Cyber (In-)security of Industrial Control Systems: A Societal Challenge

Eric Luiijf[(✉)]

Netherlands Organisation for Applied Scientific Research TNO,
P.O. Box 96864, The Hague, The Netherlands
`eric.luiijf@tno.nl`

Abstract. Our society and its citizens increasingly depend on the undisturbed functioning of critical infrastructures (CI), their products and services. Many of the CI services as well as other organizations use Industrial Control Systems (ICS) to monitor and control their mission-critical processes. Therefore, it is crucial that the functioning of ICS is well protected inter alia against cyber threats. The cyber threat areas to ICS comprise the lack of proper governance as well as cyber security aspects related to organizational, system and network management, technology and technical issues. Moreover, newer functionality entering organizations is often controlled by embedded ICS which hide itself from those that are responsible for cyber security. The immature cyber security posture of ICS and their connectivity with public networks pose a major risk to society. This article explores the threats, provide some examples of cyber incidents with ICS, and will discuss the ICS security challenges to our societies.

Keywords: Critical infrastructure · Cyber security · Cyber resilience · ICS · Industrial Control Systems · Supervisory Control and Data Acquisition · SCADA

1 Introduction

Our society and citizens increasingly depend on the undisturbed functioning of critical infrastructures (CI), their products and services. Despite national differences, most national definitions of CI have alike elements, see e.g. the CIPedia© website definitions of critical infrastructure by a manifold of nations [2]. The EU definition of CI is 'An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions' [3]. Examples of CI sectors are energy (power, oil, gas), transport (road, air, rail, ship, pipeline), drinking water, waste water, water management, financial services, and public administration [2]. Many of the mission-critical processes that are crucial to deliver CI

services in a reliable fashion rely on the correct functioning of Industrial Control Systems (ICS) 24/7. Any failure of ICS, cyber-initiated ones in particular, may both cause mission-critical processes of organizations to fail and may result in safety risk to people and or the environment. Therefore, the cyber security and cyber resilience of ICS is of utmost importance to our society as a whole, to CI operators, and many other public and private organizations. Nevertheless, organizations, manufacturers and system integrators collaboratively have failed to a large extent to address the cyber threats to ICS which stem from the lack of proper governance as well as organizational, system and network management, technology and technical issues [1].

Apart from the monitoring and control of crucial CI processes such as the power grid, ICS monitor and control processes in many other small to large organizations. ICS may be as small as a single programmable logic controller (PLC) automating and controlling a very simple process. Often such ICS are embedded in acquired functionality by the organization. As will be discussed below, such ICS hide itself from proper information security governance as the acquired function falls under the responsibility of unconscious insecure management and operators. Moreover, the physical ICS components are put in a closet or hidden within a piece of equipment which has wireless connectivity. The result is that the cyber safety and security risk related to the ICS-controlled processes is unmanaged.

Unnoticed we are surrounded by ICS controlled and monitored services which allow the well-functioning of our society. ICS make our lives easy. An illustrative example of the pervasive penetration of ICS in our daily live can be found in 'Good Morning with ICS' [8].

As the societal impact may be high, collective action is needed by all stakeholders to address the ICS cyber security challenges in order to mitigate the risk to society, our safety, health and environment. The next sections will discuss the risk aspects and need for governance in more detail.

2   Definitions

A *critical infrastructure* (CI) consists of those assets and parts there of which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economy or social well-being of people [3].

Cyber resilience is defined as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery [14].

Cyber security is defined as the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure [4].

3 Paradigm Changes to ICS

3.1 From Closed to too Open Environments

ICS were traditionally designed around process reliability and safety [12]. For long, cyber security was not a design consideration for ICS because:

1. ICS were based on specialized hardware, proprietary code and protocol standards. Only specialists knew about how to use and tweak ICS. Nobody else, including hackers, would be interested in ICS, their protocols and telecommunication means.
2. ICS are operated as a closed environment without any external connection.
3. ICS operate only in benign environments without hackers or malware. Manufacturers therefore had no reason for creating secure and robust ICS protocols and to stress-test ICS protocol implementations.
4. The end-users of ICS did not ask for cyber secure ICS; they only asked for new functionality and user friendly interfaces.

