Performance Evaluation Model for Critical Information Infrastructure Protection Activities

Chung-Wei Chen[1], Swu Yih[2], Chin-Feng Fan[1]
[1]*Dept. of Computer Science and Engineering, Yuan-Ze University, Taiwan*
[2]*Dept. of Computer Science and Information, Ching Yun University, Taiwan*
[1]csfanc@saturn.yzu.edu.tw, [2] swuyih@cyu.edu.tw

ABSTRACT

Critical Information Infrastructure Protection (CIIP) becomes an important national security issue after 911 attacks in 2001. Since many countries have devoted huge amount of effort to CIIP, it is critical to evaluate the effectiveness of CIIP activities. This research proposes a six-dimensional structure for CIIP performance maturity evaluation. Under this structure, a CIIP-CMM has been developed. Preliminary analyses and comparisons of CIIP activities in America, Australia, and Taiwan using CIIP-CMM have also been given.

1: INTRODUCTIONS

Critical infrastructures (CI) refer to infrastructures that are needed to maintain national security and the economic and social welfare of a nation. Critical infrastructures include communication, banking/finance, water supply, medicine, energy, and emergency/rescue services, etc. Attacks on these infrastructures may seriously disrupt the functioning of government, business, and way of life.

Current critical infrastructures are mainly operated by computers and connected on the internet. Therefore, they are highly interdependent. Cyber attacks may easily incur cascading effects across different sectors and even countries. Critical Infrastructure Protection (CIP) or, most of it, Critical Information Infrastructure Protection (CIIP) is perceived as a crucial part of national security in numerous countries today. Huge effort has been devoted to CIIP by different countries, especially after 911 terrorist attacks. Therefore, it is critical to provide sound performance models to evaluate CIIP effectiveness and to compare CIIP programs collectively. This paper proposes a six-dimensional structure to evaluate CIIP. Based on these dimensions, a CIIP-CMM has been developed. Preliminary analyses and comparisons of CIIP activities in America, Australia, Canada, and Taiwan using this CIIP-CMM have also been given.

2: BACKGROUND

Our case analyses are based on CIIP handbooks [1,2] and NIPP [3,4]. They are introduced in this section along with CMMI and SSE-CMM.

2.1: CIIP Handbooks

"International Critical Information Infrastructure Protection (CIIP) Handbook" [1,2] has been referred to as the Bible of the infrastructure protection practices The handbook provides a CIIP country survey and an overview of related issues including models, methods, and analysis. The first version, published in 2002, addressed national protection activities in eight countries; the 2004 version surveyed fourteen countries; the 2006 version surveyed twenty countries. We used the 2004 and 2006 version in our case studies. CIIP 2004 handbook [1] is divided into the following four parts: (1) CIIP country surveys, (2)Analysis methods, and models for CII (Critical Information Infrastructure) assessment, (3)Overview of international cooperation, legal issues, and research, and, (4)Analysis and conclusion.

2.2: US National Infrastructure Protection Plan (NIPP)

After 911, the United States established the Department of Homeland Security (DHS) in 2002 to coordinate efforts among federal, state, local governments, and private sectors in protecting national critical infrastructures and key resources. DHS has proposed a series of Infrastructure protection Plans. The most important ones are the "National Infrastructure Protection Plan" (NIPP) [3,4] and protection plans of individual sectors. The kernel part of NIPP is its Risk Management Framework including the following six steps: (1) Set Security Goals, (2) Identify Assets, (3) Assess Risk, (4) Prioritize, (5) Implement protective programs, and (6) Measure effectiveness. These steps are executed in a feedback loop for continuous improvement.

2.3: CMMI and SSE-CMM

Capability Maturity Model Integration (CMMI) [5] is a comprehensive reference model developed by SEI to assess levels of process capability and maturity for an organizations or a specific process area. It comes in two ways: a staged model and a continuous model. In the research, we use an approach similar to the continuous model. The continuous model rates 24 process areas on a scale from 1 to 6; namely, incomplete, performed, managed, defined, quantitatively managed, and optimized. Each process area has a set of generic goals and a set of specific goals; under which there are generic practices and specific practices, respectively.

