IND.2.3 Sensors and Actuators

1. Description

1.1. Introduction

Sensors are electronic components featuring a microprocessor and software that serve as measuring transducers capable of converting a physical magnitude into an electrical output value. This value is provided as a standardised unit signal (often 4 to 20mA, 0 to 10V) to a serial interface, or as digital information transmitted via a fieldbus or Ethernet protocols. Along with measurements, measuring transducers often provide interfaces for performing diagnosis and parametrisation. In addition to producing electronic output values, a sensor may also have further interfaces, such as WLAN, Bluetooth, or wireless HART interfaces for parametrisation and diagnosis.

There are many different sensors available on the market (e.g. for measuring physical values). Depending on the task at hand, the functions and performance of a sensor vary significantly. The range includes sensors that only provide measurements and do not need to be configured. However, some also allow calibration, configuration, or pre-processing of data, or even complete signal processing (smart sensors).

1.2. Objective

The aim of this module is to protect all types of sensors regardless of their manufacturer, type, purpose, and place of use. It can be applied to an individual sensor or a combined sensor assembly.

1.3. Scoping and Modelling

Module IND.2.3 *Sensors and Actuators* must be applied once to sensors and actuators.

It must be used to protect sensors. It supplements the generic module IND.2.1 *General ICS Components*, which is a prerequisite of the present module.

Simple sensors that do not have configuration interfaces or more complex processing logic are not covered by this module. The potential protective measures for such sensors are limited to securing access to them and monitoring whether they are active.

The module also does not address the protection of complex wireless sensor networks. It only describes the protection of individual sensors. It does not describe the security requirements for process control and automation technology. On this subject, module IND.1 *Process Control and Automation Technology* must be implemented.

2. Threat Landscape

For module IND.2.3 *Sensors and Actuators*, the following specific threats and vulnerabilities are of particular importance:

2.1. Insufficient Security Requirements in Procurement

Sensors for ICS components in industrial environments are frequently subject to particular conditions that affect their secure operation. Examples of this include extreme heat, cold, humidity, dust, vibration, or atmospheres with a corrosive or caustic effect. In many cases, several of these factors are present simultaneously. Such harmful environmental impacts may result in the sensors of ICS components wearing more rapidly, failing earlier, or producing incorrect measurements.

Information security is often not considered during procurement and installation due to a lack of risk awareness or for cost-related reasons. Sensors might thus include serious vulnerabilities that can only be addressed with significant effort later on.

3. Requirements

The specific requirements of module IND.2.3 *Sensors and Actuators* 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	Maintenance Personnel, OT Operations (Operational Technology, OT)

3.1. Basic Requirements

For module IND.2.3 *Sensors and Actuators*, the following requirements MUST be met as a matter of priority:

IND.2.3.A1 Installation of Sensors [OT Operations, Maintenance Personnel] (B)

Sensors MUST be appropriately installed and be sufficiently robust. They MUST be able to provide reliable measurements despite extreme environmental conditions related to heat, cold, dust, vibration, or corrosion.

3.2. Standard Requirements

For module IND.2.3 *Sensors and Actuators*, 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.2.3.A2 Calibration of Sensors [Maintenance Personnel] (S)

If necessary, sensors SHOULD be calibrated regularly. Calibrations SHOULD be documented appropriately. Access to a sensor's calibration functions MUST be protected.

3.3. Requirements in case of increased protection needs

Generic suggestions for module IND.2.3 *Sensors and Actuators* 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.2.3.A3 Wireless Communication (H)

Wireless management interfaces such as Bluetooth, WLAN, or NFC SHOULD NOT be used. Any unused communication interfaces SHOULD be disabled.

4. Additional Information

4.1. Useful Resources

No additional information is available for module IND.2.3 *Sensors and Actuators*.

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.2.3 *Sensors and Actuators*.

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation of Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems