of critical infrastructure owners and operators.[8] Two of PCIS' goals are to: (1) facilitate cross-sector collaboration with the government; and (2) identify cross-sector and interdependency risks and potential solutions. In order to achieve these goals, PCIS creates groups focused on a particular task such as the Interdependencies Committee and the Cross-Sector Cyber Security Working Group. These initiatives have resulted in briefings to congressional leaders regarding cross-sector threats and a comprehensive cross-sector study on critical interdependencies. The PCIS thus represents the private side owners and operators of critical infrastructure and is a forum for cross-sector discussion.

The public counter-part to PCIS is the Government Cross Sector Council (GCSC). The GCCS is composed of two sub-councils: the NIPP Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). The FSLC is composed of the "Sector-Specific Agencies for each of the CIKR sectors as well as several additional agencies named in HSPD-7"[9] while the SLTTGCC connects "State, local and tribal homeland security partners" in order to coordinate efforts across jurisdictions. The SLTTGCC is focused on addressing "issues and interdependencies across all sectors" and does so through a diverse membership gathered from across the country.[10] Similar to the PCIS, the SLTTGCC conducts much of its work through smaller focused groups, including the Communication and Coordination Working Group and the Regional Partnership Working Group. Together, these entities are used to address "[c]ross-sector issues and interdependencies."[11]

In addition to the standing councils described above, regional councils are created to coordinate across geography and sectors which are collectively known as the Regional Consortium Coordinating Council.[12] These are "self-organized, self-governed bod[ies]" involving "multijurisdictional, cross-sector, and public-private

(Continued on Page 17)

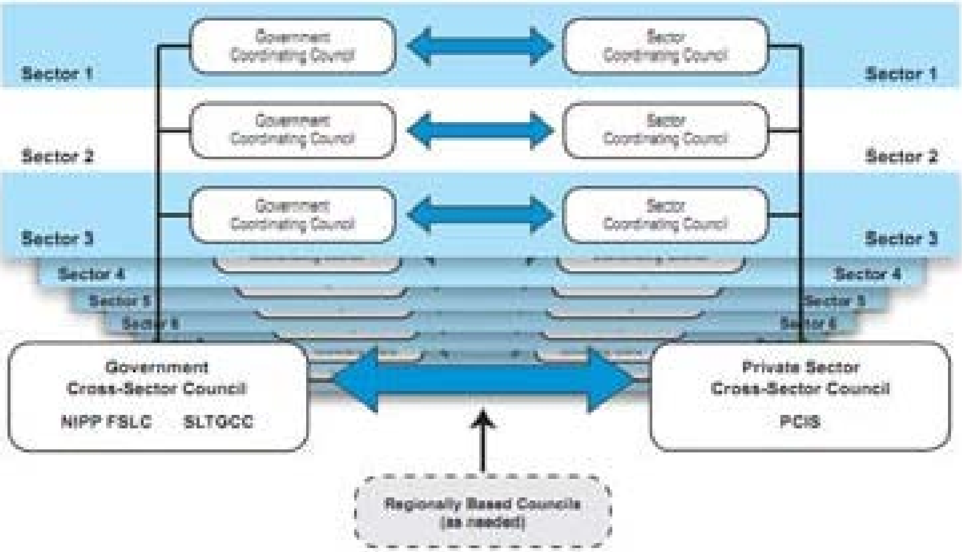

Sector 1
Government Coordinating Council
Sector Coordinating Council
Sector 1
Sector 2
Government Coordinating Council
Sector Coordinating Council
Sector 2
Sector 3
Government Coordinating Council
Sector Coordinating Council
Sector 3
Sector 4
Sector 4
Sector 5
Sector 5
Sector 6
Sector 6
Government
Cross-Sector Council
NIPP FSLC
SLTGCC
Private Sector
Cross-Sector Council
PCIS
Regionally Based Councils
(as needed)

