Guideline Cyber Security in Building Automation

BIG-EU
WG-FM 100
Version 01

Status 9/24

The BACnet Interest Group Europe (BIG-EU) is a user and industry association that promotes the successful use of the BACnet protocol in building automation (BA) through interoperability testing, training programs and promotional activities in Europe.

The BIG-EU was founded on May 14, 1998 in Frankfurt am Main by an initial 17 member companies. Today, the BIG-EU has over 120 members from all over Europe as well as Australia and North America.

The BACnet standard was developed by ASHRAE (American Society of Heating, Refrigeration and Air-Conditioning Engineers), updated and made publicly available so that manufacturers can develop interoperable products for GA. The BIG- EU supplements the work of the ASHRAE standards committee with European requirements.

Members of the BIG-EU include building owners, consulting engineers and building operators as well as companies involved in the design, manufacture, installation, commissioning and maintenance of building automation systems that use the manufacturer-neutral BACnet data transmission protocol for communication.

WG Facility Management

The aim of the guidelines WG-FM 100 – Version 01 of the Facility Management (FM) working group is to define the framework conditions for the safe operation of a property. These guidelines are based on the life cycle phases in FM as they are already established in German-speaking countries. This includes the "GEFMA 100" guideline (www.gefma.de/service/shop) and the consideration of individual service profiles of the Fee Structure for Architects and Engineers (HOAI).www.hoai.de/hoai/leistungsphasen

Contents of the guide "Cyber security in building automation"

Fig. 1: Overview of the service phases according to HOAI

Abbreviations used in the following guide:

AG	Client
AMEV	Working group for mechanical and electrical engineering in state and municipal administrations
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BACnet	Building Automation and Control Network
BACnet/SC	BACnet Secure Connect
B-BC	Building Controller (device profile)
BBMD	BACnet Broadcast Management Device
BetrSichV	Industrial Safety Ordinance
BMS	Building Management System
BSI	Federal Office for Information Security
CER	Critical Entities Resilience (EU "Critical Entities Resilience Directive")
CRA	Cyber Resilience Act
DDC	Direct Digital Control
DIN	German Institute for Standardization
GDPR	General Data Protection Regulation
EN	European standard
FM	Facility Management
FND	Company-neutral data transfer protocol
GA	Building automation
GEFMA	German Facility Management Association
JIT	Building Energy Act
HOAI	Fee schedule for architects and engineers
IBM	Commissioning management
IEC	International Electrotechnical Commission
INF.13	Building block in the BSI's IT baseline protection
INF.14	Building block in the BSI's IT baseline protection
INF.5	Building block in the BSI's IT baseline protection
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
CRITIS	Critical infrastructures
LP	Service phase (according to HOAI)
MBE	Management and operating device
NET.1.2	Building block in the BSI's IT baseline protection
NIS 2	Network and information security (2nd EU Network and Information Security Directive)
NIS2UmsuCG	NIS-2 Implementation and Cybersecurity Strengthening Act
OT	Operational Technology
RMP	Risk management process
SLA	Service Level Agreement
TGA	Technical building equipment
MOT	Technical Inspection Association
VDI	Association of German Engineers e. V.
VDMA	German Engineering Federation

Introduction

The increasing technological developments in building technology, including smart buildings, and the rapid market penetration of building technology with general information technology are also leading to an increasingly higher cyber security risk.

Due to a lack of expertise (no IT core competence) in construction management, building planning and operators in the building context, a shortage of skilled workers among integrators and commissioning companies and the potentially major impact of successful cyber attacks on the infrastructure of buildings, joint IT/OT security is not only relevant for operators of critical infrastructure and federal authorities, but must become the standard for building operations; because attackers often look for and find the weakest point. There are several prominent examples of this detour via building technology.

Legislators have recognized this potential threat and have set appropriate cyber security requirements at both European and national level:

- at European level
  NIS 2 Directive (EU 2022/2555),
  Cyber Resilience Act (CRA – EU 2022/0272),

- at national level (using Germany as an example)
  NIS-2 Implementation and Cyber Security Strengthening Act (NIS2UmsuCG).

In the increasingly modern and digitalized environment and due to increasing international political tensions, there is therefore growing concern about massive negative economic effects in the professional environment – among other things, if technical systems are compromised under one's own responsibility. These include

- Economic damage due to loss of reputation – for example through negative public perception with press releases or social media,
- Financial loss due to restricted availability of internal company options, including blackmail attempts or negative influence in production processes.

In addition, high fines have been announced, in some cases even with personal liability for the management (such as the EU's "Cyber Resilience Act").

This guideline is intended to achieve added value through recommendations for standardization processes, infrastructures, services and suitable organization (roles), among other things (security by design from the outset). This is because a failure of the information technology (IT) means that the building technology with its operational technologies (OT) can no longer fulfill its operator obligations or can only do so with enormous effort.

The circle of operators of critical infrastructures will increasingly include more business areas in the future. As a result, the requirements of various national associations and organizations to establish IT/OT security are growing [e.g. 1, 2]. Setting up and maintaining a reliable and resilient IT/OT infrastructure is a discipline for IT and building automation specialists. Therefore, the application of measures to achieve IT/OT security is not only relevant for the operation of critical infrastructure and federal authorities, but should become an integral approach to the standard of building operation.

[1] AMEV Building Automation 2023

[2] VDMA standard sheet 24774

This guideline serves to present the currently valid requirements for the IT/OT security of buildings. There are mandatory requirements for operators of critical infrastructures (CRITIS) and federal authorities. However, all parties involved in the life cycle of planning, constructing and operating technical building equipment are addressed. These guidelines are not intended to draft IT/OT security concepts. It provides an overview of the necessary activities for each construction phase with corresponding references to already established tools.

Delimitation: This guideline does not consider the established processes for functions in building automation, but focuses on the additional requirements and tasks in the IT/OT-RMP for BA. Interfaces to the use cases for smart buildings and building management systems mentioned below are not currently taken into account and should be considered separately if necessary.

