Understanding Security Requirements for Industrial Control System Supply Chains

Ye Hou
Security Lancaster Institute
Lancaster University
United Kingdom
houye14@googlemail.com

Jose Such
Department of Informatics
King's College London
United Kingdom
jose.such@kcl.ac.uk

Awais Rashid
Bristol Cyber Security Group
University of Bristol
United Kingdom
awais.rashid@bristol.ac.uk

***Abstract*—We address the need for security requirements to take into account risks arising from complex supply chains underpinning cyber-physical infrastructures such as industrial control systems (ICS). We present SEISMiC (SEcurity Industrial control SysteM supply Chains), a framework that takes into account the whole spectrum of security risks – from technical aspects through to human and organizational issues – across an ICS supply chain. We demonstrate the effectiveness of SEISMiC through a supply chain risk assessment of Natanz, Iran's nuclear facility that was the subject of the Stuxnet attack.**

***Index Terms*—security requirements, cyber-physical systems, risk decision-making, supply chains.**

I. Introduction

Industrial Control Systems (ICS) are a specific-type of cyber-physical system often used to manage critical infrastructure such as water treatment and distribution, gas and electricity supply as well as automation and manufacturing. Contemporary ICS are complex socio-technical systems that include: hardware, e.g., programmable logic controllers (PLCs) and remote telemetry units (RTUs); software to implement the logic driving such hardware that interacts with the physical process, e.g., water treatment; and social actors, e.g., humans and organizations that operate such control systems. The last 20 years have witnessed a steady increase in the number of cyber attacks on ICS. Examples include Maroochy Water Services (2000), Stuxnet (2010), German Steel Mill (2014) and the Ukrainian Power Grid (2015). Such attacks have exploited vulnerabilities in software, hardware, network architectures as well as human and organizational aspects.

Consequently, a range of standards and methods for managing ICS cyber security risks have been developed. Examples include the National Institute of Standards and Technology (NIST) SP800-82 and SP800-82r2 and the UK Centre for Protection of National Infrastructure (CPNI) Good Practice Guide for Process Control and SCADA security. These frameworks and good practice guides are often used to define security requriements. However, these standards and methods only consider the CPS infrastructure in an individual organization in isolation. They do not take into account how member organizations of an ICS supply chain assess and manage security risks—and how this, in turn, impacts the security requirements. The supply chain poses substantial cyber security risks, as ICS components and software are supplied by one or more vendors and often rely on other outsourced service suppliers. However, the owner organization of the ICS has little control over the ICS supplier systems and the risks arising from potentially varied security practices within the supply chain. Previous works on ICS cyber security risk assessment have largely focused on physical and technical issues, neglecting social, organizational, and human aspects when analyzing, assessing and managing such risks. Furthermore, systematic approaches for assessing how cyber security risks from one organization affect another organization or a whole ICS supply chain have not been developed.

SEISMiC (SEcurity Industrial control SysteM supply Chains) has been designed to treat cyber security risks in a holistic fashion across the supply chain of ICS. In SEISMiC, the ICS supply chain is viewed as a socio-technical system comprising software, hardware, physical components, humans and organizations. This ensures that security risks arising from these various elements are not treated in isolation but integrated to develop an overall picture that can guide stakeholder decisions to mitigate risks. Such mitigation may, for instance, lead to new requirements for implementing secure software development processes (e.g., SDLC: Secure Development Lifecycle), before any 3rd party software or service providers can be part of the supply chain.

II. Related work

Existing cyber security risk frameworks for ICS fall into three main categories: i) international/national standards and guidelines on ICS cyber security [1]–[3]; ii) quantitative risk assessment [4], [5]; and iii) attack tree approaches [6]–[8]. Standards provide a high level guidance for improving and managing cyber security risks in ICS contexts. However, they lack consideration of the systemic impacts arising from the supply chain. Quantitative methods provide consequence-oriented figures on vulnerabilities/threats but the probabilities and impact metrics used are difficult to estimate. Also, they mainly focus on technical risks, which align with ICS components and do not address the wider context, such as social and organizational factors [9]. Attack trees provide a

This work was funded by InnovateUK Grant ICS/SCADA Risk Framework and Passive Network Appliance (56507-425167)

logical breakdown of all possible paths to an unexpected event. However, they are limited to the attackers point of view on the target organization [9]. None of the methods in all three categories consider cyber security risks from the supply chain.

III. SEISMIC

SEISMiC's risk assessment approach is based on a socio-technical view of an ICS supply chain. Specifically, we adapt and extend an existing socio-technical threat model for software supply chains [10] with the ICS-specific elements from the Purdue Reference Architecture (PERA) [11]. As shown in Fig. 1(a), this ensures that organizations in the ICS supply chain (including non-ICS organizations with regular IT systems) are seen as socio-technical systems that interact with the local ICS organization. Furthermore, SEISMiC's socio-technical view of a supply chain organization comprises of four dimensions: organizational culture, organizational structure, ICS risk assessment methods and ICS cyber security technologies. These four dimensions collectively define the ICS cyber security status of an organization – a change in one will impact the overall cyber security of the organization and potentially the supply chain. For example, if technology is changed, say an organization implements a new authentication technique for manufacturing operating systems, then culture, structure and methods may need to be changed. A lack of cultural change, for instance, may lead to users finding ways to avoid authentication, hence leaving the system insecure.

Unlike linear models, e.g., ISO 270019 and NIST SP800-82r2, SEISMiC is a cyclic process (Fig. 1(b)) inspired by Boehm's spiral model [12]. Analysts iterate through SEISMiC's steps, allowing for an incremental and adaptive consideration of cyber security risks in the local (end-user) and other organizations in the supply chain. Each cycle represents an organization's risk process status, starting with the local (i.e. end-user) organization (cycle 0), peer-to-peer interactions in one supply chain (cycle 1), whole single supply chain (cycle 2), and multiple supply chains (cycle 3). There are four main activities in each cycle: context establishment; risk identification; risk analysis & tracing; and risk evaluation & iteration. We discuss these next through an application of SEISMiC to Stuxnet.

IV. Case Study – Stuxnet

We consider Natanz, Iran's nuclear power plant targeted by Stuxnet, as the local (end-user) organization.

Cycle 0: Local Organization

Context Establishment: It is necessary to establish the risk context before analysis, since it helps the organization to scope and appropriately focus on the subsequent ICS cyber security risk analysis and assessment process [9]. For example, Natanz should consider both technical (i.e., PP, ID, CS, MOS in Fig. 1(a)) and social elements (i.e., human, SC & P, E & R) as well as possible internal and external influences on security, such as organizational business goals, security budget, nation state threats. The context also includes objectives and constraints such as "protect safe control over centrifuges".

Risk Identification: ICS cyber security risks are identified locally using SEISMiC's socio-technical model. A comprehensive list of identified social and technical risks for Natanz is shown in Fig. 2 (column "Natanz"). Traditional risk assessments mainly focus on technical risks, i.e., level 0 to 4 of SEISMiC's socio-technical model – physical process, intelligent devices, control systems, manufacturing operating systems, and business logistics systems. In contrast, SEISMiC also considers social factors. In the Stuxnet case, initial infection began with insecure behaviour towards usage of removable storage media (i.e. USB drives, which were used to deliver Stuxnet across the air-gapped network) or malicious email attachments. Technical vulnerabilities such as weak authentication in MOS and CS level were subsequently exploited, leading to physical damage to the centrifuges.

