B&R

CYBER SECURITY

Defense in Depth for B&R products

Document information

Version	1.6
Date	2024-05-13
Publisher	B&R Industrial Automation GmbH B&R Strasse 1 5142 Eggelsberg Austria Telephone: +43 7748 6586-0 Fax: +43 7748 6586-26 office@br-automation.com
Disclaimer	All information in this document is current as of its creation. The contents of this document are subject to change without notice. B&R Industrial Automation GmbH assumes unlimited liability in particular for technical or editorial errors in this document only (i) in the event of gross negligence or (ii) for culpably inflicted personal injury. Beyond that, liability is excluded to the extent permitted by law. Liability in cases in which the law stipulates mandatory unlimited liability (such as product liability) remains unaffected. Liability for indirect damage, consequential damage, business interruption, loss of profit or loss of information and data is excluded, in particular for damage that is directly or indirectly attributable to the delivery, performance and use of this material. B&R Industrial Automation GmbH notes that the software and hardware designations and brand names of the respective companies used in this document are subject to general trademark, brand or patent protection. Hardware and software from third-party suppliers referenced in this document is subject exclusively to the respective terms of use of these third-party providers. B&R Industrial Automation GmbH assumes no liability in this regard. Any recommendations made by B&R Industrial Automation GmbH are not contractual content, but merely non-binding information for which no liability is assumed. When using hardware and software from third-party suppliers, the relevant user documentation of these third-party suppliers must additionally be consulted and, in particular, the safety guidelines and technical specifications contained therein must be observed. The compatibility of the products from B&R Industrial Automation GmbH described in this document with hardware and software from third-party suppliers is not contractual content unless this has been separately agreed in individual cases; in this respect, warranty for such compatibility is excluded in any case, and it is the sole responsibility of the customer to verify this compatibility in advance.

Table of contents

1 Introduction

The introduction to Cyber Security in industrial automation and control systems (IACS) highlights the importance of protecting these systems against security threats. A comprehensive and multi-layered approach is necessary for a robust defense, which requires continuous evaluation and adaptation to counter evolving threats.

B&R recognizes the critical nature of Cyber Security in IACS and aligns its long-term vision with internationally recognized standards, such as IEC 62443-4-1. This standard advocates for a "defense in depth" strategy, which involves implementing multiple layers of security controls throughout an information system. B&R is committed to not only adhering to these standards but also educating customers about the importance of Cyber Security. This document provides insights into common hacking techniques that target industrial control systems and shares knowledge about ways to enhance security measures.

The core concept is to establish security from diverse perspectives and across various levels within the system. The goal is to create multiple defensive barriers, making it difficult for an attacker to penetrate the system and reach their target. This document is a guide for the secure operation of B&R products. B&R provides guidelines for security, but the customer is responsible for implementing them effectively. Implementation should be tailored to individual needs and based on a thorough evaluation of specific threat scenarios relevant to each customer's environment.

The document is divided into two parts to enhance clarity and depth:

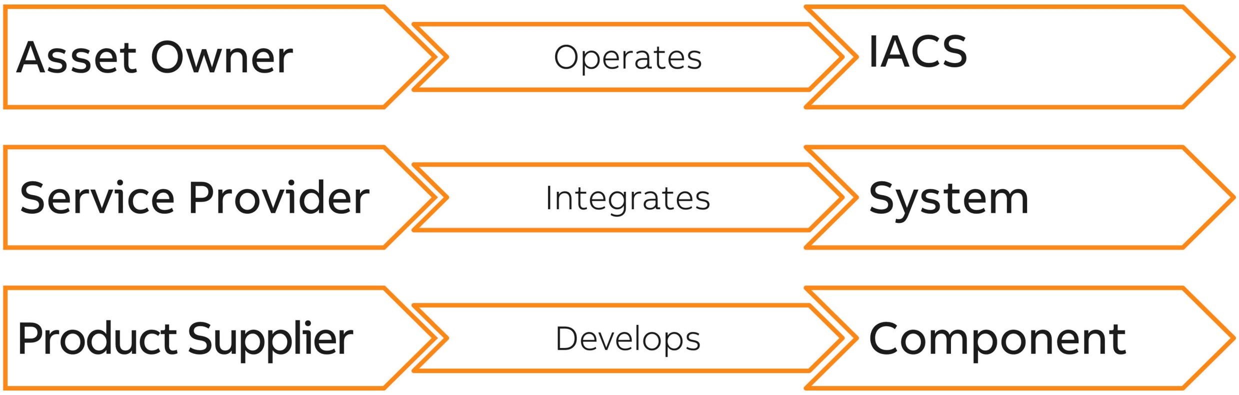
1) General guidelines
   This section offers general advice and strategies that form the foundation of a secure setup for all B&R products. It covers the fundamental principles of Cyber Security in IACS, providing overarching guidelines that apply to all.
2) Product-specific Cyber Security features and guidelines
   Each B&R product will have a document that details its specific Cyber Security features and guidelines. This section covers the complexities of individual products, including the services, ports and applications used. It offers customized advice on securing each product, taking into account its unique characteristics and potential vulnerabilities.

2 Terms and definitions

Terms and definitions are used according to IEC 62443.

3 Supply chain security

In the context of Cyber Security, especially within industrial automation and control systems (IACS), the concept of a security chain security is important. Security is a collaborative effort involving multiple stakeholders, each playing an essential role in maintaining the overall security posture. B&R understands its role in the IEC 62443 standard guide.



The security chain comprises several key roles, each with distinct responsibilities such as:

1) Asset owner

   - Inventory management for updatable IACS devices
     Maintain a current list of all electronic devices connected to the IACS that can be modified through changes to their functionality, configuration, operation, software, firmware or operating code. Categorize these devices as "updatable".
   - Tracking installed device versions
     Compile and update a log of the current software or firmware versions installed on each device, referred to as the "installed" version.
   - Regular checks for device updates and upgrades
     Regularly check for updates for each device to ensure you have the latest version.
   - Compatibility and standards verification for updates
     Periodically, identify the "released versions" of upgrades and updates that are compatible with the IACS product supplier and meet the criteria for "updatable" devices.
   - Scheduling and planning patch installations
     Plan the installation of authorized and validated patches at the earliest suitable time, taking into account the system's design considerations such as redundancy, fault tolerance and safety, as well as operational needs, such as unexpected downtime, planned maintenance and in-process operations.
   - Update documentation for devices
     Documentation should be updated regularly to reflect the installed, authorized, effective and released versions for each updatable device.
   - Setting patch installation intervals
     Establish a consistent schedule for installing patches, based on patch availability.
   - Applying patches and mitigating security vulnerabilities
     To address known vulnerabilities in the IACS, apply patches or implement alternative security measures.

2) Service provider

   - Adherence to security standards and frameworks
     The service provider should adhere to established Cyber Security standards and frameworks relevant to industrial control systems such as IEC 62443. This includes implementing security management systems, incident response plans and conducting regular security assessments.
   - Risk management
     Implementing risk management strategies involves regular risk assessments, mitigation plans and continuous monitoring of the IACS environment.
   - Testing IACS patches in production-like environments
     Conduct tests on IACS patch applications in a manner that closely mirrors the live production setting to ensure that the introduction of patches does not adversely affect the reliability and functionality of IACS in the actual operational environment. Successfully tested patches are termed "authorized patches".
   - Secure service delivery
     All services, including software updates, patch management and maintenance activities, shall be conducted securely to prevent unauthorized access or compromise of the IACS.
   - Training and awareness
     Providing continuous training and awareness programs to keep personnel informed of the latest Cyber Security threats, vulnerabilities and best practices.
   - Incident response and recovery
     To minimize downtime and operational impact in the event of a security breach or failure, it is important to have a robust incident response and recovery plan in place.

3) Product supplier

   - Patching policy
     Suppliers of IACS components must provide documentation that clearly outlines their software patching policy for the products and systems they deliver.
   - Patch qualification for applicability and compatibility
     Evaluate and validate all patches, including those issued by the operating system provider and any third-party software suppliers, to ensure compatibility and applicability with IACS components.
   - Timely updates and notifications for asset owners
     Asset owners should be regularly informed about any patches being released by the OS or third-party software providers.

  - Advance notice for end of life components
    Provide ample notice regarding components that are nearing their "end of life" or will no longer receive Cyber Security patches.
  - Providing information to IACS
    Provide relevant information to IACS to support effective Cyber Security management and operational integrity.

4 Risk management

Risk management is important for maintaining strong security in any organization, particularly for asset owners who manage complex infrastructures and processes in diverse environments. Each company's unique setup requires a customized approach to identifying and mitigating risks. This strategy ensures that specific threats and vulnerabilities are effectively addressed, enhancing the overall security posture of the organization.

Every organization should conduct a comprehensive assessment to identify potential threats that are specific to its infrastructure and operational environment. This involves understanding the nature of the assets, the processes in place and the infrastructure's configuration. By identifying these unique threats, asset owners can develop targeted strategies to mitigate them.

Risk management involves evaluating the likelihood of potential threats exploiting vulnerabilities and the impact of such exploits on valuable assets. This assessment helps prioritize risks based on severity and potential impact, allowing organizations to allocate resources effectively.

Key components of risk management include:

- Assets
  Example: Your beautiful watch and the money you have.
- Vulnerabilities
  "A vulnerability is the weaknesses that gets exploited by a threat actor/event". Example: Hotel room safe cannot be locked using a hard-coded master pin.
- Threats
  "A threat has the potential to cause harm to an asset.". Example: Service personnel steal my watch and money.
- Impact x Likelihood = Risk
  "Impact is the actual inflicted harm of the exploited vulnerability."

Regularly revisiting and updating the risk assessment is imperative due to the ever-changing landscape of cyber threats. This ongoing process ensures that the organization stays ahead of new threats and adapts to any changes in its operating environment or internal processes. Regular evaluations allow for the timely identification of emerging vulnerabilities and the implementation of appropriate countermeasures.

Security risk management is a continuous process that evolves with the organization and the broader cyber threat environment. It requires constant vigilance, adaptation and improvement to ensure that security measures remain effective against emerging threats and changing organizational dynamics.

5 Security objectives

In contexts such as industrial automation and control systems (IACS), security objectives play an important role in protecting data, systems and operations. Understanding these objectives is essential for defining and implementing a strong security strategy.

The primary security objectives include:

- Safety
  In Cyber Security, safety refers to the absence of unacceptable risks to environment, safety and health (HSE). This includes protecting systems and data from cyber threats that could cause physical harm or environmental damage.

- Availability
  This objective aims to ensure that information and systems are readily accessible and can be utilized by authorized users. Availability is important for the smooth operation of systems, ensuring that authorized users have reliable access to the resources they need when they need them.
- Integrity
  Integrity refers to protecting the accuracy and completeness of assets. It ensures that information and systems are not altered in unauthorized ways, safeguarding data from tampering and ensuring its accuracy and reliability.
- Confidentiality
  This is achieved by ensuring that information is not made available or disclosed to unauthorized users. Confidentiality involves protecting sensitive information from unauthorized access, maintaining privacy and secrecy.
- Authentication
  Authentication is the process of verifying the identity of a user, whether human, process or device, to ensure that access to systems and data is granted only to legitimate and verified users.
- Authorization
  Authorization is the process of determining and enforcing what actions a human, process or device is permitted to perform within a system. This involves granting or denying rights and privileges to resources based on established policies and the verified identity of the requester (as established during the authentication process).
- Non-repudiation
  Non-repudiation involves proving the occurrence of a claimed event or action and its originating users. It ensures that users cannot deny their involvement in an event or transaction. This is particularly important for legal and auditing purposes, where it is necessary to definitively attribute actions to specific users.

5.1 Safety

Cyber Security is not only about protecting digital assets and information, but also about mitigating risks that could harm the environment, safety and health (HSE). Cyber Security measures shall therefore be in place to prevent incidents that could lead to physical harm or environmental degradation, in addition to safeguarding data and systems from unauthorized access or damage. Organizations shall understand and implement key safety components in Cyber Security to effectively protect against multifaceted risks.

5.2 Availability

Especially in industrial automation and control systems (IACS), availability is important for continuous and reliable operations. To ensure availability, it is necessary to protect essential functionality and design systems that can withstand various types of disruptions, from cyber attacks to technical failures. To enhance the system, implement strategies such as zone design, robust data validation, minimalism in system functionality, efficient resource handling and comprehensive recovery mechanisms.

Protecting essential functionality:

- Zone design with low coupling (trust boundaries)
  Create separate network zones with clearly defined trust boundaries to minimize dependencies and interactions between different parts of the network. This design limits the spread of disruptions and isolates critical system components, enhancing overall system resilience.
- Robust Input data validation at trust boundaries
  Strong validation processes should be implemented for data entering the system at trust boundaries. This includes checking the data for correctness, legitimacy and potential threats. It is essential to drop invalid or suspicious data to prevent system compromises.
- Prefer whitelisting over blacklisting
  When controlling access or filtering traffic, we recommend the use of whitelisting instead of blacklisting. Whitelisting assumes that everything is untrusted unless explicitly allowed, which is generally more secure than blacklisting known unsafe entities.

The least functionality principle:

- Run only functionality necessary for operation
  Activate only essential system functionality to minimize potential attack vectors and reduce vulnerability exposure.
- Disable nonessential functionality by default
  We recommend disabling nonessential services and features by default. Users or administrators can enable them as needed to ensure the system operates with the minimum required functionality.

Recovery mechanism:

- Backup and recovery mechanisms
  Implement backup and recovery mechanisms for system configurations and data to quickly restore normal operations in case of system failure or compromise.
- Support redundancy mechanisms
  In high-availability environments, implement redundancy mechanisms such as redundant hardware, software or network paths to ensure continuous operation even if one component fails.

5.3 Integrity

Integrity in Cyber Security ensures that data is authentic, accurate and protected from unauthorized modification. In industrial automation and control systems (IACS), maintaining data integrity is important for ensuring the reliability and safety of operations. Hash functions are an effective method for ensuring integrity.

Hash functions have the following properties:

- Create a fingerprint of data
  A hash function generates a unique "fingerprint" or hash value from data. This value is a fixed-size representation of the data. Even a minor alteration in the original data results in a significantly different hash value. This property makes it easy to verify if data has been tampered with by comparing hash values before and after transmission or storage.
- One-way functionality
  Hash functions are designed to be one-way, making it computationally infeasible to reverse-engineer the original data from its hash value. This one-way nature ensures that the hash value does not reveal any information about the actual data, adding a layer of security.
- Collision resistant
  A collision-resistant hash function ensures that it is highly unlikely (though not impossible) for two different sets of data to produce the same hash value. This property, also known as second pre-image resistance, is crucial for preventing attackers from substituting the original data with different data that produces the same hash value.
- No secret information required
  Hash functions do not require any secret information, unlike encryption algorithms that require keys to be kept secret. This makes them simpler to implement and manage, as there is no need for key management protocols.

Integrity assurance using hash functions can be used in the following scenarios:

- Data verification
  Hash functions can be used to verify the integrity of transmitted or stored data. Comparing hash values allows for easy detection of any unauthorized modifications to the data.
- Digital signatures
  To enhance security, digital signature algorithms are always combined with hash functions. This involves signing the hash of the data with a private key and using the corresponding public key to verify the integrity of the data.
- Auditing and logging
  Hash log entries in logging and auditing systems to maintain log integrity. This helps organizations detect and prevent unauthorized changes to logs, which are crucial for security audits and investigations.

5.4 Confidentiality

Confidentiality is a critical aspect of Cyber Security, especially in environments where sensitive information is frequently communicated and stored. Robust cryptographic mechanisms must be employed to ensure confidentiality, safeguarding data during transmission and storage.

The following cryptographic aspects should be considered:

- Communication over trust boundaries
  To reduce the risk of interception or eavesdropping, we recommend the use of strong encryption protocols when transmitting data over networks, particularly across trust boundaries. This ensures that even if the data is intercepted, it remains secure and unintelligible.
- Storing information/data in places shared with other trust zones
  When storing data in shared environments or places that intersect with different trust zones, it is crucial to use strong encryption. This practice prevents unauthorized access and ensures that sensitive information remains confidential, even in shared storage spaces.

Following Kerckhoff's principle, the security of a cryptosystem should depend on the secrecy of the key, not on the secrecy of the system itself.

This principle highlights a critical aspect of cryptographic security:

- Key management
  Effective key management involves securely generating, storing and exchanging keys that are sufficiently complex to resist decryption attempts. Keys must be managed in a way that prevents unauthorized access or use.

5.5 Authentication

Effective authentication management in IACS involves a comprehensive approach that includes a variety of authenticators and regular updates to security protocols. By combining multiple authentication methods and continuously reviewing and improving these mechanisms, asset owners, product suppliers and system integrators can significantly enhance the security of their systems.

Authentication involves verifying user identity through various methods. Examples of authenticators include:

- Passwords
  To verify a user's identity, unique and complex strings of characters are used.
- Tokens
  Physical devices or software-based tokens that generate a one-time code for authentication.
- Private keys
  Private keys are kept secret by the owners, while the public keys can be shared openly. These pairs are mathematically linked, meaning anything encrypted with one key can only be decrypted by the other.
- Biometrics
  Individuals possess unique physical characteristics that can be used for identification purposes, such as fingerprints, facial recognition and iris scans.
- Physical keys
  Traditional keys or smart cards are commonly used for physical access control.

Asset owners, system integrators and product suppliers have specific roles in ensuring robust and secure authentication practices. Implementing strong authenticators is essential to this process.

For example, the product supplier shall:

- Secure default configuration
  Ship products with secure default settings, including non-generic, complex passwords and disabled unnecessary services to minimize vulnerabilities.
- Provide tools for secure authentication
  Offer tools or software that facilitate the secure generation, management and storage of authentication credentials (e.g. passwords, keys) and support secure authentication protocols.
- Regular security updates and patches
  Actively maintain and update products to address emerging vulnerabilities and threats, including updates that enhance authentication security.

For example, the system integrator shall:

- Initialize strong authenticators
  For instance, setting complex passwords.
- Change default authenticators
  Replace factory-set passwords or key configurations with unique alternatives.
- Protect authenticators
  Passwords, keys and biometric data should be safeguarded via encryption and secure storage.
- Certificate lifecycle management
  Ensure the secure issuing, renewal and revoking of digital certificates.
- Secure communication channels
  Use TLS to transmit authentication data to prevent interception.

For example, the asset owner shall:

- Change default credentials
  Replace any default passwords or keys provided with IACS equipment.
- Ensure unique credentials
  Collaborate with system integrators to obtain unique credentials or the ability to modify existing ones.

Ongoing authentication management involves the following activities:

- Regularly evaluate authentication mechanisms
  Continuously improve methods.
- Monitor certificate expirations
  Regularly review and update digital certificates.
- Password management
  We recommend changing passwords frequently and ensuring that they are strong and unique.
- Time restriction adjustments
  Review and adjust time-based restrictions on authentication methods.

5.6 Authorization

Authorization is a key aspect of security and access control in information systems, encompassing two primary perspectives: The subject view and the object view. It specifies both the actions subjects are permitted to perform and how they can interact with various resources (objects) within the system, such as databases, files, systems and network devices.

The two views of authorization:

- Subject view of authorization
  This perspective concerns the authorization of a subject, such as a user, process or device, within the system. It involves assigning permissions based on the subject's role or identity and managing access rights in a role-based or user-specific manner. Role-based access control (RBAC) is an example of this, where permissions are grouped by roles, simplifying the assignment and management of user permissions as roles change or evolve.
- Object view of authorization
  From an object perspective, the focus is on the resources themselves and the actions that can be performed on them. Access control lists (ACLs) are commonly used to implement this view by listing permissions attached to an object and indicating subjects that are granted access and what operations they are allowed to perform. This approach allows for precise control over resources, specifying detailed access rights for each object within the system.

