B&R CRA Guide for POWERLINK

Transparency is of utmost importance when it comes to Cyber Security. With the publication of this CRA Guide, B&R is taking an active role in advancing Cyber Security across the automation industry.

Abstract

The POWERLINK protocol represents an open-standard, industry-proven technology for real-time communication in industrial machine environments. However, cybersecurity was not priority during its development. This necessitates that POWERLINK deployments be secured through risk-based, system-level protective measures addressing identified threat scenarios.

This document specifies the requirement for physical access control to **POWERLINK V2** devices and demonstrates the logical protection architecture provided by the Automation Runtime. The Automation Runtime enforces critical security functions through its default configuration: network segmentation isolating POWERLINK infrastructure from external (north-bound) networks, validation and verification of firmware updates and configuration data, security event detection and alerting for anomalies within the POWERLINK network, strong user authentication with access controls on northbound services, and TLS communication for IP-based services.

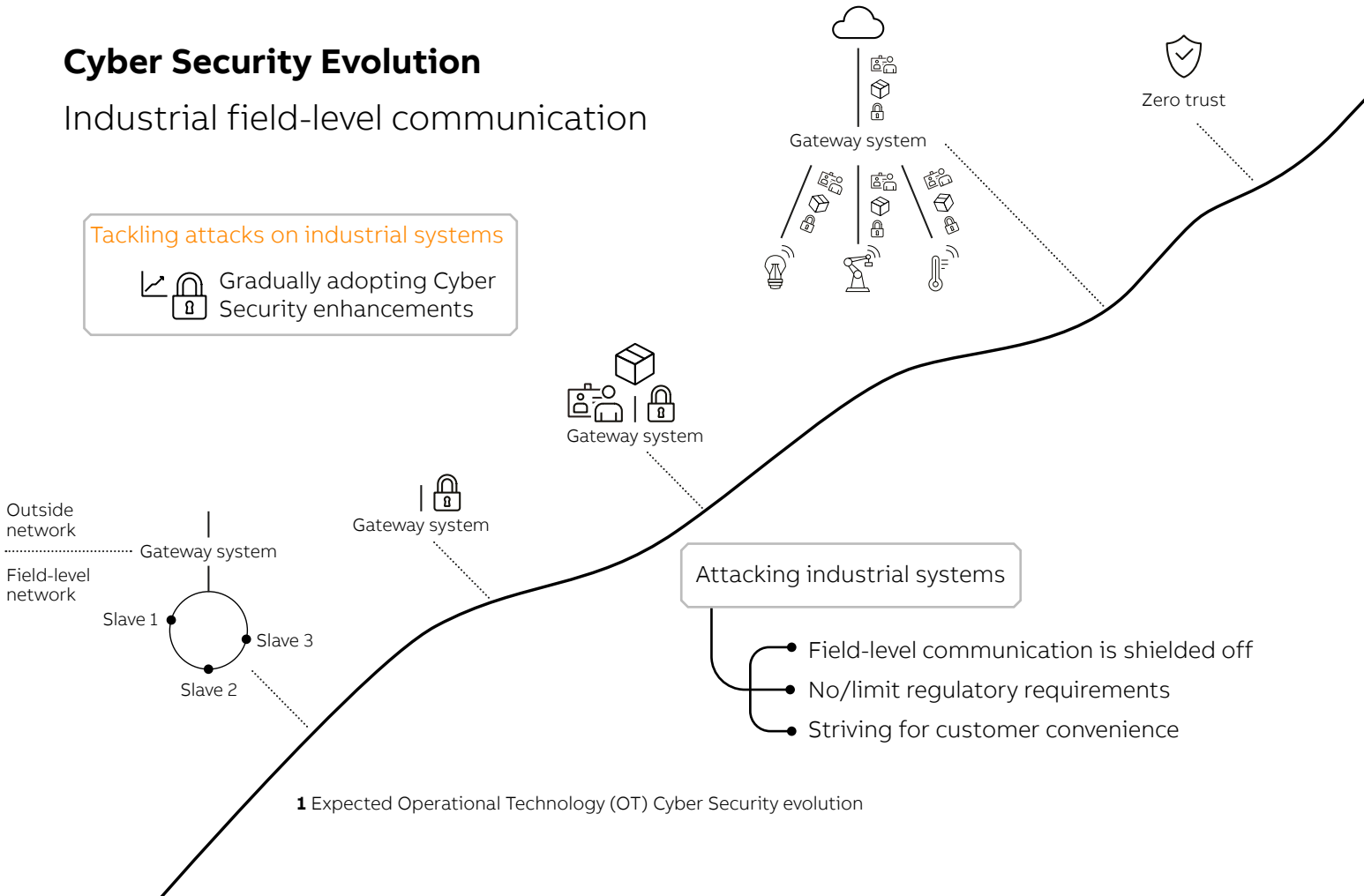
Implementation of the physical and logical protection controls presented in this document supports organizations to develop and operate industrial machinery in compliance with the Cyber Resilience Act (CRA) regulatory framework.

The Cyber Security Evolution

In the Information Technology (IT) world Cyber Security capabilities of devices and networks have evolved over time, continuously adjusting to the increasing Cyber Security threat actor capabilities. For example, with the introduction of Multi Factor Authentication (MFA) for Online Banking.

This evolution will happen in the Industrial Automation and Control System (IACS) domain as well. Where it started with Cyber Security incidents on IACS systems like Stuxnet, continued to TRITON and now existing industrial exploitation frameworks. This development triggered the development of e.g. the IEC 62443 Cyber Security standards, EU NIS 2 directive, and the EU Cyber Resilience Act (CRA). The aim is to increase the Cyber Security resilience of industrial products, to adjust to the increasing Cyber Security threat actor capabilities.

This trend is visualized in the Cyber Security evolution image, illustrating the added Cyber Security capabilities over time.



1 Expected Operational Technology (OT) Cyber Security evolution

Building Cyber Security robust products and networks

B&R adopted this Cyber Security evolution. B&R products and technologies like mapp View, Safety+, ACOPOS M4, OPC UA, and OPC UA FX lay the foundation to build, operate and maintain Cyber secure next-generation machines.

B&R recommends customers to adopt next-generation B&R products and network technologies to be build Cyber robust machines for the years to come. The Asset Owners demand in Cyber Security will rise, not just because of the EU NIS 2 directive, but also to defend against adjusted Cyber Security threat actor capabilities and because of market differentiator factors. The IT world paved the way for the Operational Technology (OT) to follow.

The risk-based Cyber Security transition

Today, the OT industry is increasingly adopting Cyber Security requirements for devices and networks, utilizing a risk-based approach. This risk-based methodology forms the foundation of Cyber Security standards such as IEC 62443 and regulations like the EU Cyber Resilience Act (CRA).

As with any industry transformation, adoption follows a predictable pattern: early adopters, early majority, late majority, and laggards. We observe similar transitions in the automotive industry‘s shift toward electric vehicles. The adoption of Cyber Security in the OT industry will likely follow this same trajectory. During this transitional phase, some Suppliers, Service Providers, and Asset Owners (following the terminology of the IEC 62443) continue utilizing their established and proven products, systems, and technologies, while others adopt newer solutions more rapidly. These decisions depend on individual risk assessments and market demand.

IACS Cyber Security requirements depend on various factors, including the system‘s intended primary use and the Cyber Security features already implemented within the Asset Owner‘s environment. When considering these factors, a risk assessment may conclude that state-of-the-art Cyber Security features - ranging from secure boot at the hardware level to multi-factor authentication with biometric iris scanning, or even physical security guards controlling shop floor access - may not be necessary or proportionate to the actual risk.

Risk assessment is a methodology for making informed security decisions by evaluating the potential risks associated with a product, system, or technology. This approach ensures that security measures are both practical and effective for the real-world deployment of Industrial Automation and Control Systems (IACS). Real-world considerations include the intended use case, existing environmental Cyber Security features, and the inherent Cyber Security capabilities of the product or system itself.