The aforementioned paradigm shift took place due to the take up of the fast innovation cycles in information and communication technologies (ICT) in general and in ICS networking. All basic assumptions mentioned above about the security by obscurity and benign environments of ICS have been flawed by those developments, as outlined by [8] at pp. 23–24:

1. ICS applications increasingly operate on commercial off-the-shelf (COTS) hardware, common operating systems such as Windows and Unix, and use the TCP/IP suite of protocols for communications. ICS applications moved to open source environments. ICS control apps can be found on smart phones and are probably migrating to smart watches right now.
2. ICS knowledge and documentation is widely available on the Internet.
3. ICS networks are either directly or indirectly connected to public networks such as the Internet to reduce communication costs and to control processes from home locations.
4. ICS have fallen victim to disgruntled insiders. Hackers have become very interested in ICS as is shown by the number of ICS-related talks at Black Hat and Def Con® hacking conventions. Moreover, ICS security testing frameworks for the MetaSploit toolset are publicly available [8].

3.2 Hide in Functionality but Connected to Internet

Functionality acquired under the responsibility of a non-IT department is 'since history' controlled and monitored by process automation. However, gradually process automation with switches and relays have been replaced 'under the hood' by ICS which in the last years evolves to ICS that is largely based on common commercial-off-the-shelf information and communication technologies. Small but powerful ICS can be found at the road site, above the ceiling, in vehicles and behind innocent looking display panels. The management and operators

of 'functionality' still think in terms of the old on/off switches and a knob to crank up the flow of the controlled process. The fact that there is ICS operating between the display with the switch or knob, and the monitored and controlled the actuator, motor or valve, etcetera, is not recognized. The notion of ICS and information and communication technologies with a potential high cyber security risk is only subconsciously present [6]. The responsible department for, e.g. the city waste water processing, traffic control, speed and observation cameras, and ferry operations allows the connection of the embedded ICS to public networks for remote management and third party maintenance in an unsecured fashion. The Industrial Risk Assessment Map (IRAM) project by the Freie Universität Berlin, Germany used the Shodan search engine [13] to globally locate ICS connected to the Internet. They mapped the discovered ICS on a geographical map of the globe. Project SHINE (SHodan INtelligence Extraction), which ran from 2012 till October 2014, did the same and found 2.2 million of Internet-connected ICS devices [11], many of them located in European nations.

According to incidents that became publicly known, hackers and malware took control of non-CI ICS which monitor and control municipal waste water systems, tropical swimming paradise pumps, the heating, ventilation and air conditioning of a hospital, a wind power farm, the building automation system of the Salvation Army, airport baggage system, robots in a car manufacturing plant, a milk processing plant, municipal street light systems, and even quiesced a large ship at the North Sea.

4   Lack of Governance of ICS Security

4.1   The Executive Level

Governance of ICS security should start at the executive level which manages the risk to the business objectives of the organization and protects the public and private shareholder interests [8]. They understand how to make business plans and earn money from for instance transport of gas, passenger transport by metro or the mass-production of innovative electronic equipment. As most top level management has no affection with technology, a gap exists with respect to executive level interest in ICS controlled production processes. For IT- and ICT-departments it is already hard to get the attention of the executive level; for most ICS departments that is even harder. When asked about cyber security of ICS, the assignment of responsibilities is clear to the executive level: cyber security is a responsibility of 'IT'. At the same time, it is not uncommon that IT departments do not understand ICS which for most IT-departments is equivalent to 'grease, pumps and motors'. IT reboots and upgrades systems and routers when necessary, even during the lunch break. Why is the process-responsible department not able to accept a router upgrade which may take ten minutes to half an hour?

On the other hand, the responsible department for process automation and ICS does not understand the ICT domain, their issues, threats and vulnerabilities. The reason is obvious: most process engineers are not educated in IT and

cyber security. Their main focus is on process efficiency and improvements. It is therefore not surprising that the cyber security of ICS does not get the proper attention in organizations. No risk analysis takes place, no security auditing of ICS, no analysis of firewall logging, and so on. In short: organizational leadership and an integrated ICT-ICS approach are missing.

At the same time, as already was made clear by the European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS) in 2003, the then ISO/IEC 17999 standard, now ISO/IEC 27000-series, lack proper controls and support for the 24/7 ICS environment. Organizations trying to close the ICS cyber security gap using these information security standards experience trouble when trying to implement the controls in the 24/7 environment with often legacy ICS. The International Society of Automation (ISA) tries to close this gap by developing international standards for the ICS domain as outlined by [8] on pages 43–45.

5   ICS Technology

5.1   Aging, Legacy and too New ICS Technology

Despite the move of ICS to common ICT, replacement plans and the financial depreciation of hardware often still follows the old technology investment and replacement cycles of the controlled processes, that is ten years or even longer. Although the support for Windows XP ended April 8th, 2014, one can still find 486 computer running Windows XP (or even older operating systems) and an ICS application on top of that controlling for instance a MRI scanner. Many years old ICS equipment may have, considered from the current point of view, only limited CPU power and memory. Their performance is often just enough to control the process. No capacity is left for running an anti-malware package or a cryptographic algorithm.

Replacing all ICS at once is often infeasible, meaning that organizations need to operate new ICS with at the same time legacy ICS in their networks. Newer security capabilities can not be switched on as they break the interaction with legacy ICS. Careful planning to deal with legacy is required, see for some good practices [10]. At the same time, new 'plug compatible' ICS components may have on-board chip sets with a mail and web server. Easy for system engineers to deep dive in a user friendly way into the ICS component input and output states or getting an emailed alarm message. However, when the component is installed without configuring or blocking such a functionality, the services are by default accessible to unauthorized persons when they manage to get access to the network which is often the case in smaller organizations or when embedded ICS gets internetted.

5.2   Weak and Insecure ICS Protocols

ICS protocols such as Modbus moved from serial communication to implementations which also run the same protocol on top of TCP/IP. Unfortunately both

the protocols and the protocol implementations were developed with a benign closed network environment in mind. This weakness comes to the fore when a system or network manager of the IT-department starts a network scan or puts the network to a load test. Connected ICS may crash or become unresponsive; according to tests by CERN the larger part of ICS may fail [9]. Just one byte too much may cause a ping-of-death reaction as happened years ago in the Internet. Internet protocols have become well-tested and robust. ICS components controlling dangerous or mission-critical processes, however, not.

5.3   Insecure ICS by Design

ICS are packaged insecure by design. During installation one is not required to change the default factory password(s). Sometimes they even cannot be changed when it concerns a legacy system or when the manufacturer has a policy of security-by-obscurity with hard-wired passwords. Stuxnet made use of such a weakness in Siemens ICS. Nevertheless, new ICS versions still show hidden functionalities and hard-wired passwords as is exposed by, for instance, ICS-CERT bulletins [5]. There is a lack of security documentation for ICS, or when available, one has to be very persistent to find it at the end of a manual hidden on a DVD that can be found in the same box as for instance a PLC.

5.4   Common TCP-IP Based Connectivity

ICS networks are coupled directly or indirectly to the Internet, some exceptions excluded. Firewalls are sometimes hard to configure to control ICS protocols. the business side, however, wants to have information from the processes and require ICS connectivity. Process and system engineers want to have 24/7 access to ICS from home to deal with alarm and maintenance situations. Third parties that support the ICS and process operations want to have such an access possibility as well. If not supplied, they create it themselves as was found when the safety panel of a nuclear power plant went down due to a virus. The risk of malware or hackers to obtain access to ICS is high as has been demonstrated by many cyber security incidents with ICS; some of them are listed in [8].

6   ICS Maintenance and Operations

Maintaining a proper cyber security posture in the ICS environment is not easy. Apart from the governance and organizational issues discussed above, topics like password management, keeping anti-malware software current, and timely patching are major challenges for organizations knowingly operating ICS [8].

Passwords are often not individual user but group passwords with indefinite or at least many months lifetime. When someone leaves the ICS department, the very well-known passwords are not changed.

When organization care for ICS security - which is not the case for the unconscious insecure operated functionality in for instance elevators, access control systems, and HVAC-systems - malware signatures may be updated once in

a number of weeks. Patching requires an agreement by the system integrator or the manufacturer which already may take long. Then one has to plan, test and apply the patch. As a result, the window of exposure of the ICS domain and therefore mission-critical processes to malware and hackers is quite long.

7 Third Parties

Third parties often have access to the ICS domain of organizations for both on-line and remote maintenance and support. They are a risk to the organizations unless the mutual trust level is high, procedures are followed, and regular audits take place. However, with the 24/7 around the globe support, the risk is that authentication information is known around the globe. The support organization wants to keep its operation as simple as possible using the same or similar passwords 'nationwide', e.g. supportBE, supportNL. Guess what the password is for Spain or Indonesia. It is hard to convince such organizations that they need to use a strong special password for their client which does not include the organization name, nation and equivalent simplicity.

Moreover, third party support engineers may bring equipment to the inside and connect that to the ICS network bypassing all cyber security measures and procedures (if any): a perfect entry path for malware in the ICS domain.

8 Conclusion: Long and Short Term Actions

As discussed above, the potential impact of cyber-related disturbances of ICS to the society may be high. Many of these challenges have to be overcome by both end-users, system integrators and ICS manufacturers at the long run:

1. executive management leadership (see [8,14]),
2. proper governance of ICS: the right level of attention, established security policies and procedures, financial means to keep ICS up-to-date and secure, and raising security awareness,
3. organizational, procedural and technical measures,
4. development of good practice standards for ICS,
5. development of secure-by-design and secure-out-of-the-box ICS,
6. proper education and workforce development (see [8]),
7. supporting cyber security oversight by the CI regulator,
8. government support to raise ICS security awareness in all CI sectors and all ICS using organizations,
9. government to stimulate information exchange(s) on security information while avoiding the pitfalls discussed in [6].

At the same time, end-user of ICS, system integrators and manufacturers have to act now. Increase the cyber resilience of ICS monitoring and controlling mission-critical processes by:

1. give ICS cyber security instruction and require change of passwords at the end of a system acceptance test (SAT),
2. introduce proper password management (individual; decent expiration interval with a grace period),
3. audit firewall logs and network connectivity on a regular basis,
4. stress test ICS network components or network parts before they are connected to the production network,
5. disconnect the engineering test system(s) from the daily operations,
6. follow ICS-CERT and alike threat, vulnerability and intelligence resources and or become member of a sectoral ISAC ([7]),
7. being - last but not least - vigilant.

References

1. Bruce, R., Dynes, S., Brechbuhl, H., Brown, B., Goetz, E., Verhoest, P., Luiijf, E., Helmus, S.: International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues, TNO report 33680, TNO, The Netherlands and Tuck School of Business/Center for Digital Strategies at Dartmouth, USA (2005). http://www.ists.dartmouth.edu/library/158.pdf
2. CIPediaMain Page. http://www.cipedia.eu
3. EC: European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ 2008 L 345/77, Brussels, Belgium (2008). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
4. EC: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, Belgium (2013). http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf
5. ICS-CERT. https://ics-cert.us-cert.gov
6. Luiijf, E.: Why are we so unconsciously insecure? Int. J. Crit. Infrastruct. Prot. **6**(3–4), 179–181 (2013). doi:10.1016/j.ijcip.2013.10.003. http://www.sciencedirect.com/science/article/pii/S1874548213000486
7. Luiijf, E., Kernkamp, A.: Sharing Cyber Security Information. TNO, The Hague (2015). http://www.tno.nl/info-share
8. Luiijf, E., te Paske, B.J.: Cyber Security of Industrial Control Systems. TNO, The Hague (2015). http://www.tno.nl/ICS-security
9. Lüders, S.: Control Systems under attack? In: 10th ICALEPCS Int. Conf. on Accelerator and Large Expt. Physics Control Systems, CERN, Geneva (2005). https://accelconf.web.cern.ch/accelconf/ica05/proceedings/pdf/O5_008.pdf
10. Oosterink, M.: Security of legacy process control systems: moving towards secure process control systems (whitepaper). CPNI.NL, The Hague, Netherlands (2012). http://publications.tno.nl/publication/102819/5psRPC/oosterlink-2012-security.pdf
11. Radvanosky, R., Brodsky, J.: Project Shine (SHodan INtelligence Extraction) Findings Report (2014). http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014

12. Russel, J.: A Brief History of SCADA/EMS (2015). http://scadahistory.com/
13. Shodan search engine. http://www.shodanhq.com
14. World Economic Forum: Risk and Responsibility in a Hyperconnected World (WEF principles), Geneva, Switzerland (2014). http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience