ATLANTIS PRESS

Advances in Engineering Research, volume 113

International Forum on Mechanical, Control and Automation (IFMCA 2016)

A Logical Risk Assessment Schema for Industrial Control Systems

WANG Yufei[1, a], YE Qian[2,b]

[1] Jiangsu Electronic Information Products Quality Supervision Inspection Research Institute, No.100 Jin Shui Road, Wuxi, 214073, China

[2] College of Control Technology, Wuxi Institute of Technology, No.1600 Gaolangxi Road, Wuxi, 214121, China

[a]wyf_1999@163.com, [b]yeqian_80@163.com

Keywords: industrial networked system, safety risk assessment, security risk assessment, critical infrastructure.

Abstract. Information and cyber security has gained considerable importance as safety of the Industrial Control Systems (ICS). Both safety and security deal with risks. Risk assessment is an essential component of safety and security assurance infrastructure mechanisms. Considering the negative or uncertain influence on running ICS, the abstracted ICS model and simulation of ICS is introduced into safety-security risk assessment to form the logical risk assessment schema. Then a risk assessment process framework considering both safety and security is presented. The proposed framework consists of context establishment, overall safety-security risk assessment process, and verification. In the safety-security risk assessment process, conflicts of the risk treatments are addressed to form conflict-free safety-security risk treatment set. The proposed logical schema and risk assessment framework can be used to guide the safety-security risk assessment process of the industrial control systems and support the utilities and organizations in their safety-security efforts.

Introduction

An ICS (Industrial Control Systems) are typically used to automate systems in critical infrastructure of industries to control process in the industrial sectors, such as such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing. The core components of ICS include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Process Control Systems (PCS), Remote Terminal Unit (RTU), and Intelligent Electronic Device (IED).

"Stuxnet" was reported as the first malware specifically targeting control systems[1]. After that, the frequency and seriousness of the cyber-attacks targeting ICSs is increasing quickly[2]. The information security of ICS in critical infrastructure has been recognized as serious, and taken seriously. For the transitioning to information and communication technology based systems, the security of ICSs is important increasingly, and the security factors may have potential negative influence on the safety of ICSs. For a long time, much attention has been taken to safety of the ICSs. Safety and security must be addressed together carefully. A comprehensive survey of existing approaches combing safety and security for ICS is provided in reference [2].

Both safety and security deal with risks. Risk assessment is an essential component of safety and security assurance infrastructure mechanisms. Reference [3] develops a formal model and risk assessment method for security-critical real-time embedded systems called OMR (Object-Message-Role) using Z notation. Reference [4] introduces multimodal-based incident prediction and risk assessment for industrial control systems. Security assessment and vulnerability assessment for critical infrastructure control systems are also discussed in [5, 6].The information security assessment methods referred in [7] can be adopted to analyze the security risks in industrial control system. Some kind of industrial control systems are often designed and expected to last for

decades and work for 24 hours 7 days a week. And risk assessment or analysis tools, which may have negative or uncertain influence on working ICSs, should not be permitted to directly connect to the industrial network. As a result, in-depth risk discover is restricted. To solve this problem, high-quality simulation testbed for ICSs is developed to analyze and evaluate safety and security condition and verify the measurements. A cyber-physical experimentation environment is established to measure the impact of attacks against the networked industrial control system [8].

First, a logical schema is presented for safety and security risk assessment considering the real industrial control environments and simulation of industrial control system. Then risk assessment process framework is developed. The proposed logical schema and risk assessment framework can be used to guide the safety-security risk assessment process of the industrial control systems and support the utilities and organizations in their safety-security efforts.

Logical Schema of the Risk Assessment

The safety and security risk assessment process for industrial control system is schematically presented in Fig.1. Industrial control system are usually real-time and running for more five years without shutting down. And many risk assessment tools may influence the normal running of the systems. So simulation industrial control system is key component for the risk assessment of real and running industrial control systems. Then the Logical schema shown in Fig.1 mainly includes real industrial control system (Real ICS), simulation industrial control system (Sim ICS), ICS model, and the safety and security risk assessment method.

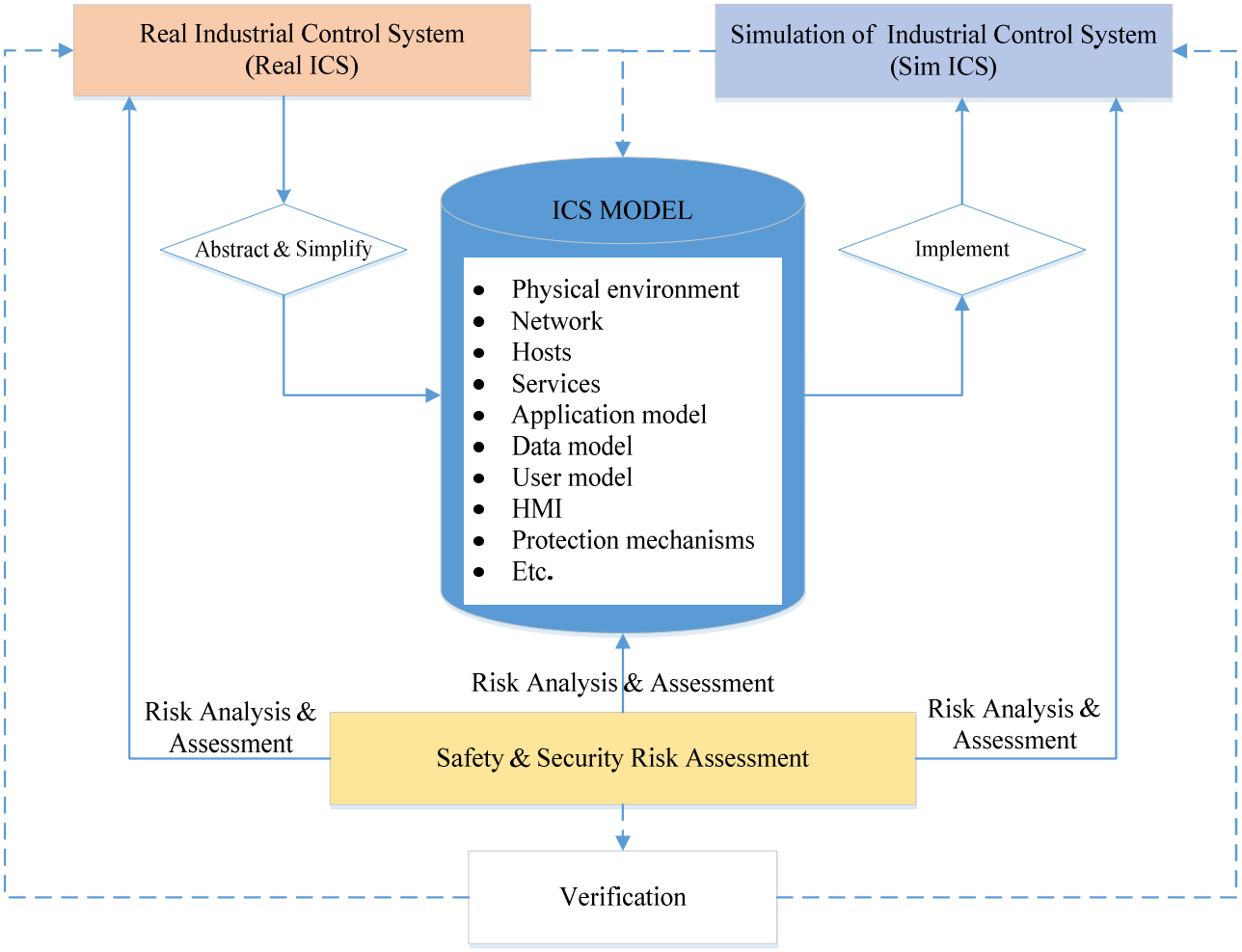

Figure 1. Logical schema of the risk assessment for industrial control system

For the real and complex industrial control system, ICS model matched with it must be abstracted first. The ICS model is simpler than real ICS, but characterize the real ICS well. We can implement the ICS model to simulate the ICS. And then risk assessment can tools can be directly connected to simulation industrial control system to scan the vulnerabilities.

The real ICS usually consists of physical environments, basic software and hardware, industrial networks, and industrial applications. So the abstracted ICS model contains physical control measurements, simplified network topology and critical devices, industrial hosts, services running on the hosts, industrial application model with interactive behaviors, data model, industrial communication protocols, HMI, protection mechanisms employed, and etc.

The objects of the safety and security assessment are real ICS, ICS model, and simulation ICS. And the results of the risk assessment will be also verified through real and simulation industrial system. By analyzing and comparing the resulting risk sets with the real ICS and its model, we can check whether the risks are actual occurrence in real ICS. We can also verify the measures and suggestions against the risks. The risk assessment process will be proposed in the next section.

Risk Assessment Process for Industrial Control Systems

Information and communication technologies are adopted in modern industrial control systems to implement “Intelligent Control”. But the networked and digital control systems must address the information security threats and risks carefully, which may endanger the safety of the industrial infrastructures. A risk assessment process framework considering both safety and security is presented in this section.

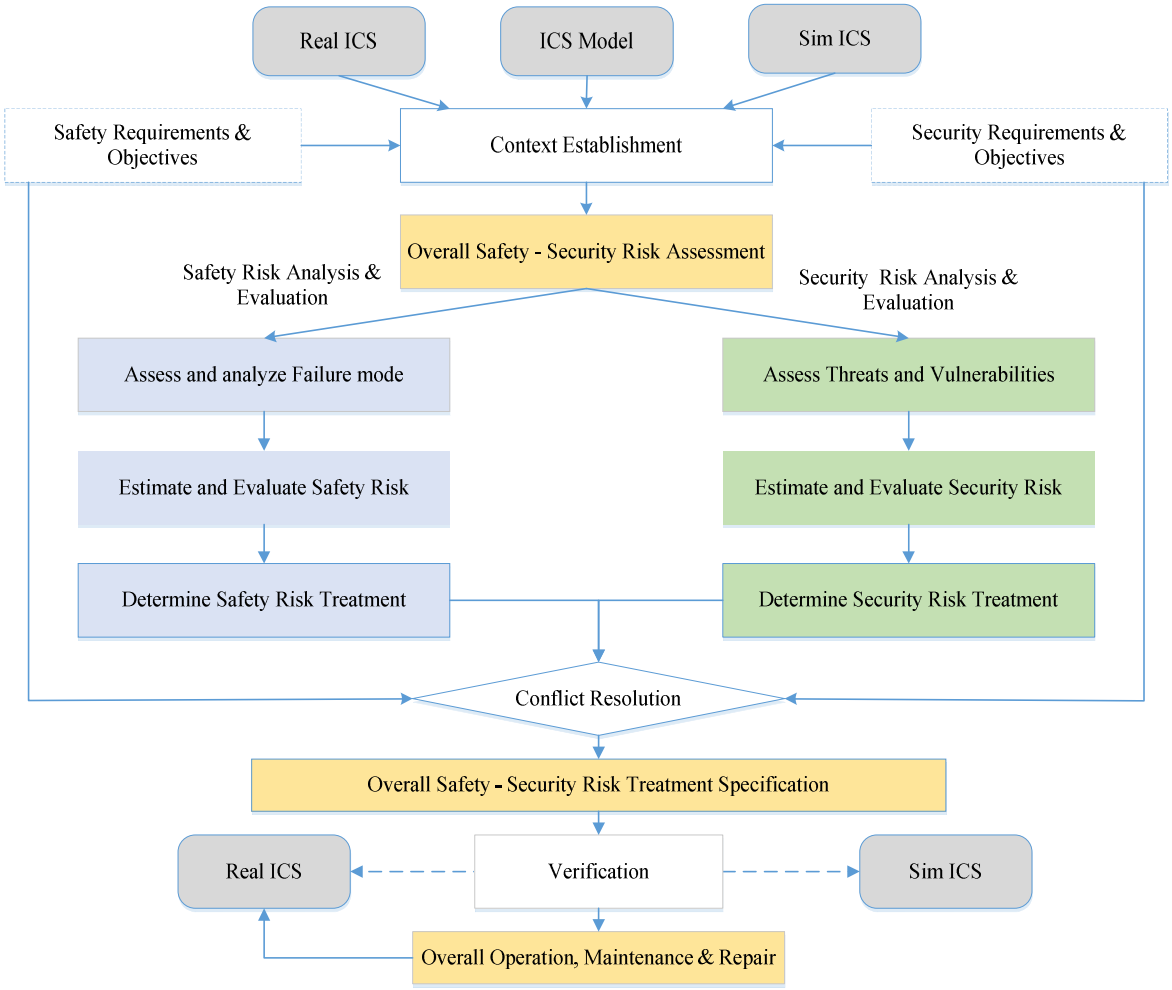

Figure 2. Risk assessment framework for industrial control system

Context Establishment. As shown in Fig.2, the first step of the safety-security risk assessment process is context establishment. The context is the in-depth knowledge of the real ICS and its environment. It is important to establish the risk assessment context from the real ICS, ICS model, and simulation ICS as well as the safety & security requirements and objectives of the ICS. The established context will help discover and identify the safety and security risks by providing system configuration, interactions among internal components, interactions with external systems, the system design information, human-machine interactions, networked structure, current safety & security protection posture or strategies, and etc. Context establishment stage can facilitate the following risk assessment work, for example, identification of critical component, control logic, industrial protocol, network edge, and other assets. On the other hand, non-technical aspect should be also considered when establishing the context of risk assessment, such as human factor, personnel knowledge, individual information security awareness, security culture, and so on[9].

Overall Safety-Security Risk Assessment. The risk assessment process should consider and combine both safety and security according the context established. First, safety risk and security are analyzed and evaluated separately by ICS safety and security experts. Failure mode analysis can be used to identify, estimate, and evaluate the safety risks. And then determine the different treatments for identified risks according to the different frequency and impact. Information security risks are assessed by analyzing the threats and vulnerabilities. Measurements for information security risks are defined appropriately. The security assessment process of ICS may consist of document analysis, mission and asset prioritization, vulnerability extrapolation, assessment environment, testing and impact, vulnerability remediation, validation testing, and monitoring[10]. Treatments to deal with safety and security risks will be integrated to satisfy both sides. And the conflicts among them must be well addressed. The interactions among safety and security treatments are cross-checked to discover and resolve conflicts. In particular context and situations, the resolution of conflict specifies which treatment should be adopted. Usually, for industrial control systems, safety have higher priority than security. If security risk treatment has a negative impact on safety, safety treatment will be select when conflict happens[2]. Otherwise, security treatment will be adopted. And the overall safety-security risk treatment set is conflict-free.

Verification. If industrial control system are running and not under maintenance, the overall safety-security risk treatments firstly implemented in simulation environment to observe and verify the influence of the treatments. It is very important to guarantee the safety and security when reinforcing the safety and security of industrial control system. Some measurements cannot be put into effect in on-working systems such as version updates. So, the maintenance schedule of industrial control system is the best chance to have an in-depth risk assessment, in which the scan and evaluation tools can be used directly on the system to find hidden error or vulnerabilities.

Conclusions

In this paper, a logical risk assessment schema is introduced. And then a safety-security risk assessment framework is also proposed. In our future research work, we will focus on the key technologies in risk assessment considering both safety and security. The methods of characterizing and abstracting the real industrial control systems will be studied as well as the conflicts resolutions among the risk treatments influence with each other. Risk assessment methods considering the human factors, personnel safety and cyber security awareness, safety and security culture and business processes, will be focused on in our future efforts.

Acknowledgements

This work was supported by the Research Program of Wuxi Institute of Technology (Research on Key Technologies of information security for Industrial Control Systems).

References

[1] R. Langner. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy, vol. 9(2011), p. 49-51.
[2] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems, Reliability Engineering & System Safety, vol. 139(2015), p. 156-178.
[3] S. Ni, Y. Zhuang, J. Gu, and Y. Huo, In: A formal model and risk assessment method for security-critical real-time embedded systems, Computers & Security, vol. 58, pp. 199-215(2016).
[4] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang. Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. PP(2015), p. 1-16.
[5] R. Leszczyna, I. N. Fovino, and M. Masera. Approach to security assessment of critical infrastructures' information systems, IET Information Security, vol. 5(2011), p. 135-144.
[6] R. C. Parks and E. Rogers. Vulnerability Assessment for Critical Infrastructure Control Systems. IEEE Security & Privacy, vol. 6(2008), p. 37-43.
[7] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet. Taxonomy of information security risk assessment (ISRA). Computers & Security, vol. 57(2016), p. 14-30.
[8] B. Genge, C. Siaterlis, I. Nai Fovino, and M. Masera. A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Computers & Electrical Engineering, vol. 38(2012), p. 1146-1161.
[9] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, et al. A review of cyber security risk assessment methods for SCADA systems. Computers & Security, vol. 56(2016), p. 1-27.
[10] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, et al. The Cybersecurity Landscape in Industrial Control Systems. Proceedings of the IEEE, vol. 104(2016), p. 1039-1057.