Risk analysis and threat modeling are fundamental practices in Cyber Security, enabling organizations to proactively identify, assess, and mitigate potential risks to their products and solutions. This process encompasses understanding possible attack vectors, defining threat models, and establishing clear relationships between these vectors, threat actors, and standardized frameworks such as IEC 62443. Threat modeling begins by defining the scope of analysis—identifying critical assets, data flows, and system boundaries. System diagrams are developed to visualize trust boundaries and potential entry points. Using established frameworks like STRIDE, organizations systematically identify potential threats by analyzing attacker behavior and cataloging vulnerabilities.

It is crucial to understand which type of threat actor the system must defend against. IEC 62443 provides a classification scheme for threat actors based on factors such as skills, resources, means, and motivation, enabling organizations to tailor Cyber Security capabilities anticipating adversaries. Threats are always associated with specific threat actor types who possess the capability to exploit these threats for personal gain. This combination is essential for deriving the resulting risks from identified threats. Threats are then assessed based on their likelihood and potential impact, with prioritized mitigation strategies developed and implemented throughout the solution lifecycle.

The risk analysis of POWERLINK technology and POWERLINK devices is based on the STRIDE model.

The STRIDE model

The STRIDE model provides a structured approach for identifying six core threat categories that directly impact IACS components.

- Spoofing involves impersonation and authentication bypass, where attackers take on the identity of legitimate users, systems, or devices to gain unauthorized access.

- Tampering refers to the modification of data or system integrity, where malicious actors alter critical information such as sensor readings, control commands, configuration parameters, or firmware. In industrial automation, tampering attacks can manipulate process variables (PV) from sensor, alter actor values in control logic, modify safety interlocks, or report false data to upper-level DCS/SCADA systems.

- Repudiation threats arise when users or systems deny having performed certain actions, exploiting weaknesses in logging or audit mechanisms. In industrial environments, such threats can hinder the ability to trace configuration changes, process adjustments, or safety overrides to specific individuals or systems, thereby compromising forensic investigations and incident response efforts.

- Information disclosure involves unauthorized access to or leakage of sensitive information, violating confidentiality requirements. Disclosure of industrial control system architecture and device vulnerabilities enables adversaries to plan targeted attacks with higher success rates.

- Denial of Service attacks aim to disrupt system availability by exhausting resources, overwhelming communication channels, or causing applications and devices to crash, preventing legitimate access and operations.

- Elevation of Privilege threats occur when attackers gain higher access rights than intended, obtaining unauthorized control or administrative privileges. In industrial automation, elevation of privilege may enable attackers to execute engineering functions, modify control logic, disable safety mechanisms, reconfigure network devices, or access restricted system areas.

The STRIDE approach involves first creating a model of the system under analysis, for example, by using a data flow diagram. Based on this model, an assessment is conducted to determine which of the threats defined by STRIDE are applicable to the system. Depending on the risk resulting from each identified threat, appropriate countermeasures—either technical or procedural—can then be implemented. Highlighting any residual threats that must be addressed by the system's user, along with providing clear mitigation guidance in the user documentation, helps protect customers from risks that cannot be managed within the product's scope.

STRIDE's widespread adoption in both IT and OT risk analysis demonstrates its practical utility and effectiveness. Service Provider should understand the security functions and technical capabilities within their technology stack to effectively mitigate risks at the product level. The IEC 62443 standards require Asset Owner, Service Provider and Product Supplier to document Cyber Security capabilities, ensuring threat modeling is performed, and regularly update mitigation measures corresponding to evolving attack vectors.

This document serves as a practical guide for customers using POWERLINK-based products to conduct robust security assessments. It supports the creation of security considerations, assists in mapping potential threats to specific industrial components and network architectures, and enables the identification of suitable mitigation measures aligned with industry best practices.


492.38
786.21
284.55
284.55

Defense in Depth Concept for POWERLINK

A risk assessment is a mandatory part of the EU Cyber Resilience Act (CRA), Machine Regulation 2023/1230, and the IEC 62443 Cyber Security standards. Depending on this risk assessment outcome the usage of the established and well-known POWERLINK network protocol is possible, applying compensating counter measures on machine level, like strong network segmentation, secure update processes and security policies.
POWERLINK V2 is a widely used industrial network communication fieldbus. Retrofitting modern state-of-the-art Cyber Security features to this open standard would break interoperability with existing IACS at the Asset Owners site (CRA recital 55).The following subsections describe measures to address potential Cyber Security risks.#

Security Context for the POWERLINK network

This section documents the intended use and expected Cyber Security environment at the Asset Owners site. These measures protect POWERLINK against any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks.

B&R POWERLINK devices and the technology are intended for industrial automation and control systems usage - close to the physical process. B&R POWERLINK devices are classified as embedded devices in the context of the IEC 62443. POWERLINK devices are close to the technical process and require hard real-time connectivity, supporting precise functional safety or motor operations. There essential functionality resides on Level 0 or 1 with respect to the ABB ICS Reference Architecture /IEC 62443-1-1 reference model).

The statements in this document refer specifically to B&R-provided POWERLINK devices. It should be noted that there is also a 3rd-party ecosystem of POWERLINK devices - developed by various vendors - that implement and adhere to the POWERLINK standard and specification.

POWERLINK usage

The following image visualizes the usage of a POWERLINK network with POWERLINK connected devices.

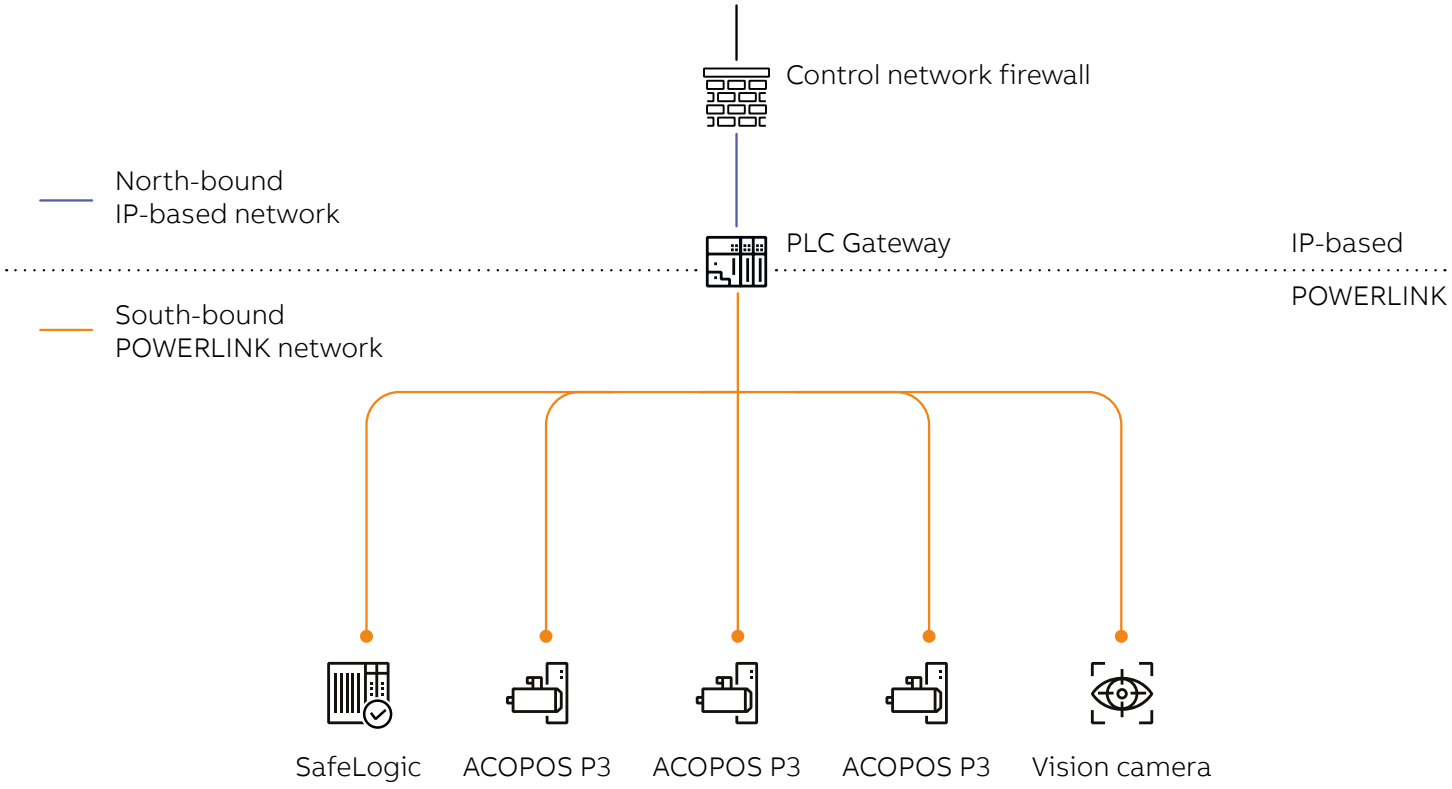
This POWERLINK example shows the PLC gateway (e.g. an X20 system) running B&R realtime operating system Automation Runtime (AR). Automation Runtime includes the so-called POWERLINK Managing Node (MN), regulating the activity on the real-time fieldbus network. POWERLINK connected devices, shown as SafeLogic, ACOPOS P3, or VISION camera are referred to as Controlled Nodes (CN). The POWERLINK network interface (orange network) is always logically separated from the north-bound IP-based network (blue network).