The following best practices for authorization can be followed:

- Regular audits and updates
  Regularly audit and update authorization policies to ensure they accurately reflect current roles, responsibilities and security requirements.
- Principle of least privilege
  This means that identities should only be granted the minimum levels of access necessary to perform their functions. To minimize potential damage from security breaches or errors, it is important to apply the principle of least privilege.
- Clear documentation and communication
  Maintain clear documentation of all authorization policies and effectively communicate them to relevant stakeholders to ensure clarity and compliance throughout the organization.
- Integration with identity management systems
  Efficiently and effectively control authorization mechanisms by seamlessly integrating them with broader identity and access management systems.

5.7 Non-repudiation

Non-repudiation is a security principle that ensures the authenticity of transactions and activities, making it impossible for the involved parties to deny their actions. In the context of Cyber Security, particularly in systems like industrial automation and control systems (IACS), non-repudiation means maintaining accountability and trust. Digital signatures and comprehensive logging of key events are typically used to implement non-repudiation effectively.

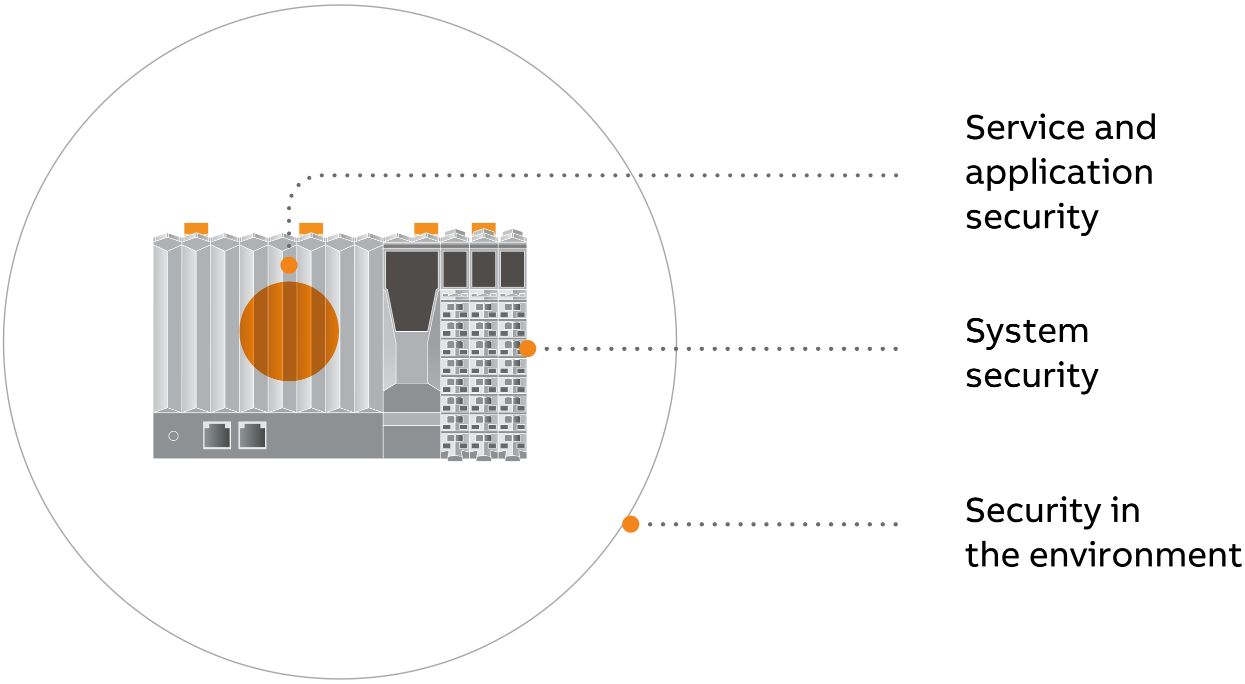
To support non-repudiation, it is important to generate detailed log entries for a range of system events, including:

- Access control logs
  All attempts to access the system, including successful and unsuccessful login attempts, as well as any access to sensitive areas or data within the system, should be recorded.
- Request/validation errors
  During requests or data validation processes, it is important to log any errors encountered. This can aid in identifying any unauthorized or malicious attempts to access or modify the system.

- System events
  Record all significant system events, including system startups, shutdowns and critical failures or anomalies. This provides an overview of the system's operational status and helps identify any unusual activities.
- Change of the system configuration
  Record all modifications to the system's configuration, including updates, changes to settings, installation of new software or hardware and modifications to user privileges. These logs are essential for tracking alterations that could impact system security or performance.
- Logging activities
  Maintain records of all logging activities themselves, including when log files are modified or exported. This ensures that the log files themselves are also subject to scrutiny and protection.
- Traceability information
  Ensure that logs contain sufficient information for traceability, including timestamps, user IDs, source and destination addresses and detailed descriptions of events or actions taken. Detailed logging is useful for forensic analysis and accountability.

6 Defense in Depth Strategy

The following figure shows B&R's Defense in Depth strategy. This strategy consists of three layers: **Security in the Environment**, **System Security** and **Service and Application Security**.



The outermost layer is referred to as **security in the environment** and defines physical and logical Cyber Security measures expected by the environment where the product is to be operated. These measures are defined in section Security in the environment.

The middle layer is referred to as **system security** and defines the Cyber Security capabilities of the product, including attributes such as system hardening, system users and physical Cyber Security capabilities. These measures are defined in section System security.

The inner layer is referred to as **service and application security** and defines the Cyber Security configuration settings of services and applications running on the product. These measures are defined in the product-specific security measures included in the "Defense in depth" documentation.

In addition to these layers, comprehensive security monitoring of the IACS equipment shall be established, monitoring of the environment, the B&R product, as well as its services and applications. Refer to section Security Monitoring.

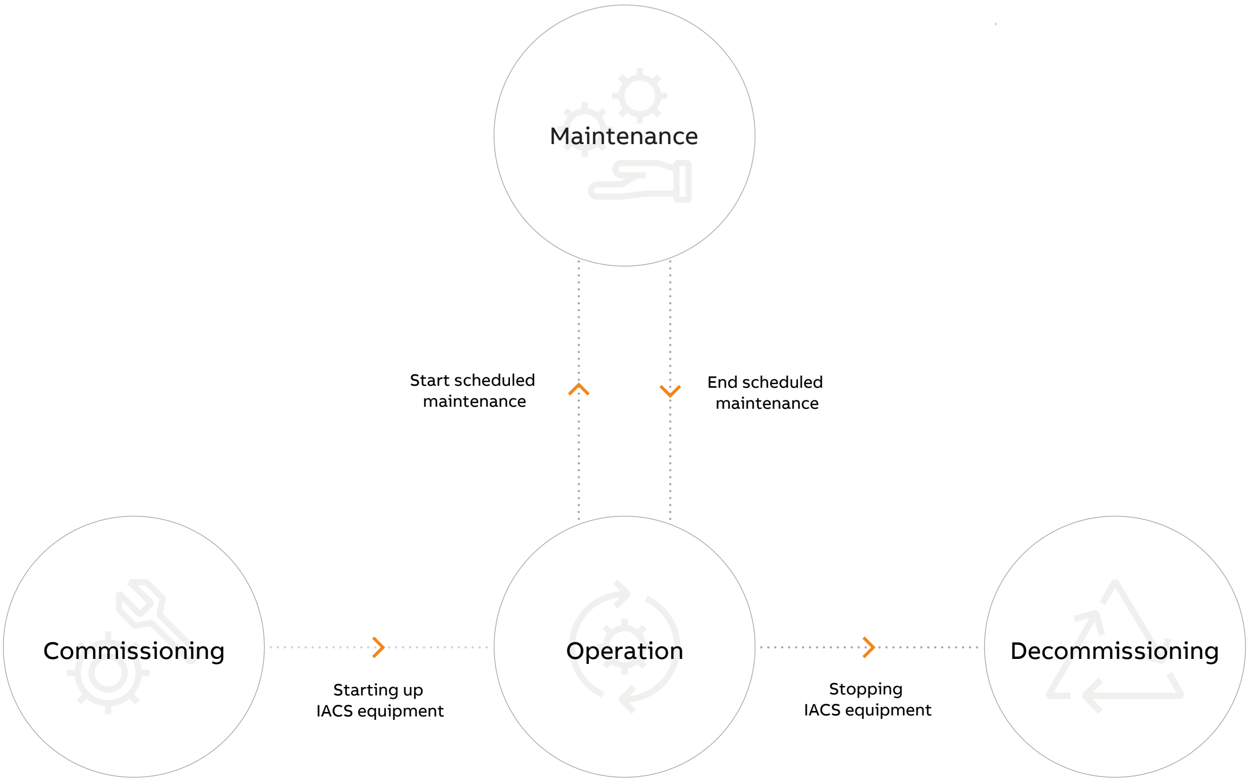
Finally, section Security testing describes B&R's Cyber Security testing processes and section Security incidents and issues describes B&R's recommendations for Incident Management.

6.1 Introduction to defense in depth strategy

The defense in depth strategy focuses on securing industrial automation and control systems (IACS). This strategy covers security in all operation states of products, as well as in various environments.

6.1.1 Product operation states

Defense in depth is a comprehensive approach to Cyber Security, particularly vital in the lifecycle of B&R products used at an asset owner's site. This approach incorporates a series of defensive mechanisms that are applicable throughout all product operation states, rather than relying on a single measure or security layer. The provided figure depicts the different phases of a product's lifecycle: Commissioning, operation, maintenance and decommissioning. Each phase presents unique security challenges that require tailored security measures to address potential threats and vulnerabilities.


Maintenance
Start scheduled maintenance
End scheduled maintenance
Commissioning
Starting up IACS equipment
Operation
Stopping IACS equipment
Decommissioning

The following figure shows the four product operation states that are assessed:

1) Commissioning
This state involves setting up and integrating B&R products into the IACS. Security measures include establishing secure configurations, ensuring proper access controls and enabling necessary available security protocols.
2) Operation
During the operation state, the product is actively being used in its intended environment. It is important to maintain ongoing security through continuous monitoring, regular security assessments and the application of updates and patches to address new vulnerabilities as they are discovered. Vigilance is required to maintain the integrity and security of the system against potential threats.
3) Maintenance
Scheduled maintenance involves routine checks and servicing to ensure optimal product functionality. Security measures during maintenance include preventing the introduction of vulnerabilities, maintaining strict access control for technicians and verifying that changes made do not compromise system security.

