A Study on Industrial Control System Risk Assessment

Kwo-Jean Farn [1], Yen-Fang Wang [2], Shu-Kuo Lin [1, *], Chung-Huang Yang [3],
Chien-Cheng Huang [4]

[1] Institute of Information Management, National Chiao Tung University, Taiwan
[2] School of Graduate Study, Macau University of Science and Technology, Macau
[3] Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, Taiwan
[4] Department of Information Management, National Taiwan University, Taiwan
[*] Corresponding Author: kuo@iim.nctu.edu.tw; kuo.iim91g@nctu.edu.tw

Abstract- *Currently the information security issues for industrial control system (ICS) are almost determined with incomplete information. With standards available, problems resulting from incomplete information can be decreased; because using standards, we can reduce the number of choices and simplify the process for reliable supply and demand decision-making. Because ICS is related to public safety and national defense, this paper aimed at analyzing relevant researches, meeting the requirements of the National Information & Communication Security Taskforce (NICST) of Executive Yuan in Taiwan, and promoting Failure Mode and Effects Analysis (FMEA) along with the ICS information security risk assessment framework of Common Methodology for Information Technology Security Evaluation (CEM) in order to offer further research of ICS risk management implementation.*

Keywords: Defense in Depth, Industrial Control System, Framework, Risk Management, Safety and Security

1. Introduction

Critical infrastructure (CI) stands for basic products and services provided for a country to maintain the people's livelihood, economy and the functioning of a society, such as energy, telecommunication, financial services, electric power, water supply, and public health, etc. When there is an outage of CI, it would have a debilitating impact on public safety or even national defense. Nowadays, the operation controls of these infrastructures have been computerized and have gradually become open systems. The Information Technology (IT) Malfunction controls have been one of the focuses in the researches of information security management in ICS.

Owing to the coming of information era, cyberspace, which is subsequent to land, the sea, the sky and the universe, has become the fifth dimension of war that solicits international competitions. While people enjoy the enormous benefits information and information system bring, they encounter the challenges of information security at the same time. The single Catastrophe caused by IT Malfunction cost 6 billion USD and financial losses were estimated at $14 billion USD. The issue about information security of Critical Infrastructure (CI) has become a common consensus around the globe [1-3].

In order to effectively protect CI information security, risk management has become the foundation stone of the periodical Critical Information Infrastructure Protection (CIIP) Handbook since 2002. CIIP risk management helps us to learn something from security events, incidents, and even catastrophes, For example, based on the analysis of "June 10, 1999, Pipeline Rupture and Subsequent Fire in Bellingham", "August 14, 2003, 814 North America Blackout Event", and "December 14, 2005, Taum Sauk Dam Reservoir Failure Catastrophic Incident", the U.S.A. proposed how to prevent the industry from Information Technology (IT) Malfunction as well as how to decrease the security guideline series of Industrial Control System (ICS), integrating CI Safety and Information Security [4]. The risk and property of ICS is different from those IT-based communication and information infrastructure such as E-Government; therefore, their security threats certainly differ. Owing to the efforts made by the U.S. Department of Homeland Security, and National Institute of Standards and Technology (NIST), the ICS industry standards have been gradually published [5].

In Taiwan, CI is closely related to the basis of people's lives and economics; hence, the "2008 Information and Communication Security Policy White Paper" officially announced on March 1, 2008, mentioned the following 3 strategies [6]:

1) Making sure the information security standards of CI Security,

2) Setting up risk evaluation maps of CI Information Security, and

3) Strengthening information protection abilities of every CI.

Besides, every CI is required to undergo risk assessment and develop its solution, standard and guidance [6]. The State-owned Enterprise Commission (SEC), Taiwan, is responsible for planning "the Safety and Information Security risk assessment methods integrating ICS danger analysis" for 3 CI --"Electric Power, Oil Gas and Tap Water" [7]. In this paper, IT Malfunction Controls of ICS security incidents occurred in Taiwan together with the implementation framework of its risk assessment are discussed respectively in Section 2 and Section 3 [7-11]. Finally, the conclusion of this paper is proposed in Section 4.

2. Brief Inquiry of CI Malfunction Controls

By millennium, the operation of CI has been fully computerized. At the same time, via information and telecommunication skills, it is closely interconnected with other activities like economy, people's livelihood and the functioning of a government. The ICS information security incidents have made its importance clear [11]. How to manage ICS safety has become the working items in developed countries [12-15]. Thus, this section explores the issues about the information security management controls that IT Malfunction needs to face, just as the ICS information security incidents that occurred in Taiwan in Table 2.1.

Table 2.1: ICS Information Security Incidents in Taiwan

Incident	Date	Description
1	June 4, 1996	The Muzha Line service of Taipei Metropolitan Rapid Transit System (MRT) has been completely disrupted for four hours and thirty-four minutes.
2	July 29, 1999	On July 29, 1999, at 11:31 p.m., the No.326 345-kV extra high voltage (EHV) electricity tower of the Tai-power system, located in Tainan County, Taiwan, suddenly collapsed and finally caused the Tai-power system to have a blackout. The power outage, failed to supply power for more than 14 hours, causing enormous losses and damages.
3	October 21, 2003	On October 21, 2003, the Financial Information Service CO., LTD. Taiwan encountered a serious problem that 2,000 ATMs were nearly paralyzed.

Sources:
1. Calton, (1996), Taipei Subway Computer Crash, The Risks Digest, Vol.18, No.17, June 4, 1996.
2. Ministry of Economic Affairs, 729 Blackout Cause National Investigation Group, (2000), Final Report of Investigation and Improvement Strategy on Tai-power 729 Blackout, Taipei, Taiwan (in Chinese), 2000-01-15.

Taipei MRT Computer Crash Event in Muzha Line on June 4, 1996 was caused by the invasion of crackers. The Blackout Event on July 29, 1999 was involved with the issues about certification, accreditation and security assessment of risk management of IT Reliability and Vulnerability [16]. On October 1, 2003, the reason why nearly 2,000 ATM were paralyzed can be classified as the problem of change management [17]. Generally speaking, Defense in Depth (DiD) is the policy that ICS cyber security should follow [11]. Its implementation includes 26 main security controls in the Human resources security, Physical and environmental security, Communications and operations management, Access control, and Information systems acquisition, development and maintenance in ISMS [18]. The risk management of Reliability and Vulnerability ought to follow the requirement of the Executive Yuan risk management operational guideline [19] as well as the ICS security standards [13, 16, 20, 21]. The capacity management controls in ISMS also need to be improved [12]. As to the change management, in addition to change control procedure, the controls like Information Security Awareness, Education and Training, Security Requirements Analysis and Specification and Input Data Validation should be involved [19]. However, the ICS Business environment is different from any other information system, because any IT Malfunction deriving from the IT Dysfunction in the CI operation (e.g. temporarily unavailable of services, reduction of function, etc.) could cause catastrophes [14]. As shown in Table 2.1, the ICS security assessment of change management is higher than the requirement of the change control procedures of ISMS certification in Financial Information Service CO., LTD. Taiwan [11, 15, 17-19]. In other words, the ISMS standards of the CIIP in our country should follow those of the developed countries [11, 13, 15-17].

3. ICS Information Security Risk Assessment Implementation

The rapid development of electronic technology, popularity of personal information equipment, improvement of network communication structures and fashion of World Wide Web push forward the manufacturing open systems. As shown in Table 3.1, owing to Supervisory Control and Data Acquisition (SCADA) systems integrating with Distributed Control System of Manufacturing Operations Management, Production Management Business Planning and Enterprise Information System (EIS) of Logistics, the application of ICS has gradually taken the place of traditional working styles of manufacturing and has become the perch of its production per day.

Table 3.1: Industrial Control System (ICS) Framework

Level	Function	Information System
4th	Business Planning & Logistics	EIS
3rd	Manufacturing Operations Management	SCADA
2nd	Supervisory Control & Automatic Control of Production Process	DCS
1st	Testing and Manipulating of Production Process	PLC
0	Production Implementation	Production Equipment

Note:
1. DCS: Distributed Control System.
2. EIS: Enterprise Information System.
3. ICS: Industrial Control System.
4. PLC: Programmable Logic Controller.
5. SCADA: Supervisory Control and Data Acquisition.