This segmentation happens at B&R Automation Runtime PLC level. The POWERLINK devices (connected to orange network) can be arranged either in a hub configuration or as a daisy chain.

Furthermore, POWERLINK technology supports redundancy. This can be achieved via a redundant second PLC, taking over as Managing Node in case of failures, keeping the POWERLINK network and the connected technical process running. Additionally, POWERLINK networks also support ring-redundancy and cable-redundancy in case of e.g. network cable failures.

The IP-based network (blue network) indicates the Local or Basic Control Level of the IEC 62443-1-1 reference model. This network shall be protected with a Control Network Firewall, managing fine-granular access to specific authenticated services and warding of high network traffic load from upper-level systems.

Details on the POWERLINK technology, operation modes of POWERLINK, or usages are described in the Automation Help section on POWERLINK.



2 POWERLINK network example

Intended use and Security in the Environment at the Asset Owners site

POWERLINK is an industrial real-time network fieldbus protocol. Its core functionality includes guaranteed transfer of time-critical data in very short isochronous cycles with configurable response time and time-synchronization of all nodes in the network with very high precision of submicroseconds, as well as the timely deterministic reading and setting of input and output variables for an industrial technical process. The open network protocol specification is available and standardized since 2001, with a 3rd party eco-system building POWERLINK compatible products (CRA recital 55).

POWERLINK, like many other real-time network fieldbus protocols for industrial applications, is intended to be used in an access restricted area, like on a shop floor with close proximity to the physical process. POWERLINK is optimized for network performance and cyclic time-sensitive communication between its participants. Furthermore, POWERLINK facilitates the transmission of less time-sensitive data through a dedicated asynchronous channel, which accommodates IP-based communication. Both the time-sensitive and the asynchronous communication - including IP-based communication - over the POWERLINK protocol are segmented at the B&R Automation Runtime PLC level by default.

Only authorized and trained personnel shall physically interact with POWERLINK devices and networks upon scheduled time frames. POWERLINK devices and networks shall be shielded of from northbound IP-based networks and be operated in the reference architecture Level 0 and 1. Refer also the logical and physical security recommendations.

POWERLINK data classification

POWERLINK data transmitted over isochronous cycle channels consists of technical process related values, like reading I/O value data or setting actor values on connected POWERLINK devices.

This time-critical data is not defined as confidential. POWERLINK data, transmitted by B&R provided mechanism over the isochronous channel, does not contain sensitive data like usernames, password, cryptographic key material, session tokens, or similar. Although this data not treated as confidential, its disclosure could still lead to reputational damage.

In cases where B&R devices need to exchange sensitive data, such as passwords, they use IP communication over the POWERLINK layer, secured with modern cryptographic protocols such as TLS.

The integrity and availability (with respect to real-time sensitive communication) of transmitted POWERLINK data shall be protected based on the described intended purpose and under conditions of reasonably foreseeable misuse. The impact of losing integrity and/or availability of POWERLINK transmitted data may result among others in financial loss, machinery down-time, and reputational damage. This document supports the implementation of appropriate countermeasures.

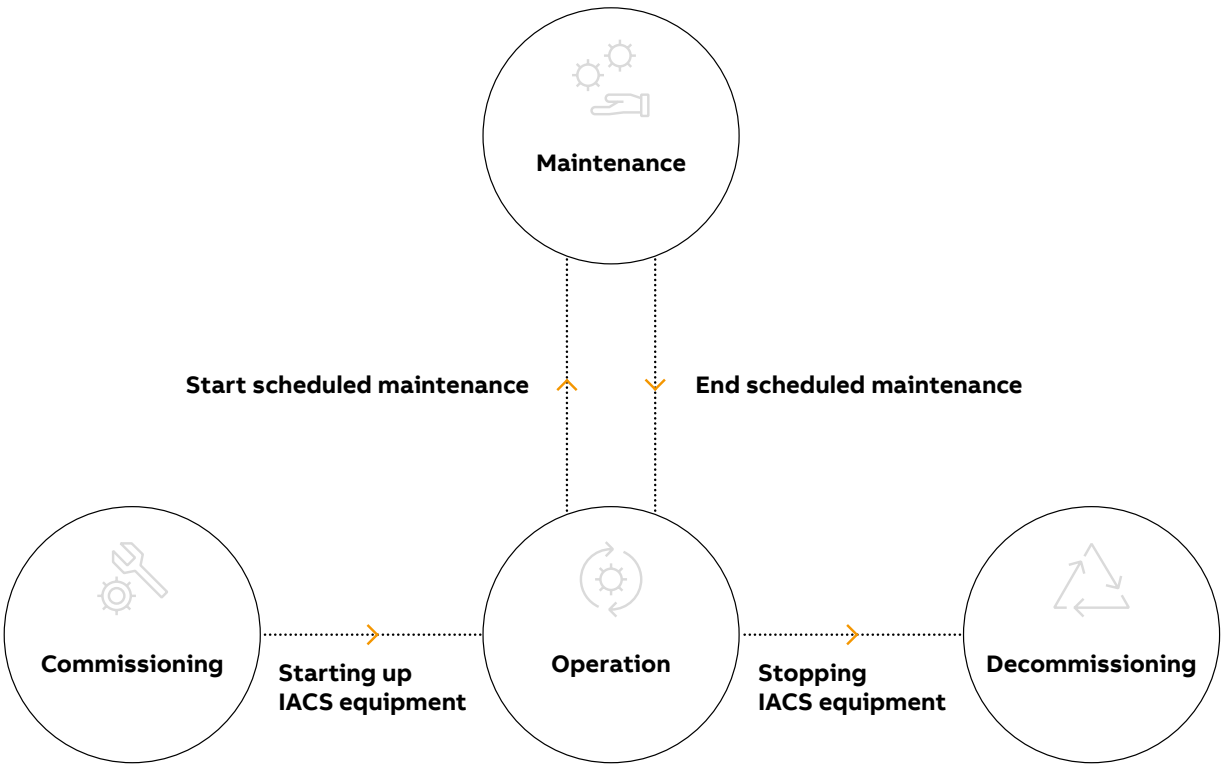
Protecting the POWERLINK devices and network at the Asset Owners site

POWERLINK operation states

Access to POWERLINK needs to consider the Industrial Automation and Control Systems (IACS) operation phases, as they entail different Cyber Security challenges: Commissioning, Operation, Maintenance and Decommissioning.

By design, POWERLINK supports the addition and removal of devices during the commissioning and maintenance phases, for example in repair scenarios, without the need to recompile the engineering project. However, during operational phases, connecting new POWERLINK components to an active and running network is not intended. In such cases, detection and logging mechanisms are implemented to identify and record any unintended connection attempts.

For POWERLINK devices and networking equipment the following usage requirements are defined for the product lifecycle phases commissioning, operation, maintenance, and decommissioning. These requirements refer to the functionality provided through the POWERLINK network. For comprehensive guidance on other device interfaces (e.g. Ethernet, HMI, USB), the respective user documentation shall be consulted.



3 Industrial Automation and Control Systems (IACS) operation states

By design, POWERLINK supports the addition and removal of devices during the commissioning and maintenance phases, for example in repair scenarios, without the need to recompile the engineering project. However, during operational phases, connecting new POWERLINK components to an active and running network is not intended. In such cases, detection and logging mechanisms are implemented to identify and record any unintended connection attempts.