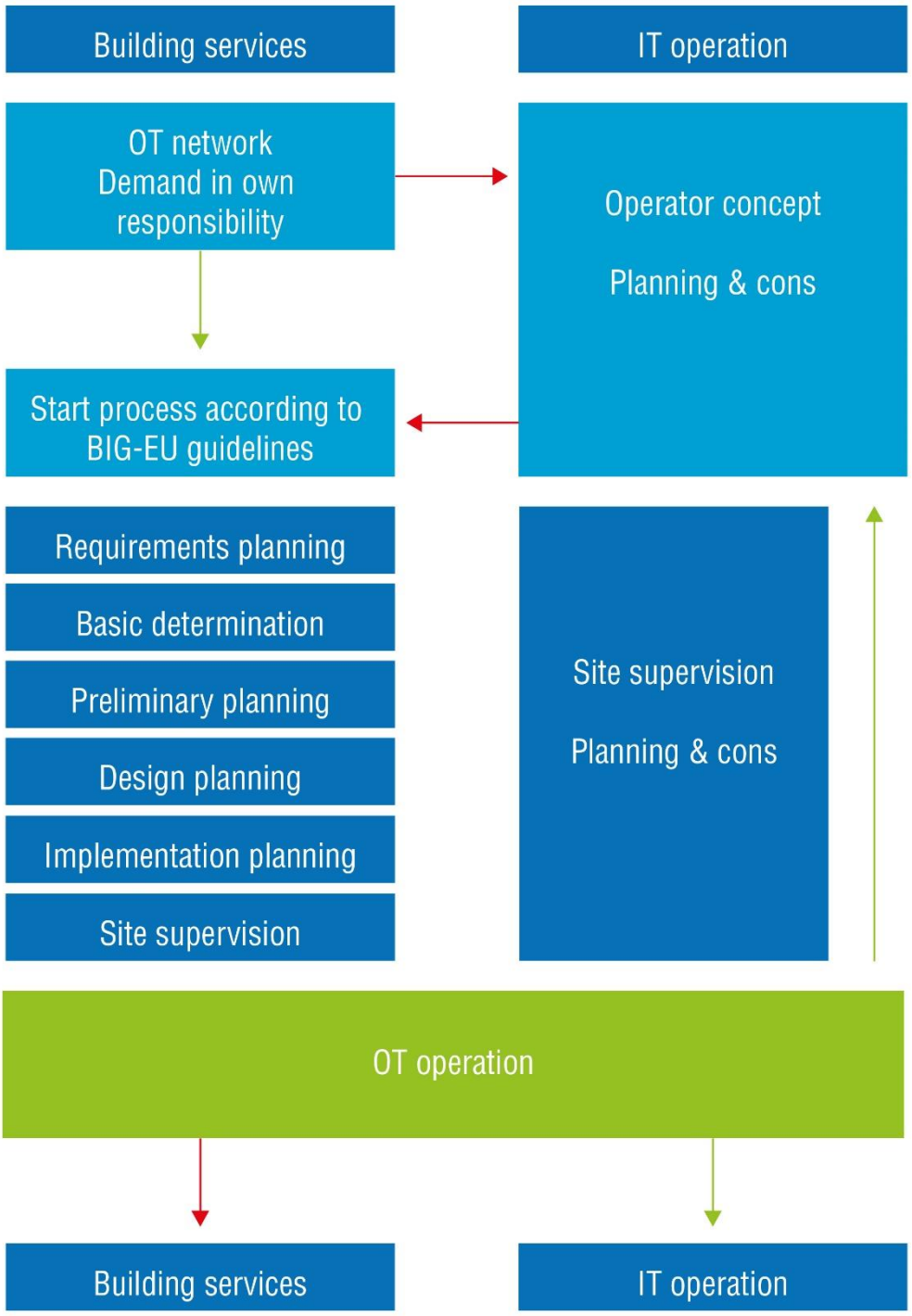

Fig. 2: Illustration of the various process steps

According to the flow chart, a large number of legal requirements must be taken into account during the construction process of a building automation system, based on the construction and service phases of the HOAI established in Germany.
Due to the large number of regulations, it is difficult for interested users to recognize which recommendations, standards or regulations need to be consulted when in the planning and construction process.
Overview for individual implementation of IT/OT security requirements:

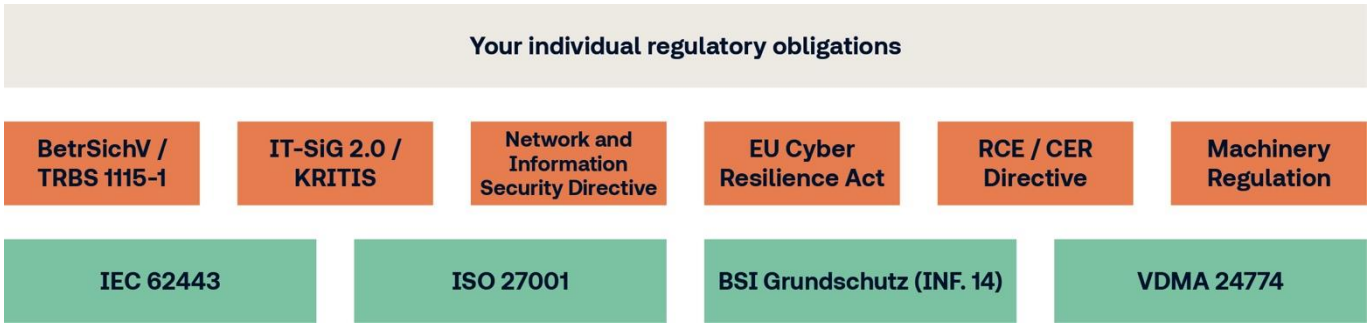

Fig. 3: Guideline GA TÜV SÜD Version 02/24

The evaluation and implementation of the respective security requirements in the company environment is carried out by various responsible persons in their roles.

The naming of the starter roles is based on the recommendation of the BSI and the "INF.14 Building automation":

Role 1: Building services

Role 2: Planner

Role 3: Administrator

Role 4: IT operations

The Basic IT Security Compendium also defines further roles. These should be filled as appropriate and reasonable.

Responsibilities	Roles
Fundamentally responsible for	Building services
Other responsibilities	Planner, administrator, IT operations

Exactly one role should be fundamentally responsible. In addition, there may be further responsibilities. If one of these other roles is primarily responsible for fulfilling a requirement, then this role is given in square brackets after the heading of the requirement.

Fig. 4: BSI – INF.14

Depending on the individual requirements/individual characteristics of the building services IT/OT systems and services, these four superordinate roles in the IT/OT risk management process (IT/OT-RMP) are specifically supplemented or renamed during the planning and construction process – in accordance with the proposals defined in the guideline and the following role cards.

Here, too, there are further implementation instructions from INF.14, which predefine additional roles.

Commissioning management must also take into account the roles for the operating and management functions of the BA, which can access the BA with fundamentally different tasks and requirements. These roles are
- Building users or demand organisations, e.g. tenants,
- internal or external operator organisations (e.g. building services) that ensure the operational management of BA and IGA systems,
- external service providers (e.g. for maintenance or servicing) who must be granted access to individual systems must be granted access,
- Facility managers who require access to management functions, e.g. as part of commercial management or to optimise life cycle costs,
- System administrators who are responsible for system maintenance, e.g. for backup and restore, system parameters, user support, and
- Installers who, for example, need to install new firmware

Fig. 5: Implementation note INF.14

The IT/OT risk management process (IT/OT-RMP) defines the tasks and roles required for all life cycle phases, which are assigned and run through several times for the respective use cases of requirements planning. The system owner has an overarching role of overall responsibility and is the person responsible for requirements. Within the overall responsibility are the additional roles of product responsibility and security management to define companies for all use cases in the organization. In the broader sense of requirements planning, use cases are also modern applications of digital building management systems (BMS) and smart building platforms. These must be taken into account in the construction planning process as requirements for building IT systems, for example:

- Facility Management / Predictive Maintenance
- Lock management / indoor navigation / room occupancy
- Parking space management / e-mobility

These systems use information from the GA systems. Their interfaces must already be taken into account during requirements planning.

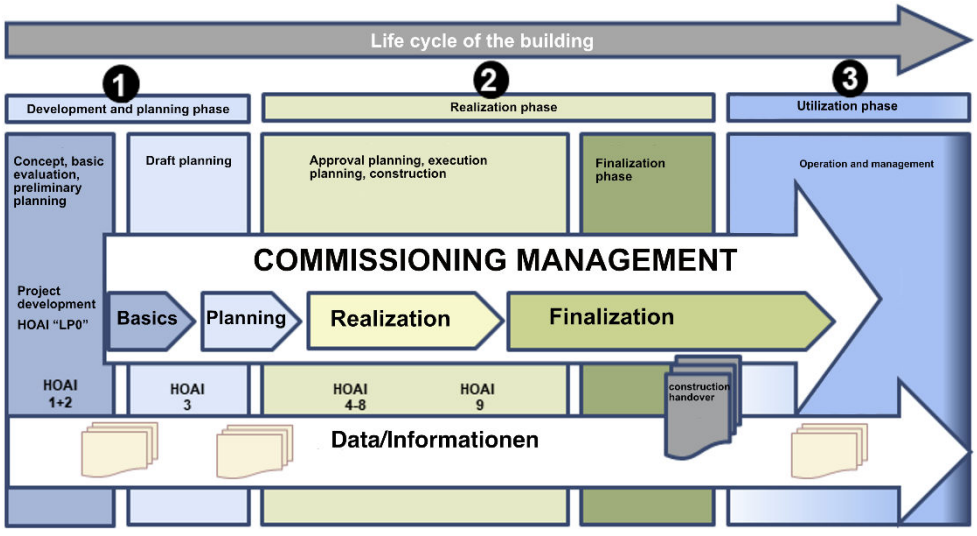

Fig. 6: Example of IT/OT security as an integral approach at the Deutsche Bundesbank

Fig. 7: Example of the IT/OT-RMP of the Deutsche Bundesbank

In the following guide, "role cards" are presented as modules suitable for a needs analysis and visualized based on the respective service phases of the HOAI.

These four roles defined in "INF.14 Building Automation" form the basic framework and serve as initial orientation in the field of IT/OT security in building automation. More precisely specified role requirements are added in square brackets [xx].

This arrangement of the "cards" provided provides an overview of the performance phase of the construction process in which responsible parties with the relevant expertise must deal with which topics so that implementation and safety are successfully implemented in the upcoming project through the required OT network structure. If required, the following cards can be handed over to the defined roles 1-4.

Overview of the maps provided:

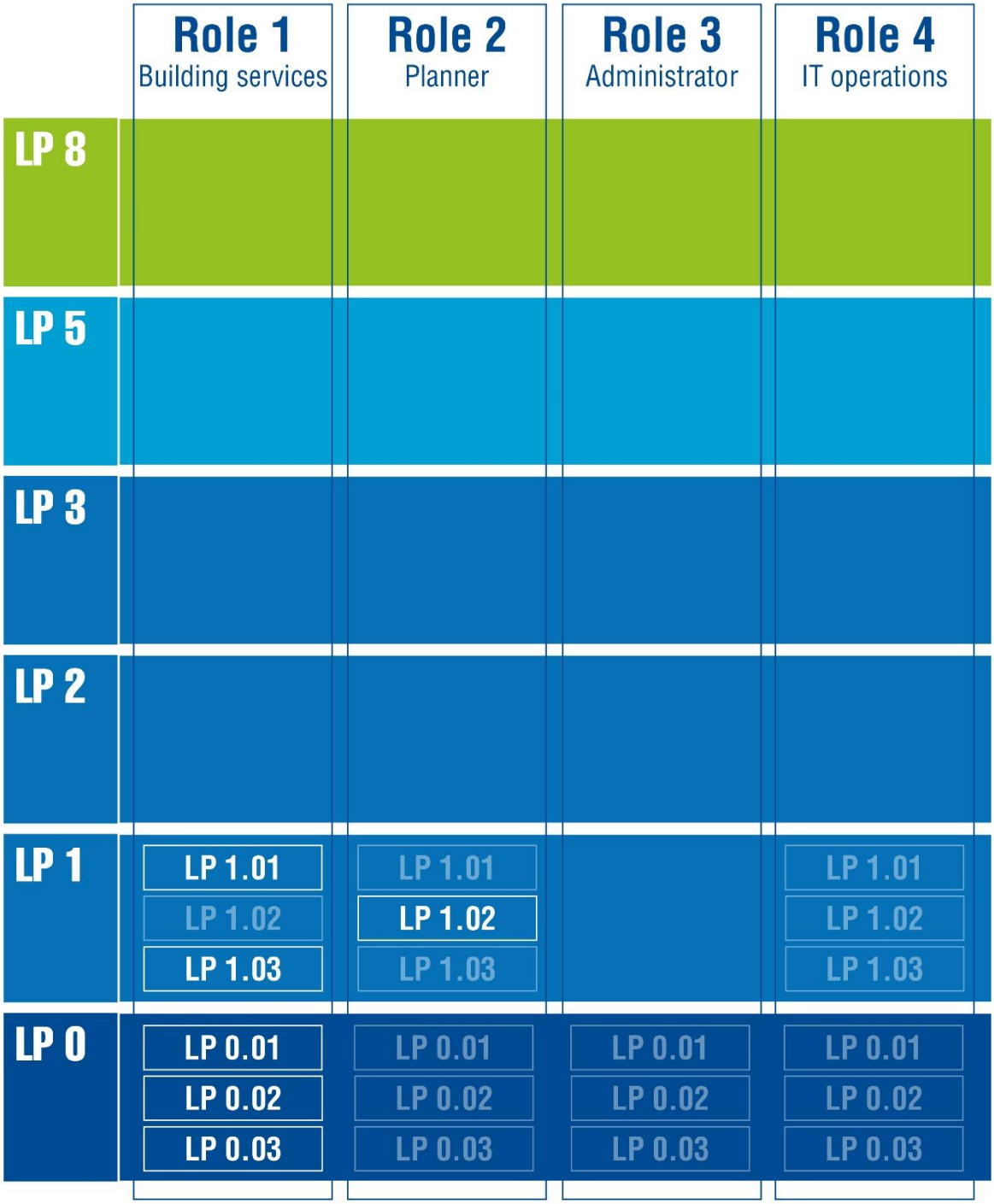

Fig. 8: Overview of the role cards

LP 0: Demand planning – operating concept

Demand planning, including IT/OT-RMP operating concepts, plays a fundamental role in efficient, economical and safe building operation. The basis for the future viability of a building is also created by the high-quality implementation of building automation, which is based on needs-based planning. Intelligent and networked systems increase user comfort and the value of a property.

Effective IT/OT-RMP security measures must be implemented in line with the systems and communication protocols used and the use of the building. The IT/OT-RMP starter roles must be involved in the entire planning and integration process for setting up the BA. The integration planner, who is also responsible for the BA, IT and OT, needs information on the specific requirements for building operation and its implementation. At the same time, the implementation of the measures by the building owners involved must be monitored throughout the entire planning, integration and commissioning process. Building owners should use quality controlling during planning and construction to ensure that the requirements are met.
are fulfilled correctly and no interface or security problems arise. If there is no expertise in this area, this service can be purchased externally as part of commissioning management (IBM).

For the future operation of the technical systems via an integrated building automation system, important basic principles in the area of network security must be considered during the requirements analysis and operating concept phase.

These include:

- Specification of the object of investigation and definition of the protection requirements,
- Determination of IT security requirements and their protection goals,
- Definition of measures to identify and assess residual technical risks,
- Reporting and approval of residual risks.

There are also further questions regarding the protection of information and the IT and OT components used:

- Confidentiality,
- Integrity,
- Availability,
- is personal data collected or processed? (GDPR).

The criteria and findings gained here are then incorporated into the further realization of the construction process in accordance with the HOAI.

LP 0.01 Map theme: Legal/mandatory requirements

Keywords:
#legislation GA #commitment GA #IT security in GA #IT security #GEG

Brief description:
Legislation is increasingly imposing requirements for the energy-optimized operation of buildings through automation. In addition, the statutory and mandatory requirements are intended to ensure secure building operation (IT security).
In order to meet the legal and mandatory requirements for the construction of BAs, it is therefore necessary to be familiar with the large number of laws and standards. This module is intended to highlight the most important laws and standards and explain their interrelationships.

References:
Building Energy Act (GEG)

DIN V 18599-11 – Energy assessment of buildings

DIN EN ISO 52120-1:2019-12 – Energy performance of buildings

INF.14 Building automation

KRITIS/NIS2 guideline/BSI basic protection compendium on industry-specific standards and requirements

Objective:
The aim of this module is to highlight the existing legal requirements for the installation of building automation systems. The requirements for the efficiency of technical building equipment (TBE), in particular , are regulated and thus energy-efficient building operation. In addition, information security is to be permanently established as an integral part of the planning, implementation and operation of BACS.

Role:
Role 1 [System owner/requirement owner/builder]

with input from
Role 2 [integral consulting internal/external]
Role 3 [GA system administrator]
Role 4 [IT Security Organization/Manager]

LP 0.02

(according to checklist Appendix A)

Map theme:

Normative requirements

Keywords:

#GA standards #Recommendations #VDI3814 #Guidelines

Brief description:

Building automation (BA) has increasingly developed into a key discipline for the sustainable operation of buildings and real estate portfolios over their entire life cycle. Since the prerequisites for this are already created during planning and construction (new build, conversion, extension, refurbishment), it is fundamentally important to consider BACS in the planning and construction processes with the applicable standards and recommendations. This module is intended to highlight the most important standards and recommendations.

References:

Technical regulations VDI 3814 – Building automation (GA)

DIN EN ISO 16484-5:2023-02 – Building automation systems – Part 5 (BACnet)

AMEV building automation
AMEV-BACnet BACnet 2017
BACtwin in public buildings

VDMA 24774 – IT security in building automation

VDI 6041:2017-07 Facility management – Technical monitoring of buildings and technical building systems

Facility management; commissioning management for buildings; methods and procedures for technical building systems

Objective:

The aim of this module is to highlight the existing standards and recommendations for the installation of building automation systems. The application of the series of guidelines, standards and recommendations intended to ensure and improve the sustainability of buildings and real estate portfolios. The building owner has an important and decisive role to play here, particularly in defining his requirements.
The application of the series of guidelines, standards and recommendations is an important part of the planning, implementation and operation of BA.

Role:

Role 1 [TGA plant manager]

with input from

Role 2 [integral consulting internal/external]
Role 3 [GA system administrator]
Role 4 [IT Security Organization/Manager]

LP 0.03
(according to checklist Appendix A)

Map theme:
Requirements planning, operator concept and specifications

Keywords:
#Building owner/user #Property planner/architect #Specialist planner TGA #Manufacturer GA components #Executing trades #Operator

Brief description:
The steps of requirements planning should ensure that the client's task is comprehensively recorded and fully described. The documents to be created as part of requirements planning – such as operator concepts and specifications – are the responsibility of the client (special service according to HOAI) and must be continuously maintained by the client. These documents form the essential basis for the planning of the BA and must be observed by all users.

References:
Technical regulations VDI 3814 – Sheet 2.1 – Building automation (BA) – Planning - Requirements planning, operator concept and specifications

VDI MT 3814 Sheet 6 – 2020-01 – Beuth.de – Building automation (BA) – Qualification, roles and competencies

AMEV commissioning management 2023-10

Objective:
The timely completion of requirements planning, operator concept and specifications is crucial for building automation. This improves the construction process by:

- **Early planning security:** clarity about objectives and scope through timely requirements planning,
- **Risk minimization:** Identification and management of potential problems through an early operator concept and specifications,
- **Efficient allocation of resources:** better allocation of materials, labor and finances through timely documents,
- **Better tenders:** precise tenders thanks to early specifications for the selection of contractors and suppliers,
- **Accelerated implementation:** faster project implementation with clear specifications from the operator concept and specifications,
- **Better coordination of trades:** improved coordination between different trades through timely documents,
- **Cost efficiency:** easier budgeting and cost control for project completion within budget,
- **Customer and user satisfaction:** Meeting the needs of users by creating an operator concept in good time for greater satisfaction.

Role:
Role 1 [TGA plant manager]

with input from
Role 2 [integral consulting internal/external]
Role 3 [GA system administrator]
Role 4 [IT Security Organization/Manager]

LP 1: Basic evaluation – project preparation

Kick-off IT/OT risk management process (RMP)

1. Participation in the coordination with the IT security management of the client by the integration planner TGA and definition of the boundary conditions for the implementation of the IT security management for the further course of the project.

2. Determination of the relevant boundary conditions and specifications, in particular from the BSI modules (including "INF.13 Technical building management" and "INF.14 Building automation") and other specifications from the departments.

   Advice from IT security management and clear allocation of roles.

LP 1.01
(according to checklist Appendix A)

Map theme:
IT infrastructure

Keywords:
#network topology, #existing situation, #legal IT requirements, #target #IT service provider, #IT operator responsibility, #IT interfaces, #IT SLA

Brief description:
- **Description and presentation of the current situation in the IT network**
  For project preparation, it is essential to carry out a detailed and correct basic survey in existing installations so that the current situation is clear in relation to the new objectives to be planned and adapted in accordance with the legal guidelines. With the help of a logical or location-based network topology, the planning team can quickly gain an overview of the existing IT infrastructure and specify this with further information in the subsequent planning process. For new and existing projects, a future network topology provides all project participants and decision-makers with a structured presentation of the objectives.
- **Who operates the IT infrastructure (internal/external)**
  Are there several internal or external service providers, who are the contact persons and knowledge carriers? Who has operator responsibility up to which interfaces?

References:
BSI, NET.1.2 – Network management

Technical regulations VDI 3814 – Sheet 2.2: Building automation (BA) – Planning - Planning content, system integration and interfaces

Objective:
The timely completion of requirements planning, operator concept and specifications is crucial for building automation. This improves the construction process by:
- Definition of responsibility and operator responsibility,
- Description of the current situation of the IT infrastructure using a topology,
- Who is responsible for ensuring that the IT infrastructure stable?
- Who are the contact persons and knowledge carriers (internal/external) at the operator?
- What are the operator contracts (also known as Service Level Agreements (SLA))?
- Where are the interfaces in the IT infrastructure?

All of this needs to be found out during project preparation.

Role:
Role 1 [IT department]

with input from
Role 2 [integral consulting internal/external]
Role 4 [IT security organization/manager]

LP 1.02
(according to checklist Appendix A)

Map theme:
OT infrastructure

Keywords:
#GA inventory, #DDC, #automation equipment, #B-BC, #BBMD

Brief description:

- **Recording the BA devices (protocol interface, IP address, BACnet revision)** The existing BA devices (DDC controllers) and OT infrastructure components (BBMDs, gateways, bus repeaters, etc.) and their technical attributes must be recorded for project preparation. In existing installations, a detailed and correct
  It is essential to carry out a baseline assessment so that the current situation is clear in relation to the new objectives to be planned and adapted in accordance with the legal guidelines.
  With the help of a logical or location-based network topology, the planning team can quickly gain an overview of the existing OT infrastructure and specify this in the further planning process with more detailed information and make it cyber-secure. For new and existing projects, a future network topology provides all project participants and decision-makers with a structured representation of the objective.
- **Access authorizations to MBE, technical centers (admin, technicians, janitors, external service providers)**
  Are there several internal or external service providers, who are the contact persons and knowledge carriers? Who has operator responsibility up to which interfaces?

References:
INF.5: Room and cabinet for technical infrastructure

INF.14 Building automation

Technical regulations VDI 3814 – sheets 1/2.1/2.2/2.3/4.2

B-PATB-PAT
Template Table
description

Objective:

- Definition of responsibility or operator responsibility,
- Description of the existing situation of the OT infrastructure using a topology,
- Who is responsible for ensuring that the OT infrastructure stable?
- Who are the contact persons and knowledge carriers (internal/external) at the BA operator?
- What are the operator contracts (also known as Service Level Agreements (SLA))?
- Where are the interfaces in the OT infrastructure?

All of this needs to be found out during project preparation.

Role:
Role 2 [integral consulting internal/external]

with input from
Role 1 [TGA plant manager] Role 4 [IT security organization/manager]

LP 1.03
(according to checklist Appendix A)

Map theme:
Operator concept

Keywords:
#GA operator concept, #GA specification sheet

Brief description:
- **Description of the boundary conditions for the operation of building automation (BA) in the property/project area/managed building stock**
  For sensible system integration in building automation, it is necessary to define the design and use of the requirements for the technical system for the new application to be designed (project/modernization/refurbishment) in advance of the planning stage.
  It is very useful to know the objectives of operating technical systems during the planning process.
- A standard, the so-called specification sheet for the property, must be defined so that different GA plans in terms of time or location also lead to comparable results that can be used in the same way.

References:
VDI/GEFMA 3810 Sheet 5: Operation of buildings and maintenance of technical building systems – Building automation

Technical regulations VDI 3814 – Sheet 2.1 – Building automation (BA) – Planning - Requirements planning, operator concept and specifications

Objective:
- **Record and prioritize the client's/builder's requirements**
  Which trades are operated with building automation and which management operating functions are required for the operation of the property. (visualization/registration/operation/archiving)
- **Definition of processes, process participants and responsibilities in the use of GA**
  Which processes and reporting chains already exist or will be needed in the future?
- **Delimitation of internal/external processes**
  Which service providers/maintenance contractors act on what basis and with what response times? Where is this set out in writing (e.g. in a service level agreement (SLA)/service contract)?
- **Secure and economical operation of BA with IT networks** across the entire property despite changing BA contractors/BA system integrators/BA installation companies

Role:
Role 1 [GA operation/system owner]

with input from
Role 2 [GA specialist planner]
Role 4 [IT Operations]

LP 2-9: Note – follow-up versions in progress

The current status of the guideline is based on established methods from Germany. The consideration of requirements planning – operational concept (LP 0) and basic evaluation – project preparation (LP 1) is not intended to suggest that the contents of the guideline should not be taken into account in the subsequent service phases.

The further compilation of the necessary recommendations, guidelines and processes are in progress and will be integrated into subsequent versions of the guide.

Acknowledgments

The President of the BACnet Interest Group Europe (BIG-EU) Thomas Kurowski would like to thank all those involved in the WG-FM working group – led by the chairmen Patrick Lützel (TÜV SÜD Industrie Service GmbH) and Rüdiger Schröder (Fraport AG) – for actively implementing this version of the guidelines.

Thanks are also due to all those who contributed to this version by providing constructive feedback during the public review.

List of illustrations

Appendix A: Checklist for cyber security in building automation

Number	Request	considered
LP 0: Needs analysis – operating concept		
LP 0.01	Legal/mandatory requirements	yes/no
LP 0.02	Normative requirements	yes/no
LP 0.03	Requirements planning, operator concept and specifications	yes/no

LP 1: Basic determination		
LP 1.01	IT infrastructure	yes/no
LP 1.02	OT infrastructure	yes/no
LP 1.03	Operator concept	yes/no

Appendix B: Explantion of German HOAI

https://archxtecture.com/en/hoai-explained