Iiro Jantunen*

Cybersecurity Considerations of Industrial Automation Supply Chain

Abstract: The assessment of reliability of industrial automation hardware and software suppliers is commonplace. The September 2024 attacks on pagers and walkie-talkies in the Middle East, however, cast a shadow over the devices of reliable suppliers, also. The possibility of someone in the supply chain hiding harmful components or software in automation devices and systems requires thorough consideration. The EU cybersecurity directive (NIS2) and similar regulations also put demands for industrial entities to manage their supply chain risks.

It is advisable for the purchaser of industrial automation to address the cybersecurity of the ordered system and its supply chain already at the request for proposal stage, just as with other technical requirements. Industry standards and guidelines help. A clear table of requirements facilitates the project by providing both the customer and the supplier with a consistent picture of the desired outcome. If cybersecurity requirements are only raised during the project, the risks are additional costs for extra work as well as superficial security.

Installation, maintenance, and servicing, including software updates, are also important parts of the supply chain from the security perspective. This applies to both on-site service personnel and transport of the devices for external maintenance.

Keywords: cybersecurity, ICT/OT, supply chain, maintenance, automation hardware, automation software, device tampering, computer viruses

***Corresponding Author: Iiro Jantunen,** Rejlers, E-mail: iiro.jantunen@rejlers.fi

1 Introduction

The September 2024 attacks [1] made visible the risk inherent in purchasing automation systems and components. Even the devices provided by reliable manufacturers can be tampered within the supply chain. An explosive is by no means necessary to cause damage: it is enough to disrupt the operation of an industrial plant with e.g. software, such as the Stuxnet virus [2]. The failure (or destruction) of industrial machinery or process equipment may also cause wider damage to the facility, the personnel, and the environment. Cybersecurity thus affects also the safety of automation systems [3]. The automation supply chain contains vulnerabilities at all stages from component suppliers to maintenance [4]. If an outsider in the supply chain gains access to the device, it can be tampered. If this outsider has the resources of a state intelligence service, the device and its packaging could probably be modified so that no changes in the supply chain are detected at a later stage. This also applies to software.

2 Standards and regulations

Certified compliance with technical standards such as the IEC 62443 family (OT) and the ISO/IEC 27000 family (ICT) as well as requirements set by the EU 2024/2847 Cyber Resilience Act (CRA) to CE markings, guarantee to a certain extent that the original manufacturer of the device has made the device secure. A supply chain still has its inherent vulnerabilities.

In Europe, the issue has been proactively addressed: the EU Cybersecurity Directive (NIS2), which came into force in October 2024, requires companies and other actors to ensure supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers [5]. The implementing regulation EU 2024/2690 specifies requirements for supply chain security [6]. These requirements should be thoroughly understood by the companies that purchase automation equipment and systems.

Guidelines for the monitoring of supply chains can also be found in public sources such as *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST). This publication advises to obtain components either directly from the manufacturer, an authorized distributor or an authorized reseller, in that order [7]. Purchasing organizations should verify the authorization of a distributor or reseller. Proper due diligence of suppliers should be performed, and the prime contractors should require similar control and requirements from relevant sub-tier contractors [8]. Also procured engineering services should be regularly evaluated from a security point-of-view.

It is worth noting that the supply chain does not only refer to equipment, but also to software as well as services. Extensive studies of system and component vulnerabilities (OT:ICEFALL [9] and INFRA:HALT [10]) have found that OT components often use poorly maintained software components, such as runtime systems and TCP/IP software.

The case of CrowdStrike Falcon software update in July 2024, as well as other similar incidents, emphasizes the risks of poorly managed software updates [11]. Timely execution of cybersecurity-related updates is crucial, but the balance between testing and speed must be set carefully. Cyber resiliency analysis of systems is needed, considering all relevant attack types. This is especially important in industrial system environments. Should a malicious party be able to insert their code into a software update, they would be able to hit several industries with a single strike.

Maintenance and servicing are also important parts of the supply chain from a security perspective as they can compromise system integrity. This applies to on-site service personnel, remote software maintenance and reconfiguration, and transportation to external maintenance. In the latter case, the security of logistics services should also be considered. Note the EU NIS2 requirement of human resources security and access control policies [12, 13]. Any trespassing of locked area containing network or automation systems can compromise system integrity (the case of break-ins in water services around Finland as an example [14]).

For all this, one needs a comprehensive asset management system to keep track of all the devices and software, as well as their dependencies, included in one's ICT/OT systems [15, 16].

3 Conclusions

Companies must understand their risk profile and adjust the measures they use accordingly. A cyberattack by a foreign state is more likely to happen in sectors critical to society (such as the essential and important entities defined by EU NIS2 [17]) than in less critical sectors. On the other hand, the risk posed by criminal actors depends more on the potential of financial damage and thus, inversely, gain.

The purchaser of industrial automation should address the cybersecurity of the ordered system and its supply chain already at the request for proposal stage, just like other technical requirements. A clear table of requirements included with the request for proposal for the supplier to fill out facilitates the project in advance by providing both the purchaser and the supplier with as consistent a picture as possible of what is desired as the outcome. Aforementioned standards and guidelines help in writing the requirements. If cybersecurity requirements are raised only during the project, the risk is low superficial security as well as additional costs for extra work.

Even the best cybersecurity practices can be thwarted by the human factor. Policies must therefore be taught to all relevant people. However, people are prone to mistakes, especially when they are stressed or in a hurry — just when they should be at their most careful. If cyber-secure operations are made difficult and laborious, the temptation for an easy shortcut is great.

4 Bibliography

1. R. Berg, Ex-Israeli agents reveal how pager attacks were carried out, BBC, 23.12.2024
2. D. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, The New York Times, 1.6.2012.
3. T. Malm, R. Tiusanen, J. Berger, Comparing cybersecurity and functional safety risk assessments, in Proc. SIAS 2024.
4. J. Simola, A. Takala, R. Lehtonen, T. Frantti, R. Savola, The Importance of Cybersecurity Governance Model in Operational Technology Environments, in Proc. 23 ECCWS 2024.
5. EU Directive 2022/2555, ch. IV, art. 21.2.d & 21.2.e, 14.12.2022.
6. EU 2024/2690, Annex I, ch. 5, 17.10.2024.
7. J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, M. Fallon, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161r1, 2022, p. 141.
8. Ibid. p. 151.
9. OT:ICEFALL — The legacy of "insecure by design" and its implications for certifications and risk management, Vedere Labs, 2022.
10. INFRA:HALT — Jointly discovering and mitigating large-scale OT vulnerabilities, Forescout Research Labs & JFrog Security Research, 2021.
11. R. Yahalom, What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk, Harward Business Review, 10.1.2025.
12. EU Directive 2022/2555, ch. IV, art. 21.2.i, 14.12.2022.
13. EU 2024/2690, Annex I, ch. 10, 17.10.2024.
14. J. Mäntysalo, Murtautumiset kriittisiin kohteisiin herättivät kesällä pelkoa Suomessa — tämä niiden tutkinnasta tiedetään nyt, YLE, 20.1.2025.
15. EU 2024/2690, Annex I, ch. 12, 17.10.2024.
16. EU 2024/2847, Annex I, pts. II.1 & II.6, 23.10.2024.
17. EU Directive 2022/2555, ch. I, art. 3, 14.12.2022.