For POWERLINK devices and networking equipment the following usage requirements are defined for the product lifecycle phases commissioning, operation, maintenance, and decommissioning. These requirements refer to the functionality provided through the POWERLINK network. For comprehensive guidance on other device interfaces (e.g. Ethernet, HMI, USB), the respective user documentation shall be consulted.

	Commissioning phase	**Operation phase**	**Maintenance phase**	**Decommissioning phase**
Physical accessibility	POWERLINK components are intended to be commissioned exclusively by instructed, qualified, and authorized service technicians. Commissioning shall take place in an access-controlled environment to ensure that only authorized personnel have access.	POWERLINK components shall not be physically accessible during operation.	POWERLINK components are intended to be maintained exclusively by instructed, qualified, and authorized service technicians. Maintenance shall take place in an access-controlled environment to ensure that only authorized personnel have access.	POWERLINK components are intended to be decommissioned exclusively by instructed, qualified, and authorized service technicians. During decommissioning of individual components within a POWERLINK network, it shall be ensured that the residual system's physical protection integrity remains intact. If necessary, the remaining system configuration and protective measures shall be adapted.
Logical accessibility	POWERLINK components are intended to be commissioned in a controlled and isolated communication network. It is not intended to connect non-POWERLINK device to the POWERLINK network. POWERLINK is a protocol intended for device-to-device communication. Logical interfaces used for human interaction required for commissioning are always handled and terminated within B&R Automation Runtime.	The POWERLINK network is logically separated from other networks by B&R Automation Runtime. Altering the POWERLINK communication configuration is not intended.	POWERLINK components are intended to be maintained in a controlled and isolated communication network. It is not intended to connect non-POWERLINK device to the POWERLINK network. POWERLINK is a protocol intended for device-to-device communication. Logical interfaces used for human interaction required for maintenance are always handled and terminated within B&R Automation Runtime	POWERLINK components are intended to be decommissioned in a controlled and isolated communication network. During decommissioning of individual components within a POWERLINK network, it shall be ensured that the residual system's logical integrity remains intact. The remaining POWERLINK system configuration shall be adapted.

Securing the logical POWERLINK layer at the Asset Owners site

The following logical compensating countermeasures shall be evaluated and tailored to the specific POWERLINK setup at the Asset Owners site. The thoroughness of each mitigation option depends on the specific risk assessment and the Asset Owners network architecture.

Only configured POWERLINK devices may be added to the POWERLINK network.

- Only devices which are intended for POWERLINK usage, following the POWERLINK specification shall be added to the POWERLINK network. Rogue or Non-POWERLINK devicesattached to the POWERLINK network may disrupt the real-time connectivity.

- In cases Service Providers and Asset Owners would like to closely monitor and evaluate all network communication within the POWERLINK network, installation of an Intrusion Detection System (IDS) may be evaluated. It is imperative to operate such IDS in listening/passive mode only, preventing unintended network traffic disrupting communication from the IDS to the POWERLINK network. The IDS would then be able to report configured network anomalies and send events/alerts to a centralized logging and event monitoring platform. Note, that installation of an IDS may impact the real-time connectivity.

- Dynamic additions or disconnections of POWERLINK devices from the POWERLINK network during operation may disrupt the real-time network traffic. As an analogy, it‘s much like removing a graphic card from a PC during operations - errors are to be expected.

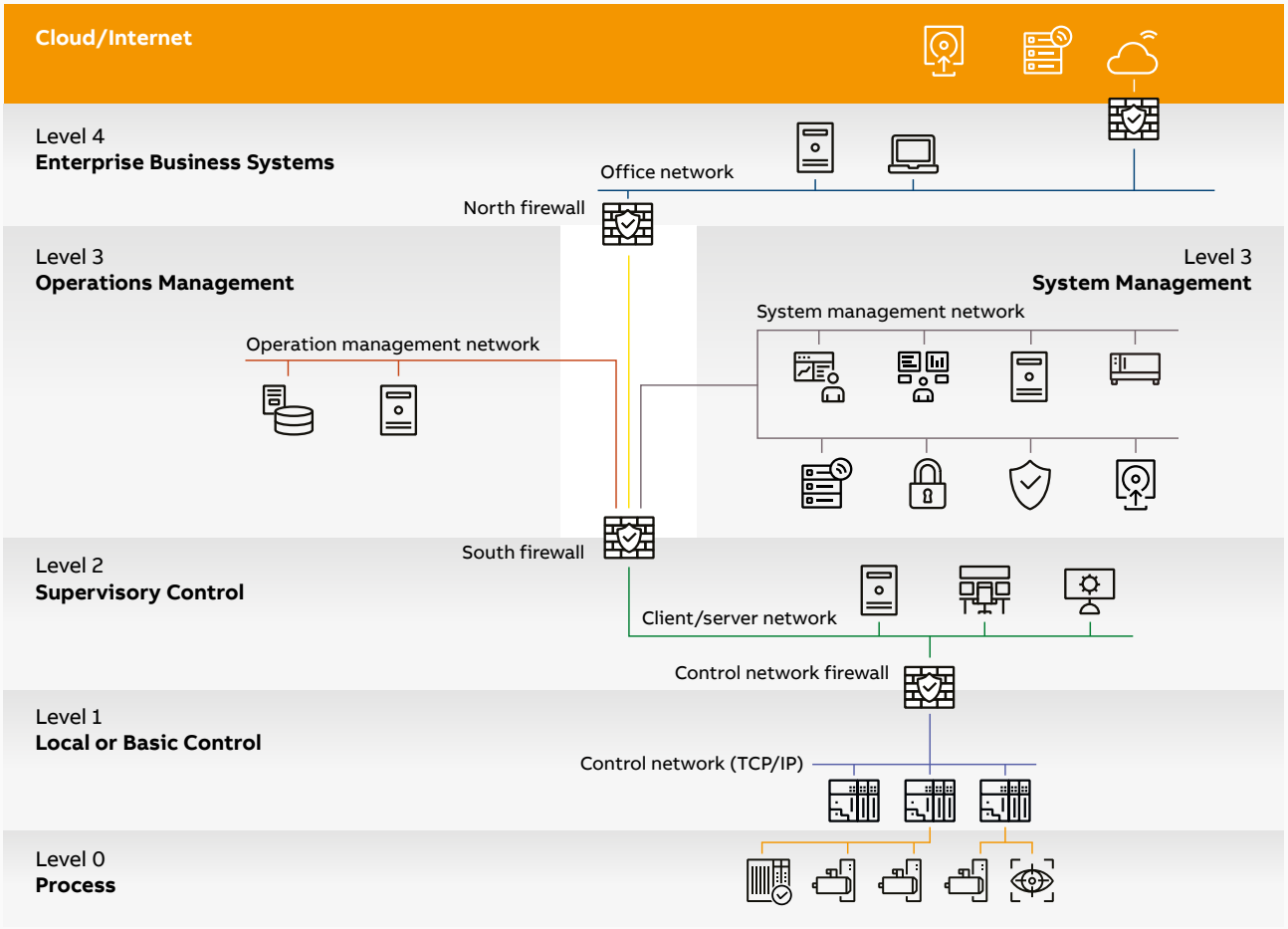
Logically segregate the POWERLINK network

- The POWERLINK fieldbus network and POWERLINK connected devices shall be segregated from other networks, particularly north-bound network routable IP-based interfaces. Here Service Provider and Asset Owner shall consider setting up VLANs and/or IP subnets.

- The following architectural image visualizes the POWERLINK network in the ABB ICS Reference Architecture, on Level 1 and Level 0 in orange color. Connected POWERLINK devices, like B&R ACOPOS P3, B&R VISION, or other Field Devices (FD) are shown as examples.

- The Level 1 - the Local or Basic Control network shall be protected by a dedicated Control Network Firewall, managing fine-granular access to specific authenticated services and warding of high network traffic load from upper-level systems.

This segregation prevents violations for devices operated in the described intended purpose and under conditions of reasonably foreseeable misuse, including network storms against the POWERLINK network. Service Providers shall additionally consider the B&R Automation Runtime Cyber Security capabilities.



