Implementation of the NOA concept in process technology

Security by design is mandatory

Every operator wants to be able to use the data from existing systems for new technologies and benefit from the added value of cloud-based evaluations. The NAMUR NOA concept explains how this is possible without changing systems completely. A key element is that the data diode should collect the important data for the cloud applications and continue to ensure the security of the system. To ensure that this is possible, the devices that map the functionality of the data diode must be developed in accordance with security directives such as IEC 62443 (lead image).

Lead Image

To be able to install Industry 4.0 technologies into an existing process-related system, the operation data must initially be collated. The objective is to not modify the system significantly. The automation pyramid in the NOA concept is therefore expanded by a side channel that provides horizontal, safe, and impact-free access to the process data on all levels. The well-known automation pyramid is made up of four levels. However, it is not possible to establish cross communication between the lower sensor/actuator level and the upper control level (Fig. 1).

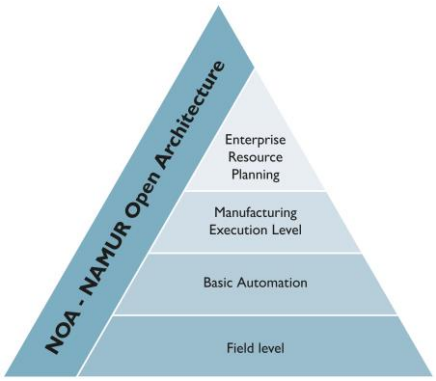

Figure 1 - Standard automation pyramid with four levels is expanded into a NOA side channel

The NOA concept therefore adds a side channel to the automation approach used to date. Cross-communication can be established using this channel so that the operator can evaluate the data recorded by the field devices. New analysis and monitoring methods are easier to use if full access is granted to the process system data, which are safely extracted from the system based on the NOA concept. The figurative data diode is used in this case. It can be used to remove data from the system, while the processes cannot be accessed. The data that is easily made available in this way forms the basis of any evaluation. The data can be saved on servers or in a cloud and forwarded to the areas where the evaluation will be completed. This can be completed by internal specialists or external service providers (Fig. 2).

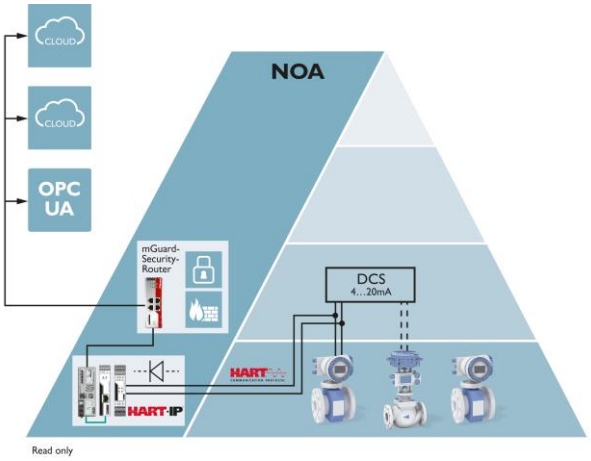

Figure 2 - To ensure smart monitoring, the data from transmitters and valves is secured by a security router and transferred to a cloud via the NOA side channel by means of the OPC UA

Specification: Safe and impact-free data access

However, the described concept is only advantageous to the operator if data can be accessed safely and without having an impact. The approach must also be able to be integrated into the Information Safety Management System (ISMS) that is part of ISO 27000 as already stipulated in the IT Security Act for critical infrastructures. Such a system is often already implemented in non-critical systems to ensure safe operation. NAMUR has worked in cooperation with the German Electrical and Electronic Manufacturers' Association (ZVEI) to develop new working groups that focus on IT security and the implementation of data diodes in actual hardware. When it comes to the automation of systems, there are various directives and standards in which the current technical standard of IT security is defined on different levels. The basic IT security stipulated by the German Federal Office for Information Security (BSI) and standard IEC 62443 "IT Security of Industrial Automation Systems" are specified as general process models.

Standard IEC 62443 – complete security approach for all participants

The IEC 62443 series of standards covers the general security standard for industrial automation systems. This series of standards is made up of 13 parts in which the process

security requirements, functional measures, and state-of-the-art are stipulated (Fig. 3). According to NOA, the main parts are:

- IEC 62443 Part 2-1 – Security Management System Requirements for Operators of Industrial Automation Systems
- IEC 62443 Part 2-4 – IT Security Program Requirements for Service Providers of Industrial Automation Systems
- IEC 62443 Part 3-3 – System Requirements for IT Security and Security Level of Industrial Automation Systems
- IEC 62443 Part 4-1 – Life Cycle Requirements for Safe Product Development of Industrial Automation Systems
- IEC 62443 Part 4-2 – Technical IT Security Requirements for Automation System Components.

When developing a device with data diode functionality it is sensible to implement a security by design approach for the hardware and software. The necessary security processes and functional measures for device manufacturers, system integrators, and operators of the machine and systems can be implemented.