Figure 1: National Infrastructure Protection Plan Sector Partnership Model

[7] http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/CIKRpartnerships.htm#item3.
[8] http://www.dhs.gov/files/partnerships/editorial_0206.shtm.
[9] http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/CIKRpartnerships.htm#item4.
[10] *Critical Infrastructure Partnership Advisory Council Annual* (2010), 8, available at http://www.dhs.gov/xlibrary/assets/cipac/cipac-annual-2010.pdf.
[11] *National Infrastructure Protection Plan Sector Partnership Model* (2009), available at http://www.dhs.gov/xlibrary/assets/NIPP_Sector Partnership.pdf.
[12] *Critical Infrastructure Partnership Advisory Council Annual* (2010).

Curriculum for Seven Graduate Courses in Critical Infrastructure Protection

The Center for Infrastructure Protection and Homeland Security (CIP/HS) at the George Mason University School of Law is pleased to announce the availability of the curriculum for seven graduate courses in critical infrastructure protection. These courses cover topics in critical infrastructure protection such as resilience; risk management; information sharing; systems analysis; policies and strategies; and cybersecurity. The courses are intended to foster critical infrastructure education programs that produce and sustain the leaders and workforce required for the government and the private sector to effectively protect critical infrastructure.

CIP/HS, with input from external subject-matter experts from the public and private sectors as well as the academic community, developed these courses during the past year. As critical infrastructure protection spans numerous fields of study, including computer science, criminal justice, engineering, homeland security, global security, and public policy, these courses are made publicly available to the higher education community to provide a foundation for critical infrastructure education. These courses may be incorporated into the curriculum of any program and used by any institution.

Critical infrastructure protection and best practices in higher education both develop and evolve at a rapid rate. Therefore, we encourage feedback from professionals and programs who use these courses. External input ensures that the foundation with which these courses were created continues to build and thrive.

For more information about the program, please see the article entitled "Education" in the August 2010 issue of *The CIP Report*, available at: http://cip.gmu.edu/archive/CIPHS_TheCIPReport_August2010_CIPHSUpdate.pdf.

The course offerings are accessible on our website at http://cip.gmu.edu/course-offerings.

CIP/HS is co-hosting the 5th Annual SARMA Conference

Tuesday, September 13th through Thursday, September 15th, 2011, at
George Mason University's Arlington Campus.

This year's event is entitled
Security Risk 10 Years After 9/11: How Far Have We Come and What Lies Ahead?

The conference will take a retrospective look back at what we have – or have not – learned and accomplished over the past decade, and delve into what lies ahead for the security risk profession.
We will be bringing together approximately 60 specialists from government, academia and the private sector, who will discuss the latest trends in community, critical infrastructure and cyber-security risk; federal, state and local government policy developments; and risk management standards, methodologies and education/training efforts.

Event summary: http://www.cvent.com/d/wdqy2z

Confirmed speakers list: http://www.cvent.com/d/wdqy2z/3K

Registration page: http://www.cvent.com/d/wdqy2z/4W

The Personal Resilience Certificate

The mission for any organization is to ensure their employees are available to support the people they serve. When an organization supports its employees and their families in rebuilding and recovering from a catastrophic event, the employees are then able to support the people the organization serves. This interdependent relationship is defined as workforce resilience.

I AM RESILIENT
so I can safeguard Americans from the many threats we face.
PROTECT MY FAMILY
SUPPORT THE MISSION
THE PERSONAL RESILIENCE CERTIFICATE
GEORGE MASON UNIVERSITY
Center for Infrastructure Protection and Homeland Security
YOUR ORGANIZATION'S EMPLOYEES can become certified by enrolling at www.resilienceisreal.com

The Center for Infrastructure Protection and Homeland Security (CIP/HS) is pleased to announce a new certificate program designed to help organizations prepare their employees so that they are able to answer the call of duty with peace-of-mind and focus. Additionally, this course helps individuals answer, "Yes, but what do I do?" for both their families and workplaces during and after catastrophic events, thereby building resilience and rapid recovery for the organization, community and our Nation.

Please visit us at
www.resilienceisreal.com
to learn more.

Preliminary Analysis *(Cont. from 10)*

stochastic process must be
constructed upon it that captures the unpredictable nature of the states of the MEs, their changes, and the interactions between CIs over time. In this stage, probabilistic models of the MEs are defined. These are state-machines, a well known formalism in software engineering, modelled after the formalism used in the Stochastic Activity Networks (SANs).

Stage 6 (optional): Adding Deterministic Models of Behavior: At this stage, the modeller may decide to extend the behaviour of the probabilistic model, adding deterministic models of behaviour. Such a step may be useful when the modeller is seeking to extend the fidelity of the simulation beyond the standard mechanisms possible with a pure probabilistic model.

Stage 7: Exploratory Interdependency Analysis: A Monte Carlo simulation is used to quantify the impact of interdependencies on the behaviour of the system under study and draw more conclusions about the probability of interdependency-related risk.

During these stages, we found that the narrative information coming from the following sources was relevant and useful:

Scenarios: PIA is a scenario-driven approach. Once the system has been modelled, "what-if" questions will be used to explore vulnerabilities and failure cascade possibilities. Scenarios can be developed from a variety of assumptions or experiences. For instance, one can begin by asking a question as abstract as "what happens if there is a flood," or "if power plant X" fails. Such questions form the basis for scenarios, which focus the analysis on particular conditions, exploring potential vulnerabilities.

Incident Description: PIA can be used to model an incident that has already occurred; this can be used as a baseline for generating and exploring variations of the same scenario or simply further exploring a system that has been compromised, or has failed, as the incident revealed unpredicted vulnerabilities and failures.

Threat or Attack Model: Here, we are considering modelling assumptions based on malicious attacks.

Model of Threat Agent: The above (scenarios, incident description, and threat or attack model) are elements that will shape the profile of a threat that is modelled in our system. This can be a malicious agent (e.g., a terrorist) or a source of natural disaster (e.g., flood). ❖

Legal Insights *(Cont. from 13)*

sector efforts" focused on a certain geographic area.[13] A future focus of the RCCC is to "focus on inter-regional dependencies."[14]

The damage caused by the disruption of critical infrastructure is exacerbated by interdependencies among critical infrastructures. This was recognized and addressed in the 2009 NIPP by providing for partnerships that span sectors and bring together public and private stakeholders. Future aims for these partnerships should be to gain a better understanding of how the sectors are interdependent and develop methods to mitigate potential disruptions. ❖

[13] *Critical Infrastructure Partnership Advisory Council Annual* (2010),10.

[14] *Critical Infrastructure Partnership Advisory Council Annual* (2010),11.

Models *(Cont. from 6)*

for a streamlined analysis of CI interdependencies, disaster management officials and decision-makers are making substantial efforts to improve the disaster mitigation technology. Given that CI interdependency data are fundamental to develop a full-fledged disaster management system and because the management of the time dimension is the most difficult task in modeling CI interdependencies, a rigorous model with time processing capabilities such as the tools used in this research can help disaster management officials retrieve relevant information on demand. Further implementation and evaluation of the CI interdependency model proposed is needed in order to demonstrate how such information technology can mitigate the impact of a disaster. ❖

Acknowledgments: This research was supported partly by the National Science Council of Taiwan under grant NSC-100-2119-M-008-007.

The authors of this publication may be contacted at the following email addresses: Ssu-Min Tseng, ssumin.t@gmail.com; Ting-Wu Ho, tingwu.h@gmail.com; Cheng-Ting Chiang, andycg0327@hotmail.com; Jau-Lang Su, jlsu@ncdr.nat.gov.tw; and Chien-Cheng Chou, ccchou@ncu.edu.tw.

References

Chou, C.C., and S.M. Tseng, (2010). "Collection and Analysis of Critical Infrastructure Interdependency Relationships." *ASCE Journal of Computing in Civil Engineering*, 24(6), 539-547.

Haimes, Y.Y. (2005). "Infrastructure Interdependencies and Homeland Security." *ASCE Journal of Infrastructure Systems*, 11(2), 65-66.

Laefer, D., A. Koss, and A. Pradhan (2006). "The Need for Baseline Data Characteristics for GIS-Based Disaster Management Systems." *ASCE Journal of Urban Planning and Development*, 132(3), 115-119.

Rinaldi, S., J. Peerenboom, and T. Kelly (2001). "Identifying, Understanding, and Analyzing Critical Infrastructure Independencies." *IEEE Control Systems Magazine*, 21, 11-25.

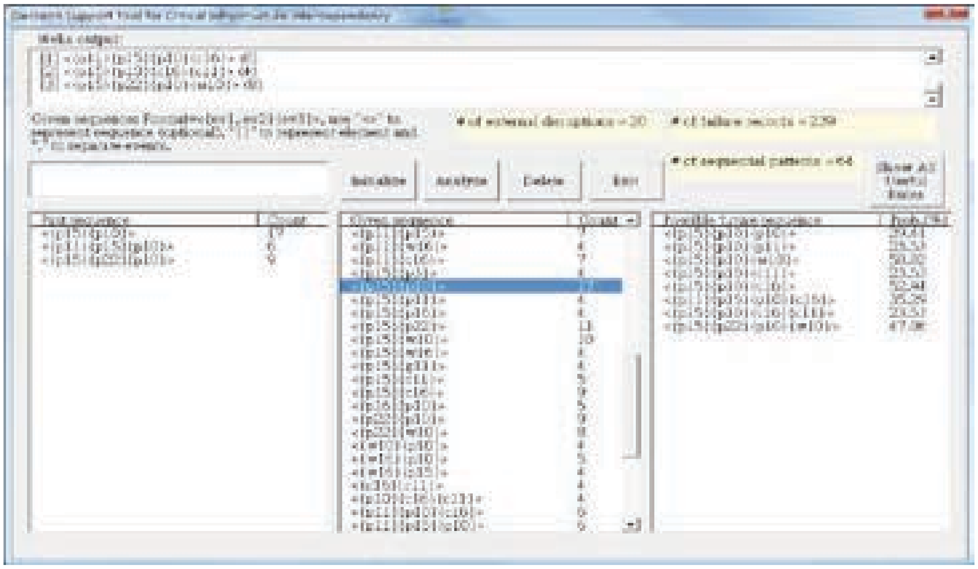


Figure 3: Using PCPD to efficiently and effectively identify interesting patterns of CI interdependencies.

Exercises *(Cont. from 4)*

provide significant value added in developing the necessary stakeholder awareness of important linkages, vulnerabilities, potential consequences and cascading impacts, and areas of priority mitigation investment. These exercises also generate cooperation among diverse individuals and organizations and build the level of trust that enables collaborative solutions. For example, recognition of the flood threat to the Green River from the Howard Hanson Dam, highlighted in *Blue Cascades VI* held in March 2010, motivated hospital suppliers and some other organizations in the region that warehouse products to relocate resources and supplies and establish MOUs for assuring services.

In addition, interdependencies exercises are an integral component and essential step in developing stakeholder-driven all-hazards regional risk mitigation strategies and can be used by organizations to improve their continuity plans and to sensitize staff, management, and leadership about interdependencies. While not expressly focused on testing existing plans, interdependency exercises can perform this function for local and State agencies, and can be readily adapted to the Homeland Security Exercise and Evaluation Program (HSEEP). Targeted interdependency exercises can be utilized to "drill down" on a particular vulnerability or consequence in a specific scenario.

Most importantly, these exercises empower the broad key stakeholder base to build and continuously upgrade security and emergency management plans and enables the creation and enhancement of public-private partnerships and sustainable collaboration for regional and community resilience. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1