Situation awareness framework for industrial control system based on cyber kill chain

Yufei Wang[1,*], *Tengbiao* Zhang[1], and *Qian* Ye[1]

[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

Abstract. Information and cyber security of Industrial Control Systems (ICS) has gained considerable importance. Situation Awareness (SA) is an exciting mechanism to achieve the perception, comprehension and projection of the ICS information security status. Based on the Purdue Enterprise Reference Architecture (PERA), a situation awareness framework for ICS is presented considering the ICS cyber kill chain. The proposed framework consists of IT SA Centre, OT SA Centre, and Comprehensive SA Centre. Comprehensive SA Centre is responsible for creating and maintaining an integrated and high level of security visibility into the whole environments. The introduced framework can be used to guide the development of the situation awareness infrastructure in organization with industrial control systems.

1 Introduction

Industrial Control Systems (ICSs), usually 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), are widely used in critical infrastructure of industries to control process in the industrial sectors, such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing. For the applications of information and communication technologies, the frequency and seriousness of the cyber-attacks targeting ICSs is increasing quickly [1]. Cyber security of ICSs is increasingly important, and may have potential impacts on the safety. The perception of cyber security status is an expectable method to detect various attacks and anomalies. And cyberspace situation awareness can help the organization to improve the ability to detect and investigate the cyber-related attacks and anomalous behaviours.

Situation Awareness (SA) is “the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” [2]. Perception, comprehension and projection are three main factors of situation awareness. Network isolation between IT and OT systems is one of the

[*] Corresponding author: wyf_1999@163.com

mainstream technologies to ensure the security and safety of the ICSs. But the cyber-attacks such as “Stuxnet” [3] can break through the network boundary, and then disable or disrupt the target ICSs. The convergence of perception data across the IT and OT systems and related equipment will be better protecting the organization from suffering the cyber-attack, especially the ICSs. Reference [4] develops a formal model and risk assessment method for security-critical real-time embedded systems called OMR (Object-Message-Role) using Z notation. Reference [5] 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 [6]. The information security assessment methods referred in [7] can be adopted to analyse the security risks in industrial control system. The well-designed SA infrastructure must deal with both safety (control zone) and security risks.

Based on the industrial control system cyber kill chain [8], a situation awareness framework for industrial control systems is developed. The framework can guide the organization to design the situation awareness infrastructure across the IT and OT networks.

2 Situation awareness framework for ICS

2.1 Typical ICS model

We use Purdue Enterprise Reference Architecture (PERA), which was developed in the 1900s by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing, to illustrate the model of an ICS. The PERA has been adopted by ISA/IEC 62443. As shown in Figure.1, the ICS network of an organization is divided into three main zones consisting of enterprise zone, DMZ, and control zone [9].

Enterprise Zone. In this zone, Office Automation (OA) and Enterprise Resource Planning (ERP) Systems are usually used to manage the supply chain of the enterprise. ICSs are rarely connected directly to the enterprise zone.

DMZ. The ICS-Demilitarized Zone is set between IT (Enterprise Zone) and OT (Control Zone). Replication servers, patch management servers, engineering workstations, and configuration management systems are commonly deployed in this area.

Control Zone. Control Zone is subdivided into four levels including operations control, supervisory control, basic control and process. The operations control level typically contains SCADA’s master station and other ICS system’s master station with supervisory function. And HMIs commonly present in the supervisory control level. Basic control level is the main location for equipment like PLCs, and the functional include batch control, discrete control, continuous control, and hybrid control. The process level usually named as Equipment Under Control (EUC), the physical equipment being controlled by basic control level is located in this level.

The situation awareness solution for ICSs should be well cover the three zones described above. That is to say, the SA infrastructure have the ability of comprehensive situation awareness across enterprise zone, DMZ, and control zone environments.

2.2 ICS cyber kill chain

The Cyber Kill Chain, adapted from the concept of military kill chains, is created for better detecting and responding to cyber-attacks [10]. Considering the nature of ICS-custom cyber-attacks, the two stage of the ICS Cyber Kill Chain is introduced [8]. The brief block diagram of ICS Cyber Kill Chain Stage1 and Stage2 is shown in the right part of the Figure.1.

Stage1 Cyber Intrusion Preparation and Execution. This stage includes five phases consisting of planning, preparation, cyber intrusion, management & enablement, sustainment, entrenchment development & execution. In this stage, the purpose of attackers may be to collect the information about ICSs, defeat internal perimeter protections, or gain access to OT environments.

Stage2 ICS Attack Development and Execution. This stage consists of three phases including attack development & tuning, validation, and ICS attack. Attackers in stage2 must use the knowledge leaned in stage1. The attack-behaviour in this stage may be trigger, deliver, modify, inject, hide, or amplify.

The situation awareness solution for ICSs should be have the ability of the perception of the clues in the ICS cyber kill chain within a volume of time and space. The ICS cyber kill chain can be used for the comprehension of the data gathered from IT and OT environment. And then the future states and events can be projected based on the situation awareness infrastructure.

2.3 Situation awareness framework

Based on the ICS cyber kill chain, a situation awareness solution framework for industrial control system is shown in Figure.1. The situation awareness solution has four basic components: Perception Probes, IT SA Centre, OT SA Centre, and Comprehensive SA Centre.

Perception robes are located in enterprise zone, DMZ, and control zone. They can be professional equipment with flow analysis function, firewall, intrusion detection system, intrusion protection system, log audit system, network switch etc. Probes are responsible for sensing and capturing important cues and elements in IT and OT environments, especially the warning messages. And then the data collected by probes will be sent to IT SA Centre or OT SA Centre. IT SA Centre is in charge of storage, integrating, and processing the perception data from various probes deployed in enterprise zone and DMZ. Then correlating among the information is analysed. Based on the perception and understanding of the IT environment, considering the ICS Cyber Kill Chain Stage1, IT SA Centre can provide a real-time, converged SA capability, a variety of cyber-attack prevention, detection, response, reporting, and mitigation capabilities within the range of IT networks of the organization. OT SA Centre provides a real-time, converged SA capability includes probe data from OT networks and equipment. Based on the perception and understanding of the OT environment, considering the ICS Cyber Kill Chain Stage2, OT SA Center can provide a variety of ICS-cyber-attack prevention, detection, response, reporting, and mitigation capabilities within the range of control zone of the organization. Comprehensive SA Centre correlates meaningful sensor data between IT SA Centre and OT SA Centre, that will produce actionable alerts. Some organizations monitor IT and OT separately. According to the whole ICS Cyber Kill Chains, a more comprehensive SA is necessary for enhancing the ability to advanced persistent threat toward ICSs.

2.4 Logical architecture of SA centre

Logical architecture of SA Centre is shown in Figure 2. In every SA Centre, the capabilities of attack prevention, detection, response, reporting, and mitigation are set up based on the analysis of the sensor data collected by perception probes. The correlation analysis models are usually related to the ICS Cyber Chain, considering the threat intelligence, user behaviour, vulnerabilities, port, security events, or statistic. The machine learning model, backtracking model, and attack scenario analysis model are also used in the comprehension of the situation, and the projection of the security status in the near future.

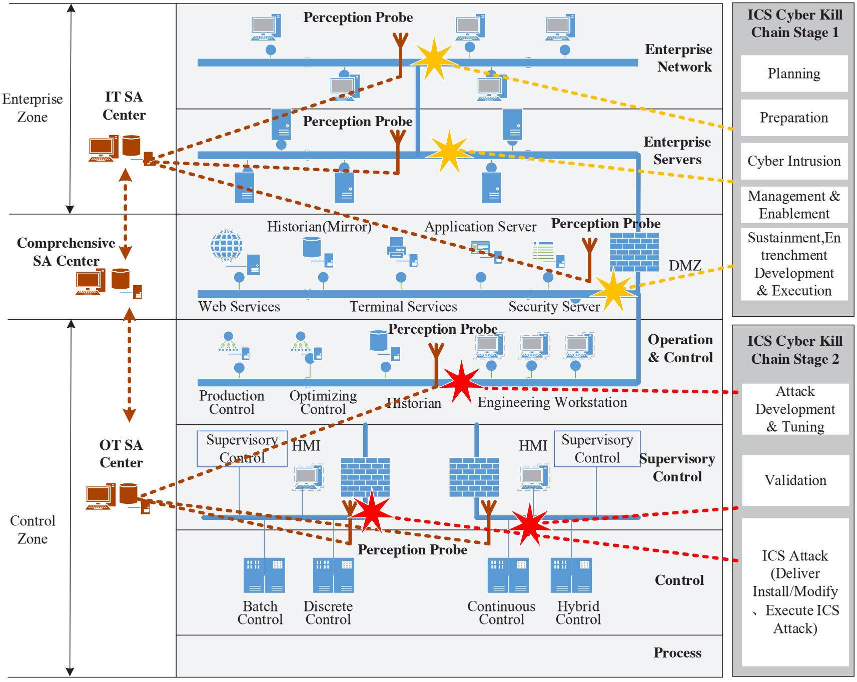

Fig. 1. Situation awareness framework for industrial control system based on cyber kill chain.

