A Study on Implementations of Information Security Risk Assessment: Application to Chlorine Processing Systems of Water Treatment Plants

Chien-Cheng Huang[1], Kwo-Jean Farn[2], and Frank Yeong-Sung Lin[1]
(Corresponding author: Chien-Cheng Huang)

Department of Information Management, National Taiwan University[1]
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan, Republic of China
Institute of Information Management, National Chiao Tung University[2]
No. 1001, University Road, Hsinchu 30010, Taiwan, Republic of China
(Email: d97725002@ntu.edu.tw)

(Received July 17, 2013; revised and accepted Nov. 28, 2013)

Abstract

The international standard of information security risk management (ISO/IEC 27005:2011(E)) adopts an iterative approach and risk assessment methodology of information security incident scenarios analyses, applying the principle of 80/20 to calculate, and therefore should be able to save cost and to increase its effectiveness. On such a basis, we propose a rigorous and systematic approach to addressing related implementation issues involved in employing such an information security risk assessment standard, and use the chlorine processing system in a water treatment plant as an example to fully demonstrate the effectiveness of the proposed method. In particular, we would discuss the is-ought side of ISO/IEC 27005:2011(E), respectively. Moreover, an implementation of information security risk assessment is carried out.

Keywords: Information security risk management, iterative approach, risk assessment, risk profile, scenario analysis

1 Introduction

The international standard of information security risk management (ISO/IEC 27005:2011(E)) adopts an iterative approach and risk assessment methodology of information security incident scenarios analyses, applying the principle of 80/20 to calculate, and therefore should be able to save cost and to increase its effectiveness. Since November 2002, the International Register of Certificated Auditors (IRCA) in the UK (United Kingdom), has officially requested to examine information security management systems (ISMSs). Their ISO/IEC TR 13335-3:1998(E) and ISO/IEC TR 13335-4:2000(E) were then added into the basic knowledge and skills of ISMSs. Consequently, risk management has become a core work for establishing and improving ISMSs [15, 16, 22].

Risk analysis is the foundation of risk management. Study and development of risk analysis has been going on for half a century. It has sufficient effect on the industrial safety implementation [7, 29]. However, the issue of information security incident aspects is still outstanding [36]. Accordingly, after reviewing relevant documents, an information security risk profile is established using a correlation matrix as a base [27]. This profile is later adjusted according to practical risk assessment, and finally, as a case study, put into implementation as a risk assessment operation of the chlorine processing system of a water treatment plant.

ISO/IEC 27005:2011(E) is the information security risk management standard of ISMSs in ISO/IEC 27001:2005(E) [22]. In Sections 2 and 3, we would discuss the is-ought side of ISO/IEC 27005:2011(E), respectively. In Section 4 an implementation of information security risk assessment is carried out, and Section 5 concludes this paper.

2 Related Works

The official issuing of ISO/IEC 27005:2011(E) was the result of 6 years and 8 months’ amendments of the previous ISO/IEC TR 13335-3:1998(E) and ISO/IEC TR 13335-4:2000(E) since October 2002. During the process of standardization, even if there is no common consensus about whether or not risk profile issues should be included. However, the model of information security risk management has become the example of establishing ISMSs [2, 22].

In the process of information security risk management, risk assessment and/or risk treatment activity in ISO/IEC 27005:2011(E) is identified to cycle according to implementations. This method, in consideration of implementations, depth and details of each evaluation in the process of risk assessment implementations, however, has to be enhanced. Iterative approaches provide the possibility to reduce cost on the identification control process, and can still ensure that high risk be balanced.

As shown in ISO/IEC 27005:2011(E), the priority of risk management procedure is to establish context, and then to proceed with risk assessment. If during this procedure adequate information can be obtained to sufficiently decide the necessary actions to amend the risks to an acceptable level, the mission is complete and we then may be able to proceed to the next step of risk treatment. If the information is insufficient, another risk assessment cycle context with adjustments (such as risk evaluation standards, risk acceptance standards or impact standards) will be established [22].

Effectiveness of risk treatment depends on the results of risk assessment. Sometimes risk treatment cannot lead to an acceptable level of residual risk due to limitations. Under such situations, another risk assessment cycle context parameter (such as risk assessment, risk acceptance or impact standards) might need to be adjusted. It further allows risk treatment to occur [22].

Risk acceptance activities must ensure that the residual risk be obviously accepted by the management of the organization. This is especially important when the control item in the implementation is neglected or postponed due to costs.

During the entire information security risk management process, it is important that both risk and its treatment are negotiated to be dealt with by suitable management and operation personnel. Even before risk treatment, identified risk information is very valuable for incident management, and can thus help lower potential damage. The cognition of controlling features such as risk, reducing risk and the focusing are of the organization by the management and operational personnel, can most efficiently assist in treatment incidents and unpredictable events. Information security risk management procedures should turn all detailed results of all activities relevant to the two risk decisions into documents.