Generally speaking, ICS implementation should follow the requirements of International Electrotechnical Commission (IEC) - IEC 61508 and IEC 61511 series standards, while IEC 61508 and IEC 61511 do not take into consideration the attacks of Malware. Because ICS uses open systems in depth, information security incidents such as configuration setting, virus infection or hacker invasion take place. These incidents will lead to Catastrophe on public safety; therefore, it is important to constitute information security standards, ranging from Safety to the attack threat of "Malicious Opponents." With the endeavor made by the organizations responsible for Electric Power or Fossil Fuel Industries and Standards in developed countries (e.g. NIST in the U.S.), ISO has formally declared to form a research team of ICS information security standards since November 2005 so as to develop the ISO ICS information security standards.

Because the collapse of ICS storage and usage might cause severe and catastrophic harm to organization operation, organization asset or even individuals, ICS should set up security policies and procedures for every level as shown in Table 3.1. Take Taiwan for an example, on February 13, 2003, NICST of Executive Yuan demanded that 20 Information Security Operation Systems which influence our nation and society a lot - "MRT Operation System", "Energy Management System", and "Inter-bank Trading System" - should pass the CNS 17800 (BS 7799-2:2002) ISMS certification by June 2004 [22]. However, they are not required to follow the Segregation in Networks in ISMS. For example, Intranet and Extranet in SCADA System should establish one-dimensional "Net Gap" of Network Segregation as shown in Fig. 3.1, but they do not conform to the ICS tasks [9-11].

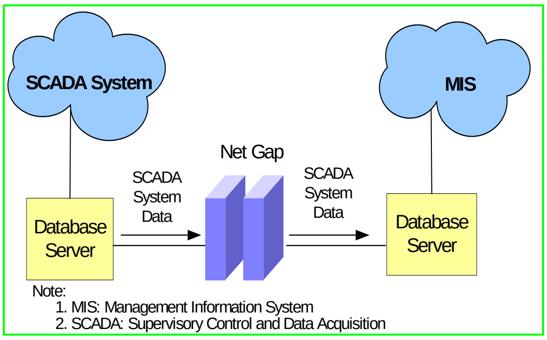


Fig. 3.1: Network Isolation Deployment of SCADA and MIS System

ICS risk assessment in our country should follow the "Handbook of Risk Management Operating" (proclaimed by Research, Development and Evaluation Commission, Executive Yuan, Taiwan, October 2005) and take into consideration standards like risk endurance and relevant goals of the organization, quantify risk identification and stipulate the priority [23]. The result will lead to proper management, manage the priority of information security risk, and select the controls to protect that risk (as shown in Table 3.2).

Table 3.2: Risk Analysis and Judgment Pattern

Influence (impact or effect)	Risk Ranking		
Very Serious (1)	H Senior site management needs to be involved	H Senior site management needs to be involved	E Immediate action required, activity must not start or if started must be stopped
Serious (2)	M Management responsibility must be defined	H Senior site management needs to be involved	H Senior site management needs to be involved
Slight (3)	L Management by routine processes	M Management responsibility must be defined	H Senior site management needs to be involved
	Rare	Possible	Almost Certain
	Probability		

Note:
1. E: Extreme Risk; H: High Risk; M: Moderate Risk; L: Low Risk.
2. Source: Research, Development and Evaluation Commission (RDEC), Executive Yuan, Taiwan, (2005), Handbook of Risk Management Operating, page 47.

The National Information & Communication Security Taskforce (NICST) of Executive Yuan in Taiwan at the end of 2002 has been the main basis of developing all sorts of information security operations of our government organization for the purpose of promoting the information security work. It vertically classifies the unit levels, the table of organization, and investment amount into four levels - A (important core), B (core), C (important), and D (general), and horizontally distinguishes the attribute of government organization into national defense, administration, academy and undertaking, and applies to all sorts of information security operations of our government organization as shown in Table 3.3 [24].