4) Decommissioning
During the final stage of decommissioning, the product is taken out of service. Measures taken in this stage include erasing data, revoking access rights, updating security policies and safely disposing of or re-purposing the hardware.

Defense in depth is a continuous process that adapts to the evolving threat landscape. Security measures are continuously evaluated and adapted to meet current needs at each stage, from commissioning to decommissioning. This ensures that the product maintains a posture that protects against unauthorized access, misuse and compromise.

6.1.2 Human/User management

Effective human/user management is essential for maintaining security in any organization. It involves strategically assigning roles and responsibilities to employees, ensuring they have the necessary rights to perform their tasks while also restricting access to minimize potential security risks. This safeguards critical systems and sensitive information from both internal and external threats.

The following steps can be taken:

- Role-based access control
  Implement role-based access control (RBAC) to divide the company's activities among different roles and ensure each role has clearly defined responsibilities and necessary access rights. This helps minimize the risk of unauthorized access or system misuse.
- Restricting rights and minimizing access
  To enhance Cyber Security, it is essential to limit the rights of each role as much as possible. Specifically, employee access to critical systems, whether for the company or its customers, should be restricted to the minimum required for their job functions. This approach reduces the attack surface and mitigates the risk of internal threats.
- Segregation of duties
  Implement policies and processes to ensure that critical activities cannot be performed by a single individual. This concept, known as segregation of duties (SoD), is crucial in preventing fraud and errors. Requiring that critical tasks or decisions involve multiple people mitigates the risk of malicious actions or mistakes.
- Employee integrity verification
  To ensure the security of the organization, it is important to regularly verify the integrity of employees, particularly those with significant access rights. This can be achieved through background checks, monitoring for unusual activities and other methods to ensure that employees are trustworthy and adhere to security protocols.
- Revoking access rights
  It is important to promptly revoke all access rights of employees who leave the company to prevent them from accessing systems or data they are no longer authorized to use.
- Employee training
  Invest in regular and ongoing employee training to cover both specific tasks and systems, as well as general Cyber Security awareness. This will equip employees to recognize and respond to new threat scenarios, making them an effective first line of defense against cyber attacks. Regular training is essential to keep up with evolving Cyber Security threats. Employees should be updated on the latest security practices, threat intelligence and technological advancements to ensure they can identify and address potential security issues.

6.2 Security in the environment

The chapter Security in the environment is important for protecting industrial automation and control systems (IACS) in operational technology (OT) environments.

6.2.1 Physical access & factory security

In industrial environments, ensuring the security of physical access to critical components is important. Access to these components should be restricted to authorized personnel only, following the principle of least privilege. This ensures that individuals are granted access only to the areas and resources necessary for their specific roles, effectively minimizing potential security breaches.

Access restrictions should be defined both spatially and temporally, covering all phases of the product's operation, from commissioning (typically handled by the system Integrator) to maintenance activities at both the asset owner's and system integrator's sites, as well as during normal operation and eventual decommissioning at the asset owner's site.

A layered approach, known as the onion principle, is recommended for structuring access controls. For example, an employee may have permission to enter the plant hall and operate machinery, but access to the control unit of the machine may be restricted. This approach creates multiple levels of security, each with increasing restrictions, to ensure that the most sensitive or critical areas are well protected.

To enhance security, asset owners and system integrators should implement protective processes and methods to prevent unauthorized actions. This includes restricting interaction with physical interfaces such as Ethernet, USB or fieldbuses, securing connected cables, controlling access to physical buttons or switches on equipment and safeguarding against power disruptions or failures.

In addition to these measures, we recommended employing strong verification methods in secure areas. Advanced access technologies, such as biometric scanners, card readers or PIN codes, can be used to ensure only authorized personnel gain entry. The presence of security guards and the use of locked cabinets for sensitive equipment are also effective in enhancing security. These measures serve not just to prevent unauthorized access but also to facilitate a quick response to any security incidents.

6.2.2 Network security

Network security is paramount in safeguarding industrial control systems, as TCP/IP network connections are a primary target for cyber attacks. It is essential to integrate various security strategies to protect the network's integrity, confidentiality and accessibility.

The following measures can be taken to improve network security:

- Authorized and intended communications
  Network security requires strict access controls to ensure only authorized communications occur. Network access control (NAC) and intrusion detection and prevention systems (IDPS) can be used to monitor, identify and block unauthorized access. Additionally, mutual Transport Layer Security (mTLS) can be used in OT environments.
- Encryption of IP-based communications
  Using encryption technologies like TLS for data in transit and VPNs for remote access is crucial for secure remote maintenance. These technologies ensure that communication remains secure and private.
- Network segmentation and isolation
  Dividing the network into segments is a crucial security strategy. It is especially important to separate machine networks from other company networks or use VLANs (Virtual Local Area Networks). For instance, placing programmable logic controllers (PLCs) in a dedicated control network isolates these systems, reducing the attack surface and enhancing performance.
- Firewalls and traffic control
  Control networks and systems must be located behind firewalls and segregated from business networks and the Internet. This creates a robust barrier against external threats. Firewalls should be configured to block all inbound traffic, except to specific engineering stations deemed necessary for operational purposes.
- Limiting outbound traffic
  Restricting outbound traffic from control systems/networks to necessary resources only is vital. This minimizes the risk of data exfiltration and exposure to external threats. Techniques like egress filtering and the use of proxy servers are effective in managing and monitoring Internet access.
- Specific IP address and port restrictions
  In addition to general access controls, restricting access to specific source/destination IP addresses and ports enhances network security. This level of control ensures that only necessary and legitimate communications are allowed, reducing the risk of unauthorized access.

6.2.2.1 Reference architecture

In the field of industrial automation and control systems (IACS), it is crucial to establish a strong network architecture to ensure Cyber Security. B&R recommends an architectural framework that adheres to the IEC 62443-1-1 standard, which provides a structured approach to network security. This reference architecture is intended to protect critical infrastructure within the asset owner's operational environment. For information about the reference architecture, see the ABB ICS Cyber Security Reference Architecture documentation.

The ABB ICS Cyber Security Reference Architecture diagram, as outlined in the documentation, serves as a blueprint for configuring networks in a manner that enhances security at various operational levels:

- Level 0 (process)
  This level represents the physical process layer, which includes field devices such as sensors and actuators that directly interact with industrial processes.

- Level 1 (local or basic control)
  This level includes devices that perform direct control tasks and are essential for process automation, encompassing basic control functions.
- Level 2 (supervisory control)
  Operators use supervisory control systems, such as SCADA or HMI, to oversee industrial processes.
- Level 3 (operations management)
  This level manages operations, including systems such as MES, historians and other applications that optimize production.
- Level 4 (enterprise business systems)
  This is the enterprise level where business systems are located, including ERP solutions and other corporate services.
- Cloud/Internet
  The Cloud/Internet level in the ICS architecture allows for remote data access and services through the cloud. This includes off-site backups and integration with ABB Ability™ for improved operational functions.

6.2.2.1.1 Levels

For Level 0, Level 1 and Level 2, the following B&R requirements are present:

- Limit physical access to network ports and cables
- Limit access of network ports to specific IP or MAC addresses
- Use network segmentation based on your needs and route communication between different segments over control network firewalls.
- If you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.

IACS equipment intended for trusted level use (Levels 0, 1 and 2) shall not be used outside of these levels.

For more details on levels, please refer to the ABB ICS Cyber Security Reference Architecture documentation.

6.2.2.2 Network firewalls

Network firewalls are essential for securing industrial automation and control systems (IACS) equipment within trusted zones at the asset owner's site. They create strong barriers against unauthorized access and establish clear boundaries between different network segments.

The control network firewall is located between Level 1 (local or basic control) and Level 2 (supervisory control) to scrutinize traffic between these operational layers. The south firewall, situated between Level 2 (supervisory control) and Level 3 (operations management), controls and monitors the flow of information to safeguard the integrity and security of data communication within the IACS network. The north firewall is located between the enterprise business systems (Level 4) and the operations management (Level 3) to protect internal networks from potential threats originating from the business systems.

The firewalls are customized and configured to suit the specific customer application running on the IACS equipment. A crucial aspect of their setup is the principle of blocking all communication by default and allowing only specifically whitelisted traffic. This approach ensures tight control, permitting only necessary and verified communications defined with as much granularity as possible.

The operational protocols of these firewalls are adaptable. During regular operation, network connections used for commissioning, administration and maintenance shall be blocked to ensure security. However, during commissioning or maintenance periods, the firewalls enable access, which is finely controlled and time bound.

The granular access controls shall be based on the network connection details of various layers of the ISO/OSI model:

- specific services
- specific IP or MAC addresses
- a defined time period or manually for a specific time
- authenticated users/processes/devices

Firewalls also include important features such as rate limiting and load management. Packet rate limiting is used for each service, user and device to protect against potential denial of service attacks caused by traffic surges. B&R advises customers to test and identify the maximum network load that automation solutions can handle without adverse effects to ensure their resilience. Firewalls are therefore configured to limit loads to a safe threshold, usually set at 80% of these tested values.

However, B&R cannot provide specific threshold values as each IACS setup is highly individualized. Thresholds depend on various factors, such as network configurations, operational requirements, connected devices and component performance. Furthermore, security policies and regulatory requirements may differ among various jurisdictions and industries, which can complicate establishing a universal threshold. Each organization should therefore conduct comprehensive testing to determine the appropriate load capacities and rate limits that align with its operational profile and risk management strategy.

Modern firewalls include advanced features like event monitoring, stateful inspection and support for unidirectional communication. These capabilities enable them to regulate traffic and understand the context of network communications, providing a more dynamic and intelligent security approach.