3 Approaches for Information Security Management, Risk Assessment and Scenario Analysis

ISO/IEC 27001:2005(E) regulates the scope, limitations and content of the ISMS, the control measures implementation is rooted due to risks. The application of information security risk management procedure should fulfil such requirement. Many risk assessment methods can be successfully applied within the organization, however, with the different cost efficiency. The organization should apply the most suitable risk assessment method according to each special procedure's suitability [2, 22].

In an ISMS, the establishment of context, risk assessment, the development of risk treatment and risk acceptance are all in the "Plan" stage. During the "Do" stage, the necessary action and control items are executed in accordance to risk treatment projects to lower the acceptance level of risk. During the "Check" stage, the management would amend the needs of risk assessment and risk treatment in accordance to the environment, incidents and changes. During the "Act" stage, including the additional information security risk management application, all necessary actions would be carried out. For this reason, the information security risk management activities during the four stages of the ISMS procedures are categorized as shown in Table 1.

Table 1: A comparison of the ISMS and the information security risk management process

ISMS Process	Information Security Risk Management Process
Plan	Context Establishment (7) Risk Assessment (8) Risk Treatment Planning (9) Risk Acceptance (10)
Do	Implementation Plan of Risk Treatment (9)
Check	Continuing Risk Monitoring and Reviewing (11)
Act	Maintaining and Improving Information Security Risk Management Process (12)

Notes:
a) (*n*) is a session number of ISO/IEC 27005:2011(E).
b) Risk treatment implementations are not regulated in ISO/IEC 27005: 2011(E).

To conclude the risk assessment procedure in ISO/IEC 27005:2011(E), after the identification of threats, assets, identification control measures, and vulnerability is completed. An organization needs to identify its assets. These assets include the primary and supporting assets. The primary assets include "business processes and activities" and "information". Moreover, the supporting assets include hardware, software, network, personnel, site, and organizational structure. The scenario analysis method is used to complete risk identification, risk estimation and risk evaluation. ISO/IEC 27005:2011(E) also shows the descriptions of the context of scenario analysis and risk assessment. On the other hand, the four options available for risk treatment include risk reduction, risk retention, risk avoidance, and risk transfer [22].

The origin of scenario analysis can be traced back to the 1950's. Table 2 is its common application and comparison within the risk assessment [8, 12, 13, 32]. Based on the features of ISMSs, we propose three risk assessment frameworks of different levels from simple to complex as shown in Figure 1 [8, 12, 13, 22, 32].

When actually conducting the operations in Figure 1, the common risk analysis methods of scenario analysis shown in Table 2, lack the model of information security incidents. We thereby propose the information security scenario analysis of the risk profile models that show the information security vulnerability measurement in the accordance to each procedure and its relevant information [17, 22, 31]. These models also show the likelihood evaluation and the risk level forecast of risk profile. Therefore, these models examine the consequences and impacts in the accordance to the level of the vulnerability and the sensitivity, as well as the technical ability of the threat proxy, respectively.

The first framework shows a vulnerability measurement of information security incident scenario analysis. The factors should be considered during analysis of vulnerability measurement. They consist of "Capability level (Specialist expertise)", "Tool box (IT hardware/software or other equipment required for exploitation)", "Time taken to vulnerability discovery", "Window of opportunity", and "Domain knowledge" [17]. Additionally, alert and audit system is a role of inhibitor in measuring vulnerability. It is used to detect vulnerability and system exception in the TOE (Target of Evaluation). On the other hand, the risk management process uses the vulnerability analysis method in ISO/IEC 18045:2008(E) to evaluate the potential attack definitions and citation. It also refers to attacks, in order to establish a risk assessment scenario security target.

In order to gain a more detailed insight into the information security specific incidents. The second framework shows a likelihood evaluation [31]. Inhibitors may deter the threat agent from executing the threat, for example, fear of being detected, losing job and gaining a criminal record. Catalysts are events or changes in circumstances that make the threat agent decide to act, for example, redundancy of employee or employee debts. In addition, amplifiers may encourage the threat agent to execute the threat, for example, belief or trust.

The third framework shows a risk level forecast of information security incident scenario analysis. An information security incident can impact more assets. These impacts are immediate or future. Immediate impact includes direct and indirect [22]. For example, direct impact is the impact results in an information security breach. Indirect impact is a potential misuse of information obtained through a security breach. Besides, relevance analysis is the occurring problem of specific information assets, which may endanger the organizational operating results. On the other hand, risk monitoring and reviewing system is a role of inhibitor in forecasting risk level.

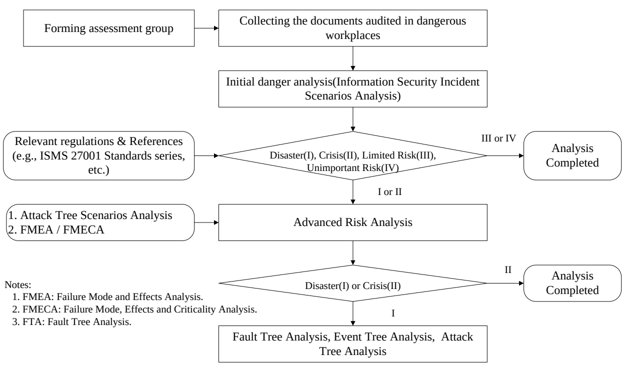

Figure 1: Framework of the iterative risk assessment approach

Table 2: A comparison of scenario analyses with risk assessment methods

Risk Assessment Method	Characteristics	Problems
Hazard and Operability Analysis (Haz-Op)	a) The systematic method of the scenario analysis; can be used as FMEA/FMECA basis. b) The process is based on the systematic deviation from the brainstorming method of the qualitative analysis. c) The requirements of the process of document management and records.	a) Difficult to quantify. b) Need experienced experts to participate in the job.
Failure Mode and Effect Analysis (FMEA/FMECA)	a) Equipped with a comprehensive analysis of qualitative and semi-quantitative analysis method. b) The complex systems can be analyzed.	a) Dependencies between equipment and human error analysis are not easy. b) Need experienced experts to participate in the job.
Fault Tree Analysis (FTA)	a) The comprehensive and systematic analysis of the qualitative and quantitative side up. b) The complex systems can be analyzed.	a) The failure rate or the rate of human error is not easy to obtain information. b) Need experienced experts to participate in the job.
Event Tree Analysis (ETA)	a) Based on the event the comprehensiveness of the inductive analysis method. b) The complex systems can be analyzed.	a) Delay analysis of an event is not easy. b) Need experienced experts to participate in the job.
Attack Tree Analysis (ATA)	a) The penetration testing and integration based on the causality analysis of ETA and FTA. b) The complex systems can be analyzed.	a) The graphics is huge and is not easy to draw. b) Need experienced experts to participate in the job.

4 Implementations of Information Security Risk Assessment

On how to identify information security demands within an organization and to establish its ISMS, ISO/IEC 27005:2011(E) proposes a systematically method of information security risk management. The effort allows effective and immediate risk treatment at the necessary time and place. The procedures of information security risk management adopt an iterative approach to implementing the depth and width of risk assessment in each cycle, and under the offer of reducing costs and time on the identification control. It still insures the high risk be suitably evaluated to form a balanced framework. Information security incident scenario analyses are the basis of the ISMS risk assessment [22].

The EU (European Union) due to such consideration, has completed a risk analysis system CORAS (Consultative Objective Risk Analysis System) framework from 2001~2007, which is considered one of the best tool options to put ISO/IEC 27005:2011(E) into implementation [2]. The main purpose of the CORAS platform is to improve the methods of the traditional risk analysis and evaluation, providing risk analysing methods as well as the computerising for Haz-Op, FMEA/FMECA and FTA as shown in Table 2. It obtains more accurate risk analysis and support for the risk evaluation procedures. In this study, we assume that the water treatment plant has completed safety risk evaluation according to standardised project methods. We use the CORAS module platform as a tool for risk estimation, and applying FMECA, an iterative risk evaluation approach as indicated in ISO/IEC 27005:2011(E) [5, 33, 34]. In addition, the clean water treating procedures of the water treatment plant are shown as Figure 2 [5]. After an risk analysis with Haz-Op and information technology vulnerability, we propose five scenarios that may cause threats. All these threats are plausible causes of damages, as detailed below:

i. Hackers attacking the chlorine processing system of the water treatment plant through the Internet, causes damaging events of chlorine leakages through fire detector failures, etc.

ii. Malware attacking the chlorine processing system of the water treatment plant through the Internet, causes damaging events of chlorine leakages through chlorinator jams, etc.

iii. The operator not being familiar with the operation procedures and the system, due to operational failure causing errors in the chlorine processing system of the water treatment plant, leads to damaging events of chlorine leakages through evaporator jams, etc.

iv. Chlorine processing system flow regulator failures of the water treatment plant caused by information technologies, lead to chlorine leakages caused by pipeline fractures, etc.

v. Automatic chlorine detector failures of the water treatment plant caused by the use of information technologies, lead to chlorine leakages caused by spontaneous obstruct system failures, etc.

We Compare the scenarios of the chlorine processing system of a water treatment plant by the Trusted Computing Group (TCG) focusing on the TOE with proposing the table of the fifteen threats in 2008, and the common vulnerability scenarios of the industrial control system (ICS). We process risk assessment in an actual chlorine processing system of the water treatment plant, referring to different types of the threats, to treat risk incidents. Thus, we hope to minimise the damage when security incidents do occur [32, 33]. Besides, the above-mentioned fifteen threats include T.Compromise, T.Bypass, T.Export, T.Hack_Crypto, T.Hack_Physical, T.Imperson, T.Import, T.Insecure_State, T.Intercept, T.Malfunction, T.Modify, T.Object_Attr_Change, T.Replay, T.Repudiate_Transact, and T.Residual_Info [35].

According to known attacking techniques [17, 22, 31], a risk profile FMEA/FMECA analysis of the chlorine processing system of the water treatment plant as shown in Table 3. The communication protocol, logical processes, and input/output processes all show a higher risk priority index and risk index value. As a result, the control measures should be improved accordingly [5, 32].

Based on the previous risk analysis and the results of the risk evaluation, Figure 3 shows the results of the fault tree analysis (FTA) of the chlorine processing system in the water treatment plant. We can hence see the basic reason of the chlorine poison situations and incidents.

Compared with the ordinary ICS, the chlorine processing system of the water treatment plant contains the process control system (PCS), which controls the chlorination, as well as the safety instrumented system (SIS) that relates to reaction towards chlorine leakages. The overall operation is indicated in Figure 4. Furthermore, based on Figure 3 and Table 3, Figure 5 is the information security incident scenario analysis framework regarding ICS of the chlorine processing system, while Figure 6 shows its event tree [1, 14].

Concluding the above, ETA, FMECA and FTA can be used to describe ICS safety features, consequences, and root causes. Under the current circumstances, the rate of the deliberate threat attacks leading to the chlorine leakage is extremely high in Figure 5. Therefore, the ICS such as the PCS and firewalls between ICSs should be improved to minimize the risk [18, 33].

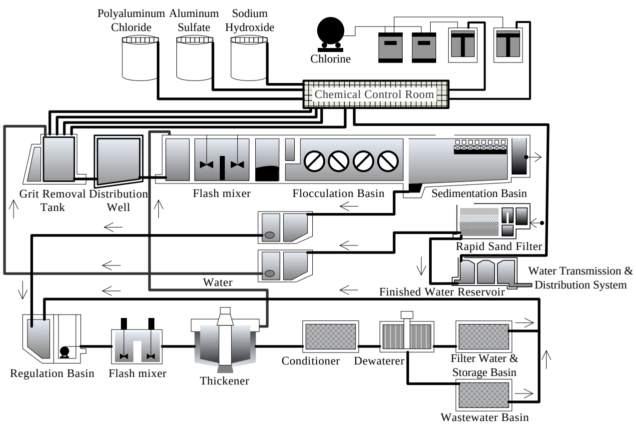

Figure 2: The clean water treatment procedures of the water treatment plants in the Taiwan Water Corporation

