BACS SECURITY IN BUILDINGS

BACS Cybersecurity Planning

Contents

1. Purpose of the Document ... 1

2. Cybersecurity for Building Automation and Control Systems (BACS) ... 1

3. Weaknesses in BACS as Risk Factors ... 2

4. Cybersecurity in the Planning and Tendering Process ... 2

5. Cybersecurity of OT Networks ... 2

6. Cybersecurity Planning Process ... 3

6.1. Assessment of the Current Condition ... 3

6.2. Responsibilities and Accountability for Cybersecurity ... 4

7. Building Automation and Control Systems Cybersecurity Requirements ... 5

7.1. Network Segmentation and Management ... 5

7.2. Basic Cybersecurity Requirements (Must Requirements) ... 5

7.3. Standard Cybersecurity Requirements (Should Requirements) ... 6

7.4. Requirements for Critical Systems with Enhanced Cybersecurity Needs ... 9

8. Conclusion: A fault-resilient BACS system also has good resilience against cybersecurity risks ... 9

1. Purpose of the Document

This overview highlights the importance of cybersecurity in planning, implementing, and operating Building Automation and Control Systems (BACS). It outlines security requirements based on the IT-Grundschutz Compendium by the German Federal Office for Information Security (BSI).

2. Cybersecurity for Building Automation and Control Systems (BACS)

BACS enhances building efficiency by automating functions such as heating, ventilation, lighting, and security. IT security for building management is crucial due to the evolving nature of regulations, risks, and opportunities. Threats can be internal, affecting system availability, integrity, authenticity, and confidentiality, or external, such as sabotage, espionage, or unauthorized access.

3. Weaknesses in BACS as Risk Factors

Several issues pose significant risks to IT security:

- Lack of IT security fundamentals during planning.
- Poor documentation, with incomplete or missing records
- Vulnerable interfaces between systems.
- Inadequate monitoring. Critical system failures might go unnoticed
- Weak role and access management.
- Long lifecycles of building systems.

4. Cybersecurity in the Planning and Tendering Process

Often, tenants and users cannot yet be identified during construction, leading to inadequate cybersecurity requirements. Adjustments may be needed once tenants move in. Future upgrades and modifications can become expensive and complicated due to the lack of detailed as-built project documentation.

Defined Requirements

Technical building management often operates in silos, leading to delays and increased fault correction costs. Cybersecurity risks are frequently overlooked at gateways and handover points.

Sufficient Documentation
Good documentation helps implement changes and prevents unnecessary costs.

Monitoring of BACS
Proper monitoring is crucial for detecting faults and security breaches. Establish a monitoring method early to ensure efficient operation and manage system access.

Role and Authorization Management
A dedicated system for managing user identities and access rights is crucial. Address access management and monitor user access rights early in the process.

5. Cybersecurity of OT Networks

IT (Information Technology) and OT (Operational Technology, including Building Controls) networks differ in purpose, environment, and priorities. Here's a comparison:

IT (Information Technology) Networks

- Purpose: Manage data, communication, and business processes.
- Environment: Offices, data centers, cloud infrastructure.
- Examples include Email systems, ERP software, databases, and websites.
- Priorities:
    - Confidentiality (protecting data from unauthorized access)

    - Integrity (ensuring data is accurate and unaltered)
    - Availability (systems are up and running)

OT (Operational Technology) Networks

- Purpose: Monitor and control physical devices and processes.
- Environment: Industrial settings like factories, power plants, and building automation.
- Examples include Programmable Logic Controllers (PLCs), SCADA systems, sensors, and actuators.
- Priorities:
    - Availability (systems must run continuously)
    - Safety (preventing harm to people and equipment)
    - Integrity (accurate control of physical processes)

As stakeholders from IT and building control likely have different priorities, aligning on requirements, cybersecurity deliverables, and priorities is crucial.

Each requirement needs a primary stakeholder. Other stakeholders or suppliers can participate, but the main responsible party should be clear. Cybersecurity for BACS involves IT and building control stakeholders, each with different safety and operational priorities. Recognizing these differences is crucial to avoid misunderstandings.

6. Cybersecurity Planning Process

Establish core security principles while creating BACS requirement specifications. Utilize resources such as AMEV, VDMA 24774, and the BSI Cybersecurity Compendium for guidance.

Although these guides and regulations are designed for the German construction market, they are based on common IT standards and practices, making them a helpful reference for other markets as well. The guides include relevant security topics:

- Building automation networks (interfaces, remote maintenance, etc.)
- Hardening of building automation components (services, accounts, encryption)
- Password policies (complexity, expiration, failed attempts, auto-logout, history)
- Updates, upgrades, and maintenance (hardware, internal/external laptops, interfaces)
- Logging (user actions, data changes, switching, and configuration actions, while respecting data protection laws)

Due to these risks, the following principles should always be considered when planning building automation systems:

- Integrate IT security from the outset.
- Ensure thorough documentation and system transparency.
- Design secure interfaces and implement access controls.
- Plan for ongoing system maintenance and updates to ensure optimal performance.

6.1. Assessment of the Current Condition

Begin by evaluating the cybersecurity of existing equipment, installations, or specified technologies. Do not assume devices are secure. Often, network segmentation is necessary for proper security.

- What cybersecurity properties does the existing or specified equipment provide?
- Does the equipment support secure communication protocols, such as encrypted KNX Secure, BACnet/SC, or OPC UA?
- Has the existing equipment been configured to utilize encrypted communication?
- Does the specification explicitly require secure equipment to be commissioned for use with secure protocols whenever possible?
- If proprietary communication protocols are employed, is the communication encrypted, or is the vendor relying on security by obscurity?
- If non-encrypted communication is used, can a sufficient level of security be achieved through network segmentation and IT security?
- Is enough information available to ensure that the system meets the customer's security needs and policies?
- Who will provide and maintain the OT-Network IT infrastructure and its components?
- What is the handover process for passwords, security keys, or certificates?
- What is the process to monitor who has access to the password, project data, or even the system itself?

6.2. Responsibilities and Accountability for Cybersecurity

For each managed system or group, clearly define and document who holds responsibility and accountability. Specific tasks may require additional clarification. Responsibility and accountability can differ; the responsible person, such as the system integrator, should regularly report to the accountable individual, typically the contractor. This communication is crucial for informed decision-making and effective risk management, particularly when multiple parties, such as building owners, tenants, or organizations, are involved in the process.

The terms **"responsibility"** and **"accountability"** are often used in conjunction, but they have distinct meanings, particularly in management and organizational contexts. Here's a simple breakdown:

Responsibility

Definition: Overseeing the performance of a task or duty.

Focus: Action — what someone is supposed to do.

Example: A technician is responsible for maintaining the air conditioning system.

Responsibility refers to the "doing" part. The Building Control System Integrator typically fulfils this role.

Accountability

Definition: Being answerable for the outcome of a task or decision.

Focus: Ownership — The party that is ultimately responsible if something goes wrong.

Example: The Contractor is accountable for ensuring that the building systems function correctly, even if others perform the actual work.

Accountability means "owning the result" and usually refers to the party responsible by contract, often the mechanical or electrical contractor in building controls.

Recognizing the organizational structure is essential.

7. Building Automation and Control Systems Cybersecurity Requirements

The following requirements are based on the BSI IT-Grundschutz-Baustein INF.14 Gebäudeautomation. This guide offers recommendations and guidance for authorities, companies, and institutions seeking to safeguard their data, systems, and information.

The BSI emphasizes a comprehensive approach to information security, addressing not only technical aspects but also infrastructural, organizational, and personnel issues. This provides a systematic method for identifying and implementing necessary security measures. This guideline is officially only applicable in Germany. However, it is based on best practice IT network security methods and can be used outside of Germany, even though it is not formally binding.

7.1. Network Segmentation and Management

A security strategy for Building Automation and Control Systems (BACS) must include protective measures like data backups, firewalls, and uninterruptible power supplies. Usability requirements should align with the operational concept, aiming to protect the entire building system, including connected systems. Objectives should be set during planning as part of an Operational Technology (OT) security strategy, detailing measures for all OT components. Responsibilities must be assigned to suppliers, system integrators, and the building operator. The security strategy should incorporate specific elements for building automation systems.

- **OT Architecture:** Define the structure and components of the operational technology environment.
- **Network Design and Segmentation**: Plan the network structure and divide it into secure zones to limit access and reduce risks.
- **Patch Management**: Ensure regular updates and security patches are applied to all systems and devices.
- **Asset Management:** Maintain an up-to-date inventory of all hardware and software assets in the system.
- **Emergency Management:** Implement backup solutions and redundancy strategies to maintain operations in the event of IT network failures or incidents.
- **Risk Assessment and Protection Needs:** Identify potential risks and determine the necessary level of protection for each system or component to ensure optimal security and safety.
- **Staffing Recommendations:** Guide the number and qualifications of personnel required to operate and maintain the system securely. It is essential to have staff who understand the specific IT requirements of building control systems.

7.2. Basic Cybersecurity Requirements (Must Requirements)

Planning the Building Automation and Control Systems (BACS)

Building Automation and Control Systems (BACS) must integrate cybersecurity requirements into their design and development processes to ensure the security of their systems. The design should incorporate all BACS controls, including HVAC, lighting, shading, and energy management, using secure, standardized systems and protocols. Regular updates to specifications and drawings are crucial.

Technology Definition and Selection
Determine the number of siloed automation systems based on:

- Equipment and appliances to be connected.
- Wiring, product availability, and needs.
- Required connection and communication technologies.

- Ensure alignment with regulatory and security requirements.

Implementation Planning
Implementation planning outlines how the detailed planning will be executed. It includes:

- Specifying each required step.
- Defining the sequence, responsibilities, and timeline.

During the final acceptance phase, it must be verified that the implementation exactly follows the detailed plan and that all specified requirements are met. Any deviations should be reported to the planning team for analysis and potential correction.

Commissioning Management
Coordinate various trades and stakeholders throughout all project stages and during the building's initial use. Define the order of commissioning building systems and the process for connecting BACS to other systems.

Documentation of BACS
Document all components and access points. Regularly review and update documentation to reflect any changes that occur.

System Segmentation and Integration of Various Building Systems & Control Siloes
Carefully plan and test the integration of siloed control systems with BACS to ensure seamless operation. Ensure only explicitly defined data and actions are exchanged between BACS and connected systems.

7.3. Standard Cybersecurity Requirements (Should Requirements)

In addition to the basic requirements, the following criteria reflect current technology standards and should generally be met.

Definition of Cybersecurity Policy
A BACS security policy should align with IT guidelines, be clearly documented, regularly updated, and easily accessible. It establishes general requirements for BACS and its components, excluding technical details. The policy and any updates must be promptly communicated to all stakeholders.

Building Automation and Control Systems Cybersecurity Specification
These specifications must cover all key aspects related to the architecture, design, and connections of each system. These documents must be consistently updated to incorporate technological advancements and undergo periodic review during the implementation process. The requirements specification establishes the BACS security policy through a two-step process: first, a detailed requirements analysis is performed to assess and organize the collected requirements, and then, precise requirements are defined for all relevant BACS components. According to the Cybersecurity Policy, the specification should provide a complete requirement specification for the Building Automation and Control Systems (BACS), separate requirement specifications for each BACS subsystem, and evidence of compliance with relevant legal and regulatory standards.

Building Automation and Control System Concept and Specification
A comprehensive Building Automation and Control System (BACS) plan should be developed. Each BACS system must comply with cybersecurity standards and include a detailed strategy for both connected and siloed systems, including communication links. The plan should define technical and organizational requirements, with regular reviews. BACS segments and silos should limit dependencies to contain failures. Each building segment should remain controllable if another segment fails. The BACS concept provides a foundation for reliable and cost-effective operations by outlining the architecture, tasks, and rules for routine use and system modifications. It acts as a high-level framework during

planning, addressing organizational and technical issues. Regularly review and update the BACS concept to reflect current technology and practices, ensuring it aligns with the actual system and detects any unauthorized changes.

Self-sufficiency as a Security Principle
Building Automation and Control System (BACS), subsystems, and system segments should be designed to operate independently based on protection needs, even if the primary BACS connection fails. They should minimize critical dependencies on central BACS, other subsystems, or segments. If the connection fails, BACS segments should remain locally operational. It's essential to identify dependencies among control silo systems, devices, and connected systems. Some BACS and IoT devices need uninterrupted internet access. If a device can't function without an internet connection, consider alternative products or a secure, dedicated internet connection for BACS.

Standardizing BACS Areas for Efficiency and Stability
BACS areas with similar functions should use the same technology for easier planning, smoother operations, and stability. For example, spaces like offices or meeting rooms with independent lighting, shading, and climate control should be locally managed. Whenever feasible, a BACS zone should remain operational in the event of a primary system failure.

BACS Segmentation
Segment building automation networks to isolate systems and zones, establishing transition rules enforced by security components like routers and filters. Divide BACS into segments based on security needs, starting with a communication matrix that illustrates component interactions, protocols, and the organizations involved. Internal communication is usually unrestricted; inter-segment communication should be limited and managed with firewalls, typically from higher to lower security zones. Review segmentation areas, including entire BACS, control groups, individual silos, and cross-organizational components.

Access Control for Central BACS Devices and Software.
Implement an Access Control system for central or critical building automation devices tailored to BACS requirements, either deploying a dedicated BACS authentication or integrating with the institution's central IT system. Clearly define roles and permissions for BACS operators, technical staff, and users, especially in complex control environments. Assign roles, such as tenants and operators, with limited permissions, and update them promptly after any organizational changes. Standard permissions include read-only, read/write, and full admin, reserved for qualified personnel during setup or when significant changes are made.

Secure IP Communication
Use secure protocols for building automation over Ethernet/IP, especially on untrusted networks. Encrypt BACS IP traffic with standards like KNXnet/IP Secure or BACnet/SC. Sensitive info outside native protocols should be sent securely via HTTPS or FTPS with TLS. If proprietary protocols are used, evaluate their security and safety.

Security Mechanisms for BACS Networks
Utilize security measures such as KNXnet/IP Secure and BACnet/SC for BACnet IP protocols. Monitor and restrict communication with BACS networks through a secure gateway or system component with suitable filter functionality. Ensure authentication and encryption on IP networks, such as TLS 1.3 for BACnet/SC and AES 128 encryption for KNX IP Secure. Review the use of components with limited security features. If their continued use is necessary, isolate and monitor them with gateways or firewalls, following best practices. Allow only authorized network access, using switches for Ethernet networks. Design the BACS network architecture to prevent unauthorized connections between segments, employing strict controls like filters in KNX IP Routers.

Communication Interfaces to External Systems
Communication between the Building Automation and Control System (BACS) and external systems should occur only through clearly defined, secure interfaces that include authentication and encryption. Limit external interfaces to essential ones. When connecting to external systems, such as facility management or office IT, document all connections and dependencies.

Use of Dedicated IP Address Range for BACS
Dedicated IP ranges should be explicitly assigned for Building Automation and Control Systems (BACS) and separated from office IT or other operational technology (OT). It's crucial to identify which parts of the address range are used for static IP addresses and which BACS components require these. IP addresses should be assigned systematically to reflect building and device type. When using DHCP, distinguish between dynamic and static IP addresses, as many BACS devices require a static IP address. Proper IP management ensures separation, clarity, and efficient administration.

Broadcast Communication
In OT building automation networks, minimize broadcast traffic to prevent overload—prefer unicast or multicast. Use broadcasts only when necessary and segment the network. Configure BACS routers to avoid forwarding broadcasts unless needed. Devices needing broadcasts should be on a shared, isolated subnet.

Ensuring Displayed and Control Values are Up to Date
For remotely monitored building control systems, it must be clear whether displayed data—such as values or status—is current. The system should detect outdated critical data and either alert users or activate a fault response to protect occupants and the building. Simulated or "frozen" data should be flagged or trigger an alarm as required.

Robust Components
Use durable components in challenging environments or implement compensatory measures if unavailable.

Time Synchronization
Components and systems should utilize synchronized time for automated measurement, control, and regulation, particularly in connected Building Automation and Control Systems (BACS) spanning multiple buildings or sites. For real-time communication within a BACS, native BACS time synchronization methods should be used, rather than relying solely on NTP.

Status Logs
Security-related runtime events and device availability should be logged for BACS critical devices. An appropriate monitoring plan should be developed and implemented. The availability and key parameters of BACS-related components should be continuously monitored. If errors or set limits are reached, these should be automatically reported to the operating organization. The BACS should at least trigger alarms if systems fail or if essential automated control functions are unavailable. It should also specify which security-related or other events should automatically generate alarm messages. Status reports and monitoring data should only be transmitted over secure communication channels.

Change Logs
In addition to logging status changes on building automation components, security events should be logged. All configuration changes to technical building systems, BACS-relevant components, and manual or automated changes to their states must be documented, including software or firmware updates. Specify what log data is stored centrally. Since these changes may involve wiring, physical modifications, or configuration adjustments via external tools, direct logging from BACS may not always be possible. Instead, commissioning and site reports from installers, maintenance staff, and system integrators can be used.

Emergency Planning
Regularly evaluate how Building Automation and Control Systems (BACS) affect emergency planning. Develop guidelines to minimize disruptions resulting from BACS failures due to technical issues or cyberattacks. Emergency plans should include contact information for maintenance staff and

designated emergency personnel. Include procedures to maintain vital operations during BACS outages and document restart plans.

7.4. Requirements for Critical Systems with Enhanced Cybersecurity Needs

Consider additional requirements for higher protection based on risk assessment.

Dedicated Physical Network for BACS
For greater protection, BACS networks should be physically isolated from other networks. Connections to external cloud services must go through dedicated, tightly controlled internet access. Additionally, connections to untrusted networks, including internal offices, should be blocked in accordance with BACS protection requirements.

OT-Network Segmentation
To protect high-security building systems, such as those related to health, safety, or security, consider isolating them on a separate OT network segment for monitoring and control.

Dedicated Time Server for Critical Systems
Provide a dedicated time server for BACS or individual building subsystems. This server may utilize GPS or another time source, in addition to NTP, for accurate timekeeping.

8. Conclusion: A fault-resilient BACS system also has good resilience against cybersecurity risks.

The first line of defense against cybersecurity threats is a well-designed and fault-resilient building control system. If the system is well-segmented, there are no central points of failure, and the control functionality is distributed and kept as local as possible. This approach minimizes vulnerability and enhances the overall security of the automation solutions, such as those offered by ABB's KNX systems. Ensuring robust segmentation and local control can significantly reduce the risks associated with cyberattacks.