4 Refer to ABB ICS Reference Architecture for a detailed description of product-independent definitions of the reference architecture. Additionally, B&R classifies Level 0, Level 1, and Level 2 as trusted zones.

Securing the physical POWERLINK layer at the Asset Owners site

The following physical compensating countermeasures shall be evaluated and tailored to the specific POWERLINK setup at the Asset Owners site. The thoroughness of each mitigation option depends on the specific risk assessment.

- The Asset Owner and Service Provider install POWERLINK components in trusted areas and rooms, where only authorized personnel are able to physically interact with e.g. POWERLINK devices, POWERLINK cables, or POWERLINK network ports during scheduled maintenance time frames.

- POWERLINK components shall be installed within secured enclosures, locked cabinets and/or access controlled sites. The use of custom or personalized locking mechanisms enhances protection from unauthorized access.

- The POWERLINK communication cables and sockets shall be protected from physical interaction, like cutting the POWERLINK cable or hooking up and additional device via an open POWERLINK network port. Here it may be required to have POWERLINK cables in steel tubes, depending on the Asset Owner‘s/Service Provider‘s risk assessment.

- Where access restrictions such as secured enclosures, locked cabinets and/or door locks are not considered sufficient, unused open network ports (RJ45) can be physically secured using port locks that are further protected with a physical key.

  Examples include: SmartKeeper Pro (personalized keys), RJ45 Port Lock (universal key), or Ethernet Port Protector (like a universal key)

- Physical access control shall be exercised during all product lifecycle phases.

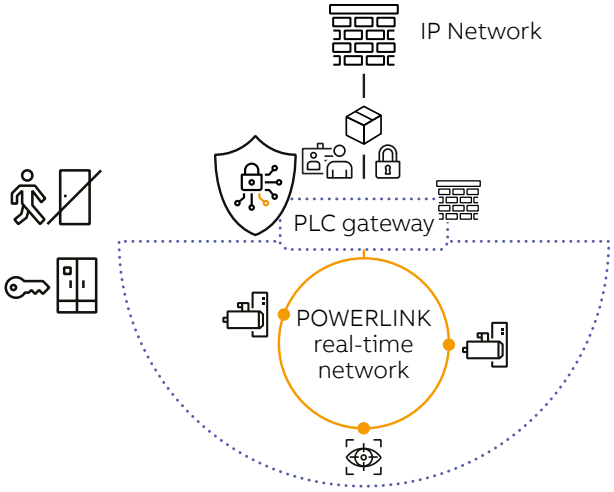
Applying these physical measures supports protection based on the described intended purpose and under conditions of reasonably foreseeable misuse.

System security - Taking advantage of existing security capabilities

From a Cyber Security architectural point of view, the B&R Automation Runtime shields off the POWERLINK network. On the B&R Automation Runtime PLC level Cyber Security features like Transport Layer Security (TLS) support for data in transit, or Human user identification and authentication are available and continuously being strengthened. The shielded off POWERLINK network and POWERLINK devices, implementing and following the POWERLINK industry wide standard do not support Cyber Security features, like TLS support. This is why compensating countermeasures shall be applied to securely operate a POWERLINK network, in order to not break compatibility with existing POWERLINK installations (CRA recital 55).

The following image visualizes this Cyber Security architecture. Here, Cyber Security features on B&R Automation Runtime PLC level are shown, strengthening the Cyber Security posture on the northbound Ethernet interface (IP network).

The dashed blue line shows the secured and shielded off logical and physical POWERLINK network and devices.



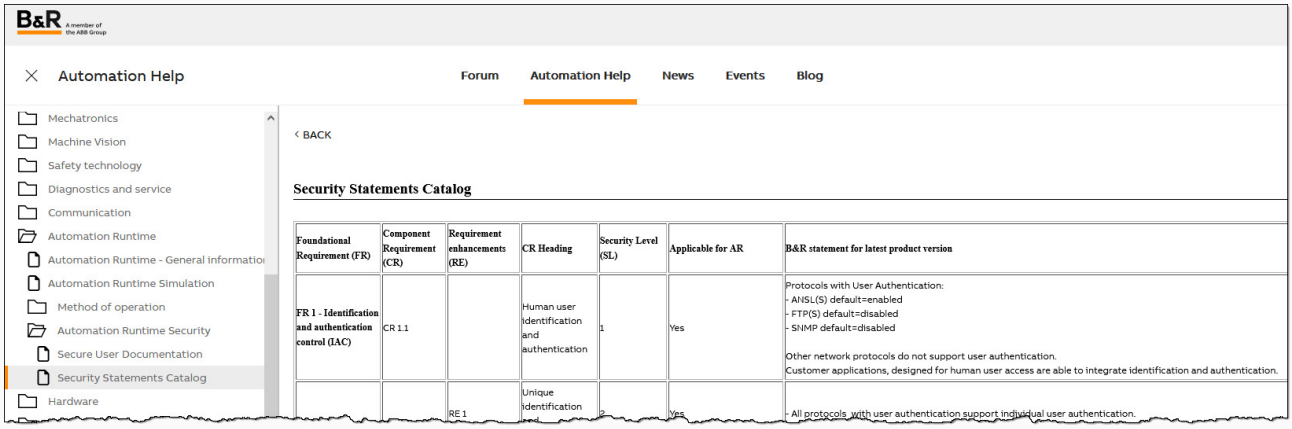
5 Example POWERLINK network, with PLC gateway protection mechanisms and security measures at the Asset Owners site

The Security gateway - B&R Automation Runtime

B&R provides a security user documentation for its B&R PLC operating system Automation Runtime, guiding users how to securely commission, operate, maintain, and decommission the system. The chapter „Services and Applications Security“, provides details on the available services and potential threats. Furthermore, it is recommended to align with the B&R Defense in Depth guideline for B&R products, providing general Cyber Security guidance.

In this security user documentation, the Automation Runtime IEC 62443-4-2 statements catalog explain how to take advantage of Cyber Security capabilities like TLS support for data in transit, or Human user identification and authentication.

The following screenshot visualized the statements catalog.



6 Automation Runtime IEC 62443-4-2 statements catalog

With the certified B&R wide Secure Development Lifecycle according to the IEC 62443-4-1, B&R Automation Runtime >= 6 adopted the Secure by Default paradigm, like disabling non-essential services or restrictively blocking network communications across interfaces by default, using the host-based firewall. Furthermore, additional Cyber Security capabilities are being introduced and added, like automated certificate management via OPC UA Global Discovery Service (GDS). These security design decisions and continuously added Cyber Security capabilities, like firmware validation support shielding off the POWERLINK network. For information on security capability availability across different product versions, please refer to the B&R Automation Runtime user documentation.

POWERLINK configuration on Automation Runtime >=6 also adheres to the Secure by Default principle and is implemented as documented in the Automation Help for the Automation Runtime's POWERLINK interface as well as for POWERLINK Controlled Nodes. Core implementation points include security logging enabled by default, deactivated DNA (Dynamic Node Allocation) functionality on Controlled Nodes, and restriction of active IP-based services to the DHCP server service on the Automation Runtime POWERLINK Interface side.

The shielded off POWERLINK network

The industry-wide used POWERLINK technology does not consider Cyber Security capabilities on the protocol level. This is why compensating countermeasures shall be applied on the logical and physical layer of the IACS at the Asset Owners site, along with the application of the Cyber Security capabilities, provided by the B&R Automation Runtime achieving the targeted security requirements.

B&R Automation Runtime running on the PLC gateway segments the IP-based network on the northbound interface from the POWERLINK network on the south-bound interface. This entails no network traversal from and to the POWERLINK network are supported on default. Furthermore, B&R Automation Runtime comes with a host-based firewall, allowing additional restrictions on ports and services. Refer to Automation Help for more information on using the host-based firewall on Automation Runtime.

Network communication between the south-bound POWERLINK network and the north-bound IPbased network is terminated at B&R Automation Runtime by default. B&R Automation Runtime acts as a media and application logic gateway, where requests and responses are evaluated and transformed, before they are transmitted to communication partners to the respective communication partners.

The POWERLINK Managing Node (MN) on B&R Automation Runtime scans the network during bootup/initialization for other Managing Nodes, if this is the case a log event is written. There is always just one active MN in a POWERLINK network, coordinating the required real-time capabilities of the technology.

Security concept for EU Cyber Resilience Act (CRA)

This section describes statements, possible threats and when using POWERLINK technology in relation to the EU Cyber Resilience Act (CRA) 2024/2847.

The CRA establishes Cyber Security requirements for products. In this context, the document also focuses on the POWERLINK technology and its standard specification, serving as a practical guide for users seeking to achieve compliance with the CRA.

This section covers Annex 1 (part I and part II) as well as Annex 2 of the EU CRA. Subsequent Annexes are not covered by this risk assessment guideline. Moreover, this document does not cover the procedural requirements applicable to the Service Provider, such as monitoring for device vulnerabilities reported by B&R or reporting security incidents.

Annex I, Part I - Cyber Security requirements

Considering CRA requirements in POWERLINK settings

This section addresses Annex I Part I, (1), (2)(b) and CRA recital (55)

POWERLINK is a well-established industrial real-time fieldbus networking protocol (IEC 61508 „proven in use“). B&R offering POWERLINK devices follows this widely recognized fieldbus networking standard.

B&R product development teams, working on POWERLINK devices and technologies follow the certified B&R wide Secure Development Lifecycle according to the IEC 62443-4-1. This includes conducting Cyber Security risk assessments, the adoption of the Secure by Default paradigm, conduction of extensive Cyber Security tests, both internally and externally, and implementing a modern state-of-the-art Vulnerability issue handling process.

B&R POWERLINK devices are operated in combination with the PLC operating system Automation Runtime, which ensures a Secure by Default configuration to segment the POWERLINK network and prevent unauthorized logical access. Users are guided by the engineering software Automation Studio to configure the product following security best practices. Automation Studio clearly indicates changes from the default configuration. A Service Provider can restore POWERLINK-based devices to their factory configuration by deploying a default Automation Studio project to Automation Runtime.

Threat	Commissioning phase
An attacker may change the firmware in the context of the engineering software Automation Studio	Automation Studio is installed in an access restricted Microsoft Windows directory requiring administrative privileges for changes by default. Furthermore, Automation Studio project bundles can be exported. To ensure the integrity and authenticity of the exported project users can cryptographically hash or sign the bundle, using off-the-shelf cryptographic software (like OpenSSL). The verification step prior to deployment is mandatory. This is recommended especially when this project bundle is shared/forwarded between multiple parties and users.
An attacker may change the firmware during transfer from the engineering software Automation Studio to the PLC	On default firmware and configuration data transfer to Automation Runtime uses role-based authentication with username and password and TLS support.
An attacker may update tampered software or configuration files on POWERLINK devices	This type of attack would require the attacker to connect to the POWERLINK network. The following compensating countermeasures shall be applied throughout the POWERLINK network and connected devices lifecycle states. • Strong network segmentation by applying the logical and physical security enhancements • Defining and following a security update process at Service Provider and Asset Owners site, ensuring the authenticity and integrity of the firmware files and configuration data deployed to POWERLINK devices

POWERLINK devices and POWERLINK equipment like hubs or interface cards are intended to be used in areas with strict access control.

Security updates and handling of vulnerabilities

This section addresses Annex I, Part I, (2)(a), (2)(c) and CRA recital (56)

B&R recommends keeping all products and systems up to date, applying latest security patches and taking advantage of continuously added new Cyber Security capabilities. Additionally, discovered security-related issues either internally or externally will be handled according to B&Rs IEC 62443-4-1 certified vulnerability issue handling process. This entails fixing known exploitable vulnerabilities. Updates for POWERLINK devices are provided to customers via the engineering software Automation Studio.

Automatic software updates are not intended, as they could cause interference with industrial process operations at the Asset Owners site. Software updates, including security relevant patches are intended to be deployed upon scheduled maintenance time frames by authorized personnel only.

Updates for POWERLINK devices are signed by B&R. Automation Studio is validating the signature prior to installing the update into the engineering software. For more details, refer to section Vulnerability and update management of B&R POWERLINK devices.

Authentication and Authorization

This section addresses CRA Annex I, Part I, (2)(d)

Access to the POWERLINK network shall be permitted only to authorized personnel during scheduled commissioning, maintenance, and decommissioning phases, refer also to secure the physical and logical POWERLINK layer sections. On the north-bound IP-based network interface, robust authentication mechanisms and strong access controls are configured preventing unauthorized access by default.

Additionally, it is recommended to apply the „Identification and authentication control“ and „Use Control“ measures, described Automation Runtime IEC 62443-4-2 statements catalog for B&R Automation Runtime, where applicable and needed.

Threat	Service Provider mitigation guidance
An attacker may spoof his identity on the north-bound IP-based network services	On the north-bound network interfaces Automation Runtime supports strong role-based authentication with username and password, refer also to respective Automation Help sections. Additionally, these services can be configured with TLS support, including mutual TLS for enhanced authentication needs. Refer also to the respective Automation Help sections.
An attacker may physically connect to the POWERLINK network, circumventing authentication	Asset Owner and Service Provider are required to prevent unauthorized physical access to the device. The logical and physical security enhancements for POWERLINK networks shall be applied.
An attacker may resend/replay a legitimate POWERLINK network package, confusing the POWERLINK recipients	The injection of data packets by nodes other than the Managing Node (MN) can cause data collisions, which may result in communication failures detected at the MN and indicated as node disconnection. The logical and physical security enhancements for POWERLINK networks shall be applied.
An attacker may change data of a legitimate POWERLINK network package, confusing the POWERLINK recipients	The modification of data packets requires a daisy-chain topology, in which the attacker succeeds in altering a data packet before it is forwarded to the next node. In addition to extensive technical skills for implementing the POWERLINK protocol, the attacker must be capable of disrupting an existing connection between two CNs and inserting a malicious, specially manipulated CN. Disruptions in the communication are detected and indicated by the Automation Runtime as a CN failure. In addition, The logical and physical security enhancements for POWERLINK networks shall be applied.

Confidentiality of data

This section addresses CRA Annex I, Part I, (2)(e)

On the north-bound IP-based network interface, TLS communication channels are used protecting the confidentiality of transmitted data by default.

Additionally, it is recommended to apply the „Data confidentiality“ measures, described Automation Runtime IEC 62443-4-2 statements catalog for B&R Automation Runtime, where applicable and needed.

The protection of the confidentiality of transmitted data to the south-bound POWERLINK network requires logical and physical security enhancements at the Asset Owner‘s site. Meanwhile, the confidentiality of data transmitted over the asynchronous south-bound POWERLINK network channel using TCP/IP is, by default, ensured by TLS.

Threat	Service Provider mitigation guidance
An attacker may physically connect to the POWERLINK network, reading data transmitted over the POWERLINK network.	Data transferred over the POWERLINK network is not defined as confidential. To address confidentiality for transmitted POWERLINK data logical and physical security enhancements for POWERLINK networks shall be applied.

Integrity of data

This section addresses CRA Annex I, Part I, (2)(f)

On the north-bound IP-based network interface, TLS communication channels are used protecting the integrity of transmitted data by default.

Additionally, it is recommended to apply the „System integrity“ measures, described Automation Runtime IEC 62443-4-2 statements catalog for B&R Automation Runtime, where applicable and needed.

The firmware and configuration of POWERLINK devices is checked during the boot-up and network initialization routine on B&R Automation Runtime. In case firmware and/or configuration deviations are detected at B&R Automation Runtime level, Automation Runtime will enforce a redeployment of firmware and/or configuration to relevant POWERLINK devices. The Automation Runtime configuration is protected by the security capabilities of the Automation Runtime system.

B&R signs all POWERLINK firmware packages, and the Automation Runtime performs signature verification before deployment to the Controlled Nodes. Once data passes through the Automation Runtime‘s southbound POWERLINK interface, integrity protection downgrades to CRC checksums, which protect only against accidental corruption from technical errors, not intentional tampering.

The protection of the integrity of transmitted data to the south-bound POWERLINK network requires logical and physical security enhancements at the Asset Owner‘s site. Meanwhile, the integrity of data transmitted over the asynchronous south-bound POWERLINK network channel using TCP/IP is, by default, ensured by TLS.

Threat	Service Provider mitigation guidance
An attacker may change data, state information, or parameters on POWERLINK devices via the north-bound interface.	In a Secure by Default configuration, the north-bound interface is segmented from the south-bound POWERLINK interface. No >= ISO Layer 2 network traffic is traversing between these two interfaces. Furthermore, B&R Automation Runtime acts as a media and application logic gateway, where requests and responses are evaluated and analyzed, before they are transmitted to communication partners on either the POWERLINK network (south-bound communication) or pure IP-based network (north-bound interface). Furthermore, the logical and physical security enhancements for POWERLINK networks shall be applied.
An attacker may physically connect to the POWERLINK network, changing data during transit.	Service Provider and Asset Owners are required to prevent unauthorized physical access to the POWERLINK network and devices. This type of attack would require the attacker to change, inject, or remove POWERLINK network packages on the POWERLINK network. Furthermore, the attacker may replace an existing POWERLINK device with a malicious one under his control. Automation Runtime events/alarms are triggered, indicating if a node is getting temporally unavailable as a result of the interception activity. Furthermore, the logical and physical security enhancements for POWERLINK networks shall be applied.
An attacker may physically tamper with POWERLINK device data and configuration settings.	Service Provider and Asset Owners are required to prevent unauthorized physical access to the POWERLINK network and devices. Automation Runtime events/alarms are triggered, indicating if a node is getting temporally unavailable as a result of the interception activity. Furthermore, the logical and physical security enhancements for POWERLINK networks shall be applied.

Data privacy and processing of data

This section addresses CRA Annex I, Part I, (2)(g)

B&R POWERLINK devices by default do not collect, forward or store business, personal, or otherwise sensitive data. No data is shared with 3rd parties, unless explicitly programmed by the Service Provider. Data transferred over the POWERLINK network is not defined as confidential.

Availability and attack surface reduction

This section addresses CRA Annex I, Part I, (2)(h) and (2)(j)

On the north-bound IP-based network interface, the attack surface shall be limited and hardened by removing non-essential functionality and services to the required minimum. The B&R security user documentation for Automation Runtime in chapter „Services and Applications Security“, provides an overview on available services and limiting their exposure. Automation Runtime provides customers with a host-based firewall to further restrict activities to specific interfaces if required.

Additionally, it is recommended to apply the „Resource availability“ measures, described Automation Runtime IEC 62443-4-2 statements catalog for B&R Automation Runtime, where applicable and needed.

Threat	Service Provider mitigation guidance
An attacker may perform network storms on the POWERLINK network or specific POWERLINK device. This may lead to DoS conditions of the POWERLINK network and directly impact the control process.	This type of attack would require the attacker to connect to the POWERLINK network. On a Secure by Default configuration, the north-bound interface is segmented from the south-bound POWERLINK interface. No >= ISO Layer 2 network packages are traversing between these two interfaces. The logical and physical security enhancements for POWERLINK networks shall be applied.

Restricted data flow and impact to neighboring systems

This section addresses CRA Annex I, Part I, (2)(i) and (2)(k)

B&Rs Automation Runtime protects the time-critical isochronous transfer of cyclic I/O and motion data of the POWERLINK non-routable ISO Layer 2 network protocol, as well as the asynchronous communication between network nodes by blocking network communication between the Ethernet and POWERLINK interfaces on default. In case customers need to deviate from this secure default setting bridging the two networks, the Automation Runtime host-based firewall shall be configured limiting the exposure to the required minimum.

Additionally, it is recommended to apply the „Restricted data flow“ measures, described Automation Runtime IEC 62443-4-2 statements catalog for B&R Automation Runtime, where applicable and needed.

As POWERLINK devices and networks are intended to be segmented and shield off logically and physically, negative impact to neighboring systems is not expected.

Threat	Service Provider mitigation guidance
A rouge POWERLINK device causes a network storm or otherwise negatively impacts neighboring devices	POWERLINK inherently implements an error counter mechanism for each connected POWERLINK device. Once a certain threshold on errors is reached, a reboot of this POWERLINK device is issued by the B&R Automation Runtime. Additionally, events/alerts are being logged at B&R Automation Runtime. Furthermore, POWERLINK is „proven-in-use“ for years in various machine installations, with different complexities. On a Secure by Default configuration, the north-bound interface is segmented from the south-bound POWERLINK interface. No >= ISO Layer 2 network packages are traversing between these two interfaces. The logical and physical security enhancements for POWERLINK networks shall be applied.

Providing security related information

This section addresses CRA Annex I, Part I, (2)(l)

Logging and monitoring are centrally collected by the B&R Automation Runtime. POWERLINK devices are not actively pushing information to the Automation Runtime but are rather observed. Security related information about events on the POWERLINK network is stored in the Automation Runtime logbook. This logging service can be enabled or disabled and will be active after the POWERLINK network boot-up is completed.

Logbooks can be accessed via the engineering software Automation Studio or be programmatically accessed. Programmatic monitoring is also possible, using a dedicated process variable (PV) on Automation Runtime indicating if POWERLINK devices are no longer accessible or if non-configured additional POWERLINK participants are attached to the network. The PV can be programmatically reset.

Also refer to the information on software updates for POWERLINK devices.

Removal of data

This section addresses CRA Annex I, Part I, (2)(m)

The Service Provider can reset all configurations by running an initial transfer to Automation Runtime with an Automation Studio project including a default device configuration.

Additionally, it is recommended to apply the „Data confidentiality“ measures, described Automation Runtime IEC 62443-4-2 statements catalog for B&R Automation Runtime, where applicable and needed.

Annex I, Part II - Vulnerability handling requirements

This section addresses CRA Annex I, Part II

B&R organizations following the certified B&R wide Secure Development Lifecycle according to the IEC 62443-4-1, also follow B&Rs and ABBs joint vulnerability handling policy and coordinated vulnerability disclosure process described in the publication „ABB‘s approach to vulnerability handling“.

These processes build the foundation, addressing the vulnerability handling requirements set out by the EU CRA in Annex I part II.

The following table provides B&R guidance on EU CRA Annex I part II requirements. Please note, vulnerability handling requirements will eventually be available for all B&R products which will be CRA compliant. This is an ongoing adoption process at B&R. The current CRA status for each product can be reviewed at the B&R website under certifications.

Annex I, Part II requirement	B&R guidance
1	B&R creates and maintains Software Bill of Materials (SBOM) for each released product version. The SBOM is then ingested in a component analysis platform, monitoring for known exploitable vulnerabilities in top-level 3rd-party dependencies. Identified exploitable vulnerabilities will be addressed and documented, following the IEC 62443-4-1 processes, vulnerability handling policy, and coordinated vulnerability disclosure process.
2	Exploitable vulnerabilities in product versions are addressed following the IEC 62443-4-1 processes, vulnerability handling policy, and coordinated vulnerability disclosure process. The product‘s lifecycle state is also considered in the remediation process.
3	B&Rs certified Secure Development Lifecycle according to the IEC 62443-4-1 includes both internal as external security tests. This includes also regular Device Security Assurance Center (DSAC) tests and Penetration tests. Identified issues will be addressed, following the IEC 62443-4-1 processes, vulnerability handling policy, and coordinated vulnerability disclosure process.
4	B&R organizations follow the IEC 62443-4-1 processes, vulnerability handling policy, and coordinated vulnerability disclosure process disclosure to fix exploitable vulnerabilities, including their description, affected products, impacts, severity, and remediation guidance are published on the B&R Cyber Security website, under Security Advisories.
5	Exploitable vulnerabilities in product versions are addressed following the IEC 62443-4-1 processes, vulnerability handling policy, and coordinated vulnerability disclosure process.
6	Publication of exploitable vulnerabilities on the B&R Cyber Security website. This site also describes how to get securely in touch with the B&R Cyber Security team. B&Rs and ABBs joint vulnerability handling policy and coordinated vulnerability disclosure process is described in the publication „ABB‘s approach to vulnerability handling“.
7	Security updates for POWERLINK devices are described in section Vulnerability and update management of B&R POWERLINK devices of this document.
8	Security updates for product versions are addressed following the IEC 62443-4-1 processes, vulnerability handling policy, and coordinated vulnerability disclosure process. Security updates are released in a timely manner.