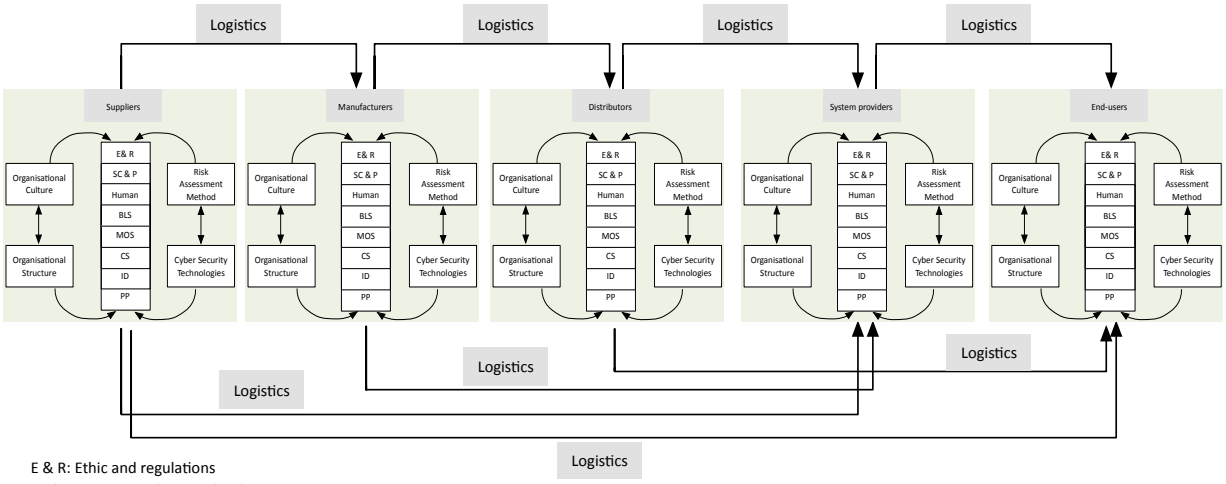
Risk Analysis and Tracing: SEISMiC's recursive risk analysis integrates context analysis (CA) [13], performance shaping factor (PSF) analysis [14], and fault tree analysis (FTA) [15], to understand human and social aspects in organizations together with technical factors. CA is used to explain how social and organizational factors affect organizations. PSF analysis focuses on how individual-level factors influence human performance. The outputs of the CA and PSF form input to the FTA to analyze the causes that may contribute to a potential risk. The recursive risk analysis starts with initial social and technical risk events, which are then traced toward their consequences, providing a clear causal relationship between risks and their causes. For example, insecure human behaviour regarding USB drives at Natanz can be traced to underlying causes, such as ICS security culture, values & norms, ICS security knowledge, opportunity or physical access.

Risk Evaluation and Next Iteration: Following completion of local risk analysis and assessment, organizations identify relevant security requirements. They can then decide whether to plan for a new iteration of SEISMiC. For example, Natanz analysis reveals that the human error risk is caused by weak ICS security culture. This, in turn, leads to requirements such as, clearer security policies on removable storage media and need for developing a cyber security culture through regular training and awareness raising.

Cycle 1: Risks in Supply Chain

Context establishment: In Cycle 1, stakeholders in the supply chain are integrated into the risk context. There are many stakeholders in the ICS supply chain for Natanz. For simplification we consider the five stakeholders compromised by Stuxnet before Nantanz itself: Foolad (ICS system provider and vendor), Behpajooh (ICS supplier and vendor), Control-Gostar Jahed (ICS system provider and vendor), Neda (ICS component supplier), and Kala (ICS manufacturer).

Risk Identification: Similar to Natanz in Cycle 0, risk identification is done for each organization in the supply chain (cf. Fig. 2). For example, in order to infect the target, Stuxnet would need to infect stakeholders in Natanz's supply chain, such as malware affecting Behpajooh transferred to Natanz via



E & R: Ethic and regulations
SC & P: Security culture and policies
Human
BLS: Business Logistics Systems
MOS: Manufacturing Operating Systems
CS: Control Systems
ID: Intelligent Devices
PP: Physical Processes

(a)

(b)

Fig. 1. (a) SEISMiC's socio-technical model of ICS supply chain (b) SEISMiC's spiral ICS risk assessment process model

			Natanz (End-user)	Foolad (Vendor1)	Behpajooh (Vendor2)	Control-Gostar (Vendor3)	Neda (Supplier)	Kala (Manufacture)
ICS social aspects	ICS regulations		N/A	N/A	N/A	N/A	N/A	N/A
	ICS security culture		Operational risks; Communication risks	Operational risks	Operational risks	Operational risks;	Communication risks	Operational risks; Communication risks
	ICS security policy		Malware	Social engineering attack; Malware	Social engineering attack; Malware	Malware	Malware	Social engineering attack; Malware
	Human		Sabotage Human error	Human error	Human error	N/A	N/A	Human error
ICS technical aspects	BLS	CPU, IT/IS systems, Servers	Network scanning/probing	Malware; Abuse of authorized access; Network scanning/probing; Information leakage	Malware; Abuse of authorized access; Network scanning/probing; Information leakage	Network scanning/probing; Information leakage	Network scanning/probing; Information leakage	Malware; Abuse of authorized access; Network scanning/probing; Information leakage
	M OS	Historians, Accounting services	Weak authentication Abuse of authorized access;	Abuse of authorized access	Weak authentication	Abuse of authorized access	Abuse of authorized access	Weak authentication Abuse of authorized access
	CS	HMI, SCADA, Alert systems, Firewalls	Man-in-the-middle attack;	Man-in-the-middle attack	Network scanning & probing; Man-in-the-middle attack	Network scanning/probing	Network scanning/probing	Man-in-the-middle attack
	ID	DCS, PLCs, RTUs,	N/A	Malware	Malware	N/A	N/A	Malware
	PP	Sensors,	N/A	N/A	N/A	N/A	N/A	N/A

Legend: BLS: Business Logistics Systems; MOS: Manufacturing Operations Systems; CS: Control Systems; ID: Intelligent Devices; PP: Physical processes

Fig. 2. Security risks in the Natanz supply chain

infected USBs carried by Behpajooh employees for service update. Malware could also be transferred via any infected laptop carried over by either Kala's or Behpajooh's employees. By comparing risks with other stakeholders in the supply chain, Natanz could identify such risks and whether they are transferable to itself.

Risk analysis, tracing and evaluation. Once such supply chain risks are identified, Natanz could identify relevant security requirements, e.g., security awareness training regarding external contractors' devices, strengthening anti-malware tools and analysis, enforcing mandatory scanning of external drives, etc. Alternatively, there could be mandatory security requirements for suppliers and/or strict service-level agreements regarding security.

Cycles 2 and 3 These operate in a similar fashion to Cycles 0 and 1 but enable treatment of a supply chain as an entity being risk assessed (Cycle 2) and comparison of risks across multiple supply chains (Cycle 3). For instance, Natanz could use a Cycle 3 analysis to identify the potentially most vulnerable supply chain or contrast the levels of risk arising from different supply chains.

V. Conclusion

SEISMiC is a comprehensive and iterative socio-technical framework for identify security requirements arising from risks in ICS supply chains. The Natanz case demonstrates that such a holistic socio-technical perspective can uncover risks from the supply chain early on, supporting effective risk decision-making and identification of security requirements.

References

[1] C. Chittester and Y. Haimes, "Risks of terrorism to information technology and to critical interdependent infrastructures," *Journal of Homeland Secure Emergency Management, 1(4)*, 2004.

[2] C. Beggs and M. Warren, "Safeguarding australia from cyber-terrorism: a proposed cyber-terrorism SCADA risk framework for industry adoption," in *Proc. Australian Inf. Warfare and Sec. Conf.*, 2009, pp. 5–20.

[3] A. Jillepalli *et al.*, "Security management of cyber physical control systems using nist sp 800-82r2," in *Proc. International Wireless Communications and Mobile Computing Conference*, 2017, pp. 1864–1870.

[4] J. Yan *et al.*, "A PMU-based risk assessment framework for power control systems," in *IEEE Power & Energy Soc.*, 2013, pp. 1–5.

[5] Q. Zhang *et al.*, "Multimodel-based incident prediction and risk assessment in dynamic cyber security protection for industrial control systems," *IEEE Trans. Sys., Man, & Cybernetics*, pp. 1429–1444, 2016.

[6] A. Roy *et al.*, "Cyber security analysis using attack countermeasure tree," in *Proc. 6th Workshop on Cyber Security and Information Intelligence Research, ACM*, 2010, pp. 28–32.

[7] J. Lopez *et al.*, "Using attack tree to assess security controls for supervisory control and data acquisition systems," in *7th International Conf. Information Warfare and Security*, 2012, pp. 166–177.

[8] S. Kriaa *et al.*, "Modeling the stuxnet attack with bdmp: towards more formal risk assessments," in *Proc. International Conf. Risks and Security of Internet and Systems*, 2012.

[9] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, pp. 1–27, 2016.

[10] B. A. Sabbagh and S. Kowalski, "A socio-technical framework for threat modeling a software supply chain," *IEEE Sec. & Priv.*, pp. 30–39, 2015.

[11] P. Didier *et al.*, *Converged Plantwide Ethernet Design and Implementation Guide*. CISCO Systems and Rockwell Automation, 2011.

[12] B. Boehm, "A spiral model of software development and enhancement," *IEEE Computer, 21(5)*, pp. 61–72, 1988.

[13] A. E. Scheflen, "Communication and regulation in psychotherapy," *Psychiatry, 26*, pp. 126–136, 1963.

[14] Y. Chang and A. Mosleh, "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents part5," *Reliability Engg. & System Safety*, pp. 1076–1101, 2006.

[15] E. Henley and H. Kumamoto, *Reliability Engineering and Risk Assessment*. Prentice-Hall, Englewood Cliffs, NJ., 1981.