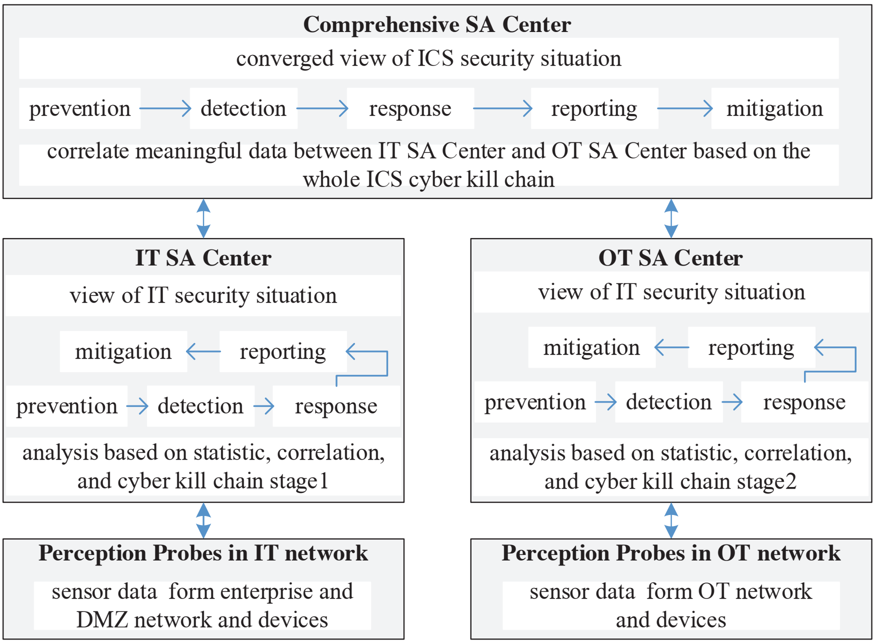
Comprehensive SA Center
converged view of ICS security situation
prevention
detection
response
reporting
mitigation
correlate meaningful data between IT SA Center and OT SA Center based on the whole ICS cyber kill chain
IT SA Center
view of IT security situation
mitigation
reporting
prevention
detection
response
analysis based on statistic, correlation, and cyber kill chain stage1
OT SA Center
view of IT security situation
mitigation
reporting
prevention
detection
response
analysis based on statistic, correlation, and cyber kill chain stage2
Perception Probes in IT network
sensor data form enterprise and DMZ network and devices
Perception Probes in OT network
sensor data form OT network and devices

Fig. 2. Block diagram for the logical architecture of SA Centre.

Visualization technology is adopted for intelligent analysis presentation. The situation of threat, risk, external attacks, insider attacks, and data security can be friendly shown to the manager. The view of data monitoring, collection, aggregation, and analysis is helpful in making decisions with the goal of enabling a state prediction.

The function of a SA solution may include: advanced security dashboard views, intrusion detection, IT and ICS devices management, security event management, and so on. A well designed and developed ICS SA Centre is expected to provide alerting mechanism.

3 Conclusions

In this paper, we propose a reference framework for ICS situation awareness based on Purdue ICS Model. Also the block diagram for the logical architecture of SA Center is presented. The proposed framework can be used to design ICS SA to monitor the whole cyber kill chain of attacks target to ICSs. The development of ICS SA solutions for different scenes will be focused on in the future.

In this paper, the research was sponsored by the 333 Project in Jiangsu Province of China under Grant No. BRA2018317.

References

1. S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, In:A survey of approaches combining safety and security for industrial control systems, Reliability Engineering & System Safety, vol. 139, pp. 156-178(2015).
2. M.R. Endsley, “Toward a theory of situation awareness in dynamic systems,” Human factors, vol. 37, no.1 pp. 32-46,(1995).
3. R. Langner. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy, p. 49-51, vol. 9 (2011).
4. 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).
5. 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, , p. 1-16(2015).
6. R. Leszczyna, I. N. Fovino, and M. Masera. Approach to security assessment of critical infrastructures' information systems, IET Information Security, p. 135-144, vol. 5(2011).
7. A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet. Taxonomy of information security risk assessment (ISRA). Computers & Security, p. 14-30, vol. 57(2016).
8. Micheale J. Assante and Robert M. Lee, The Industrial Control System Cyber Kill Chain. SANS Institute InfoSec Reading Room. (2015).
9. Cline E. Bodungen, Bryan L. Singer, Aaron Shbeeb, Stephen Hilt, Kyle Wilhoit. Hacking exposed industrial control systems. Mc Graw Hill Education.(2017).
10. Eric M. Hutchins, Michael J. Clopper and Rohan M. Amin, Ph.D., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.
11. https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf