CYBER SECURITY

Defense in Depth for B&R products

Document information

Version	1.00
Date	2023-11-06
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

Industrial Automation and Control Systems (IACS) are exposed to security threats. To address them, it is not sufficient to implement a single measure. It is necessary to implement a series of measures that must be continuously evaluated and adapted.

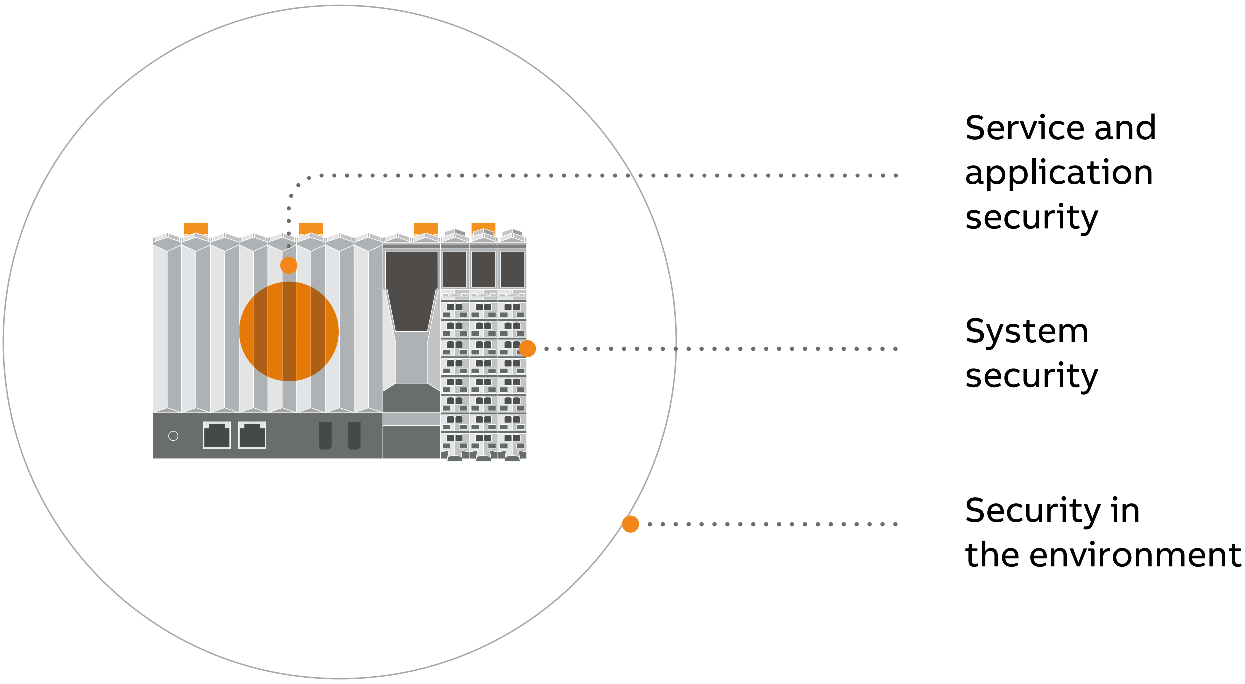
As an example, the approach recommended by IEC 62443-4-1 is to implement a Defense in Depth concept.
The concept is designed to ensure security from different perspectives and at different levels. An attacker must overcome various protective barriers in order to reach the target.
This document provides an overview of security practices that B&R recommends for the secure operation of its products.
It is the customer's responsibility to implement these measures based on their needs after evaluating applicable threat scenarios.

2 Terms and definitions

Terms and definitions are used according to IEC 62443.

3 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 the environment, the B&R product and also its services and applications.
Refer to section Security Monitoring.

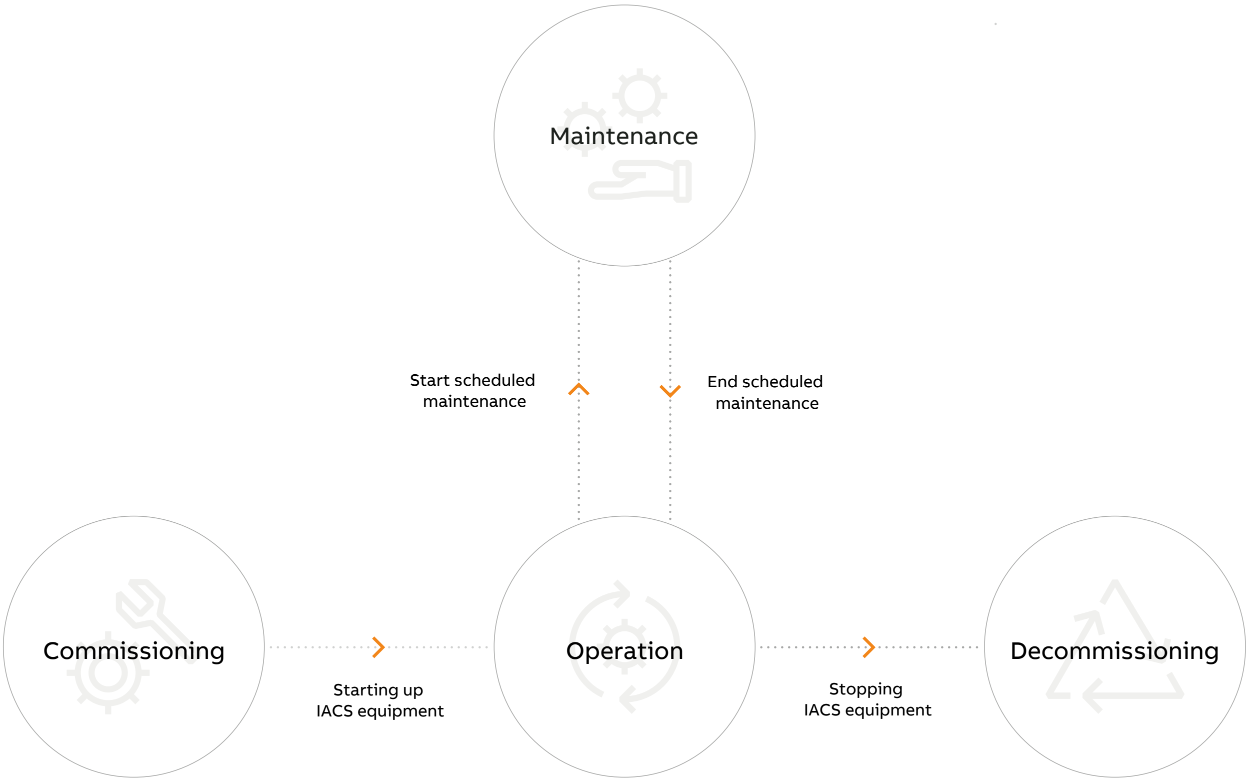
Finally, section Security testing describes B&R's Cyber Security testing processes and section Security incidents and issues describes B&R's recommendations for Incident Management.

3.1 Product operation states

B&R's Defense in Depth measures shall be applicable throughout all product operation states.

The product operation states describe the states of the B&R product during use, e.g. at the asset owner's site.

The following figure shows the four product operation states that are considered.


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

Further details about the Defense in Depth strategy are explained in this document, including aspects relevant to Cyber Security throughout the product's operation states.

3.2 General recommendations

3.2.1 Risk management

Every company has its own infrastructure, processes and environment.
Therefore, it is important for the Asset Owners to identify possible threats individually. It is then possible to implement plans to optimally address those threats. Risk is determined by considering the likelihood that threats will exploit vulnerabilities and the impact such exploits would have on valuable assets.

It is important to repeat this evaluation regularly in order to be able to react to changes in the company or new threat scenarios. Security risk management is an ongoing process.

3.2.2 Human/User management

- Assign the company's activities to different roles.
- Ensure through policies that each role has the necessary rights to perform its activities.
- At the same time, restrict the rights of each role as much as possible.
- Keep employee access to systems that are critical to you or your customers to a minimum. Ensure through the use of policies and processes that critical activities cannot be executed by one single person.
- Verify the integrity of your employees according to the rights granted to them.
- Ensure that all access rights are revoked after an employee leaves.
- Ensure that employees have the training required for their activities. Regular ongoing training ensures that employees are able to identify and eliminate new threat scenarios.

3.2.3 Authentication

Identities and corresponding authenticators are required to prove the identity of a user. An authenticator is the general term for e.g. a password, token, symmetric key, private key, biometrics or physical key.

The System Integrator shall:

- initialize strong authenticator content
- change all default authenticators
- protect all authenticators from unauthorized disclosure and modification when stored and transmitted
- support robust and automated certificate life cycle management
- determine if integration into an account management system is required
- determine if a secure communication channel is required to prevent exposure

Furthermore, the System Integrator shall ensure sensitive authentication data is being entered, stored and transmitted in a way that prevents third parties from obtaining this information. For example, to securely transmit usernames and passwords, a TLS-based communication channel should be used.

The Asset Owner shall change any default credentials for IACS equipment. The System Integrator shall ensure credentials for each Asset Owner are different or can be changed by them.

We strongly recommend that the authentication mechanisms be continuously evaluated and improved. Implement policies to ensure this is done at regular intervals.

- Check the certificates you use for an expiration date
- Change passwords for all users (implement policies to ensure that old passwords cannot reused as the new one)
- Check time restrictions and adjust if possible.

4 Security in the environment

4.1 Physical access Factory security

Only authorized users shall have physical access to critical components. Access must be restricted according to the principle of least privilege. Access may be restricted both spatially and temporally.

Access restriction should be applied during all phases of the product's operation states. During commissioning of the component, usually by the System Integrator, during maintenance on the Asset Owner's and System Integrator's site and during operation and decommissioning on the Asset Owner's site.

Form access restrictions based on the onion principle. For example, an employee can enter the plant hall and operate a machine, but the control unit of the machine is not accessible to that person.

Asset Owner and System Integration have to implement protection processes and methods to avoid unauthorized:

- hardware modifications on devices
- interaction with physical interfaces such as ethernet, USB or fieldbuses on B&R hardware components
- interaction with connected cables
- interaction with physical buttons or switches on B&R hardware components
- power disruptions or failures

Use strong access checks for secure areas, security guards and locked cabinets to ensure security.

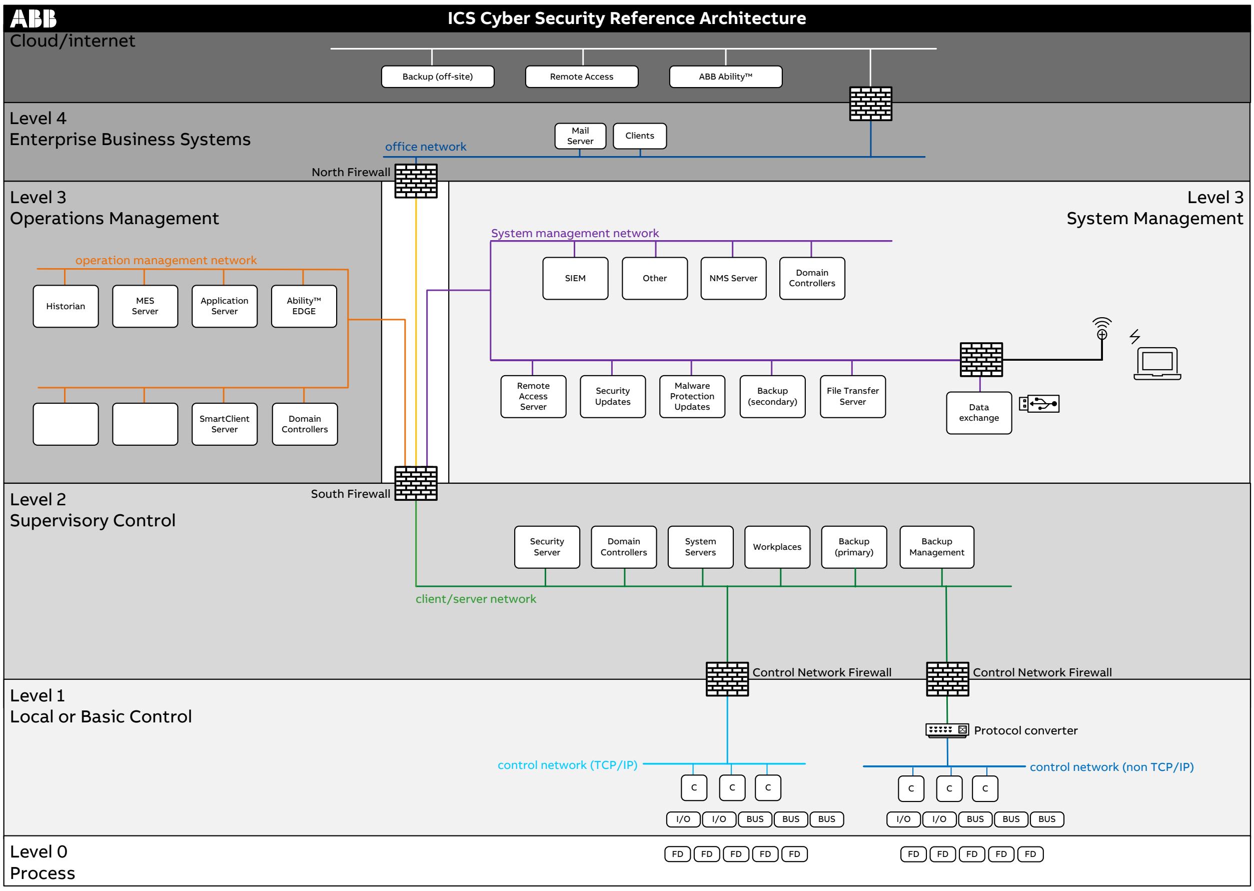
4.2 Network security

In general, the network needs to be split into different segments on the Asset Owner's site. For example, place PLCs in a dedicated control network containing control systems only.
Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet. Limit outbound Internet traffic originating from control systems/networks as much as possible.

4.2.1 Reference architecture

To ensure security, B&R recommends implementing a network architecture in alignment with the IEC 62443-1-1 reference architecture. This reference architecture reflects the network configuration recommended for Cyber Security at the Asset Owner's site.

For details about the reference architecture, please refer to the ABB ICS Cyber Security Reference Architecture documentation.



As defined in the ABB ICS Cyber Security Reference Architecture documentation, Level 0 and 1 are trusted zones with restricted (physical and network) access at the Asset Owner's site.

Additionally, B&R classifies Level 2 as trusted.

4.2.1.1 Levels

The definition of the levels used in the reference architecture aligns with the IEC 62443-1-1 reference model describing a generic view of an integrated manufacturing or production system expressed as a series of logical levels.

B&R classifies Level 0, Level 1, and Level 2 as trusted, with restricted (physical and network) access at the Asset Owner's site. Level 3 is defined as the DMZ (Demilitarized Zone), separating the Enterprise Business Systems (Level 4) from Supervisory Control (the control system in Level 2). Level 4 and Level 5 are considered untrusted.

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.

Components placed in two levels at the same time shall be avoided because they bypass firewall protection or circumvent network segmentation.

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.

4.2.2 Network firewalls

Firewalls ensure the security of IACS equipment in the trusted zones with restricted (physical and network) access at the Asset Owner's site. They shall protect the network from unauthorized access and create boundaries between network segments.

The Control Network Firewall is located between Level 1 and Level 2. The South Firewall separates the DMZ on Level 3 from the trusted OT (Operational Technology) network on Level 2 and below. The North Firewall is located between the Enterprise Business Systems (Level 4) and the DMZ (Level 3).

These Firewalls are configured at the Asset Owner's site and are dependent on the customer application running on the IACS equipment.

Firewalls shall be configured to block all communication (inbound and outbound) except for communication that is explicitly permitted. Explicitly permitted communication shall be as granular as possible, for example only allowing a specific IPv4 address to access the target IPv4 address on a certain TCP port.

During operation of the product, network connections to IACS equipment that are only required for commissioning, administration, and maintenance shall be blocked. During commissioning, administration and maintenance of the product, firewalls shall allow fine-grained access based on the scheduled time frame.

The granular access controls shall be based on the following network connection details:

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

Additionally, the firewalls shall use packet rate limiting based on your needs for each open service, user and device.

The use of rate limiters protects the device from denial of service due to network storms. B&R advises that automation solutions should be tested to determine the maximum load from network requests they can handle without negative impact to the behavior defined by the service provider before they are put into operation. This can be done, e. g., by storm testing or by testing the maximum concurrent connections to the device. The firewall upstream of the device shall be configured so that this maximum load cannot be reached. B&R recommends limiting the load to 80% of the measured values.

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

Furthermore, firewalls should support event monitoring and stateful inspections as well as unidirectional communication.

4.2.3 Remote access

When remote access is required on the Asset Owner's site, use secure methods such as Virtual Private Networks (VPN). Ensure that VPN solutions are updated to the latest version available and use multifactor authentication for login. Limit existing connections to a maximum time and disconnect automatically after this time interval.

Remote access systems shall be located in the DMZ, located in the reference architecture at Level 3 System Management.

5 System security

System Security concerns the security of IACS equipment such as workstations, servers, PLCs or HMI devices. System Security is an important aspect of B&R's Defense in Depth strategy.

System Security of IACS equipment for the operation state is set for commissioning and maintenance and removed from the operation state for decommissioning. B&R recommends applying the following guidelines to the IACS equipment whenever technically feasible.

5.1 Commissioning state

Product commissioning is usually performed by the System Integrator at the Asset Owner's site. However, dedicated Cyber Security equipment may be operated by the Asset Owner and therefore an alignment should be done.

- Configure and maintain a host-based firewall allowing only fine-grained access to services and ports required in operation mode. Disable unnecessary services and block all unused network ports. The firewall configuration should take ingress and egress traffic into consideration.
- Prevent physical and logical access to the component by unauthorized users
- Remove unnecessary software components
- Install and maintain an anti-malware solution
- Configure strong cryptographic mechanisms
- Update the default settings to the Asset Owner as needed
- Collect and monitor the log and auditable events. We recommend collecting the logs on a centralized system like a SIEM in order to monitor them and create alerts
- Create strong passwords and apply a strong password policy for all users (human and non-human)
- Change any default or well-known credentials
- Configure users, groups, and roles according to the Cyber Security principle of least privilege

5.2 Maintenance state

- If services and ports on the IACS equipment are required for maintenance, they should be permitted using fine grained access rights based on the scheduled time frame for the authorized maintenance personnel
- Restrict permissions for critical operations to a time frame and remove permissions after finishing the scheduled maintenance cycle
- Create backups and store them securely, so only authorized personnel have access. We recommend storing backups on encrypted devices
- Delete users, groups and roles that are obsolete (no longer needed)
- Update the anti-malware solution

5.2.1 Patch and vulnerability management

B&R recommends keeping software components updated. Prior to installation, the integrity of deliverable software should be verified. Patches should be applied in scheduled maintenance time frames and be installed by authorized personnel.

5.3 Decommissioning state

- Network security components, like SIEM or IDS systems, can be configured to monitor components and their available services and network communications. Scheduled and authorized component decommissioning or service deactivation should be done for the IACS equipment.
- Delete software licenses
- Delete user, groups and roles (including all authenticators)
- Delete certificates
- Delete intellectual property
- Safe disposal of the IACS equipment

6 Security Monitoring

Recommended Cyber Security best practice is to monitor systems and networks for changes, anomalous behavior or for attack signatures. Security monitoring is also an important part of a Defense in Depth strategy because it detects potential malicious behavior and sends alerts. These detection and altering capabilities are usually located at the Asset Owner's site and allow Cyber Security personnel to detect potential breaches early on.

A risk-based approach should be applied using solutions such as IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) to detect and prevent malicious network traffic. Keep these systems up-to-date to detect new threats. Adapt the rules to the respective levels and try to make them as strict as possible.

Create logging policies for security-related events and protect logs by making regular backups. Always consider events such as the unexpected heavy use of resources or the failure of services and devices as a possible sign of a security incident.

6.1 Security-related tools and utilities

- B&R recommends using network scanners to evaluate the B&R product configuration and its available services and applications. These network scanners assist in uncovering product configuration shortcomings, like the unintended running of network services.
- B&R recommends regularly scanning the network for unauthorized changes and modifications of components
- B&R recommends implementing IDS/IPS systems on Level 1 and Level 2 because the legitimate network traffic is known on these levels.
- B&R recommends to configuring and maintaining a SIEM system on Level 1 and Level 2, where log entries and events are collected and an alerting system is configured to trigger alarms in case of anomalies.

7 Security testing

The ABB Device Security Assurance Center (DSAC) labs perform security tests for selected B&R products.

The personnel at the DSAC labs are trained and certified to provide security testing services and follow modern and commonly accepted industry standards and practices.

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

- Robustness and Denial-of-Service (DoS) tests
- Network-protocol fuzzing and flooding tests
- Measurements of supported network and load tests
- Service and network port enumeration
- Vulnerability scanning for known vulnerabilities and exploits

The comprehensive results gathered during the security tests are reported to B&R. At B&R, the vulnerability handling process will be triggered for each of the discovered security-related issues.

8 Security incidents and issues

Asset Owners are advised to prepare their organization for possible security incidents. This includes, but is not limited to:

- Establishing policies
- Planning activities
- Determining responsibilities
- Identifying key indicators and making them available for analysis

If security vulnerabilities are discovered, they must be reported to the product supplier immediately.
For B&R products, please visit the website https://www.br-automation.com/en/service/cyber-security/ and follow the steps described there.

For detailed information about security incident handling in organizations, see the Computer Security Incident Handling Guide (nist.gov)

9 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/.