Table 3.3: Classes of Information Security Operation Service Targets in Taiwan

Class	G1	G2	G3	G4 – G7	Sum (2003)	Sum (2007)
A	27	71	0	28	126	61
B	102	190	26	81	399	294
C	63	755	25	156	999	756
D	0	1,261	837	91	2,189	5,686
Total	192	2,277	888	356	3,713	6,797

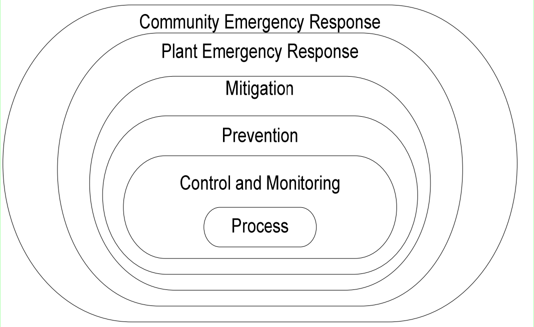
Notes:
1. Sources:
   1.1 Nan-Shian, Chi, (2003), An Aide of Information Security in Taiwan -- National Information and Communication Infrastructure Security Mechanism Plan, Table 2, pp. 4-10, Journal of Information Security, Vol. 1.
   1.2 General Operations Working Group (Executive Yuan, NICST, Taiwan), Presentation data, 2007-12-07.
2. G1: National Defense Division; G2: Administration Division; G3: Academic Division; G4: Business Division (1); G5: Business Division (2); G6: Business Division (3); G7: Business Division (4).

Since June 10, 2004, our country has required that dangerous workplaces should follow the laws and regulations as shown in Table 3.4, and should accomplish the following plans:
1) Plans of basic data of security and sanitation management;
2) Plans of evaluation reports of manufacture procedure security;
3) Security plans of manufacture procedure modification;
4) Plans of dealing with an emergency; and
5) Plans of audit management.

Table 3.4: Safety Legislations of Risk Assessment in Taiwan

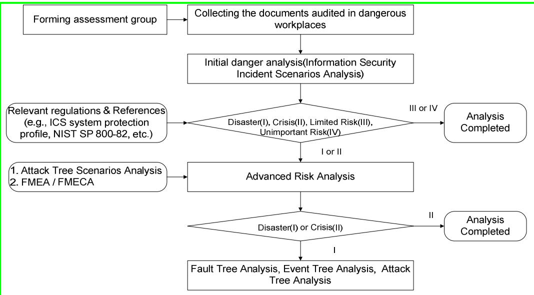
Date	Legislations name
2002-02-16	Public gas and oil pipeline, transmission line of electricity disaster prevention and protection practice plan
2002-05-29	Disaster Prevention and Protection Act
2002-05-29	Labor Inspection Law
2002-06-12	Labor Safety and Health Act
2002-12-31	Enforcement Rules of the Labor Inspection Law
2004-06-10	Hazardous Work Place Review and Inspection Rules

The aforementioned plans have set up a certain foundation for the security of ICS. In light of this, as shown in Fig. 3.2, in this paper we proposed that the vulnerability of “Control & Monitoring” and “Prevention” Levels in CI are supposed to be the scenarios analysis on the basis of different levels of attack (high, medium, low), and the risk assessment framework for ICS (as shown in Fig. 3.3). Besides, ICS information security should be gradually improved according to its relevance, and the priority of CI strategies should be defined. What’s more, the strategies and concrete solutions that the government should have for the critical information security events ought to be planned so as to enhance the protection and promote the capacity of information & communication security of the country.



Source: IEC 61511-1: Functional Safety - Safety instrumented systems for the process industry sector - Part1: Framework, definition, system, hardware and software requirements (2003-01), Figure 9, p.89.

Fig. 3.2: Risk Reduction Framework in ICS


Forming assessment group
Collecting the documents audited in dangerous workplaces
Initial danger analysis(Information Security Incident Scenarios Analysis)
Relevant regulations & References (e.g., ICS system protection profile, NIST SP 800-82, etc.)
Disaster(I), Crisis(II), Limited Risk(III), Unimportant Risk(IV)
III or IV
Analysis Completed
I or II
1. Attack Tree Scenarios Analysis
2. FMEA / FMECA
Advanced Risk Analysis
Disaster(I) or Crisis(II)
II
Analysis Completed
I
Fault Tree Analysis, Event Tree Analysis, Attack Tree Analysis

Notes:
1. FMEA: Failure mode and effects analysis.
2. FMECA: Failure mode, effects and criticality analysis.
3. FTA: Fault tree analysis.
4. Sources:
   4.1 ISO/IEC FDIS 27005:2007-11-15.
   4.2 Stephans, R. A., (2004), System Safety for the 21st Century, Wiley.
   4.3 This study.

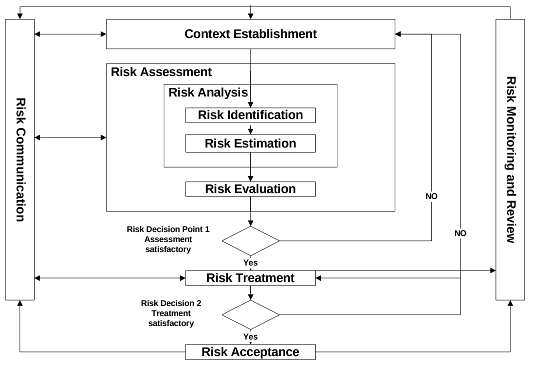
Fig. 3.3: Risk Assessment Framework for ICS

At 12:16 August 14, 2003, Resource Race Condition Event occurred in ICS electrical power grids in the Northeast of the U.S. At 13:02 p.m., it began to influence the reliability of this electrical power grid. From 13:31 to 14:02, the first 345-kV line failed. At 15:41, this 345-kV in electric power network was completely disconnected section by section. At 15:39, the First Energy 138-kV line failed. At 16:05, more than 15 138-kV lines failed after the First Energy 138-kV line recovered. The financial loss of the 814 North America Blackout was estimated at 140 billion USD. According to the investigation analysis before and during the massive power outage happened, nobody, including the staff dealing with emergency on the spot, pointed out that there was the indication that SCADA system had shown the vulnerability. The 814 Blackout Incident exposed the vulnerability of CI information technology malfunction shown in Fig. 3.3. These controls have become the most urgent ICS Emerging Security Capabilities working item for the federal government of the United State. Based on this, we can construct the indicators on the basis of the problems that endanger the Maintenance Hook management of the national security, examine the Effectiveness of its controls periodically, and lessen the possibility of making the risk come true.

4. Conclusion

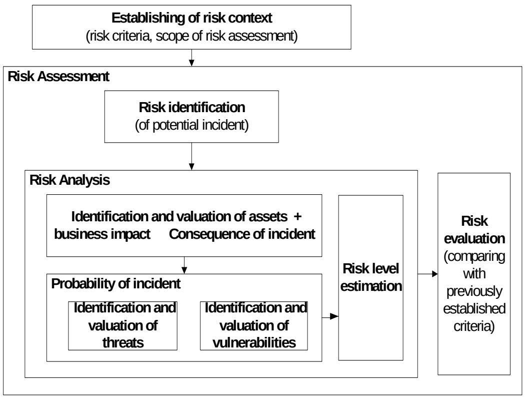
Due to the rapid development of electronic technology, popularity of personal information equipment, improvement of network communication structures and fashion of World Wide Web, the Internet grows at an astonishing pace, making the information circulation far-reaching. Every day, tens of thousands of people are searching all sorts of information via the Internet, whereas some of the information is stored in the computer half an earth away. Although most users access the data legally, illegal invasion and access to other computers sometimes still take place. The experienced hackers make their efforts to find weakness and invade information systems. In addition to the exterior attacks, there is still the possibility of interior invasion from the staff. These attacks might only aim at causing temporary chaos to organization operation such as Denial of Service (DoS) but might tend to cause great damage to the organization information structure. Nowadays, the Internet has been thriving and the invasion incidents occur frequently; Information warfare has become the toolbox of Internet Zombie when the hackers establish Bot (Note: abbreviation of Robot) system instead of being the mysterious research in the laboratory. High-tech crimes and information warfare has been one of the public issues in our society. As ICS has become the aim for high-tech crimes, terrorists and information warfare. Terrorists abduct the ICS in our country like Electric Power or Petroleum Refinement; this might be the Catastrophe and the issue concerning public safety and national defense [24].

Based on ISMS risk management standards [25], we proposed Vulnerability Assessment integrating FMEA and Common Methodology for Information Technology Security Evaluation (CEM) in the ICS risk assessment process shown in Fig. 4.1 and Fig. 4.2 [26]. The results, as indicated in Table 4.1, can be a corresponding reference for ICS to follow the risk rating of IEC 61508 / IEC 61511 as well as a basis for risk management.



Sources:
1. Guerin, F., (2006), Build CC assurance package dedicated to your risk assessment, Presentation to the 7th ICCC Conference, 2006-09-19.
2. ISO/IEC 27005:2008-06-15, Figure 1.

Fig. 4.1: Risk Management Process


Establishing of risk context
(risk criteria, scope of risk assessment)
Risk Assessment
Risk identification
(of potential incident)
Risk Analysis
Identification and valuation of assets + business impact Consequence of incident
Probability of incident
Identification and valuation of threats
Identification and valuation of vulnerabilities
Risk level estimation
Risk evaluation
(comparing with previously established criteria)

Sources: Dr. Elzbieta Andrukiewicz, (2005), Importance of Risk Management, Presentation to the ISO/IEC JTC1/SC27 Security Workshop, 2005-12-05.

Fig. 4.2: Risk Assessment Process Based on ISO/IEC 27005:2008-06-15

Based on Federal Information Security Management Act (FISMA) declared in December 2002, National Institute of Standards & Technology (NIST) in America has begun the second phase of ICS Security Guidance and Credentialing (Phase II: 2007-2010) in FISMA as shown in Table 4.2. The ICS Standards and Guidelines that NIST has issued [5, 8-9] are worthy of learning for ICS risk assessment.

Table 4.1: IT Vulnerability Rating

Rating Scope	0-9	10-13	14-19	20-24	>=25
Level of preventing attackers from potential invasion	No Rating	B	E-B	M	H
Corresponding Evaluation Assurance Level (EAL)	None	EAL1-EAL2	EAL3	EAL4	EAL6-EAL7
Corresponding Reference to IEC 61508 / IEC 61511 Risk Rating	None	1	2	3	4

Notes:
1. Source: ISO/IEC JTC1/SC27, (2008), ISO/IEC FDIS 18045:2008-01-07, p 283, and this study.
2. B: Basic; E-B: Extended-Basic; M: Moderate; H: High.

Table 4.2: Introduction to ICS Security Guidance - taking FISMA for example

1. Federal Information Security Management Act (FISMA) declared in December 2002 required the National Institute of Standards & Technology (NIST) to constitute Critical Infrastructure Information Protection (CIIP) Standards and Guidelines (S&Gs).
2. In 2002, NIST began to enforce FISMA Project. Phase I (2003-2008) aimed at constituting relevant S&Gs for federal government. In January 2006, based on S&Gs that FISMA had established and industrial standards every sector had set up (e.g., CIP-002-1-CIP-009-1, ISA99, IEC 62443, etc.), NIST started ICS Security Project.
3. On April 14 2004, NIST Process Control Security Requirements Forum (PCSRF), which was promoted by NIST in the spring of 2001 and formed by ICS users, vendors, system integrators, the U.S. National Laboratory, and information dealers, proclaimed the ICS System Protection Profile (ICS-SPP) and began the Protection Profile (PP) projects of ICS Control Center and Field Device.
4. On April 19-20 2006, NIST convened the first ICS Workshop. Based on NIST SP 800-53: Recommended Security Controls for Federal Systems, the security requirements that need to be added or deleted when applying ICS are elaborated. Besides, NIST SP 800-82: Guide to Industrial Control System (ICS) Security was constituted. In September 2007, Second Public Draft (NIST SP 800-82) was issued and is going to complete the S&Gs in 2008.
5. On December 2007, NIST SP 800-53 Revision 2: Recommended Security Controls for Federal

Information Systems was issued and included the security controls for ICS.
6. Source: Katzke, S. et al., (2006), Applying NIST SP 800-53 to Industrial Control Systems, Presented at ISO EXPO 2006, October 17-19, 2006, and this study.

Our country begins to concern the risk management operation of ICS information security, and there is not much accumulation of time and experience. Everybody is trying to find out the value, idea, or system that should be set up. As information technology progresses rapidly and under the environment of information system security of cyberspace, the issue of information system security that is relevant to our country people's livelihood needs deeper thinking and discussion. As a member of digital era, we mustn't fail to live up to the opportunity that all the people participate in setting up the model of information society security.

References

[1] Murray, A.T. and T.H. Grubesic eds., (2007), Critical Infrastructure, Springer.

[2] Goetz, E. and S. Shenoi eds., (2007), Critical Infrastructure Protection, Springer.

[3] Skanata, D. and D.M. Byrd eds., (2007), Computational Models of Risks to Infrastructure, IOS Press.

[4] Alrams, M. and J. Weiss, (2007), Bellingham Control System Cyber Security Case Study (2007) MITRE Corporation.

[5] Ross, R. et al., (2007), Recommended Security Controls for Federal Information Systems, NIST SP 800-53, Revision 2, NIST.

[6] General Operations Working Group of the National Information and Communication Security Taskforce (NICST), Executive Yuan, Taiwan, (2008), White Paper of Information and Communication Security Policy, Science and Technology Advisory Group of Executive Yuan, Taiwan.

[7] State-owned Enterprise Commission (SEC), Taiwan, (2007), Critical Infrastructure Information Sharing and Analysis Center (electric power, natural gas & fuel oil, water supply) Establishment Project (in Chinese).

[8] Melton, R. et al., (2004), System Protection Profile - Industrial Control Systems, Version 1.0, NIST.

[9] Staffer, K. et al., (2007), Guide to Industrial Control Systems (ICS) Security (Second Public Draft), NIST Special Publication 800-82.

[10] Kwo-Jean Farn, et al., (2008), A Study on Critical Infrastructure Information Technology Malfunction Control - Illustration of Taiwan, Posted on IEEE International Conference on Intelligence and Security Informatics, June 17-20, 2008, Taipei, Taiwan.

[11] Idaho National Laboratory, (2006), Control Systems Cyber Security: Defense in depth Strategies, May 2006.

[12] Ministry of Economic Affairs, 729 Blackout Cause National Investigation Group, (2000), Final Report of Investigation and Improvement Strategy on Tai-power 729 Blackout, Taipei, Taiwan (in Chinese), 2000-01-15.

[13] http://www.isd.mel.nist.gov/projects/processcontrol/ (2006-09-15)

[14] Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection, (2006), SCADA (Supervisory Control and Data Acquisition) Security - Advise for CEOs.

[15] Digital Bond, Inc., (2006), Field Device Protection Profile for SCADA Systems in Medium Robustness Environments Version 0.71, 2006-05-18, Process Control Security Requirements Forum (PCSRF), NIST.

[16] http://www.dhs.gov/nipp/ (2007-09-15)

[17] ISO, (2006), Information technology - Security techniques - Security assessment of operational systems, ISO/IEC TR 19791:2006-05-05.

[18] ISO, (2005), Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27001:2005-10-15.

[19] Research, Development and Evaluation Commission (RDEC), Executive Yuan, Taiwan, (2005), Handbook of Risk Management Operating, October 2005.

[20] Stephens, R. S., (2004), System Safety for the 21st Century, Wiley.

[21] ISO, (2007), Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, ISO/IEC 27006:2007-03-01.

[22] Nan-Shian, Chi, (2003), An Aide of Information Security in Taiwan -- National Information & Communication Infrastructure Security Mechanism Plan, Table 2, pp. 4-10, Journal of Information Security, Vol. 1.

[23] Research, Development and Evaluation Commission (RDEC), Executive Yuan, Taiwan, (2006), Handbook of Risk Management Operating, Version 2, November 2006.

[24] Chinese Cryptology and Information Security Association (CCISA), Taiwan, (2007), the Research Report of Information Sharing and Analysis Center, 2007-12-03.

[25] E. Andrukiewicz, (2008), Text for ISO/IEC 27005:2008-06-15: Information technology - Security techniques - Information security risk management.

[26] M. Banon, (2008), Text for FDIS 18045:2008-04-23: Information technology - Security techniques - Methodology for IT security evaluation.