Limit network traffic based on the ISO/OSI layer model for example as follows:

- limit based on source and destination IP addresses
- limit based on target TCP and UDP services
- limit number of sessions
- limit the access per second based on the user to avoid brute force attacks on services

In conclusion, firewalls are essential in IACS environments and require careful configuration, management and updates to counter evolving cyber threats. They play a crucial role in ensuring the safety and continuity of operations in these critical industrial systems.

6.2.2.3 Remote access

When implementing remote access on an asset owner's site, it is essential to prioritize secure and reliable methods to maintain the integrity of the system and safeguard sensitive data. Virtual private networks (VPNs) are a highly recommended solution for this purpose. VPNs create a secure and encrypted connection over the Internet, which effectively shields any data transferred between the remote user and the asset owner's network from external threats.

To maximize the security benefits of VPNs, it is important to keep the VPN solutions updated to the latest version available. Regular updates ensure that any known vulnerabilities are patched, thus reducing the risk of security breaches. Additionally, employing multifactor authentication (MFA) for login significantly enhances security.

It is important to manage remote access sessions carefully. Limit existing connections to a maximum time and set the system to automatically disconnect after this time interval to mitigate risks associated with idle or forgotten sessions. This practice not only strengthens security but also aids in managing network resources more effectively.

Remote access systems should ideally be located in the demilitarized zone (DMZ) in terms of network architecture. The DMZ is situated at Level 3, which is the system management level, in the reference architecture. Placing remote access systems in the DMZ offers several advantages.

- Isolation
  The DMZ serves as a buffer zone between the public Internet and the asset owner's internal network. Remote access systems are located here to avoid direct access to the core network, reducing the risk of direct attacks on sensitive areas of the network.
- Controlled access
  The DMZ enhances regulation and surveillance of network resource access by sequestering a separate network layer for external users. This makes it easier to enforce security policies such as access controls and authentication protocols, thereby strengthening the network's security posture. This structured approach to access management helps mitigate unauthorized entry and potential network breaches.
- Enhanced monitoring
  The DMZ's location in the network makes it an optimal point for monitoring incoming and outgoing traffic. This enables better detection and response to potential security incidents involving remote access.
- Segmentation
  By segmenting remote access from the rest of the network, any potential security breach can be contained within the DMZ. This minimizes the impact on the critical internal network.

In summary, to set up remote access on the asset owner's site, we recommend using updated VPN solutions with multi-factor authentication, time-limited sessions and strategically placed remote access systems in the DMZ. These strategies enhance physically triggered authorization and protect the network against unauthorized access and potential cyber threats.

For more details, see the ABB ICS Cyber Security Reference Architecture documentation.

6.3 System security

System security in the context of industrial automation and control systems (IACS) refers to the measures and strategies implemented to protect the computerized systems and networks that manage industrial processes. This includes safeguarding against unauthorized access, cyber attacks and other vulnerabilities that could disrupt or manipulate the operation of these systems. As part of B&R's defense in depth strategy, system security is a multi-layered approach designed to shield these systems from a multitude of cyber threats.

The security of IACS equipment is a continuous process that starts with its commissioning and continues throughout its operational lifespan until its final decommissioning. Each phase of the equipment's lifecycle presents unique security challenges that require specific protective measures to ensure system integrity and availability. B&R's system security guidelines are designed to be universally applicable, covering a wide range of IACS components and use cases.

During the commissioning phase, strict security measures are put in place to establish a foundation for secure system operations. Once in operation, it is essential to maintain and update these security measures to address emerging threats and seamlessly integrate system updates. Operational measures include monitoring for anomalies, maintaining robust access control and ensuring that all security systems are functioning optimally. When decommissioning systems, it is important to have protocols in place to securely purge sensitive data, prevent unauthorized access and facilitate the secure removal of equipment from service.

B&R advocates for strict adherence to a set of comprehensive security guidelines that should be implemented where technically and operationally viable. These guidelines are crafted to establish a resilient operational environment capable of resisting both internal and external security threats, ultimately safeguarding the operational integrity of the IACS and the safety of the processes they manage.

6.3.1 Commissioning state

During the commissioning state of a product, a collaborative approach between the system integrator and the asset owner is important for ensuring robust Cyber Security. This phase, primarily conducted by the system integrator at the asset owner's site, involves several critical steps that require careful consideration and implementation to safeguard the system against potential cyber threats.

The following security measures should be taken during commissioning:

- Configuring and maintaining a host-based firewall
  During operation mode, it is important to establish a firewall that permits only fine-grained access to necessary services and ports. This requires disabling any unnecessary services and blocking all unused network ports. The firewall's configuration must be comprehensive, taking into account both ingress and egress traffic to ensure complete protection.
- Configuring users, groups and roles
  Align users, groups and roles with the principle of least privilege in Cyber Security. This ensures that each user has only the necessary access for their role, reducing the risk of internal threats and unintended errors.
- Preventing unauthorized access
  Access to the component must be strictly controlled, both physically and logically, to prevent unauthorized tampering or data breaches. Only authorized personnel should be granted access.
- Change default credentials
  Default or commonly used credentials present a significant security risk and should be replaced with unique and strong credentials during the initial setup.
- Removing unnecessary software components
  To enhance the product's security, remove any non-essential software components from the system. This will minimize potential vulnerabilities that could be exploited.
- Implementing strong password policies
  It is essential to create strong passwords and enforce a strict password policy for all users, including both human and non-human, to minimize the risk of unauthorized access through weak or compromised credentials.
- Installing and maintaining an anti-malware solution
  Anti-malware software is essential in protecting against malicious software. Regular updates and maintenance are necessary to defend against the latest threats.

- Log collection and monitoring
  Collecting and monitoring logs and auditable events is essential for identifying and responding to potential security incidents. A centralized system, such as a security information and event management (SIEM) platform, enables more effective monitoring and alert generation.
- Configuring strong cryptographic mechanisms
  Using robust cryptographic methods is crucial for safeguarding sensitive information. This includes encrypting data both in transit and at rest, guaranteeing that even if the data is intercepted, it remains secure and unreadable.
- Updating default settings
  To meet the unique requirements and security measures of the asset owner, it is essential to modify the default configurations of the system.
- Installing the latest updates at the initial startup
  Upon commissioning, it is important to immediately check for and install the latest software updates and patches for all system components. This involves checking for and installing the latest software updates and patches for all system components to address any known vulnerabilities before the product enters operation mode.

6.3.2 Operating state

Once a system is set up and functioning, it must remain alert and adhere to security protocols to continuously guard against cyber threats. This stage involves actively utilizing the product within its designated setting, requiring both the asset owner and the system integrator to diligently maintain and oversee the Cyber Security strategies established during the commissioning phase.

Active Cyber Security measures during operation:

- Continuous monitoring and incident response
  Active monitoring involves regularly checking network traffic, system logs and security device alerts. The asset owner should have an incident response plan ready to address any security events that are detected.
- Regular security assessment
  Regular security assessments should be conducted on the system to identify any new vulnerabilities. Any identified vulnerabilities should be mitigated by promptly updating the system with patches and security fixes.
- User access management
  Regularly review and adjust user roles and permissions to adhere to the principle of least privilege, preventing unauthorized access and minimizing the potential impact of a security breach.
- Physical security enforcement
  To prevent unauthorized physical access to critical Cyber Security assets, it is necessary to enforce physical security controls. This involves ensuring that servers and workstations are located in secure areas and that access to these areas is strictly controlled.
- Credential management
  Continuously managing credentials is necessary, which includes enforcing strong password policies and regularly changing passwords to protect against unauthorized access.
- Malware protection
  Anti-malware solutions require active management and regular updates to ensure protection against new strains of malware.
- Ongoing log analysis
  Continuous collection and analysis of logs is necessary to detect any unusual activity or potential security incidents. Advanced SIEM systems can facilitate this analysis.
- Encryption practices
  To ensure the security of sensitive data both in transit and at rest, it is important to continue using strong encryption. Regular reviews should be conducted to ensure that the encryption remains effective against new threats.
- Adaptive configuration and patch management
  Regularly review and update the system's configuration to meet evolving security needs and align with the asset owner's operational environment. Refine patch management processes to ensure timely and secure application of updates.

6.3.3 Maintenance state

The maintenance state is important and requires careful management to maintain system integrity and security. This phase is typically managed by authorized technicians and involves critical tasks to ensure continued robustness and that the system is functioning optimally.

The following security measures should be taken during maintenance:

- Fine-grained access for maintenance
  Maintenance activities require access to specific services and ports on the IACS equipment. To ensure secure management, access should be granted in a finely-grained manner and aligned with the scheduled maintenance time frame. This approach ensures that technicians have access only to the necessary resources and only for the duration of the maintenance period. Implementing controlled access minimizes the risk of unauthorized use or exploitation of system vulnerabilities during maintenance.
- Time-bound permissions
  Permissions for critical operations must be time-bound. Access rights should only be granted during scheduled maintenance and promptly revoked once maintenance is completed. This strategy helps prevent any lingering access that could be misused after maintenance.
- Secure backup creation and storage
  Creating backups of critical system data during maintenance is essential for disaster recovery and business continuity. These backups should be stored securely, ensuring that only authorized personnel can access them. To enhance security, we recommend storing these backups on encrypted devices. This not only protects the data from unauthorized access but also ensures data integrity in case of physical theft or loss of the storage device.
- Deleting obsolete users and groups
  Regular maintenance cycles should include reviewing and cleaning up system access controls. This involves deleting any users, groups and roles that are no longer needed or have become obsolete. Keeping user and group permissions up to date reduces the risk of unauthorized access and potential security breaches.
- Updating anti-malware solutions
  Maintenance also involves updating the anti-malware solution to protect against new and evolving cyber threats. Regular updates are essential to ensure that the system can detect and defend against the latest viruses and malware.

6.3.3.1 Patch and vulnerability management

B&R guides managing software updates and addressing vulnerabilities in industrial automation and control systems (IACS). Effective patch and vulnerability management is for maintaining system security and functionality, as it addresses potential weaknesses that could be exploited by cyber threats.

In the field of industrial automation and control systems (IACS), the maintenance phase is crucial and requires careful management to maintain system integrity and security. This phase is typically managed by authorized technicians and involves critical tasks to ensure continued robustness and that the system is functioning optimally.

The following security measures should be taken during maintenance:

- Regular software updates
  B&R stresses the significance of regularly updating all software components. These updates frequently contain security patches for vulnerabilities that have been identified since the previous version of the software was released. Regular updates not only fix these vulnerabilities but also enhance the system's functionality and efficiency.
- Integrity verification of software deliverables
  Before installing new software or updates, it is crucial to verify the integrity of the deliverable. This involves checking that the software has not been tampered with or corrupted during transit. Techniques such as checking digital signatures or hash values provided by the software vendor can be used to confirm that the software is genuine and unaltered.
- Scheduled maintenance for patch application
  Patches should only be applied during scheduled maintenance to allow for thorough testing in a controlled environment and to minimize operational downtime.
- Installation by authorized personnel
  Only authorized personnel should install patches to ensure that those handling updates are trained and knowledgeable about the system and patching process. This also helps maintain clear records of system changes, which is crucial for tracking and auditing purposes.

- Managing patch priorities
  To ensure effective patch management, it is important to prioritize the patches based on the severity of the vulnerabilities and the criticality of the affected system components. Patches that address high-risk vulnerabilities in critical systems should be given priority to minimize the potential impact on the organization.
- Testing and backup
  Before applying patches, it is advisable to test them in a non-production environment to assess their impact and effectiveness. It is also important to back up the system before applying patches to ensure that it can be restored to its previous state if the patch causes any issues.
- Monitoring and reviewing patch effectiveness
  After applying patches, it is important to continuously monitor their performance to ensure they are functioning as intended and not causing any unexpected issues. Regular reviews of the patching process and its effectiveness in mitigating vulnerabilities are also essential to improve future patch management practices.

6.3.4 Decommissioning state

The decommissioning of industrial automation and control systems (IACS) is a critical phase that requires careful planning and execution to ensure security and compliance. Although it marks the end of the equipment's lifecycle, obligations regarding data security, intellectual property and environmental considerations persist. To mitigate any potential risks that could arise from improper handling or disposal of the system components, a comprehensive approach is required that encompasses both the digital and physical aspects of the equipment.

Effective decommissioning requires a series of steps to ensure the security of the organization's data and network. It involves managing each component, from software licenses to user credentials, in a systematic and secure manner to prevent unauthorized access or data breaches after decommissioning.

The following security measures should be taken during decommissioning:

- Monitoring network security components
  During the decommissioning phase, network security components like SIEM (Security Information and Event Management) or IDS (Intrusion Detection System) should continue to monitor the components, services and network communications, denoting they are no longer expected to be there. This will help detect any unexpected activities or potential security threats during this critical transition phase.
- Scheduled and authorized decommissioning
  To ensure a smooth and error-free process, it is important to schedule and authorize the decommissioning or deactivation of IACS equipment services. This planned approach will make all stakeholders aware of the timeline and steps involved, minimizing the risk of errors or oversights.
- Deletion of software licenses
  As part of the decommissioning process, it is important to delete all software licenses associated with the equipment. This prevents unauthorized use of the software after decommissioning and ensures compliance with licensing agreements.
- Deleting users, groups and roles
  Thoroughly delete all user accounts, groups and roles, along with their authenticators. This important step prevents unauthorized access to the system and ensures that no residual access rights remain after decommissioning.
- Deleting certificates
  To prevent misuse or exploitation after decommissioning, any certificates, including SSL/TLS certificates and sensitive crypto-material used by the IACS equipment should be revoked and deleted.
- Deleting intellectual property
  It is important to securely delete any intellectual property stored on the IACS equipment, including proprietary algorithms, configurations and system-specific data, to prevent its recovery after decommissioning. Use proper deletion methods to ensure sensitive information is irretrievable.
- Safe disposal of IACS equipment
  The safe and environmentally responsible disposal of IACS equipment involves securely wiping or physically destroying all data storage components to prevent data recovery. It is also important to recycle parts in an environmentally responsible manner while following all relevant security regulations.

7 Security Monitoring

Security monitoring is an essential component in the Cyber Security arsenal for safeguarding industrial automation and control systems (IACS). In today's era of increasingly sophisticated and pervasive threats, monitoring systems and networks for any signs of compromise is not just a recommendation, but an imperative. Security monitoring is a crucial component of a comprehensive defense in depth strategy. It acts as a sentinel and early warning system, detecting unusual patterns or behaviors that may indicate a security breach.

The asset owner's site must have advanced detection and alerting mechanisms in place to swiftly respond to any potential malicious behavior. This requires deploying sophisticated solutions designed to recognize attack signatures and irregularities in system behavior.

A risk-based approach customizes the monitoring system to the organization's specific threat landscape. It is essential to use technologies such as intrusion detection systems (IDS) and intrusion prevention systems (IPS). These systems not only detect but can also take action to prevent malicious activity from affecting the network. It is paramount to keep these systems up to date to ensure they can combat the latest threats. Customizing the rules for different levels of the network architecture and making them as strict as necessary can enhance the security posture.

Developing and enforcing clear and concise logging policies for security-related events is an important aspect of effective security monitoring. Logs are essential for forensic investigations and should be protected through regular backups and secure storage practices. It is also important to remain vigilant about seemingly benign events, such as unexpected spikes in resource utilization or service and device failures, as they could be indicators of a security incident and require immediate investigation.

Security monitoring requires ongoing evaluation and adaptation as threat actors evolve their tactics. Asset owners must continuously refine detection algorithms, update monitoring tools and stay abreast of the latest Cyber Security developments.

7.1 Security-related tools and utilities

B&R recognizes the complexities and unique challenges in this area and offers comprehensive recommendations for utilizing security-related tools and utilities.

These tools play an important role in preserving the integrity and resilience of IACS environments:

- Utilization of network scanners
  B&R emphasizes the significance of network scanners in optimizing asset and inventory management systems for B&R products. These scanners not only evaluate configurations, services and applications but also identify assets. Network scanners aid asset owners in maintaining an up-to-date inventory by detecting configuration discrepancies, such as unintentionally activated network services. This statement ensures that all network services and applications are configured securely and in compliance with strict security standards, thereby improving overall asset management efficiency.
- Regular network scanning for unauthorized changes
  To prevent unauthorized modifications, B&R suggests conducting frequent network scans. This proactive measure is essential for detecting any unauthorized changes to components, which may indicate security breaches or non-compliance. Continuous monitoring helps maintain a secure and stable network environment by enabling quick identification and remediation of any discrepancies or vulnerabilities.
- Implementation of IDS/IPS systems on critical levels
  To enhance security, B&R recommends implementing intrusion detection systems (IDS) and intrusion prevention systems (IPS) on levels 1 and 2 of the IACS. These levels have predictable and known network traffic patterns, making them ideal for IDS/IPS deployment. IDS/IPS systems effectively monitor network traffic for unusual activity and can alert administrators or actively prevent malicious actions, adding a robust layer of security to the system.
- Configuring and Maintaining a SIEM System
  Configuring and maintaining a security information and event management (SIEM) system is recommended, also for components on level 1 and level 2 of the IACS. SIEM systems analyze log entries and events from various sources within the network, providing a comprehensive view of the network's security posture. The SIEM should be configured meticulously with an advanced alerting system to detect and promptly notify relevant personnel of any anomalies or security incidents. This enables a quick response to potential threats, ensuring prompt containment and resolution of security issues.

8 Security testing

The ABB Device Security Assurance Center (DSAC) assists in ensuring the security of selected B&R products. Trained and certified personnel conduct thorough security assessments at the DSAC labs, adhering to modern industry standards and practices. This testing regime is part of B&R's commitment to maintaining high product security.

The DSAC labs can perform various specialized security tests to evaluate different aspects of a product's resilience against potential cyber threats.

The following security tests are covered by the DSAC labs and are applied where technically feasible:

- Robustness and denial-of-service (DoS) tests
  These tests evaluate the product's capacity to endure and maintain functionality in unfavorable circumstances, including DoS attacks that attempt to disrupt service availability.
- Network-protocol fuzzing and flooding tests
  Fuzzing tests entail sending malformed or unexpected data to the product to uncover vulnerabilities. Flooding tests assess how the product handles excessive amounts of data or requests.
- Measurements of supported network and load tests
  This involves testing the network performance of the product and its ability to handle both expected and peak load conditions without compromising functionality or security.
- Service and network port enumeration
  This process identifies all open ports and running services on the product, providing a complete overview of potential entry points that require securing.
- Vulnerability scanning for known vulnerabilities and exploits
  The laboratories perform comprehensive scans to detect any known vulnerabilities or exploits in the product, guaranteeing that all potential security weaknesses are resolved.

The security test results are carefully documented and reported to B&R. Upon receiving the results, B&R reviews and responds to each identified security issue. This triggers the issue-handling process, which develops appropriate mitigations or patches and implements them promptly.

For more information, please read the ABB DSAC Whitepaper.

9 Security incidents and issues

An effective security strategy requires proactive preparation and response planning, which involves steps beyond technical measures. These steps include policy formulation, planning, responsibility allocation and data analysis.

The key elements of security incident preparedness

- Establishing policies
  Developing clear and concise security policies is essential for incident preparedness. These policies must define the organization's approach to managing and mitigating security incidents, including prevention strategies, response protocols and recovery plans.
- Planning activities
  Detailed planning is crucial to ensure that the organization can effectively handle security incidents. This involves creating incident response and recovery plans that outline the necessary steps to take in the event of a security breach, to restore normal operations as quickly and safely as possible.
- Determining responsibilities
  Defining roles and responsibilities for handling security incidents within the organization is crucial. This involves assigning a response team, outlining each member's responsibilities and ensuring that all employees understand their roles in maintaining security.
- Identifying key indicators and making them available for analysis
  Continuous monitoring and analysis of system performance and security indicators can aid in early detection of potential security incidents. This data analysis is crucial for identifying trends, anomalies and potential vulnerabilities in the system.

If any security vulnerabilities are discovered, it is imperative to report them immediately to the product supplier. Asset owners using B&R products should visit the dedicated Cyber Security website at https://www.br-automation.com/en/service/cyber-security/ and follow the outlined reporting steps. Prompt reporting enables the supplier to quickly address vulnerabilities, mitigating potential risks to the system and its users.

For a complete understanding of security incident handling, asset owners should refer to the Computer Security Incident Handling Guideprovided by NIST (National Institute of Standards and Technology). This guide provides information and best practices for organizing and managing responses to computer security incidents. It includes guidelines for establishing an incident response team, analyzing and responding to incidents and maintaining communication throughout the process. It can be a valuable tool for organizations seeking to enhance their security incident preparedness and response capabilities.

9.1 Common attacks in OT environments

This section shall provide an overview for understanding the Cyber Security landscape in industrial automation and control systems (IACS). OT environments are increasingly targeted by sophisticated cyber threats that can compromise system integrity, disrupt operations and have significant safety and financial implications. This section presents an overview of common cyber attacks that asset owners and operators may face.

DoS attacks can overwhelm systems with traffic, making them unresponsive.

Man-in-the-middle (MiTM) attacks intercept and may alter communications between two parties. Spoofing involves impersonating a legitimate user on the network to deceive and gain access to sensitive systems.

Cross-site scripting (XSS) typically affects web applications, injecting malicious scripts to manipulate end-user interactions.

Brute-force attacks systematically attempt to crack passwords in order to gain unauthorized access. Malware encompasses various types of malicious software designed to damage or exploit systems.

Remote code execution (RCE) allows an attacker to run arbitrary code on a victim machine, potentially taking over the system.

Elevation of privileges (EoP) occurs when attackers gain higher access levels than initially granted, resulting in unauthorized control over system resources. Project file infection targets the blueprints of IACS operations by embedding malware within project files that can be activated upon deployment or integration.

Understanding common attacks is the first step in fortifying OT environments against breaches. Asset owners shall recognize these threats and implement strong security measures to mitigate them.

9.1.1 Denial-of-service (DoS)

A denial-of-service (DoS) attack is a significant threat in operational technology (OT) environments. It aims to disrupt or prevent legitimate users, including humans, processes or devices, from accessing essential services or resources. These attacks can impair the infrastructure of industrial automation and control systems (IACS), leading to significant operational downtime and potential safety hazards.

DoS attacks overwhelm the target system with excessive traffic, causing it to slow down or crash. This can render services unavailable to legitimate users and interrupt critical industrial processes. Distributed denial-of-service (DDoS) attacks are a type of cyber attack that uses multiple compromised systems to launch a coordinated attack, making them more challenging to mitigate.

DoS attacks often exploit a range of system weaknesses, including but not limited to:

- Weak input validation
  Systems that do not properly validate input can be overloaded with unexpected or malicious data, resulting in excessive resource consumption and system crashes.
- Weak authentication
  If authentication mechanisms are not strong enough, attackers can flood a system with false authentication requests, causing service degradation or shutdown.
- Weak throttling and rate limiting
  An attacker can overwhelm the system with a high volume of traffic, exceeding its capacity to handle concurrent sessions, if there are no controls in place to limit the rate of user requests.

Effective strategies to counter DoS attacks include:

- Robust input validation
  Strong validation checks should be implemented for all input data to ensure that only legitimate requests are processed.
- Strong authentication controls
  Strong validation checks should be implemented for all input data to ensure that only legitimate requests are processed.
- Effective throttling mechanisms
  Implement rate-limiting controls to manage the traffic load from any single source on a service.
- Comprehensive error handling
  Design systems with strong error-handling capabilities that can manage unexpected conditions without compromising service availability.
- Redundancy and resilience
  Systems and networks should be designed with redundancy to ensure uninterrupted service in case of component compromise.
- Regular testing and updating
  Conduct stress testing to identify potential points of failure and update the system architecture to address any identified weaknesses.

9.1.2 Project file infection

Project file infection is a specific Cyber Security threat to operational technology (OT) environments. Attackers insert malicious code into an OT project file, which is then unknowingly downloaded to programmable logic controllers (PLCs) or other control system components. This can lead to unauthorized control of industrial processes, data corruption or system disruption.

The following flaws are exploited in project file infection attacks:

- Insufficient auditing
  Without thorough auditing procedures, it can be challenging to track changes to project files, which can lead to malicious modifications going unnoticed until they cause harm.
- Code signing algorithm
  Using weak or compromised code signing algorithms can allow attackers to create fake signatures, which can make malicious code seem legitimate and authorized.
- Weak authentication and access control
  Insufficient authentication measures and lax access controls may allow unauthorized individuals to modify project files or deploy infected programs to critical systems.

The following strategies exist to mitigate project file infection:

- Enhanced auditing practices
  Comprehensively audit project files to log all changes, including the identity of the person who made the change, what was changed and when the change occurred.
- Robust code signing protocols
  Use strong, industry-standard algorithms for code signing to ensure that all changes to project files are properly authenticated and verified before being accepted.
- Strict authentication and access Control
  To ensure that only authorized individuals can modify and deploy project files, it is important to strengthen authentication mechanisms and enforce strict access controls.
- Regular code reviews
  Perform regular code reviews and utilize automated tools to scan for any abnormal code segments or patterns that may indicate the presence of malicious code.
- Employee training and awareness
  All personnel involved in the development and deployment of OT project files should be educated on the risks of project file infection and best practices for security.
- Use of trusted sources
  Make sure to obtain all software and updates from trusted sources and verify them against known good versions.

9.1.3 Brute-force

Brute-force attacks pose a significant threat to Cyber Security, especially in the context of industrial automation and control systems (IACS). This type of attack involves systematically submitting all possible combinations of secrets, such as passwords, to eventually guess the correct one. Brute-force attacks exploit the vulnerability of systems that are not adequately prepared to resist such relentless and methodical guessing attempts.

The key flaws exploited in brute-force attacks are:

- Missing throttling and limiting
  Systems can be vulnerable to overwhelming brute-force attacks due to the high volume of guesses they can generate. To prevent this, mechanisms should be implemented to limit the number and rate of login attempts.
- Weak encryption of secrets
  Weak encryption of sensitive information, such as passwords, can expedite brute-force attacks by making the process faster and more feasible for attackers. Strong encryption methods can significantly impede or deter brute-force attacks.
- Lack of robust credential policies
  The lack of strong credential policies, such as minimum password length, complexity and regular changes, can make it easier for attackers to successfully execute brute force attacks. Simple and short passwords are particularly susceptible to being quickly cracked by these methods.

The following mitigation strategies can be used:

- Implement rate limiting and account lockout
  To hinder brute-force attacks, set up controls that limit the number of login attempts within a certain time frame and lock accounts after repeated failed attempts.
- Use strong encryption techniques
  Use robust encryption methods to store and transmit credentials. This makes it much more difficult for attackers to decrypt the encrypted information.
- Enforce strong password policies
  Implement policies that require passwords to be of a certain length, include a mix of characters and be changed regularly. This increases the complexity and time required for a successful brute-force attack.
- Two-factor authentication
  Use two-factor or multi-factor authentication, which adds an extra layer of security beyond the password.
- Monitor for suspicious activity
  Continuously monitor systems for any unusual login patterns or spikes in authentication requests. These could indicate a brute-force attack in progress.
- Educate users
  Inform users about the importance of using strong passwords and the risks associated with weak credentials. Educating users can increase compliance with strong password policies.

9.1.4 Cross-site scripting (XSS)

Cross-site scripting (XSS) is a common security vulnerability in web-based applications. It occurs when an attacker injects malicious scripts into trusted websites, which are then executed on the client-side, usually in the web browser of unsuspecting users. This type of attack can result in various malicious activities, such as stealing cookies, session tokens or other sensitive information from users' browsers.

The key flaws exploited in XSS attacks are:

- Weak input validation
  Inadequate input validation is one of the primary flaws that enable XSS attacks. Applications that fail to properly validate user input can unintentionally permit the injection of malicious scripts into web pages.
- Insecure output handling
  When an application includes user-supplied data in its output, it must be properly sanitized or escaped to prevent the execution of malicious scripts. This is particularly dangerous when input data is reflected back to the user, such as in error messages or search results.

The following mitigation strategies against XSS Attacks can be used:

- Robust input validation
  Implement strict input validation checks to ensure that only safe and expected data is accepted. This includes rejecting or sanitizing inputs that contain script or HTML tags.
- Output encoding and escaping
  When outputting data in HTML, it is important to escape user inputs to prevent any potentially harmful characters from causing issues being treated as executable code.
- Content security policy (CSP)
  To prevent attackers from injecting malicious scripts from external sources, utilize CSP headers to restrict the sources from which scripts can be executed.

- Use of anti-XSS libraries
  Use libraries and frameworks that automatically handle user input escaping and sanitization.
- Regular code reviews and testing
  Perform code reviews and security testing, including penetration testing, to identify and fix XSS vulnerabilities in applications.
- Security education and awareness
  Educate developers on the risks of XSS and best practices for preventing it. Awareness and training can significantly reduce the likelihood of introducing XSS vulnerabilities in code.

9.1.5 Elevation of privileges (EoP)

Elevation of privileges (EoP) is a security threat in which an attacker gains access to higher-level permissions than originally assigned. This breach allows unauthorized access to resources and methods typically protected from standard users, processes or devices, potentially leading to significant security and operational risks. EoP attacks can compromise the entire system, allowing attackers to modify system functions, access sensitive data and disrupt normal operations.

The key flaws exploited in EoP attacks are:

- Execution of data outside authorized scope
  This flaw happens when a user or process can access data that is intended for others or from a different security scope, which breaches the intended access control limits.
- Improper software integrity mechanisms
  Weaknesses in software integrity checks can allow unauthorized code or modifications to be executed without detection, which can lead to privilege escalation.
- Inadequate authentication mechanisms
  Weak authentication controls can be exploited to gain elevated access. Attackers can impersonate legitimate users or processes with higher privileges due to weaknesses in the authentication process.
- Hardcoded credentials
  Including fixed credentials within software, such as passwords or cryptographic keys, poses a significant security risk. If attackers discover these hardcoded credentials, they can use them to escalate their privileges within the system.

