National Cyber Security Centre
Ministry of Security and Justice

Checklist security of ICS/SCADA systems

Take organisational and technical measures

Factsheet FS-2012-02 | version 1.2 | 11 May 2016

Malicious persons and security researchers show interest in the (lack of) security of industrial control systems (ICS/SCADA systems). Systems which are directly accessible from the internet are criticised in particular. However, ICS/SCADA systems have more aspects that require specific attention. With this factsheet you can determine whether your ICS/SCADA systems are sufficiently protected. These measures are considered as good practice.

Target audience

Owners and administrators of ICS/SCADA systems and building management systems.

This factsheet was written in collaboration with:

Representatives of the vital infrastructure and other NCSC partners.

Background

The area of application of ICS/SCADA systems is broad and varies from simple to critical systems and processes. The owners must decide which security level and depth of measures are suitable. This decision has to be made based on a risk analysis.

Starting points

In the checklist a distinction is made between organisational and technical measures. Each measure is briefly explained, including references to more background information and implementation tips. The checklist includes measures to solve the most frequent vulnerabilities and security problems.

Checklist organisational measures 1/1

Measure	Explanation and references
1. The organisation has a security policy that also applies to the ICS/SCADA systems.	Many organisations have a security policy, but ICS/SCADA systems do not always fall within the scope of this policy. You can choose to have one policy for all systems, whereby the differences between the office and process environment are taken into account. You can also choose to have two separate documents. A sound policy contributes to taking the correct security measures against real risks. *References: ISO-2700x [1], chapter 2.1 of [2], chapter 4.2 of [5], chapter 4 of [22], ISA99/IEC62443 [23], chapter 2 of [24].*
2. The senior management has expressed its commitment regarding the security of ICS/SCADA systems and acts accordingly.	Cyber security is a shared responsibility of all employees within an organisation and in particular of managers. You must have clear agreements with the senior management about the importance of the security of ICS/SCADA systems, the use of the required resources and the budget to take measures where necessary. *References: chapter 4.2 of [5], chapter 1 of [24].*
3. Risk management is applied to all operational processes, including ICS/SCADA systems that are responsible for the primary processes. Incident management, including management reporting, has also been organised for ICS/SCADA systems.	With risk management you can determine the required security level and decide about appropriate measures. *References: chapter 2.12 and 2.18 of [2], [3], chapter 6.1 of [5], [16], [18], chapter 3 of [24].*
4. Periodically an EDP audit is carried out, during which the security of ICS/SCADA systems is also assessed.	Besides the audits, it is advisable to also periodically carry out self-assessments and penetration tests, or arrange to have these tests carried out by a third party. *References: chapter 2.16 of [2], [4], [11], chapter 11 of [24].*
5. Security requirements are set which cover the total cycle of development, purchase, management, maintenance and replacement of ICS/SCADA systems (hardware and software) and applying these requirements is ensured.	The work performed by third parties and purchased products and services must also comply with the security requirements. Therefore it is necessary to make binding arrangements. *References: part 2-4 of [5], [6], [20], chapter 6 of [24].*
6. Periodically all employees, also the employees who work with ICS/SCADA systems, must follow a security awareness training.	Humans are an important link in information security. Without sufficient awareness each (technical) measure may fail. Periodically test the awareness level of the employees. *References: chapter 2.11 of [2], [10], [19], chapter 2, 7 and 15 of [24].*
7. Be clear about the roles, tasks and responsibilities. Make a team responsible for the security of ICS/SCADA systems. Let these employees periodically follow additional security training courses. The IT department must also show commitment and offer their support.	Ownership of ICS/SCADA security is important. It must be clear who is responsible for what task. In order to carry out this ownership well, employees must also have the required knowledge and skills. *References: chapter 4.2 of [5], chapter 2, 7 and 15 of [24].*

Checklist technical and operational measures 1/2

Measure	Explanation and references
1. The ICS/SCADA systems make use of a separate network infrastructure. This network infrastructure is separated from other networks. The separation can be organised physically or logically.	By making use of a separate network infrastructure, it is prevented that disruptions or failures and security incidents in other networks (for example, the standard office network) have a direct effect on the ICS/SCADA systems. When networks are not separated from each other, it is possible that a vulnerability in the office network may also be abused to gain access to the ICS/SCADA systems. *References: [17], [23], chapter 8 of [24].*
2. Limit the connections of ICS/SCADA systems with the Internet and other networks.	Each connection is a potential risk. Periodically (at least once a year) draw up an overview of all connections of your systems with the Internet and other networks. Carry out a risk analysis for these connections to determine the correct measures. Use security equipment such as firewalls, proxy servers and data diodes and an accompanying policy. There may be a valid reason for a connection, for example for a quick failure analysis, management or process monitoring. Information between various networks should be exchanged through a separate network segment (DMZ). Make sure to use a centrally protected facility for remote access and use two-factor authentication. *References: chapter 2.15 of [2], chapter 5.8 and 6.3 of [5], Configuring remote access [9], [12], [25].*
3. A password policy has been drawn up and measures have been taken to enforce this policy. This policy minimally includes: - complexity of passwords; - change frequency; - change of default accounts and passwords, including a guarantee for deleting such accounts; - requirements regarding administrator accounts.	Password policy is an aspect that requires great attention with ICS/SCADA systems. However, it is not always possible to use user accounts/passwords. In such cases additional measures, such as physical access restrictions, will be necessary. *References: chapter 2.15 of [2], chapter 6.3 of [5], chapter 4.2 of [7].*
4. There is a policy for the use of (removable) media (such as USB sticks, hard disks and CD-ROMs) and technical measures have been taken to enforce this policy.	Many virus and malware infections on ICS/SCADA systems are caused by using contaminated storage media. Explicitly include this policy in awareness campaigns. *References: chapter 2.13 of [2], chapter 6.2 of [5].*
5. The ICS/SCADA infrastructures and systems are protected according to principles of 'defence in depth': - Subject systems as minimal as possible to other network infrastructures. - Apply hardening: switch off superfluous functions and unused services, delete non-used or unnecessary user accounts and change default passwords. - See to it that adding and changing systems and configurations is a documented and controlled process. - If possible, use antivirus software and whitelisting of applications. - Create a distinction between administrator functions and user functions and the accompanying network traffic.	As is the case with standard ICT applications, many ICS/SCADA applications are also sensitive to manipulation of the input. The chapter 'Uitvoeringsdomein Webapplicaties' of the ICT-Beveiligingsrichtlijnen voor webapplicaties – Verdieping (not yet available in English) offers an extensive description of these problems [8]. *References: chapter 2.8 of [2], chapter 4 of [7], [13], chapter 8 of [24].*

Checklist technical and operational measures 2/2

Measure	Explanation and references
6. Organise patch management: define a patch policy and remain informed about vulnerabilities, security patches and workarounds of all your system components.	Vulnerabilities in software are an important cause of many security problems. Suppliers of ICS/SCADA systems increasingly make use of standard software, systems and protocols. This also causes the accompanying security problems. Standard tooling and exploit kits can then be applied more easily. It is therefore necessary that all used software is up to date. Maintenance of systems, including security patches, may be part of maintenance contracts. Introducing security patches may also be part of the release management of a company and should also always be done in consultation with the system supplier. *References: [14], chapter 14 of [24].*
7. There is a policy for connecting mobile equipment, such as laptops, tablets, smartphones, on the business networks and technical measures have been taken to enforce this policy.	Infected equipment that is connected to the ICS/SCADA network infrastructure may cause virus and malware infections. Many suppliers use laptops for service work. This is why a total ban is not always possible in practice. Ensure that at least the system to be connected is always scanned before it is connected. You may also consider to let the external supplier only use laptops which remain under control of your own organisation (and keep these laptops on location). *Reference: chapter 2.13 of [2].*
8. Use technical tools to detect attacks. This includes a, preferably central, logging facility. This will make it easier to find out what happened in the event of incidents. Also carry out proactive inspections on this logging. In addition, make use of an Intrusion Detection System (IDS) for detecting attacks.	When reporting a hack attempt to the police, having good log files is a good thing also. An IDS can be used very well for detecting attacks because of the predictable system behaviour of many process environments. *References: chapter 2.16 of [2], [15], chapter 9 of [24].*
9. Provide appropriate physical access security to systems and locations.	Many ICS/SCADA systems cover a larger area. Local physical access to an ICS/SCADA system may have as a consequence that several or all systems in the ICS/SCADA network are accessible. In this case the weakest link determines the strength of the security chain as well. *References: chapter 2.4 of [2], chapter 12 of [24].*
10. Take measures in order to guarantee the integrity of your configurations. - Document configurations, settings and connections and register changes that have been made. - Periodically check the actual settings/configurations with the documentation and examine possible differences. - Organise change management. Check the integrity of the software when implementing in operational systems, for example by testing changes in advance in a test environment with simulation options (FAT). - Be sure that you know that the configuration which is tested in the FAT (and approved), is also implemented accordingly in the production environment (SAT).	In many configurations of ICS/SCADA systems there is no authentication for making system changes. Examples are possibilities to download new software or firmware. The options to offer protection against this greatly depend on the system and configuration. *References: chapter 2.15 of [2], chapter 4.1 of [7], chapter 4 of [24].*

Reference list

[1] ISO 27000-serie: NEN-ISO/IEC 27001 Information Security management systems. More information via www.nen.nl

[2] DHS, ICS-Cert: Catalog of Control Systems Security: Recommendations for Standards Developers

[3] DHS, ICS-Cert: Developing an Industrial Control Systems Cybersecurity Incident Response Capability

[4] DHS, ICS-Cert: Cyber Security Assessments of Industrial Control Systems

[5] National Institute of Standards and Technology (NIST): Guide to Industrial Control Systems (ICS) Security

[6] DHS, ICS-Cert: Cyber Security Procurement Language for Control Systems

[7] DHS, ICS-Cert: Common Cyber Security Vulnerabilities in Industrial Control Systems.

[8] NCSC.NL : ICT-Beveiligingsrichtlijnen voor webapplicaties

[9] DHS, ICS-Cert: Configuring and Managing Remote Access for Industrial Control Systems

[10] DHS, ICS-Cert: Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments (draft)

[11] CPNI.UK Cyber security assessments of industrial control systems - A good practice guide

[12] US-Cert: Backdoors and Holes in Network Perimeters: A Case Study for Improving Your Control System Security

[13] DHS ICS-Cert: Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

[14] DHS ICS-Cert: Recommended Practice for Patch Management of Control Systems

[15] DHS ICS-Cert: Creating Cyber Forensics Plans for Control Systems

[16] CPNI.UK : Good practice guide: 1 understand the business risk

[17] CPNI.UK : Good practice guide: 2 Implement secure architecture

[18] CPNI.UK : Good practice guide: 3 Establish response capabilities

[19] CPNI.UK : Good practice guide: 4 Improve awareness and skills

[20] CPNI.UK : Good practice guide: 5 Manage third party risk

[21] CPNI.UK : Good practice guide: 6 Engage projects

[22] CPNI.UK : Good practice guide: 7 Establish ongoing governance

[23] ISA99/IEC62443 : Standard for Industrial Automation and Control Systems Security

[24] Swedish Civil Contingencies Agency (MSB): Guide to Increased Security in Industrial Information and Control Systems

[25] NCSC Factsheet 2012-01 'Your ICS/SCADA and building management systems online'

Publication
Nationaal Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2012-02 | version 1.2 | 11 May 2016

This information is not legally binding.