Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Finance FDF
General Secretariat

National Cybersecurity Centre NCSC
www.ncsc.admin.ch

NCSC

Checklist and instructions
Measures to protect industrial control systems (ICSs)

Contents

1 Introduction

Control systems consist of one or more devices that control, regulate and/or monitor the behaviour of other devices or systems. In industrial production, the term "industrial control systems" (ICSs) is commonly used. For some time now, industrial control systems have also been found more frequently in applications outside the manufacturing industry, such as home automation and traffic control. In principle, an industrial control system can refer to any system that regulates and/or monitors a physical process. Most of the basic rules for protecting such systems can also be applied beyond industrial manufacturing. For this reason, industrial control systems are generally referred to as "ICSs" in this article.

SANS[1], a security institute in the United States, has published 20 critical security controls[2] indicating how IT infrastructures can be protected in general. Some of these may also be used on ICSs. Further recommendations have been issued by the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[3]) and the National Institute of Standards and Technology (NIST[4]).

The following recommendations are based on these documents.

2 Summary

Detailed instructions can be found on the last pages of this document.

11 Measures to protect industrial control systems (ICSs)

1. Create and maintain asset databases for all devices
2. Establish life cycle and patch management for software
3. Define and use secure configurations
4. Plan and build robust network architectures
5. Implement multi-stage malware protection
6. Authentication and authorisation
7. Set up central log analysis
8. Ensure physical protection
9. Carry out and regularly test backup and recovery
10. Establish and practice security identity management processes
11. Establish a security culture

[1] SANS: http://www.sans.org

[2] SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/

[3] ICS-CERT: http://ics-cert.us-cert.gov/

[4] NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

3 Measures to protect industrial control systems (ICSs)

The measures listed should be embedded in an overarching security process which ensures that the measures are applied, regularly verified and continuously improved. Moreover, the operators of installations should know the current threat situation, monitor that situation regularly and incorporate the findings into the implementation and improvement of the security measures. For this purpose, close cooperation between risk management, engineering and operations is of the utmost importance.

In most cases, security cannot be increased with a one-off action. It is a continuous process that should never end. Set realistic, achievable goals and first work on the points that will noticeably increase security with relatively little effort. For example, you can first change all default passwords and protect control interfaces that can be accessed externally.

3.1 Asset database for devices

Measure	Keep a database in which all the elements of the control system, of peripheral systems and also of normal end devices are listed.
Reason	Effective and efficient protection is impossible without knowing which elements need to be protected and which elements are trustworthy.
Implementation notes	Various technical aids exist for achieving this goal. A network-based inventory tool can be used to gain an initial overview. However, great caution is advised with active scanners. Many ICSs are not prepared to receive unexpected network traffic, which can lead to a malfunction. Unknown devices that connect to the network for the first time should trigger an alarm. This can be based on the MAC addresses of the devices. Although a MAC address can easily be falsified, this measure already has a considerable detection effect.

3.2 Handling software

Measure	Keep a database in which all software elements are listed. This is also the basis for good patch, release and life cycle management. Wherever possible, create a white list, especially on all critical devices, so that only known software is executed.
Reason	The asset database for software provides the basis for change, patch and release management. Many attacks, especially targeted attacks, are carried out via poorly protected systems having high permissions (for example administration or developer devices). If this attack path is made more difficult, the effort needed for a successful attack is much more substantial.

	In general, life cycle management is of great importance for ICSs because of their very long life cycle.
Implementation notes	The initial creation of the database can be facilitated with technical aids (software inventory tools). Patch management for ICSs is very tricky and (for warranty reasons) can usually be done only in collaboration with the supplier. This means that there are generally longer timeframes during which a system is vulnerable to attack. This risk can be reduced by whitelisting executable applications. For almost every attack, software must be launched on the attacked device. Whitelisting is intended to ensure that only approved programs can be executed.

3.3 Secure configurations

Measure	Secure configurations
Reason	Attackers often exploit weak passwords or default passwords.
Implementation notes	Administration interfaces should never be accessible directly from the internet. If this is necessary, the permitted IP addresses must be restricted. Security guidelines and manufacturer instructions for strengthening defensive measures must be followed. If the ICS provides the option of signing software and triggering an alarm if the software used is changed, this option must be used without fail. Configurations should also be checked to ensure that there are no weak passwords or default passwords.

3.4 Robust network architecture

Measure	Robust network architecture with segregated network zones
Reason	Insofar as possible, ICSs should be operated in segregated networks without direct internet access. This minimises the scope for attack and maximises the effort for overcoming the remaining obstacles. Where possible, the office automation network and the ICS network should be completely separated. If this is not possible, an appropriate zone concept must control communication.
Implementation notes	If elements have to be reachable from the internet, access must be given special protection. The use of VPN technologies with two-factor authentication (e.g. a one-time password token and a PIN) is highly recommended. Similarly, only certain IP addresses should be specifically enabled for maintenance. This same is true of internal

	segmentation. If access from a normal network to the ICS network is necessary, it must be channelled through a dedicated point where authentication and monitoring take place. The networks should be monitored using dedicated, network-based intrusion detection systems (IDS) specialised in ICS protocols. Network protocols should be realised in encrypted form wherever possible. If there is no corresponding protocol variant, network traffic can be packed into a tunnel. Especially in the case of access to web-based administration interfaces, SSL/TLS should always be used. If data from the production environment is to be transferred regularly to the office network (e.g. for statistics), it can be channelled via an optical isolator (data diode) that permits communication in only one direction, which prevents this path from being used to transfer malicious code from the office network to the control systems.

3.5 Multi-layer malware protection

Measure	Multi-layer malware protection
Reason	ICSs built on commercially available operating systems are vulnerable to malware, especially since they often have to be kept at an old patch level (due to manufacturer instructions, validation, production security). Malware is often used to take over auxiliary systems, administration devices or database servers connected with ICSs. Old ICS platforms built on Windows-based operating systems are particularly vulnerable to malware attacks.
Implementation notes	Good malware protection is generally key to the correct functioning of every ICS. Often it is neither possible nor expedient to install malware protection products on critical ICSs. However, administration devices and normal Windows servers should always have up-to-date virus protection. Malware protection should be at multiple levels so that malware that is not recognised at one level can be detected at another level. Moreover, the network should be monitored for suspicious data flows that indicate malware infections. It makes a lot of sense to ensure that none of the systems involved may connect directly to the internet and that only restricted point-to-point connections via a proxy server are permitted.

3.6 Authentication and authorisation

Measure	Secure authentication and authorisation of all persons and systems involved
Reason	Great importance should be attached to authentication and the assignment of permissions, as deficiencies in this area can be exploited very quickly and easily by attackers.
Implementation notes	Wherever possible, authentication should be required and authorisation should be implemented according to the principle of minimal permissions. Various ICSs and/or ICS protocols support only rudimentary authentication or none at all. In this case, compensating measures have to be taken, such as authentication at the boundary between the network and the ICS. Make sure that no standard user accounts with default passwords exist. All passwords should be as strong as possible, and two-factor authentication should be used for exposed administration interfaces. Users – especially maintenance companies – should receive only the permissions actually needed to carry out the task in question.

3.7 Central log analysis

Measure	Logs of all systems should be collected, analysed and stored centrally.
Reason	Only by collecting all logs can connections between different incidents be understood and attacks detected.
Implementation notes	It is necessary to determine which incidents are to be recorded for every system class, regardless of whether it is an ICS, administration device or peripheral system. The recorded data should be kept for as long as possible. Sometimes, successful attacks are not discovered until months or years later and often can be traced only with the help of logs. Define a baseline of incidents that represents normal and trouble-free functioning. Deviations, errors and unexpected behaviour are always to be clarified.

3.8 Physical protection

Measure	ICSs and peripheral systems connected directly or indirectly to them must be protected against unauthorised physical access.
Reason	Physical access protection for ICSs is generally very strong. However, you should also consider peripheral systems and remote maintenance locations, as well as detached, remotely administered systems. Physical access to a connection usually allows security measures at network level to be circumvented.
Implementation notes	Expand the search for vulnerabilities in the existing physical protection of the ICS to include peripheral systems and administration systems, as well as any systems in remote locations. Each physical interface offers easier access to the network.

3.9 Backup and recovery processes

Measure	Backup and recovery processes must be defined and regularly tested. This is true for the actual ICSs as well as the peripheral systems connected to them. The integrity of the backup files must be checked regularly.
Reason	In many cases, backups are not tested. Although backup files may be available in the event of a crisis, they may not always be readable or usable for the unproblematic restoration of files.
Implementation notes	Backup files must be saved in a secure location at some distance from the backed-up system. Backups should encompass not only data, but also configuration files. Restoring from backups should be rehearsed at least once a year, and preferably every six months. The integrity of the backup files must be checked regularly. Cryptographic hash values should be calculated and stored for all backup files for this purpose.

3.10 Security incident management processes

Measure	Prepared and rehearsed processes are defined for an incident, including detection, reaction and prevention.
Reason	A proper and decisive reaction to an incident can usually reduce the damage substantially.
Implementation notes	ICSs should be integrated into the normal security incident response process. Security incidents cannot always be detected at first glance. For this reason, unexplained behaviour of an ICS must always be investigated. After a security incident, an analysis of the causes must always be carried out, and measures for future prevention must be defined. A continuous improvement can be achieved in this way.

3.11 Establish a security culture

Measure	Creation of a security culture with corresponding responsibilities and processes which explicitly include ICS
Reason	Security has to be integrated into all business processes. It should be possible to report necessary measures and the risk landscape directly and without distortions to the general management via an internal control system. The general management must be informed about the specific risks and characteristics of industrial control systems.
Implementation notes	The security processes should be embedded in the normal business processes and in the control loop. Proper functioning and the achievement of objectives should be regularly reviewed at the technical and organisational level, and improvements should be planned and implemented where necessary. Performance of the reviews and communication of the findings to the general management should be delegated to an appropriate body with the necessary resources and powers that is as independent as possible. Responsibility always remains with the general management.