The mitigation strategies against EoP attacks consist of:

- Principle of least privilege
  Implement and enforce the principle of least privilege, ensuring that users and processes have only the minimum level of access required to perform their functions.
- Regular software integrity checks
  Use strong mechanisms to verify software integrity and prevent unauthorized modifications.
- Strong authentication controls
  Implement multi-factor authentication and regularly update and strengthen authentication protocols to prevent unauthorized access.
- Avoid hardcoded credentials
  Use secure methods for storing and accessing credentials, such as encrypted key management systems, instead of hard coding them into the software.
- Security audits and code Reviews
  Regularly conduct security audits and code reviews to identify and fix potential vulnerabilities that could result in privilege escalation.
- User education and training
  Educate users about the risks associated with privilege escalation and the importance of adhering to security protocols.

9.1.6 Malware

Malware, which is short for malicious software, refers to software programs that are designed to disrupt, damage or gain unauthorized access to computer systems. Common types of malware include viruses, worms, ransomware, adware and keyloggers. These malicious programs can compromise system integrity, steal sensitive information and disrupt normal operations, posing significant risks to industrial automation and control systems (IACS).

The key flaws exploited by malware are:

- Improper software integrity mechanisms
  Inadequate software integrity verification can allow malware to infiltrate a system without detection, increasing the risk of unauthorized or malicious code execution.
- Unbound read/write in memory
  Malware can exploit vulnerabilities that allow unrestricted reading or writing to system memory, leading to system compromise by executing arbitrary code.
- Insertion of untrusted data into execution code
  Malicious code can be injected into a system either statically (during compilation) or dynamically (during runtime). If untrusted data is executed without proper validation, it can result in severe security breaches.

The following mitigation strategies against malware can be considered:

- Robust software integrity checks
  Implement robust validation mechanisms for software and system updates, such as digital signatures, checksums and regular scanning.
- Secure coding practices
  To prevent the insertion of untrusted data into executable code, it is important to use secure coding practices. This includes input validation, output encoding and the use of prepared statements in database queries.
- Regular updates and patching
  To protect against known vulnerabilities that malware might exploit, it is important to keep all systems and software up to date with the latest patches.
- Antivirus and anti-malware solutions
  Deploy reliable antivirus and anti-malware software to detect and neutralize malware threats. Ensure that these solutions are regularly updated to counter the latest malware variants.
- User education and awareness
  Educate users about the risks of malware and safe practices, such as not opening suspicious emails or downloading files from untrusted sources.
- Network segmentation and monitoring
  Segmenting networks can limit the spread of malware. Continuously monitoring network traffic for signs of malicious activity is also important.

9.1.7 Man-in-the-middle (MiTM)

A man-in-the-middle (MiTM) attack is a security breach in which an attacker secretly intercepts and may modify communication between two legitimate parties. This intrusion compromises the confidentiality and integrity of the communication and can also lead to further exploitation of the targeted network or system.

The following flaws are exploited in MiTM attacks:

- Weak authentication
  Inadequate authentication processes can allow attackers to impersonate legitimate users, facilitating their insertion into a communication stream.
- Weak communication encryption
  Using poor encryption practices or outdated encryption protocols can create vulnerabilities that allow attackers to decrypt and access communication data.
- Insufficient handling of digital signatures and secrets
  Improper implementation and validation of digital signatures, as well as insecure management of secrets such as keys and certificates, can allow attackers to forge identities or decrypt sensitive data.

MiTM attacks can be mitigated using:

- Strong authentication protocols
  Implement strong authentication mechanisms, such as two-factor authentication (2FA) or multi-factor authentication (MFA), to make it more difficult for attackers to impersonate legitimate users.
- Robust encryption
  Strong encryption standards should be used for all data in transit. It is important to properly configure and keep protocols like TLS (Transport Layer Security) up to date to prevent attackers from easily intercepting or deciphering communications.
- Secure management of keys and certificates
  Make sure to securely manage all digital keys and certificates by periodically rotating and revoking them as needed. Additionally, use certificate pinning where appropriate to prevent attackers from presenting fraudulent certificates.

- Network security measures
  Use network security tools such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and prevent potential man-in-the-middle (MiTM) attacks.
- Employee training
  Educate users about the risks of MiTM attacks and how to identify potential signs, such as unexpected certificate warnings or changes in communication patterns.

9.1.8 Spoofing

Spoofing is a cyber attack in which an attacker pretends to be a legitimate user, process or device by falsifying data. This can lead to unauthorized access, data interception and other malicious activities that rely on the attacker's ability to deceive. It is important to be aware of this type of attack and take measures to prevent it.

The following flaws are exploited in spoofing attacks:

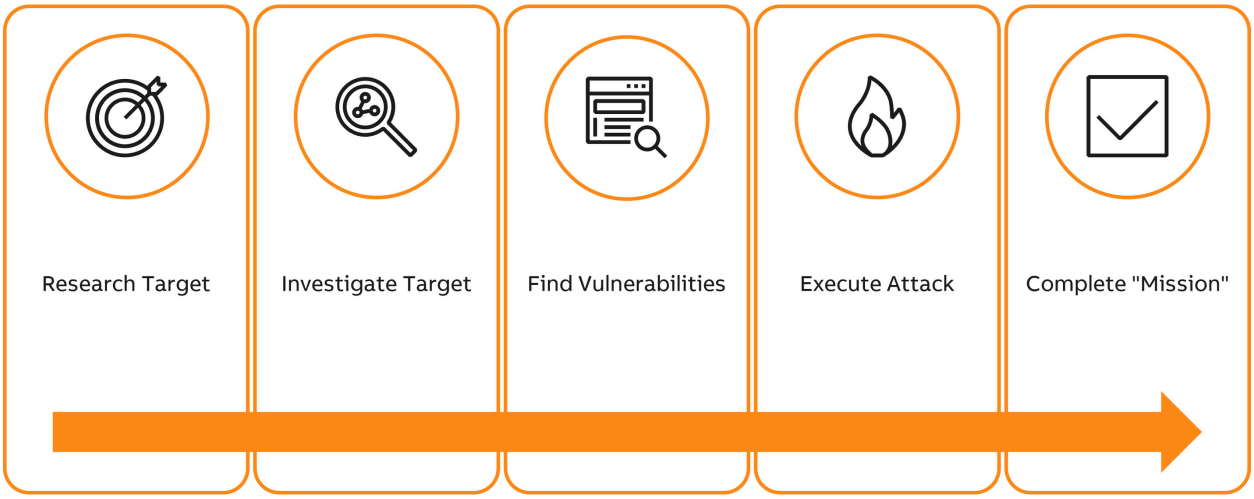
- Weak authentication
  Spoofing occurs when attackers impersonate legitimate users by guessing passwords, exploiting stolen credentials or circumventing authentication mechanisms. This is often possible due to inadequate authentication protocols. To prevent spoofing, it is important to implement strong authentication mechanisms and regularly update passwords.
- Weak communication encryption
  Inadequate encryption can make it easier for attackers to intercept and falsify data during transmission, which can facilitate spoofing attacks.
- Insufficient handling of digital signatures
  Improper management and validation of digital signatures can result in situations where attackers are able to forge signatures and impersonate legitimate users or devices. This is especially true if the system does not adequately verify the authenticity of signatures.

The mitigation strategies against spoofing attacks are:

- Strong authentication measures
  Use strong authentication methods like 2FA or MFA to add extra security layers, making it harder for attackers to impersonate real users.
- End-to-end encryption
  Use strong end-to-end encryption to protect data in transit from interception and falsification. Ensure that protocols such as TLS and SSL are properly configured and kept up-to-date.
- Secure digital signature processes
  Ensure secure handling of digital signatures with proper authentication checks, including the use of certificate authorities and public key infrastructure (PKI).
- Regular security audits
  Conduct routine security audits to evaluate the strength of authentication and encryption mechanisms in place and to identify any potential vulnerabilities that could be exploited for spoofing.
- Network security tools
  Deploy network security tools such as firewalls and intrusion detection systems (IDS) to detect and prevent spoofing activities.
- User and staff training
  Educate users and staff on the risks associated with spoofing attacks and train them to recognize signs of suspicious activity.

9.2 Cyber attack lifecycle in ICS environments

Industrial automation and control systems (IACS) are not immune to cyber threats. Understanding the anatomy of a cyber attack is crucial for developing effective defense strategies. This chapter outlines the typical lifecycle of an attack against IACS, providing insights into the stages an attacker goes through from initial reconnaissance to the completion of their mission.



9.2.1 Research target

The first step in an attack is conducting thorough research on the intended target. Attackers gather information using various means, including:

- Search engines to find relevant data about the organization.
- Social engineering techniques to manipulate insiders into revealing confidential information.
- Publicly available records such as WHOIS and domain registries to gather intelligence on the network infrastructure.

9.2.2 Investigate target

Once preliminary data is gathered, attackers investigate the target more thoroughly. This can include:

- Analyzing company websites for clues about internal systems.
- Physically inspecting facilities if possible.
- Acquiring detailed DNS information to map the network landscape.

9.2.3 Find vulnerabilities

With enough information, attackers look for weaknesses. Key steps include:

- Port scanning to discover open ports and associated services.
- Banner grabbing to determine software versions and potential vulnerabilities.
- Employing vulnerability scanners to automatically detect known security issues.

9.2.4 Execute attack

After identifying vulnerabilities, attackers proceed with the actual assault. Execution might involve:

- Exploiting databases using frameworks like Metasploit.
- Developing or deploying custom exploits for unpatched vulnerabilities.
- Optionally conducting Denial of Service (DoS) attacks to disrupt operations.

9.2.5 Complete "mission"

The final phase often involves actions taken post-exploitation, such as:

- Pivoting to access further systems within the network.
- Covering tracks by clearing logs or using sophisticated methods to avoid detection.
- Installing backdoors for persistent access or deploying rootkits to maintain control.
- Exfiltrating valuable data from the compromised system.

10 Support

For additional information and support, please refer to the Cyber Security contact information on the B&R website https://www.br-automation.com/en/service/cyber-security/.