Vulnerability and update management of B&R POWERLINK devices

Devices with a POWERLINK interface from B&R are developed and maintained in accordance with the requirements of IEC 62443-4-1 Practice 6 and Practice 7. This includes - but is not limited to - the documentation of utilized components and the regular analysis of potential threats. Identified exploitable vulnerabilities from ongoing monitoring activities are addressed and disclosed through industry-standard channels such as security advisories, revision notes, and/or CVE entries. Service providers using POWERLINK devices are responsible for continuously monitoring vulnerability publications, conducting risk assessments specific to their environments, and either applying B&Rprovided patches or deploying appropriate countermeasures.

Manufacturers who use the POWERLINK stack in their devices directly can obtain updates from the respective suppliers. B&R will continue to maintain the POWERLINK stack for at least the support of the last POWERLINK device supplied by B&R (min. 5 years). For further details, please refer to: https://www.br-automation.com/en/technologies/powerlink/faq/#How-does-ensure

The firmware of POWERLINK devices is never obtained directly from external networks or cloud-based services. Instead, the B&R update server provides verified and approved software packages. These packages are retrieved, validated, and installed through the B&R engineering software Automation Studio, within the scope of a defined project.

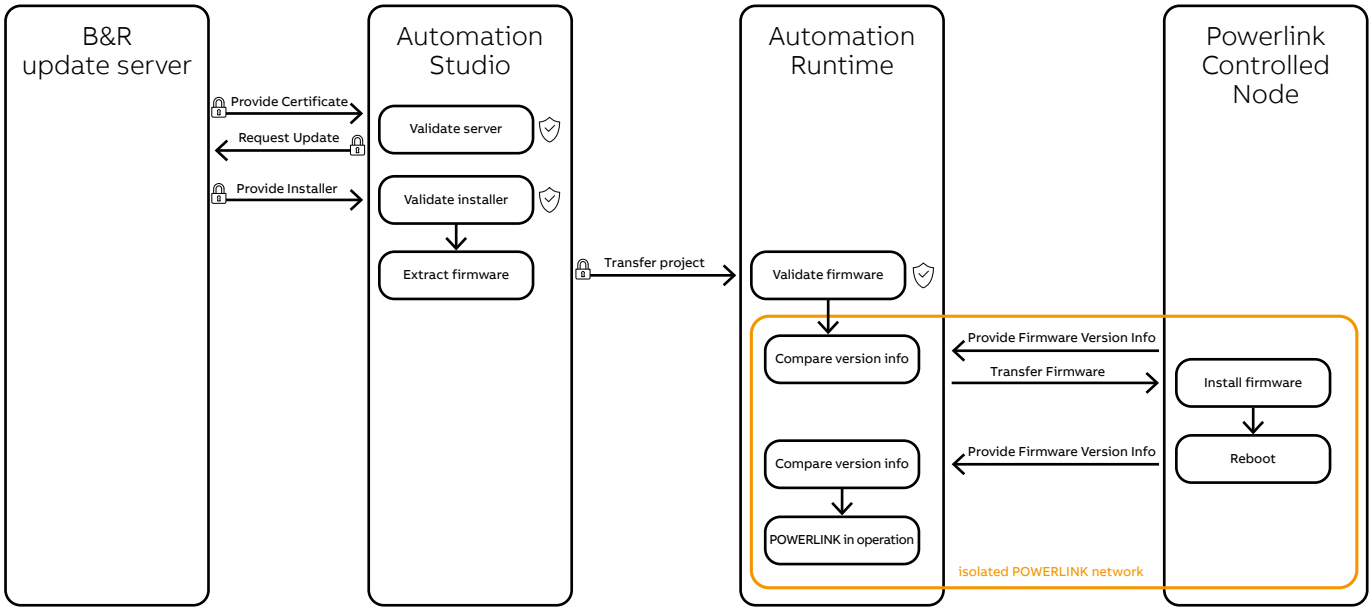
The developed, tested, and maintained Service Provider project includes firmware updates for the configured POWERLINK devices (Controlled Nodes) as well as the necessary configuration data for those nodes. The firmware and configuration data are transferred as part of the Service Provider's compiled application package to the Automation Runtime via the ANSL service. By default, the ANSL service is securely configured, using a TLS-encrypted communication channel and granting access exclusively to privileged users through the Automation Runtime's RBAC system. Access to firmware and configuration data within the Automation Runtime is, by default, restricted to privileged ANSL users. All transfers of POWERLINK firmware or configuration performed via the ANSL service are logged within the Automation Runtime for traceability and audit purposes.

During system boot-up, the Automation Runtime verifies the Controlled Nodes' software and configuration, then distributes the required POWERLINK software updates to the Controlled Nodes.

The update of POWERLINK firmware is performed only during the network initialization phase. Updating the firmware during normal operation would trigger a reboot, resulting in a temporary outage of the POWERLINK devices.

Firmware updates (successful or unsuccessful) of POWERLINK Controlled Nodes are being logged in the logging system of Automation Runtime. Also, configuration changes on Controlled Nodes are being logged.

This multi-layer approach ensures that only authorized software packages are used in the supply chain.



7 Multi-layered secure update approach for POWERLINK devices

Threat	Service Provider mitigation guidance
An unauthenticated attacker may deploy malicious firmware to the Managing Node on Automation Runtime.	Access to the POWERLINK Managing Node (MN) running on Automation Runtime over the Online Communication protocol (ANSL) is authenticated. Furthermore, data communication over the Online Communication protocol is protected using TLS, including support for mutual TLS.
An unauthenticated attacker may trigger a firmware update from a network segment outside of the POWERLINK network	The POWERLINK network is logically separated from other network segments. Network communication is always terminated at the Automation Runtime PLC gateway.
An unauthenticated attacker may physically connect to POWERLINK network and trigger a firmware update on the POWERLINK Controlled Node.	Physical access to the POWERLINK wiring and POWERLINK devices shall be only granted to authorized users. The physical security enhancements for POWERLINK networks and devices shall be applied.

Annex II Information and instruction to the user

This section addresses CRA Annex II

The following table provides B&R guidance on EU CRA Annex II requirements. Please note, information and instructions to the user will eventually be available for all B&R products which will be CRA compliant. This is an ongoing adoption process at B&R. The current CRA status for each product can be reviewed at the B&R website under certifications. CRA compliant products are developed and maintained by B&R organizations following the certified B&R wide Secure Development Lifecycle according to the IEC 62443-4-1.

Annex II requirement	B&R guidance
1	This information is available on the B&R website / About us.
2	Publication of exploitable vulnerabilities on the B&R Cyber Security website. This site also describes how to get securely in touch with the B&R Cyber Security team. B&Rs and ABBs joint vulnerability handling policy and coordinated vulnerability disclosure process is described in the publication „ABB's approach to vulnerability handling“.
3	This document refers to the Powerlink V2 standard version 1.5.2. B&R employs a version designation for the unique identification of its Powerlink stack implementation, which comprises the version number of the stack specification and a sequential revision number. The current version number is 1.5.2.1. Please note that versioning schemes may vary among different Powerlink stack implementation vendors. The user documentation of Powerlink devices contains a reference to the specifically implemented Powerlink version. Product specific information, like its unique identification can be reviewed in the products user manual published in the Download section on B&Rs website.
4	Documentation on the security environment, intended purpose, essential information, and security properties of the product can be reviewed in the products user manual and/or Automation Help published on B&Rs website for the product with digital elements.
5	Documentation on Cyber threats and risk can be reviewed in the products user manual and/or Automation Help published on B&Rs website for the product with digital elements.
6	The CE declarations for specific products are published in the Download section on B&Rs website.
7	Lifecycle information for specific products can be accessed upon user login on the product specific page on the B&R website. This includes also information on technical (security) support offered by B&R for a specific product in a specific lifecycle stage. B&R ensures vulnerability handling for the POWERLINK stack during the support periods of the individual products (min. 5 years).
8	These detailed instructions and information is available in either the products user manual and/or Automation Help published on B&Rs website.
9	Access to the products Software Bill of Materials (SBOM) is handled via the local sales representative.

B&R
Industrial Automation GmbH
A member of the ABB Group
B&R Strasse 1
5142 Eggelsberg, Austria
office@br-automation.com

t +43 7748 6586-0
f +43 7748 6586-26

br-automation.com