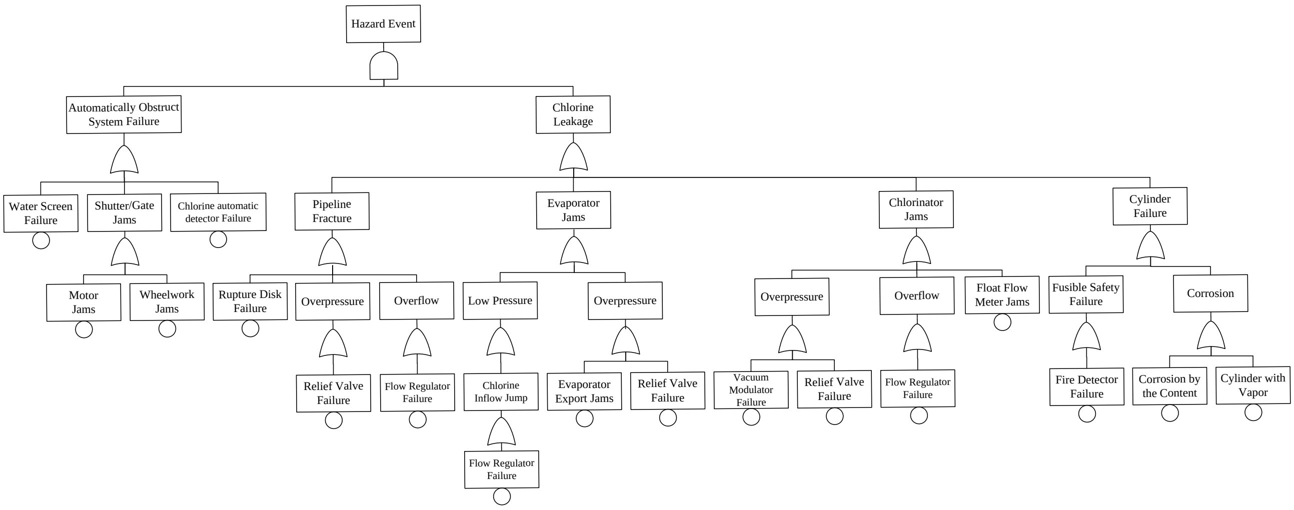

Figure 3: The chlorine leakage fault tree

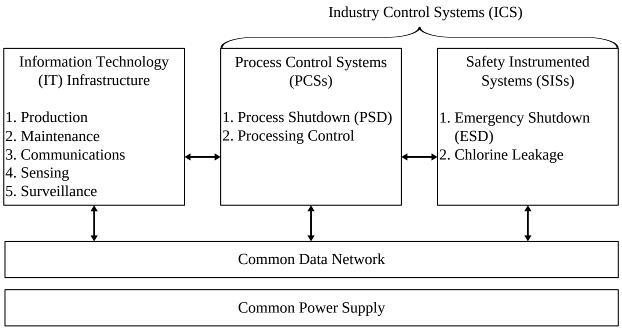

Figure 4: Framework of the chlorine processing system

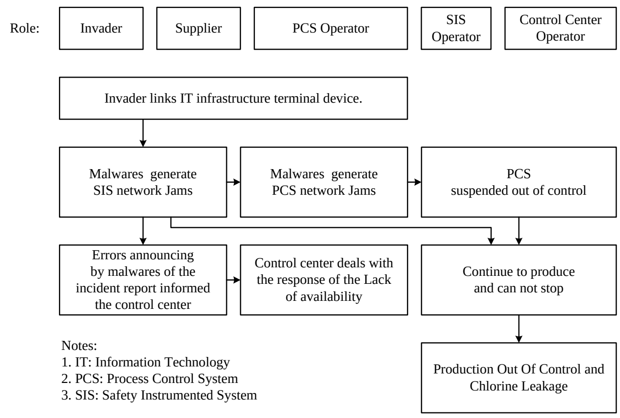

Figure 5: Framework of the ICS scenario analysis for the chlorine processing system

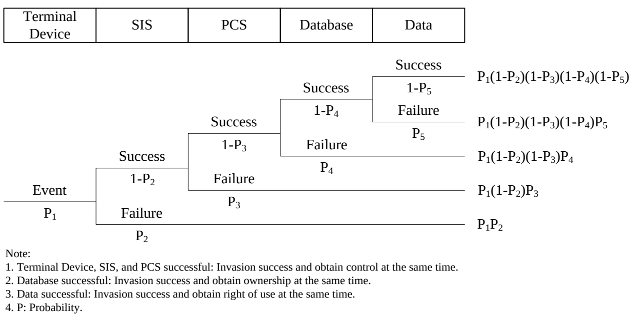

Figure 6: Event tree analysis

Table 3: The chlorine processing system FMEA/FMECA worksheet for the water treatment plant

Target	Potential failure model	Potential failure effect
a) Communication Protocol b) Logical Processes c) Input/Output Processes	a) Fire Detector Failure b) Float Flow Meter Jams c) Flow Regulator Failure d) Relief Valve Failure e) Vacuum Modulator Failure f) Chlorine Detector Failure	a) Cylinder Failure b) Chlorinator Jams c) Evaporator Jams d) Pipeline Fracture e) Spontaneous Obstruct System Failure

Notes:
a) Every attack target can detonate all potential failure models, and generate all potential failure effect.
b) Every attack target brings about the highest likelihood of the failure models.
c) Every attack target brings about the failure models which lack in countermeasures.

To achieve the objectives of this study, a group decision making method based on the vague set theory is proposed. By using the proposed group decision making method, evaluators' opinions and preferences on the questions can be elicited and described by the vague values [3, 6].

Let X be a space of the points (objects), with a generic elements of X denoted by x. A vague set V in X is characterized by a truth-membership function t_V and a false-membership function f_V. $t_V(x)$ is a lower bound on the grade of membership of x, and $f_V(x)$ is a lower bound on the negation of x derived from the evidence against x. $t_V(x)$ and $f_V(x)$ both associate a real number in the interval [0, 1] with each point in X, where $t_V(x) + f_V(x) \leq 1$. That is $t_V: X \rightarrow [0, 1]$, $f_V : X \rightarrow [0, 1]$. The grade of the membership of x in the vague set V is bounded to a subinterval $[t_V(x), 1-f_V(x)]$ of [0, 1]. The vague value $[t_V(x), 1-f_V(x)]$ indicates that the exact grade of the membership $\mu_V(x)$ of x may be unknown, but is bounded by $t_V(x) \leq \mu_V(x) \leq 1-f_V(x)$, where $t_V(x) + f_V(x) \leq 1$, μ_V is the membership function of the vague set V, and $\mu_V(x)$ indicates the grade of the membership of x in V.

The vague value at a specific element of the universe of discourse can be elicited by the vague polling procedure.

- **Step 1:** Propose a fuzzy question.

The respondents are asked to reply to the following question:
"Do you agree that *x* is *p*?", or, say, "Do you agree that the statement is True?", where the proposition "*x* is *p*" can be viewed as a combination of one subject *x*, and the predicate which characterizes a property *p*.

- **Step 2:** Elicit the responses.

The question is answered by allocating a total of 100 points among the different votes, e.g. "True, Vague or False", "Yes, Hesitation or No", or "Yes, Abstention or No". The allocated points on a specific vote reflect the subject's degree of belief in that vote.

- **Step 3:** Translate the responses into values of the membership functions.

