IND.2.1 General ICS Components

1. Description

1.1. Introduction

An ICS component is an electronic component that controls or regulates a machine or system. It is thus part of an industrial control system (ICS) or, in more general terms, operational technology (OT). These components may include programmable logic controllers (PLC), sensors, actuators, a machine, or other parts of an ICS.

Due to the typically high availability requirements in OT environments and the often extreme environmental conditions (such as heat, cold, dust, vibration, or corrosion), ICS components have always been designed to be robust devices with high reliability and long service life.

ICS components are normally configured and programmed using special software from the respective manufacturer. This is performed either using programming devices (e.g. as an application under Windows or Linux) or via an engineering station that loads application programs into the programmable logic controllers.

The Information Security Officer role may have different names in the field of industrial automation depending on the type and orientation of the organisation in question. These alternative names include "ICS Information Security Officer (ICS-ISO)" and "Industrial Security Officer".

1.2. Objective

The objective of this module is to secure all kinds of ICS components regardless of their manufacturer, type, purpose, and application site. The module may be used for an individual device or for a modular device consisting of several components.

1.3. Scoping and Modelling

Module IND.2.1 *General ICS Components* must be applied to each ICS component used in the information domain under consideration.

The requirements have been drawn up for a generic ICS component. Additional modules are available for specific ICS components such as sensors and actuators or machines; see, for example, IND.2.3 *Sensors and Actuators* or IND.2.4 *Machine*. These describe requirements that go beyond the general requirements of this module and must be met additionally.

This module does not contain organisational requirements for safeguarding an ICS component. The requirements of module IND.1 *Process Control and Automation Technology* must be implemented for this purpose.

2. Threat Landscape

For module IND.2.1 *General ICS Components*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insecure System Configuration

The default configuration of ICS components is typically designed to ensure that the components work properly and can be put into operation easily. Security mechanisms often play a subordinate role in this regard. All services, protocols, and connections are usually activated and remain active in the default setting even if they are not used. Preset authorisations often remain unchanged, as well.

For attackers, it is easy to take over and manipulate such ICS components. It is also possible for an attacker to exploit an insecure system configuration in order to use the ICS component as a starting point for additional attacks. As a result, critical information may be leaked or the entire operation of the organisation in question may be impaired.

2.2. Insufficient User and Authorisation Management

Some ICS components have their own user and authorisation management system. If this is inadequately designed, employees may share the same user accounts, or the authorisations of employees who have left the company or service providers no longer working for the company may not be deleted. This may ultimately allow unauthorised persons to access ICS components.

2.3. Insufficient Logging

Logging related to ICS components is often limited to process-relevant events. Data relevant to information security is often not recorded. As a consequence, security incidents can only be detected with difficulty and cannot be reconstructed after the fact.

2.4. Manipulation and Sabotage of an ICS Component

The manifold interfaces of ICS components put IT systems, software, and transmitted information at an increased risk of manipulation. Depending on the motivation and knowledge of a potential attacker, this may have effects locally or across multiple locations.

Furthermore, status and alarm messages or other measured values may be suppressed or changed.

Manipulated measurements may cause ICS components or the personnel operating them to make improper decisions. Manipulated systems may be used to attack other systems or locations, or to cover up an ongoing manipulation.

2.5. Use of Insecure Protocols

Some of the protocols used within the framework of industrial control systems only offer limited security mechanisms (or none at all). Technical information such as measured and control values are often transmitted in plain text and without integrity protection or authentication. An attacker with access to the transmission medium may, in this case, read out and modify the communication contents or implement control commands. This could provoke actions or directly influence operations. An attack at the protocol level is possible even if the ICS component is configured securely otherwise and does not have any vulnerabilities.

2.6. Denial-of-Service (DoS) Attacks

An attacker may impair operations of ICS components using DoS attacks. For processes that run under real-time conditions, even a short disruption can lead to a loss of information or control.

2.7. Malware

The threat of malware is also increasingly severe for industrial control systems. Opportunities for infection arise through interfaces to office IT (vertical integration) and to the outside world. Mobile end devices such as service laptops or removable media used for programming and maintaining ICS components also pose a threat. The latter can introduce malware into isolated environments, as well.

2.8. Interception of Information/Espionage

ICS components frequently contain detailed information on the processes they control or monitor. This information may also be partially reconstructed from other transmitted values such as measured or control data. The same holds true for control programs or parameters.

Attackers could obtain trade secrets such as recipes, processes, or other intellectual property in the context of industrial espionage. They may also obtain information on the mode of operation of an ICS component and its security mechanisms and use this for additional attacks.

2.9. Manipulated Firmware

In addition to application programs, the operating system (firmware) of ICS components can be changed. This can enable manipulated software to enter the system. Internal memory could be changed by an attacker by means of a compromised programming device, a local data interface (e.g. USB), or any other existing network connection. A software update might also

have been manipulated along its path from the manufacturer to the operator. Ultimately, the operator might receive an ICS component whose firmware has already been compromised—for example, in the event of a manipulated supply chain or in procuring components from insecure sources. As a consequence, an attacker may modify or falsify processes and procedures.

3. Requirements

The specific requirements of module IND.2.1 *General ICS Components* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Responsibility	**Role**
Overall responsibility	ICS Information Security Officer
Further responsibilities	Employee, Planner, Maintenance Personnel, OT Operations (Operational Technology, OT)

3.1. Basic Requirements

For module IND.2.1 *General ICS Components*, the following requirements MUST be met as a matter of priority:

IND.2.1.A1 Restriction of Access to Configuration and Maintenance Interfaces [OT Operations] (B)

Passwords set by default or by the manufacturer MUST be changed (see ORP.4 *Identity and Access Management)*. These changes MUST be documented. Passwords MUST be stored securely.

It MUST be ensured that only authorised employees are allowed to access the configuration and maintenance interfaces of ICS components. The configuration of an ICS component MUST ONLY be changed after the approval or authentication of the person in charge.

IND.2.1.A2 Using Secure Transmission Protocols for Configuration and Maintenance [Maintenance Personnel, OT Operations] (B)

Secure protocols MUST be implemented for configuring and maintaining ICS components. Information MUST be protected during transmission.

IND.2.1.A3 ELIMINATED (B)

This requirement has been eliminated.

IND.2.1.A4 Disabling or Uninstalling Unused Services, Functions, and Interfaces [Maintenance Personnel, OT Operations] (B)

All services, features, and interfaces of ICS components that are not being used MUST be disabled or uninstalled.

IND.2.1.A5 ELIMINATED (B)

This requirement has been eliminated.

IND.2.1.A6 Network Segmentation [OT Operations, Planner] (B)

ICS components MUST be separated from office IT. If ICS components depend on other components in the network in question, this SHOULD be documented sufficiently. ICS components SHOULD communicate as little as possible with other ICS components.

3.2. Standard Requirements

For module IND.2.1 *General ICS Components*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They SHOULD be met as a matter of principle.

IND.2.1.A7 Creating Backups [OT Operations] (S)

Backups MUST be created prior to each system change in an ICS component.

IND.2.1.A8 Protection Against Malware [OT Operations] (S)

ICS components SHOULD be protected against malware by suitable mechanisms (see OPS.1.1.4 *Protection Against Malware*). If an anti-virus protection program is used in this regard, the program and the virus signatures approved by the manufacturer SHOULD always be up to date.

If the resources on the ICS component are not sufficient or real-time requests could be endangered by the use of anti-virus protection programs, alternative safeguards (such as the isolation of the ICS component or the production network) SHOULD be implemented.

IND.2.1.A9 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A10 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A11 Maintenance of ICS Components [Employee, OT Operations, Maintenance Personnel] (S)

The latest approved security updates SHOULD always be installed when maintaining an ICS component. Updates for the respective operating system SHOULD only be installed following approval by the manufacturer of a given ICS component. Alternatively, updates SHOULD be checked in a test environment before they are used in a productive ICS component. Maintenance SHOULD be performed on short notice for critical security updates.

IND.2.1.A12 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A13 Appropriate Commissioning of ICS Components [OT Operations] (S)

Before they are commissioned, ICS components SHOULD correspond to the latest internally approved firmware, software, and patch status.

New ICS components SHOULD be integrated into existing operating, monitoring, and information security management processes.

IND.2.1.A14 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A15 ELIMINATED (S)

This requirement has been eliminated.

IND.2.1.A16 Protecting External Interfaces [OT Operations] (S)

Externally accessible interfaces SHOULD be protected against misuse.

IND.2.1.A17 Use of Secure Protocols for the Transmission of Measurement and Control Data [OT Operations] (S)

Measurement or control data SHOULD be protected against unauthorised access or changes during transmission. Whether this is necessary or feasible SHOULD be checked in situations involving applications with real-time requirements. If measurement or control data is transmitted using public networks, it SHOULD be protected appropriately.

3.3. Requirements in Case of Increased Protection Needs

Generic suggestions for module IND.2.1 *General ICS Components* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis.

IND.2.1.A18 Communication in the Event of Incidents [OT Operations, Employee] (S)

There SHOULD be alternative and independent communication options that an organisation can use to maintain its ability to function in the event of malfunctions.

IND.2.1.A19 Security Tests [OT Operations] (H)

Regular security tests SHOULD be carried out to check whether the technical security safeguards in place are still implemented efficiently. The security tests SHOULD NOT be carried out while the system is running. Such tests SHOULD be scheduled for maintenance periods. The results SHOULD be documented. Identified risks SHOULD be evaluated and addressed.

IND.2.1.A20 Trustworthy Code [OT Operations] (H)

Firmware updates or new control programs SHOULD ONLY be installed after their integrity has been checked. They SHOULD only come from trusted sources.

4. Additional Information

4.1. Useful Resources

In the “ICS Security Compendium”, the Federal Office for Information Security (BSI) provides assistance for manufacturers and integrators of ICS in terms of testing components and IT security safeguards in ICS.

The German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft offer assistance on the secure operation of control and telecommunication systems in the white paper “Requirements for Secure Control and Telecommunication Systems”.

NIST Special Publication 800-82, “Guide to Industrial Control Systems (ICS) Security”, describes how IT security can be implemented for industrial control systems.

5. Appendix: Cross-Reference Table for Elementary Threats

This cross-reference table lists the Elementary Threats with which the requirements of this module are associated. This table can be used to determine which Elementary Threats are covered by which requirements. Implementing the security safeguards derived from the requirements will help mitigate the corresponding Elementary Threats. The letters in the second column (C = confidentiality, I = integrity, A = availability) indicate which key security objectives are primarily addressed by each requirement. The following Elementary Threats are relevant for module IND.2.1 *General ICS Components*.

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.10 Failure or Disruption of Supply Networks

G 0.12 Electromagnetic Interference

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information