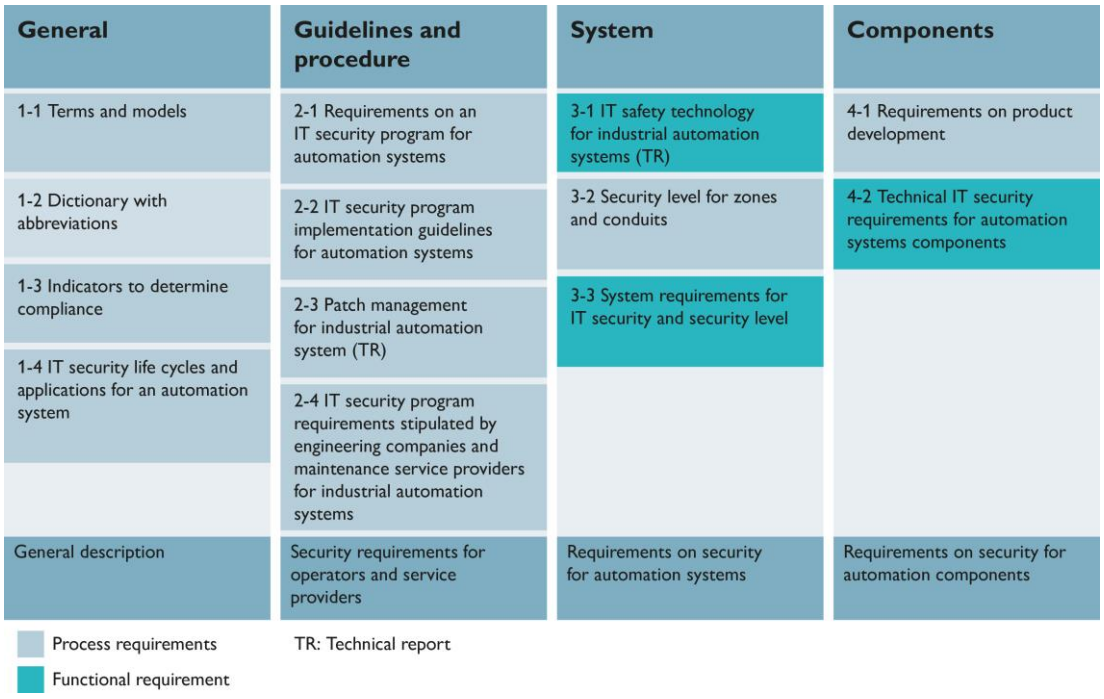

Figure 3 - Overview of the various parts of IEC 62443

Part 4-1: The product development process

IEC 62443-4-1 describes the product development process for automation devices. The main element represents a process that can be used to safely determine whether all of the security requirements have been implemented and checked. This process is completed by other security implementation features. These, for example, include a threat analysis based on the security context, i.e. the operational strategy of the product, the "Defence in Depth" concept, and security vulnerability management, which nowadays is generally implemented by a Product Security Incident Response Team (PSRIT).

Part 4-2 and 3-3: Technical devices and system requirements

IEC 62443-4-2 defines the technical requirements for industrial automation devices. Based on the security threat, a security level (SL) of 0 to 4 is determined and adjusted in accordance with the capabilities of the attacker (Fig. 4). Different functional requirements are set out for the products based on the attack vector and security level (Fig. 5). However, the implementation of functional measures must not be considered in isolation. An SL can only be achieved if the framework conditions stipulated in Part 4-1 regarding a secure development process have been met. The security level of a device/system can therefore only be met by combining processes and functional measures.

Functional requirements				
Capabilities of the attacker				
Security level	**Medium**	**Resources**	**Skills**	**Motivation**
SL-0	No danger of impairment/manipulation			
SL-1	Accidental/random impairment/manipulation			
SL-2	Easy	Limited	General	Low
SL-3	Sophisticated	Medium	Automation expertise	Medium
SL-4	Sophisticated	Comprehensive	Automation expertise	High

Figure 4 - Definition of the security level as per IEC 62443-4-2

The functional security requirements regarding the capabilities of automation systems are detailed in IEC 62443-3-3. Here, an evaluation determines to what extent the components comply with the operator's functional requirements. This part of the standard also determines the interface between the system integrator and device manufacturer. On this basis, devices required for implementing the security level defined by the operator can be selected.

Component requirement (CR) / Requirement enhancement (RE)	SL-1	SL-2	SL-3	SL-4
CR 1.1 Identification and authentication of human users	✓	✓	✓	✓
RE (1) Clear identification and authentication		✓	✓	✓
RE (2) Multi-factor authentication				✓
CR 1.2 Identification and authentication of software processes and devices	✓	✓	✓	✓
RE (1) Clear identification and authentication			✓	✓

Figure 5 - Definition of the functional measures for the security level as per IEC 62443-4-2

Part 2-4 and 2-1: Requirements for system integrators and operators

IEC 62443-2-4 specifies the requirements on the capabilities in terms of the IT security of service providers for industrial automation systems. It clarifies the interface between the operator and system integrator, as well as the core processes during integration, commissioning, and maintenance. This, for example, includes the architecture and configuration of the automation solution, the management of user accounts, processing of events, and patch management including backing up and restoring the automation solution.

IEC 62443-2-1 covers the requirements regarding an IT security program for the operator. A table specifies the requirements that should basically enable the transition of the ISO 27000 to ISMS. This part of the standard also determines the security level of the system based on a threat analysis.

Recommendation – Start with available security routers

The requirements for implementing the NOA concept are currently being defined in various working groups. These will ultimately decide which standards, technologies, and processes should be used. To ensure a gradual introduction of the approach, it is important to establish a safe connection from the NOA side channel to external systems, such as a cloud or server, that already have security routers. In subsequent steps, devices that have been specially developed for implementing data diodes can then be used.

More information:
www.phoenixcontact.de/security

If you are interested in publishing this article, please contact Becky Smith: marketing@phoenixcontact.co.uk or telephone 0845 881 2222.

The protocol: OPC UA for safe data transmission

Although the working groups have only just started work, it can already be confirmed that the OPC UA technology will be used for the NOA concept. During the development of the OPC UA standard, security by design has played an important role when designing the architecture. OPC UA has a robust security model based on x.509 certificates. A global discovery server is responsible for handling the certificates. User/password mechanisms ensure that access rights are restricted so that certain groups of users can only read the data, for example. Signed and/or encrypted data transmission with various security policies is available for the communication between the client and server.