The grade of the membership of *x* in the vague set *V* is bounded to a subinterval $[t_V(x), 1-f_V(x)]$ of [0, 1]. By using the following formulas, the degree of the truth-membership function $t_V(x)$ and the degree of the false-membership function $f_V(x)$ can be estimated as follows:

$$t_V(x)=\frac{\text{Total number of the points of "yes" responses for } x}{\text{Total number of the points of "yes"+"no"+"abstention" responses for } x}$$

$$f_V(x)=\frac{\text{Total number of the points of "no" responses for } x}{\text{Total number of the points of "yes"+"no"+"abstention" responses for } x}$$

In addition to the truth-membership function, $t_V: x\rightarrow [0,1]$, and the false-membership function $f_V: x\rightarrow [0,1]$, we further defined an abstention-membership function $a_V: x\rightarrow [0,1]$, for reflecting the grey area of the decision making. The degree of the abstention-membership function $a_V(x)$ is estimated as follows:

$$a_V(x)=\frac{\text{Total number of the points of "abstention" responses for } x}{\text{Total number of the points of "yes"+"no"+"abstention" responses for } x}$$

To take a simple example as follows: Please allocate your points among the different "Yes-Abstention-No" votes to represent your response to the following question: "Do you agree that the Statement is True?" (The total numbers of the points for the question is 100.) The points allocated among different votes can be elicited and the result of the polling procedure is calculated as shown in Figure 7. By employing the above formulas of the membership functions, the degree of belief that "the Statement is True" is 0.5, *i.e.* $t_V(x) = 0.5$; the degree of disbelief that "the Statement is True" is 0.15, *i.e.* $f_V(x) = 0.15$; the degree of uncertainty or hesitation that "the Statement is True" is 0.35, *i.e.* $a_V(x) = 0.35$. According to the above-mentioned definition, the vague value can be obtained as $[t_V(x), 1- f_V(x)]$ or $[t_V(x), t_V^*(x)] = [0.5, 0.85]$.

In this study, we used a Lin et al.'s transformation method and utilized a scoring function to transform a vague value *V* into a crisp value (comparable numerical value) $S(V)$ [25, 26]. Let $V(x)= [t_V(x), 1-f_V(x)]$ be a vague value, where $t_V(x)\in[0, 1]$, $f_V(x)\in[0, 1]$, and $t_V(x) + f_V(x)\leq 1$. The membership values of the quantities in the vague interval $[t_V(x), 1-f_V(x)]$ can be expressed by a triangular fuzzy number TFN $(t_V(x), t_V(x), 1-f_V(x))$. The numerical value of the membership values of the quantities in the vague interval can be regarded as the geometric centre of the triangular fuzzy number TFN $(t_V(x), t_V(x), 1-f_V(x))$, as shown in Figure 7. Thus, the score of $V(x)$ can be evaluated by the score function $S(V)$ as shown in Eq. (1).

$$\begin{aligned} S(V) &= \int_{t_V(x)}^{1-f_V(x)} \frac{y(1-f_V(x)-y)}{1-f_V(x)-t_V(x)}dy \Big/ \int_{t_V(x)}^{1-f_V(x)} \frac{(1-f_V(x)-y)}{1-f_V(x)-t_V(x)}dy \\ &= t_V(x)+(1-f_V(x)-t_V(x))/3 \\ &= t_V(x)+(t_V^*(x)-t_V(x))/3 \\ &= (2/3)\,t_V(x)+(1/3)\,t_V^*(x) \end{aligned} \quad (1)$$

To illustrate, the membership values of the quantities in the vague value $V(x) = [t_V(x), 1-f_V(x)]= [t_V(x), t_V^*(x)] = [0.4, 0.9]$ can be expressed as $TFN_V(0.4, 0.4, 0.9)$. Further, the score of $V(x)$ can be evaluated by the score function $S(V)$ as follows:

$S(V) = (2/3) \times 0.4 + (1/3) \times 0.9 = 0.567$.

Table 4: Example of the risk estimation quantitative model based on vague polling procedures

Responses / Subject	Yes	Abstention	No
x	50	35	15
Function	$t_V(x)$	$a_V(x)$	$f_V(x)$
Membership value	0.50	0.35	0.15
Note: The information assets face the threat of the x^{th} subject.			

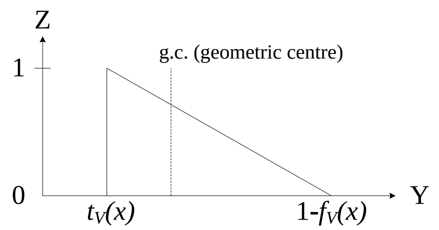

Figure 7: The membership function of a vague value $V(x) = [t_V(x), 1-f_V(x)]$.

5 Discussions and Conclusion

The risk assessment integrating safety and security as shown in Figure 1 can be used to analyze the industrial control system (ICS) potential and critical failure modes, propose proper controls for the effects of this failure, prevent failure from happening, and protect personnels from the loss of safety and property [19, 20, 21].

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 supervisory control and data acquisition (SCADA) system had shown the vulnerability. The 814 Blackout Incident exposed the vulnerability of critical infrastructure information technology malfunction shown in Figure 1. These controls have become the most urgent ICS emerging security capabilities working item for the federal government of the United State as shown in Table 5 [24]. Based on this, on January 18 2008, United States Department of Energy proclaimed the eight items of the mandatory reliability standards for critical infrastructure protection based on Federal Power Act [4]. The standards enhance the contents of de facto standards for the information security scenario analysis framework as shown in Figure 8 [9, 10, 11]. Moreover, the standards have been developing ISO standards [23].

In conclusion, an old Chinese proverb says: "to do a good job, one must first sharpen one's tools". Indeed, Haz-Op, FMEA/FMECA and FTA can help us increase and accumulate our knowledge and experience. In this paper, the proposed risk profile module of vulnerability measurement, likelihood evaluation, risk level forecast as well as scenario analysis of information security risk management, would allow knowledge and experience of different areas to be gathered and compiled. In addition, effectiveness achieved by adopting the proposed iterative risk assessment approach is clearly demonstrated in Figure 1. Further studies can be directed at how to enhance the sensitivity analysis and risk treatment procedures [4, 28, 30].

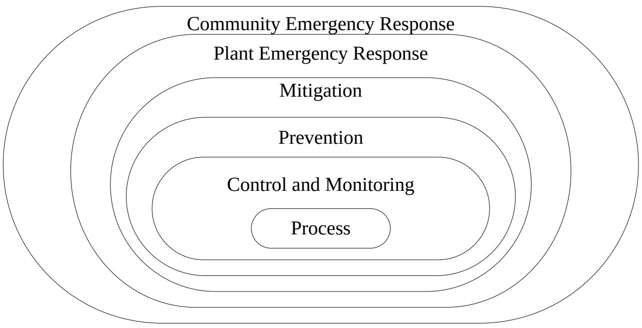

Figure 8: Information security scenario analysis framework.

Acknowledgments

The authors would like to express our appreciation to the Taiwan Water Corporation, for their invaluable help, and this study was supported in part by the National Science Council under contract number NSC 96-3114-P-653-001-Y14. And the authors would also like to thank Dr. Kuo-Sui Lin and Dr. Shu-Kuo Lin for their invaluable help.

Table 5: Introduction to ICS security guidance - taking FISMA for example

a)	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).
b)	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.
c)	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.
d)	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. Furthermore, in December 2007, NIST SP 800-53 Revision 2: Recommended Security Controls for Federal Information Systems was issued and included the security controls for ICS.
e)	In January 2008, "Catalog of Control Systems Security: Recommendations for Standards Developers" was published by United States Department of Homeland Security (DHS). Besides, on January 18 2008, United States Department of Energy proclaimed the eight standards of the mandatory reliability standards for critical infrastructure protection based on Federal Power Act.

References

[1] M. Amin, "North America's electricity infrastructure: are we ready for more perfect storms?," *IEEE Security & Privacy*, vol. 1, no. 5, pp. 19-25, 2003.

[2] F. D. Braber, G. Bræ ndeland, H. E. I. Dahl, I. Engan, I. Hogganvik, M. S. Lund, B. Solhaug, K. Stølen, and F. Vraalsen, "The CORAS model-based method for security risk analysis," SINTEF, 2006.

[3] S. M. Chen and J. M. Tan, "Handling multicriteria fuzzy decision-making problems based on vague set theory," *Fuzzy Sets and Systems*, vol. 67, no. 2, pp. 163-172, 1994.

[4] Federal Energy Regulatory Commission, "Mandatory reliability standards for critical infrastructure protection," 2008.

[5] Fongyuan Water Treatment Plant, "Overview of monitoring system," Fourth Branch, Taiwan Water Corporation, 2008.

[6] W. L. Gau and D.J. Buehrer, "Vague sets," *IEEE Transaction on Systems, Man, Cybernetics*, vol. 23, no. 2, pp. 610-614, 1993.

[7] H. Hakim, "Application of pattern recognition in transient security assessment," *Electric Machines and Power Systems*, vol. 20, no. 1, pp. 1-15, 1992.

[8] IEC, "Hazard and operability studies (HAZOP studies) – application guide," IEC 61882, 2001.

[9] IEC, "Functional safety – safety instrumented systems for the process industry sector – part 1: framework, definitions, system, hardware and software requirements," IEC 61511-1, 2003.

[10] IEC, "Functional safety – safety instrumented systems for the process industry sector – part 2: guidelines for the application of IEC 61511-1," IEC 61511-2, 2003.
[11] IEC, "Functional safety – safety instrumented systems for the process industry sector – part 3: guidance for the determination of the required safety integrity levels," IEC 61511-3, 2003.
[12] IEC, "Analysis techniques for system reliability – procedure for failure mode and effects analysis (FMEA)," IEC 60812, 2006.
[13] IEC, "Fault tree analysis (FTA)," IEC 61025, 2006.
[14] IEEE Computer Society, "Process control security," *IEEE Security & Privacy*, vol. 6, no. 6, pp. 22-51, 2008.
[15] International Register of Certificated Auditors, "Certification criteria for the information security management systems auditor/load auditor training course," IRCA/2016, 2002.
[16] ISO/IEC, "Information technology – security techniques – information security management systems – requirements," ISO/IEC 27001(E), 2005.
[17] ISO/IEC, "Information technology – security techniques – methodology for IT security evaluation," ISO/IEC 18045:2008(E) 2nd edition, 2008.
[18] ISO/IEC, "Risk management – risk assessment techriques," ISO/IEC 31010, 2009.
[19] ISO/IEC, "Systems and software engineering – systems and software assurance – part 1: concepts and vocabulary," ISO/IEC TR 15026-1, 2010.
[20] ISO/IEC, "Systems and software engineering – systems and software assurance – part 2: assurance case," ISO/IEC 15026-2, 2011.
[21] ISO/IEC, "Systems and software engineering – systems and software assurance – part 3: system integrity levels," ISO/IEC 15026-3, 2011.
[22] ISO/IEC, "Information technology – security techniques – information security risk management," ISO/IEC 27005(E), 2011.
[23] ISO/IEC, "Resolutions of the 25th SC 27 plenary meeting held in Sophia Antipolis," ISO/IEC JTC 1/SC 27 N12739 draft, 2013.
[24] S. Katzke and K. Stouffer, "Applying NIST SP 800-53 to industrial control systems," Presented at ISO EXPO 2006, 2006.
[25] K.S. Lin and K.J. Farn, "A group decision making method for evaluating information incident management capability," in *Proceedings of the 18th Cryptology and Information Security Conference*, pp. 405-419, 2008.
[26] K.S. Lin, W. McEwan, and J.H. Liechti, "A software quality strategy for the development of automatic control systems," *International Journal of Computer Applications in Technology*, vol. 12, no. 2-5, pp. 131-140, 1999.
[27] C. C. Lo and W. J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," *Expert Systems with Applications*, vol. 39, no. 1, pp. 247-257, 2012.
[28] National Information and Communication Security Taskforce, "National information and communication security development program (2009~2012)," Information security dispatch document no. 0980100055, 2009.
[29] S. Oh, "A pattern recognition and associative memory approach to power system security assessment," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 16, no. 1, pp. 62-72, 1986.
[30] S. Salicone, *Measurement uncertainty: An approach via the mathematical theory of evidence* (1st edition), Springer, 2006.
[31] J. Sherwood, A. Clark, and D. Lynas, *Enterprise security architecture: A business-driven approach*, CMP Books, 2005.
[32] R. A. Stephans, System safety for the 21st century: The updated and revised edition of system safety 2000, Wiley Interscience, 2004.
[33] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control system (ICS) security," National Institute of Standards and Technology (NIST) Special Publications 800-82, 2011.
[34] Taiwan Safety Council, "Using quantitative chlorine risk assessment in Fongyuan Water Treatment Plant," 2003.
[35] Trusted Computing Group, "Protection profile PC client specific trusted platform module; TPM family 1.2, level 2, version 1.1, part B," BSI-CC-PP-0030-2008, pp. 24-25, 2008.
[36] T. Tryfonas, and B. Kearney, "Standardising business application security assessments with pattern-driven audit automations," *Computer Standards and Interfaces*, vol. 30, no. 4, pp. 262-270, 2008.

Chien-Cheng Huang received his MS degree in information management from the National Chiao Tung University, Taiwan, in 2008. He is currently a Ph.D. student in information management at the National Taiwan University. His research interests include information systems, database systems, data mining, and information security.

Kwo-Jean Farn is an adjunct associate professor with the National Chiao Tung University in Taiwan. He received his Ph.D. degree in 1982. He has had a 30-year career at Information Technology and about 20-year career at Information Security. He was the chair of the Implementation National Critical Information Infrastructure Protection Project at the Computer & Communications Research Laboratories/Industrial Technology Research Institute (CCL/ITRI) from 1999 to 2000. He had worked at the ITRI for more than 18 years until the summer of 2001. He has 9 patents in the information security area. He also received the National Standardization Award in 2009.

Frank Yeong-Sung Lin received his BS degree in electrical engineering from the National Taiwan University in 1983, and his Ph.D. degree in electrical engineering from the University of Southern California in 1991. After graduating from the USC, he joined Telcordia Technologies (formerly Bell Communications Research, abbreviated as Bellcore) in New Jersey, U.S.A. Since 1996, he has been with the faculty of the Information Management Department, National Taiwan University. His research interests include network optimization, network planning, network survivability, performance evaluation, high-speed networks, distributed algorithms, content-based information retrieval/filtering, biometrics and network/information security.