National Cyber Security Centre
Ministry of Security and Justice

Your ICS/SCADA and building management systems online

Ensure an up-to-date overview and take measures

Factsheet FS-2012-01 | version 2.2 | 6 June 2016

Malicious persons and security researchers show interest in the (lack of) security of industrial control systems. This relates not only to 'traditional' ICS/SCADA systems, but also to building management systems (incl. HVAC and CCTV). These latter systems in particular can often be accessed directly from the Internet. Industrial control systems do not always fall within the scope of the security policy. Many organisations are not aware of the resultant risks. In addition, many organisations do not have an up-to-date overview of all the systems that are connected to the Internet. As a result, they do not always make a proper assessment of the risks or take the right measures.

Target audience

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

This factsheet was written in collaboration with:

Representatives of the critical infrastructure and other NCSC partners.

Background

ICS/SCADA systems are used in critical and (other) industrial sectors to automatically monitor and control physical processes. ICS/SCADA systems are used for production, transportation and distribution within our energy and drinking water supply networks. The production processes in refineries and in the chemicals, foods and pharmaceutical industries are also (largely) controlled by ICS/SCADA systems. Camera monitoring systems (CCTV), climate control systems (HVAC) and other building management systems are often classified as ICS/SCADA as well.

In the past ICS/SCADA systems communicated directly with one another in a completely closed network, and the systems were not connected to the Internet or other networks. However,

nowadays ICS/SCADA systems are often linked to the company's office IT environment and also accessible via the Internet.

When ICS/SCADA systems are connected to the Internet, for instance to enable remote management, the correct security measures are not always implemented. The security of ICS/SCADA systems is not always covered by security policies. On the one hand, people are insufficiently aware of the risks resulting from an Internet connection. On the other hand, many organisations do not have an up-to-date overview of all the systems that are connected to the Internet. Making a sound assessment of the risks and taking the correct measures is therefore not possible.

Key facts

1. For the general public an ICS/SCADA system is a very wide-ranging concept. Camera monitoring systems (CCTV), climate control systems (HVAC) and other building management systems are often classified as ICS/SCADA as well. Around 80% of the reports which the NCSC has received in the past concerning 'vulnerable ICS/SCADA systems' were found to relate to systems in these categories.
2. Many organisations do not know which of their systems can be accessed via the Internet. This lack of knowledge is partly caused by the fact that systems are installed and/or managed by third parties with whom no or inadequate agreements have been made about security.
3. More and more tools and knowledge are becoming available that make it easier to identify systems that are connected to the Internet and to search for vulnerabilities in ICS/SCADA systems.
4. If ICS/SCADA systems that are connected to the Internet are insufficiently secured, they can be remotely manipulated and/or taken over. This can result in physical damage. Depending on the nature of the systems, this can have major consequences for an organisation and its customers.
5. Malicious persons and security researchers regularly make their findings public. As a result, organisations can suffer negative publicity and damage to their image. It is also possible that the reports will attract curious people who wil try to gain access to the systems.

Finding online ICS/SCADA systems

The availability of readily available - and generally speaking also free - search engines and other tools reduces the time and knowledge required to identify systems linked to the Internet.

According to media reports, access to ICS/SCADA systems is also being sold in underground forums.[1]

SHODAN is a search engine that is often used to identify potential vulnerable systems. Well-known network scanners such as Nmap[2] or Nessus[3] can also be used. The freely available tool Metasploit[4] offers options for targeted searches for ICS/SCADA-related vulnerabilities and systems as well.

Searching with SHODAN

SHODAN is a search engine, but a special one. Whilst other search engines index on the basis of the content of the webpage, SHODAN indexes on the basis of systems' banner information. If you know what search terms to choose, it's easy to find potentially vulnerable systems. SHODAN also offers a number of filter options (e.g. by country, IP address, port number etc.) for even more targeted searching.

SHODAN, which can be accessed via www.shodan.io, offers limited search options for free and without registration. You can access additional search options by registering, and more advanced options are available in return for payment. If you use SHODAN with the filter option for the IP addresses of your own organisation, you can quickly see which of your systems can be found online. Be aware that search terms are saved, as a result of which you may appear high in the list of popular search terms. You can reduce the ability of search engines to find you by limiting the banner information released by your systems where possible.

SHODAN is still being expanded. Multiple specific ports and protocols for ICS/SCADA systems are currently being indexed.

What can happen?

A successful hack took place at a German steel factory in 2014. The attackers were able to access the ICS/SCADA systems by means of spear phishing. They then stopped the control components in the factory from working, as a result of which a blast furnace could not be shut down in a controlled manner. This resulted in damage to the equipment.[5]

[1] http://www.infosecisland.com/blogview/24608-SCADA-Systems-Offered-for-Sale-in-the-Underground-Economy.html
[2] www nmap org
[3] www.tenable.com
[4] www.metasploit.com
[5] See the 2014 annual report of the German Federal Office for Information Security (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

If your ICS/SCADA systems that are connected to the Internet are inadequately secured, they can be remotely manipulated and taken over. if the central control is directly accessible via the Internet, no specific knowledge is required. Digital vandalism, such as turning on or off random systems or programs, is then very easy. It's also possible to gain access to (process) information. How serious the consequences are, is partly determined by the nature of the process and whether additional security measures are in place.

Malicious persons and security researchers regularly make their findings public via social media such as Twitter, on public websites such as Pastebin or by informing journalists. This can lead to negative publicity and damage to the image of the organisation concerned. But more importantly, the risk of abuse of the published vulnerabilities increases.

What can you do?

You will find a checklist with measures on this page. First make sure that you have an up-to-date overview of all the systems within your organisation which are connected to the Internet (and the internal network). For each system ask yourself whether access via the Internet is necessary. Do not just look at 'Internet connection or no Internet connection', but also at which ports and services are active.

Regularly check that the overview is up-to-date, periodically scan which systems (in your public IP range) can be found on the Internet, and compare this with the overview that you maintain yourself. You can check this yourself using the aforementioned search engines and tools. You can also include it in a periodic penetration test.

The NCSC strongly recommends not to connect ICS/SCADA systems or any other form of process monitoring and/or control to the Internet. Should remote access nonetheless be required, make sure that this is set up securely. Preferably arrange this using a VPN connection designed for this purpose.[6]

Be aware that there are also options for remote access which do not make use of your organisation's IP range. Think of suppliers and users who install dial-in and dial-out connections, Wifi access points or ADSL lines themselves for the installation, management and/or maintenance of their products and services. Also make agreements with external suppliers about the security requirements stipulated for the systems used.

Checklist security online ICS/SCADA systems

1. Draw up an overview of all systems and network connection points within your organisation which are connected to the Internet.
   This involves all systems that can be accessed from the Internet. Also ask your suppliers and maintenance providers what connections they use. Bear in mind that if a supplier provides remote service, there must be a a connection. Don't overlook old-fashioned dial-in connections or GPRS modems. Enquire with your purchasing department as well; they may be able to help you listing the agreements with suppliers.
2. For each system ask whether access via the Internet is necessary. Make an assessment of the risks of this connection, and define appropriate security measures.
   Do not just look at the question whether there is an Internet connection, but also at which ports and services are active. Preferably arrange access through a VPN connection designed for this purpose with which the connection can only be activated at your initiative.
3. Check your overview against the situation in practice. You can do this using the SHODAN search engine or various scan tools.
   There are often more connections in practice than previously thought. Checking is therefore necessary. Make this check part of your periodic penetration test. Examine the filter rules for your firewalls and other security equipment. Examine the traffic allowed in from outside, and compare this with your overview.
4. Determine for each connection point whether the security matches the risks for the underlying systems in the event of unauthorised access and operation.
   Preferably use security equipment such as firewalls and proxy servers for your connection points. Do not rely on your equipment's factory settings: these are regularly found to contain flaws (such as default passwords).
5. Make clear agreements with suppliers about remote access.
   You should include agreements about the type of use (what actions may be carried out via the connection), the level of security and the reporting of incidents.
6. Monitor the security of your connection points.
   Log access to your connection points and check these logs for unusual activity. This might include many failed log-in attempts, or logging in at unusual times. Make sure your software and systems are always up-to-date.
7. Also complete the NCSC's extensive 'Checklist security of ICS/SCADA systems'.[7]
   Accessibility from the Internet is not the only potential security problem for ICS/SCADA systems. The checklist helps you to determine whether the ICS/SCADA systems are adequately secured.

[6] Further information about securely structuring remote access can be found on the CPNI.UK website: http://www.cpni.gov.uk/documents/publications/2011/2011022-remote_access_for_ics_gpg.pdf?epslanguage=en-gb

[7] https://www.ncsc.nl/english/current-topics/factsheets/checklist-security-of-ics-scada-systems.html

Responsible disclosure

It's important that vulnerabilities can be responsibly reported to your organisation and that these are dealt with correctly. Establish a policy for responsible disclosure and make this policy publicly accessible so that people know where to report their findings.[8]

What if something nonetheless goes wrong?

You have done everything possible to secure your systems, but things still go wrong. How do you prepare for that?

- Prepare for possible press enquiries or reports from researchers. Even if systems are intentionally connected to the Internet, security-related questions may be raised. You should therefore inform press spokespeople and telephone operators how to deal with press enquiries or reports.
- Ensure that the WHOIS contact information about the IP range that you use is up-to-date. This makes you easier to find for anyone seeking to report a vulnerability.[9]

Finally

There are many good publications in English available about securing ICS/SCADA systems. The following websites and publications are recommended:

- Control Systems Security Program (CSSP) from the American DHS and ICS-CERT: https://ics-cert.us-cert.gov/
- Centre for the Protection of National Infrastructure (UK): http://www.cpni.gov.uk/advice/cyber/Security-for-Industrial-Control-Systems/
- International Society of Automation (ISA): https://www.isa.org/isa99/
- National Institute of Standards and Technology (NIST): http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- Swedish Civil Contingencies Agency (MSB):https://www.msb.se/en/Tools/News/Guide-to-IncreasedSecurity-in-Industrial-Information-and-Control-Systems/

[8] More information about establishing a responsible disclosure policy can be found in the NCSC's Responsible Disclosure Guideline: https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html

[9] Bear in mind that the WHOIS database not only makes you easier to find for people wanting to report, but also for possible malicious persons. Therefore run through this checklist periodically in order to check that the security of your ICS/SCADA systems is still sufficient.

Publication
National 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-2012-01 | version 2.2 | 6 June 2016