System Security Engineering Capability Maturity Model (SSE-CMM)[6] focuses on implementing security in IT systems. It provides process areas of security base practices as well as project and organization base practices. Each Process Area (PA) has several Basic Practices (BP). We have adapted some of its security process areas. However, the nature of CIIP is different from system security. Besides security, CIIP needs to consider safety related issues due to potential sabotages after intrusion. Furthermore, interdependency is the key concern for CIIP; while it is not considered in SSE-CMM.

3: PROPOSED PERFORMANCE MODEL

3.1: Six dimensions for Analysis

We propose using the following six dimensions to analyze CIIP maturity:

1. Risk characteristics
2. Regulation system
3. Technical system
4. Execution
5. Integration
6. Continuous improvement

Risks faced by different countries are quite different. Terrorist attacks, for example, are the major risks faced by the US, Britain, and Australia, but this may not be true for other countries. Geographical differences may also incur different kinds of natural risks such as earthquakes, tsunami, hurricanes, forest fires, etc. Thus, R*isk characteristics* of different countries need to be identified first. *Risk characteristics* pave the foundations for different protection measures.

Besides, CIIP involves private and public sectors, and its execution needs law enforcement; thus, *regulation system* is needed. *Regulation system* includes codes, guidelines, and standards for federal/central government, local governments, and private enterprises.

Furthermore, *technical* effort and *execution* effectiveness of CIIP form the core of evaluation. *Technical system* dimension of CIIP mainly involve risk analysis activities such as threat analysis, vulnerability analysis, impact analysis, and risk analysis. Different countries have developed their own technical methods for these activities. *Execution* dimension involves the responsible organizations and the execution process.

Since infrastructures are connected on the internet, they are highly interdependent. Thus, the *integration* dimension deals with interdependencies and coordination among different infrastructures and sectors.

Finally, *continuous improvement* addresses the improvement and optimization. It demonstrates the capability to incorporate new techniques and that to correct past defects.

CIIP can be evaluated using the above six dimensions. Then evaluation results can be represented using a radar diagram with 5 scales on each dimension, like the one shown in Fig. 1. The radar diagram can highlight CIIP activities' strength and weakness. An unbalanced shape of the diagram reveals that resource allocation among these dimensions is not balanced. Thus, a reallocation for a more balanced performance diagram may be desired.

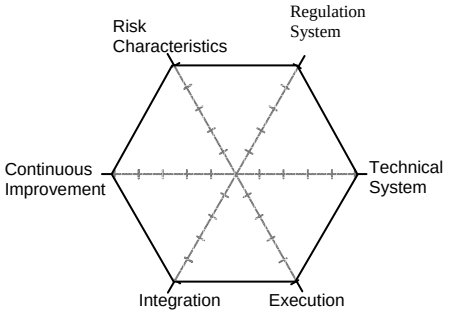


Fig. 1 Performance Radar Diagram

3.2: The Proposed CIIP-CMM

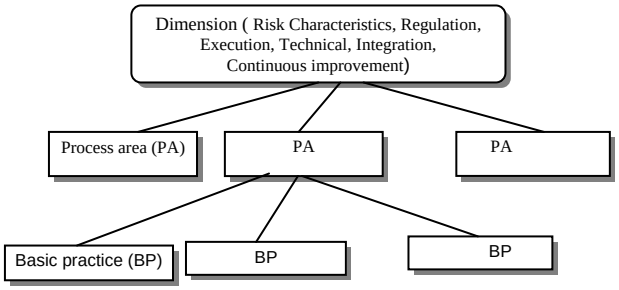


Fig. 2 CIIP-CMM Structure

Table 1. Proposed CIIP- CMM

Dimension	Process Area (PA)
Risk Characteristics	(PA02) Asset Analysis (PA04) Threat Analysis (identification)
Regulation System	(PA03) Legislation
Technical System	(PA04) Threat Analysis (PA05)Vulnerability analysis (PA06) Impact Analysis (PA07) Risk Analysis
Execution System	(PA01) Establish organizations responsible for CIIP (PA10) Establish Performance baselines and models
Integration System	(PA08) Interdependencies Analysis (PA09) System Analysis
Continuous Improvement	(PA11) Innovation and Deployment (PA12) Case Analysis and Resolution

Based on the above six dimensions, we propose a CIIIP- CMM reference model to evaluate the maturity of each country's CIIP plan. CIIP-CMM includes several process areas for each of the six dimensions; several Basic Practices (BP) are specified for each Process Areas (PA). This structure is shown in Fig. 2. Twelve process areas are defined; they are listed in Table 1. A style similar like continuous CMMI is used. The proposed process areas and their BPs are presented in the following subsections.

3.2.1: Risk Characteristics

The *risk characteristics* dimension includes Asset Analysis (PA02) and Threat Analysis (PA04).

Asset analysis (PA02) is carried out by first identifying critical sectors, including major departments, sub-departments, their core functions and resources. The rest BPs consists of establishing asset inventories, and establishing a national asset database. These BPs are shown in Table 2.

Threat analysis (PA04) includes threat identification and threat analysis. The former belongs to the *Risk Characteristics* dimension, the latter belongs to *Technical System* dimension. Threats consist of natural threats, human errors, and human malicious sabotages. The basic practices of this process area, shown in Table 3, include identification of these three types of threats, the development of potential threat scenarios, and threat monitoring at execution time.

Table 2 BPs of PA02 (Asset analysis)

BP02.01	Identify critical sectors
BP02.02	Establish critical infrastructure sectors asset inventory
BP02.03	Establish of National critical infrastructure assets database

Table 3 BPs of PA04 (threat analysis)

BP04.01	Identify natural threats
BP04.02	Identify human threats
BP04.03	Identify malicious threats
BP04.04	Threat scenario analysis
BP04.05	Monitor threats

3.2.2: Regulation System

This dimension comprises establishing regulation system process (PA03). The regulation system includes governing laws, regulatory guides, and industrial standards. Thus, the basic practices, shown in Table 4, consist of legislating for governing laws, developing regulatory guidance, and developing industrial standards.

Table 4 BPs of PA03 (legislation)

BP.03.01	Legislate for governing laws
BP.03.02	Develop regulatory guidance
BP.03.03	Develop industrial standards

3.2.3: Technical System

The analysis part of threat analysis (BP04.04-BP04.05) belongs to the technical dimension, as shown in Table 3

Vulnerability analysis (PA05) refers to the potential weaknesses brought about during system design, development, operation, and maintenance. BPs of this process area (shown in Table 5) include developing vulnerability analysis methods, identifying vulnerabilities, assessing vulnerabilities, and monitoring vulnerabilities.

Impact Analysis (PA06) quantifies potential effects for infrastructures under attacks. It is related to threat analysis, vulnerability analysis and interdependency analysis. Its BPs are given in Table 6.

Risk Analysis (PA07) is based on threat analysis, vulnerability analysis, impact analysis, and interdependency analysis to calculate the risk, which is the product of the damage cost multiplied by the occurring probability. BPs of PA07 are listed in Table 7.

Table 5 BPs of PA05 (vulnerability analysis)

BP05.01	Develop vulnerability analysis method
BP05.02	Identify vulnerabilities
BP05.03	Assess vulnerability
BP05.04	Monitor vulnerability

Table 6 BPs of PA06 (impact analysis)

BP06.01	Identify targets of impacts
BP06.02	Define impact metrics
BP06.03	Impact scenario analysis
BP06.04	Monitor impacts

Table 7 BPs of PA07 (risk analysis)

BP07.01	Develop risk analysis techniques
BP07.02	Identify risks
BP07.03	Identify risks related to safety
BP07.04	Identify probability of risk exposure
BP07.05	Risk analysis
BP07.06	Develop risk alleviation and contingency plans
BP07.07	Monitor risks

3.24: Execution

The *Execution* dimension includes "Establishing responsible organizations" (PA01) and "Establish performance baselines and models" (PA10).

Establishing responsible organizations (PA01) has the BPs shown in Table 8, namely, establishing national, local, and sector responsible organizations.

Establish performance (PA10) baselines and models process area provides quantitative control for protection measures. Its BPs are given in Table 9.

Table 8 BPs of PA01
(Establish responsible organizations)

BP01.01	Establish national organizations responsible for CIIP
BP01.02	Establish local organizations responsible for CIIP
BP01.03	Establish sector responsible organizations

Table 9 BPs of PA10
(Establish performance baselines and models)

BP10.01	Establish performance objectives
BP10.02	Establish process performance measures
BP10.03	Establish process performance baselines
BP10.04	Establish process performance models

3.2.5: Integration

The i*ntegration* dimension includes "interdependency analysis" (PA08) and "system analysis" (PA09).

Interdependency analysis (PA08) identifies and analyzes the relations among infrastructures and sectors. It is the core of critical infrastructure protection. Rinaldi et al. proposed six dimensions to analyze critical infrastructure interdependencies [7]. Rinaldi's six dimensions are listed as follows:

1. Types of interdependencies
2. Infrastructure environment
3. Couplings and response among infrastructures
4. Infrastructure characteristics
5. Types of failures
6. State of operation

The proposed BPs are : identifying Rinaldi's six dimensions and then analyzing interdependencies. These are shown in Table 10.

System analysis (PA08) uses modeling and simulation to study infrastructure interdependency and potential risk scenarios. Its BPs includes selecting critical sectors and attributes as well as modeling and simulation. These are shown in Table 11.

3.2.6: Continuous Improvement

The *Continuous Improvement* dimension includes "innovation and deployment" (PA11) and "problem analysis and resolution" (PA12). Solving problems and performing innovation enable CIIP to improve and reach an optimal level. BPs of these two process areas are given in Table 12 and 13, respectively.

4 APPLICATION

To demonstrate the use of the above CIIP-CMM, we have applied it to evaluate CIIP activities of several countries, and to a particular sector, a nuclear power plant. Due to page limits, we will only show the case studies of USA, Australia, and Taiwan in the paper. Other details can be seen in [8]. Our evaluation of these countries' CIIP activities is based on the information from CIIP handbooks 2004 [1], 2006[2], and NIPP 2005[3], 2006[4]. Details are not provided in these handbooks; therefore, for country-level assessment, we only evaluate process-area level. While, for sector-level evaluation (a power plant), we have used CMM-CIIP basic practices [8]. Our analyses may not be very accurate due to the limitation of available information. However, our methods should be sound if more information is available.

We used process-based evaluation approach, similar to continuous CMMI. Each PA is evaluated as F(fully performed), L (largely performed), P(partially performed), and N (not perform). Then, a 5-scale rating for each proposed dimension can then be assigned. Basically, an average of N evaluation will get level 1, P for level 2, and L for level 3, while F for 5. The middle of L and F will get level 4. The radar diagram for the performance of the proposed six dimensions can then be drawn for comparison.

Table 10 BPs of PA08 (interdependency analysis)

BP.08.01	Identify types of interdependencies
BP.08.02	Identify infrastructure environment
BP.08.03	Identify couplings and response among infrastructures
BP.08.04	Identify infrastructure characteristics
BP.08.05	Identify types of failures
BP.08.06	Identify state of operation
BP.08.07	Analysis of interdependencies

Table 11 BPs of PA09 (System analysis)

BP09.01	Select critical sectors and their attributes
BP09.02	Modeling and simulation

Table 12 BPs of PA 11
(Innovation and deployment)

BP11.01	collect improvement proposals and identify innovations
BP11.02	analyze improvement proposals and innovation
BP11.03	Pilot improvement
BP11.04	select improvement for deployment
BP11.05	plan the deployment
BP11.06	Measure improvement effects

Table 13 BPs of PA12
(Problem Analysis and Resolutions)

BP12.01	Select defect data for analysis
BP12.02	Analyze defect causes
BP12.03	Implement the action proposal

The USA has identified that its major threats come from terrorists. Furthermore, after hurricane attacks in 2005, the USA is engaged in all-hazard protection. A summary of USA CIIP measures is given in Table 14; process area assessment is given in Table 15; a performance radar diagram of the proposed six dimensions is given in Fig. 3

Australia's major threat is also from terrorists. Australia has established several responsible agencies for CIIP; moreover, technical methods have been developed. The summary, assessment and radar diagram of Australia's CIIP activities is shown in Table 16, Table 17, and Fig. 4, respectively.

Taiwan's major threat is information war. The Executive Yuan's "National Information and Communication Security Taskforce" (NICST) is in charge of national CIIP/CIP. NICST executes "National Information and Communication Infrastructure Security Mechanism Plan". The plan includes 69 activities in the second 4 year period (2004-2008). Most of these activities are related to warning, information sharing and management. In technical aspect, Taiwan follows ISMS (Information Security Management System, ISO 17799/BS7799). Besides, Taiwan has not engaged in other technical methods. The summary, assessment and radar diagram of Taiwan's CIIP is shown in Table 18, Table 19, and Fig. 5, respectively.

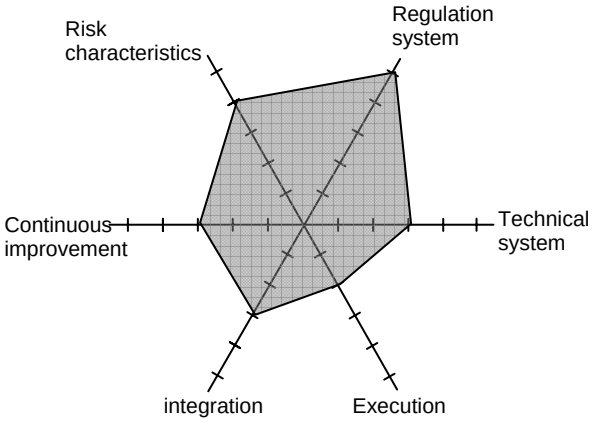
Fig. 6 shows the performance comparison of these three countries' CIIP activities.

Table 14 Summarized USA's CIIP

USA	
Risk Characteristics	Terrorists, all-hazard approach
Regulation System	-Homeland Security Act of 2002 established DHS - DHS's National Strategy for Homeland Security - Homeland Security Presidential Directive-7
Technical System	Risk Assessment: RAMCAP, NIST, OCTAV Interdependency, vulnerability analysis : DoE's methods
Execution System	DHS
Integration System	DHS international, sector partnership, state and territorial, regional, national-level Interdependencies: DoE modeling
Continuous Improvement	DHS's types of changes and improvement GAO report

Table 15 Assessment of USA's CIIP

Process area	**F**	**L**	**P**	**N**
PA01 Establish organizations responsible for CIIP	ˇ			
PA02 Asset Analysis	ˇ			
PA03 Legislation		ˇ		
PA04 Threat Analysis		ˇ		
PA05 Vulnerability analysis		ˇ		
PA06 Impact Analysis		ˇ		
PA07 Risk Analysis		ˇ		
PA08 Interdependencies Analysis			ˇ	
PA09 System Analysis			ˇ	
PA10 Establish Performance baselines and models			ˇ	
PA11 Innovation and Deployment		ˇ		
PA12 Innovation and Deployment		ˇ		



USA

Fig. 3 Radar Diagram of USA's CIIP Activities

Table 16 Summarized Australia's CIIP

Australia	
Risk Characteristics	Terrorists
Regulation System	- president approved NCTC (National Counter Terrorism Committee) which developed National Counter Terrorism Plan (NCTP) in 2003
Technical System	System assessment: CIPMA, PreDict Industrial Profiles Interdependency: CIPMA IT: ISMS, CNVA
Execution System	NCTC DSD, ASIO, AFP
Integration System	Organization: TISN Interdependencies: TISN-CIPMA PreDict Industry Profiles
Continuous Improvement	NCTC review every three years

Table 17 Assessment of Australia's CIIP

Process area	**F**	**L**	**P**	**N**
PA01 Establish organizations responsible for CIIP		ˇ		
PA02 Asset Analysis		ˇ		
PA03 Legislation		ˇ		
PA04 Threat Analysis		ˇ		
PA05 Vulnerability analysis		ˇ		
PA06 Impact Analysis		ˇ		
PA07 Risk Analysis		ˇ		
PA08 Interdependencies Analysis		ˇ		
PA09 System Analysis			ˇ	
PA10 Establish Performance baselines and models				ˇ
PA11 Innovation and Deployment				ˇ
PA12 Innovation and Deployment			ˇ	

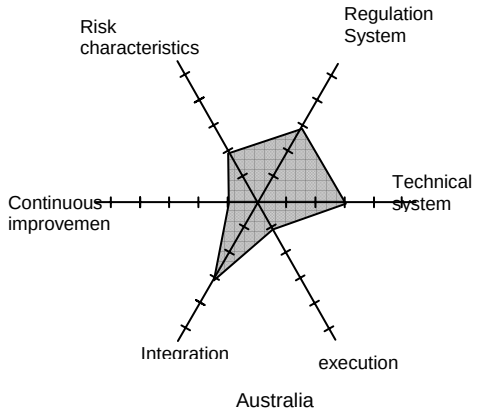


Fig. 4 Radar Diagram of Australia's CIIP Activities

Table 18 Summary of Taiwan's CIIP

Taiwan	
Risk Characteristics	Information war
Regulation System	- "Criteria for maintaining computer and information security for organizations under the Executive Yuan," 1987 - "Guidelines for Information Security for organizations under the Executive Yuan," 1999 - National Information and Communication Infrastructure Security Mechanism Plan, 2000-2004, 2004-2008
Technical System	Follow ISMS (ISO 17799/BS7799)
Execution System	Executive Yuan's "National Information and Communication Security Taskforce" (NICST)
Integration System	Organization: NICST Interdependencies: None
Continuous Improvement	NICST Regular meeting every half a year

Table19 Assessment of Taiwan's CIIP

Process area	F	L	P	N
PA01 Establish organizations responsible for CIIP		ˇ		
PA02 Asset Analysis		ˇ		
PA03 Legislation			ˇ	
PA04 Threat Analysis			ˇ	
PA05 Vulnerability analysis			ˇ	
PA06 Impact Analysis			ˇ	
PA07 Risk Analysis			ˇ	
PA08 Interdependencies Analysis				ˇ
PA09 System Analysis				ˇ
PA10 Establish Performance baselines and models			ˇ	
PA11 Innovation and Deployment				ˇ
PA12 Innovation and Deployment			ˇ	

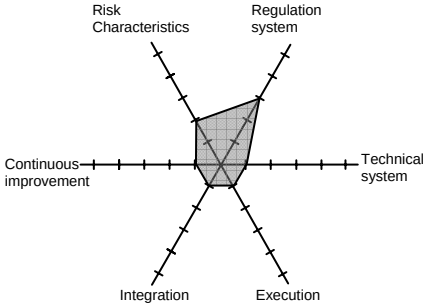


Fig. 5 Radar Diagram of Taiwan's CIIP Activities

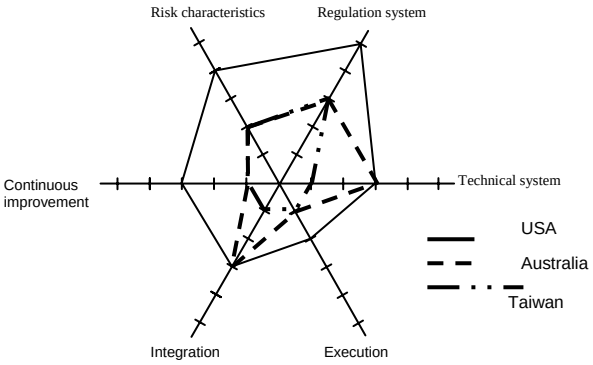


Fig. 6. Comparison of CIIP Activities Among Nations

5. CONCLUSION

Critical Information Infrastructure Protection is vital to national defense. Huge effort has been invested in it in many countries. CIIP effectiveness needs to be analyzed. Moreover, most critical infrastructures are connected on the internet; thus, they are highly interdependent. Consequently, the effectiveness of CIIP of different countries needs to be evaluated and compared collectively. This research proposed a six-dimensional structure for CIIP evaluation; based on these dimensions, a CIIP-CMM has been developed. Preliminary assessment of several countries' CIIP activities has also been presented. Using CIIP-CMM, CIIP activities of different countries can be assessed qualitatively. This is a step towards potentially quantitative metrics for CIIP evaluation.

REFERENCES

[1]Swiss Federal Institute of Technology Zurich, International CIIP Handbook 2004, http://www.isn.ethz.ch/pubs/ph/details.cfm?id=452.

[2]International CIIP Handbook 2006, http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_06_Vol.1.pdf#search='CIIP%202006.

[3]U.S. Department of Homeland Security, DHS- NIPP 2005, http://www.fas.org/irp/agency/dhs/nipp110205.pdf.

[4]U.S. Department of Homeland Security, DHS-NIPP 2006, http://www.dhs.gov/interweb/assetlibrary/NIPP_Plan.pdf

[5] SSE-CMM, http://www.sse-cmm.org/docs/ssecmmv3final.pdf

[6] CMMI, http://www.sei.cmu.edu/publications/documents/05.reports/05tr011.html

[7] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analysis Critical Infrastructure Interdependencies", 2001 Control Systems Magazine, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

[8] Chung-Wei Chen, "Development and Application of Effective Assessment Model for Critical Information Infrastructure Protection Measures," Master's thesis, Dept. of Computer Science and Engineering, Yuan-Ze U., July 2006. (in Chinese)