IND.2.2 Programmable Logic Controller (PLC)

1. Description

1.1. Introduction

A programmable logic controller (PLC) is an ICS component. It performs control tasks in the context of operational technology (OT). The boundaries between different device classes and designs with regard to PLCs are fluid. For example, a remote terminal unit (RTU) may take on the functions of a PLC, or a programmable automation controller (PAC) may try to combine the benefits of a PLC and an industrial PC. However, the PLC is still the classic automation device, which is why the terms "PLC", "RTU", and "PAC" are used synonymously in this module.

A PLC has digital inputs and outputs, a real-time operating system (firmware), and further interfaces for Ethernet or fieldbuses. In connects to sensors and actuators via analogue or digital inputs and outputs, or via a fieldbus. Communication with the process control system typically occurs via the Ethernet interface and IP-based networks.

The possible realisations are manifold: A programmable logic controller can be used as an assembly, a single device, a PC plug-in card (slot PLC), or as software emulation (soft PLC). Modular programmable logic controllers composed of various functional plug-in modules are the most frequent type. Further functions like visualisation, alerting, and logging are also performed increasingly by PLCs.

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.

A PLC is normally configured and programmed using special software from the respective manufacturer. This is performed either by programming devices (such as an application under Windows or Linux) or by an engineering station that distributes the data via a network.

1.2. Objective

The aim of this module is to protect all types of programmable logic controllers regardless of their manufacturer, type, purpose, and place of use.

1.3. Scoping and Modelling

Module IND.2.2 *Programmable Logic Controller (PLC)* must be applied once to every PLC component.

This module is to be used to protect all types of programmable logic controllers and devices with similar functions. It supplements module IND.2.1 *General ICS Components*, which must also be taken into account.

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. Functional security is not addressed either; module IND.2.7 *Safety Instrumented Systems* must be applied in this regard.

2. Threat Landscape

For module IND.2.2 *Programmable Logic Controller (PLC)*, the following specific threats and vulnerabilities are of particular importance:

2.1. Incomplete Documentation

Programmable logic controllers are often documented incompletely, which means not all their functions are known. In particular, the information on services, protocols, communication ports, and authorisation management is often incomplete. This complicates the analysis of threats because interfaces, functions, and security-relevant mechanisms can be overlooked. Potential dangers may not be considered as a result. Furthermore, if new vulnerabilities are not documented, an organisation may only be able to respond to them to a limited extent (if at all).

3. Requirements

The specific requirements of module IND.2.2 *Programmable Logic Controller (PLC)* 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	OT Operations (Operational Technology, OT)

3.1. Basic Requirements

No Basic Requirements are defined for module IND.2.2 *Programmable Logic Controller (PLC)*.

3.2. Standard Requirements

For module IND.2.2 *Programmable Logic Controller (PLC)*, the following requirements correspond to the state-of-the-art technology. They SHOULD be met as a matter of principle.

IND.2.2.A1 Extended System Documentation for Programmable Logic Controllers [OT Operations] (S)

Control programs and configurations SHOULD always be backed up before they are changed. Changes in configurations and the replacement of components SHOULD be fully documented.

IND.2.2.A2 ELIMINATED (S)

This requirement has been eliminated.

IND.2.2.A3 Time Synchronisation [OT Operations] (S)

The system time SHOULD be set automatically through centrally automated time synchronisation.

3.3. Requirements in Case of Increased Protection Needs

No requirements with increased protection needs are defined for module IND.2.2 *Programmable Logic Controller (PLC)*.

4. Additional Information

4.1. Useful Resources

No additional information is available for module IND.2.2 Programmable Logic Controller.

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.2.2 *Programmable Logic Controller (PLC)*.

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.41 Sabotage