



BSI Standards Publication

General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)

Part 7: IT security and data protection — User Guide

National foreword

This Published Document is the UK implementation of CLC/TS 50491-7:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/6/-/12, Home Electronic Systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 32867 7

ICS 35.030; 97.120

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2024.

Amendments/corrigenda issued since publication

Date	Text affected

English Version

**General requirements for Home and Building Electronic Systems
(HBES) and Building Automation and Control Systems (BACS) -
Part 7: IT security and data protection - User Guide**

Systèmes Électroniques pour les Foyers Domestiques et
les Bâtiments - Sécurité informatique et protection des
données - User Guide

Elektrische Systemtechnik in Heim und Gebäude - IT-
Sicherheit und Datenschutz - User Guide

This Technical Specification was approved by CENELEC on 2024-10-21.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword	3
Introduction	4
1 Scope	6
2 Normative references	6
3 Terms and definitions	7
4 Abbreviations	13
5 Awareness about the threat landscape	13
5.1 ENISA reference documents	13
6 User guidance for cyber security measures	16
6.1 Recommended hardening measures	16
6.1.1 General	16
6.1.2 General hardening measures	16
6.1.3 Hardening measures for unmanaged networks	16
6.1.4 Hardening measures for managed networks	18
6.2 Generic Risk analysis for managed networks to select the right product security	20
6.2.1 Introduction	20
6.2.2 Risk analysis for the product selection in managed networks	20
6.2.3 Security level classification	22
6.2.4 Device Security class for managed networks	23
6.3 Zoning for logical network segmentation for managed networks	23
6.3.1 Introduction	23
6.3.2 Residential buildings	23
6.3.3 Non-residential buildings	26
6.3.4 Guidelines for device assignment to zones	27
6.3.5 Filtering	27
6.3.6 Mixed Networks	29
6.4 System enrolment and configuration for managed networks	29
6.5 Update management by user for managed networks	29
6.6 Documentation	29
6.6.1 Check lists for Installers, system integrators and administrators	29
6.6.2 Check lists for users	31
6.6.3 Check lists for HBES/BACS manufacturers	31
7 Security level classification for HBES/BACS devices by manufactures	32
7.1 Security class	32
7.2 Security level indication	32
Annex A (normative) Constraints for HBES and BASC risk analysis by solving a constraint satisfaction problem	33
Annex B (informative) Update management (Good practice for the manufacturer)	37
B.1 General	37
B.2 Patches	37
B.3 Minor Updates	37
B.4 Major Updates	38
Annex C (informative) Mapping threat ENISA to OWSAP	39
Bibliography	40

European foreword

This document (CLC/TS 50491-7:2024) has been prepared by CLC/TC TC 205, “Home and Building Electronic Systems (HBES)”.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

This document is part of the EN 50491 series of European Standards — General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) — which will comprise the following parts:

- Part 1: General requirements.
- Part 2: Environmental Conditions.
- Part 3: Electric Safety Requirements.
- Part 4-1: General functional safety requirements for products intended to be integrated in Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS);
- Part 5-1: EMC requirements, conditions and test set-up.
- Part 5-2: EMC requirements for HBES/BACS used in residential, commercial and light industry environment.
- Part 5-3: EMC requirements for HBES/BACS used in industry environment
- Part 6-1: HBES installations — Installation and planning.
- Part 6-3: HBES installations — Assessment and definition of levels.
- Part 7: IT security and data protection - User Guide
- Part 11: Smart Metering — Application Specification — Simple External Consumer Display.
- Part 12: Smart grid — Application specification — Interface and framework for customer.
- Part 12-1: Interface between the CEM and Home/Building Resource manager– General Requirements and Architecture.
- Part 12-2: Interface between the Home/Building CEM and Resource manager(s) – Data model and messaging.
- Future Part 12-3: Home/Building Customer Energy Manager (CEM);
- Future Part 12-4: Resource manager.

Any feedback and questions on this document should be directed to the users’ national committee. A complete listing of these bodies can be found on the CENELEC website.

Introduction

When an HBES/BACS system is installed in a home or building and connected to internet, it should keep the integrity of the connected cyberspace during all the products' lifetime from installation and configuration throughout all operation to the end of life.

Cybersecurity is a continuous process as cyber threats evolve over time. Thus, countermeasures should follow any new threat also after the product has been installed.

The risk of cyber-attacks highly depends on the type of application, type of communication medium and the location where the data are intercepted.

As examples,

- data that is transmitted wireless can be more easily intercepted than data transmitted via wire;
- devices installed in public areas (garden, hallways) or public buildings (schools, hotels, sports complex, ...) are more susceptible to attack than devices that are installed in private and closed areas;
- data that is transmitted to switch on light may be of lesser importance than data containing metering data;
- HBES/BACS connected to cloud servers may be more vulnerable to attack than HBES/BACS devices that are stand-alone, i.e. not connected.

In buildings, two types of networks can be identified: managed and unmanaged, depending on available resources (e.g. network administrator) to ensure cybersecurity update during the products' lifetime.

Examples of applications typically implemented as

- unmanaged network: Home or small office including building control applications, ... where no or insufficient resources (e.g. network administrator) are available for network cybersecurity updates and device access control. Cybersecurity updates at device level may be ensured by device manufacturers, provided the final user has given consent;
- managed networks: larger size installations including building control applications where typically an organization (e.g. an administrator) updates components and the network including its structure: Resources (e.g. integrator, maintenance provider, asset owner) are available for cybersecurity updates.

Cybersecurity updates in HBES/BACS systems installed and connected to internet systems can be managed at two different levels: device level and system level. Updates at device level are possible both for managed and unmanaged networks, while updates at system level is possible for managed networks only.

Considering the two levels, two main areas of application for managed and unmanaged networks can be identified:

- 1) in case of unmanaged networks, for device update one is relying on the device fulfilling the cybersecurity requirements identified by risk analysis for their intended use (e.g. in EU: RED Delegated Act on cybersecurity).
- 2) managed networks apply when:
 - a) an organization is available for updates of the devices and the network; or
 - b) some devices cannot be updated at the level identified by risk analysis: in this case, protection is to be ensured at system level and access to non-updateable devices is to be protected/controlled (e.g. old equipment's that cannot be updated nor substituted with new ones) by moving it out of the trusted security zone; or
 - c) additional cybersecurity requirements are necessary at system level on top of the device level updates (e.g. defining trusted and untrusted zones).

In all cases a), b), c), use of system resources (e.g. devices) should be regulated according to a security policy and permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.

When providing networked system for HBES and BACS, large organizations often have dedicated well trained teams to provide full service cyber security from risk assessment, product selection to the operational management.

For heterogeneous systems and in general smaller systems the cyber security aspect is often not covered so well.

While on the product level several standards exist, there is a gap for the cyber secure system management in this kind of installations.

Risk analysis for each device should be done by manufacturers for the intended use. Accordingly, cybersecurity updates for devices should be made available by manufacturers.

Risk analysis for each system should be done by the system responsible person. Accordingly, cybersecurity updates for systems should be made available and implemented by resources (e.g. end users).

For risk analysis of systems, it is therefore needed that appropriate guidelines are developed in order to support both the end-users (as owner of a home or building) and all the persons involved in the building design, installation, commissioning and operation, to make them aware about the risks, help to assess the risk to find the appropriate minimum-security levels needed or desired for a product and give rules for securing the whole network.

Depending on this security level, appropriate products could then be selected based on the indications given by the suppliers on the product label and/or instruction sheet.

The security level classification gives to the market a classification scheme like the energy classification A, B, C ...

CEN-Cenelec have been requested by European Commission to publish harmonized standards supporting RED Directive and Cyber Resilience Act (CRA). These draft standards are in progress at the time of the publication of this document and when RED / CRA will enter into force this document could be reviewed.

1 Scope

This document provides guidance to set-up and manage/update a cybersecure HBES/BACS connected to Internet.

This document provides:

- 1) categories of HBES/BACS networks related to cybersecurity updates:
 - managed networks;
 - unmanaged networks;
- 2) risk analysis guide for the above-mentioned categories:
 - at device level for both managed and unmanaged networks;
 - at system level for managed ones only.

For manufacturers, the document provides a classification based on the security levels from existing standards (ETSI EN 303 645, EN IEC 62443 (all parts)).

For installers, system integrators and administrators of HBES/BACS this document provides guidance for each responsible actor, as listed below:

- system integrators and administrators:
 - a generic method for assessment of the security risk for each product in the perspective of the overall system. The result of the evaluation gives the minimum required security level on product level corresponding to the manufacturer classification;
 - best practice measures on the system security level;
 - a guide to enhance the maturity level of the cyber security management process.
- installers, system integrators and administrators:
 - a guide to select products to comply with the required security level during configuration and operation.

In some commercial applications, dedicated standards can apply per country that are not covered by this document, e.g.:

- fire (e.g. detection, alarm);
- medical;
- security applications: Intruder alarms, video surveillance, access control;
- critical infrastructure;
- AAL (Active assisted living).

For such applications not covered by this document the specification could be used as guidance.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp/>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

administrator

user who has been authorized to manage security policies/capabilities for a product or system

[SOURCE: EN IEC 62443-4-1:2018, 3.1.4]

3.2

asset owner

individual or company responsible for one or more IACS

Note 1 to entry: In this document IACS is equivalent to HBES / BACS.

Note 2 to entry: The term “asset owner” is used in place of the generic term “end user” to provide differentiation.

Note 3 to entry: This definition includes the components that are part of the IACS.

Note 4 to entry: In the context of this standard, an asset owner also includes the operator of the IACS.

[SOURCE: EN IEC 62443-3-3:2019, 3.1.2, modified, new Note 1 to entry has been added.]

3.3

authenticity

property of data that ensures that the identity of an entity is the one claimed

Note 1 to entry: The entity can be, for example, a user, a process, a system, information.

[SOURCE: IEC 171-08-07]

3.4

availability

property of being accessible and usable upon demand by an authorised entity (with timely response to the intended use case)

3.5

behavioural PII

data that allows to infer behavioral information of a PII principal

Examples:

- status of light, heating;
- current energy consumption;
- presence detection.

3.6

cybersecurity

activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

3.7

conduit

logical grouping of communication channels, connecting two or more zones, that share common security requirements

Note 1 to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

[SOURCE: EN IEC 62443-4-2:2019, 3.1.11]

3.8

gateway

functional unit that connects two computer networks with different architectures and protocols

3.9

HBES/BACS

Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)

combination of HBES/BACS products (including their separate connected/detachable devices) linked together via one or more HBES/BACS networks

Note 1 to entry: Other names used such as “home control network”, “home control systems”, “home and building electronic systems”, “building systems”, “building automation system”, etc. describe types of HBES/BACS systems.

[SOURCE: EN 63044-1:2017¹, 3.1.3]

3.10

HBES/BACS network

interconnection between HBES/BACS products used for communication, that can carry digital data as well as analogue signals

[SOURCE: EN 63044-1:2017², 3.1.2]

3.11

HBES/BACS product

device intended to be used for control, monitoring, operation or management of building services and/or home electronic systems, able to interact via a dedicated HBES/BACS network

3.12

information security

protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional

Note 1 to entry: In addition, properties, such as authenticity, accountability, non-repudiation, and reliability can be involved.

Note 2 to entry: Information security is a broad term that can be used regardless of the form the data can take (e.g. electronic, physical)

[SOURCE: IEC 721-08-57, modified – Notes 1 and 2 to entry have been added.]

¹ As impacted by EN 63044-1:2017/A1:2021.

² As impacted by EN 63044-1:2017/A1:2021.

3.13**integration service provider**

service provider that provides integration activities for an automation solution including design, installation, configuration, testing, commissioning, and handover

Note 1 to entry: Integration service providers are often referred to as integrators or Main Automation Contractors (MAC)

[SOURCE: EN IEC 62443-2-4:2024, 3.1.9]

3.14**integrity**

property of accuracy and completeness

3.15**intended use**

use of a product, process, or service in accordance with the information for use provided by the supplier

[SOURCE: ISO/IEC GUIDE 51:2014, 3.6]

3.16**maintenance provider**

service provider that provides support activities for a HBES / BACS after handover

Note 1 to entry: Maintenance is often distinguished from operation (e.g. in common colloquial language it is often assumed that an automation solution is either in operation or under maintenance). Maintenance service providers can perform support activities during operations, e.g. managing user accounts, security monitoring, and security assessments

3.17**managed network**

installations including building control applications where typically an organization (e.g., an administrator) updates components and the network including its structure, and in which resources (e.g., integrator, maintenance provider, asset owner) are available for cybersecurity updates

3.18**non-sensitive PII**

data requiring more data elements to be linked together to establish an individual's identity

Note 1 to entry: This kind of information is also referred to as linkable data.

Note 2 to entry: On the other hand, sensitive PII can reveal identity on its own or with very limited combined information sources.

Examples:

- voice recording (local and/or cloud);
- first or last name;
- mother's maiden name;
- partial address;
- age range;
- date of birth;
- gender;
- employer.

3.19

operational environment

physical environment of a functional component

3.20

organization

body that is based on the membership of other bodies or individuals and has an established constitution and its own administration

[SOURCE: IEV 901-03-02]

3.21

personal data

information relating to an identified or identifiable natural person

[SOURCE: Article 4 of the EU Data Protection Regulation, (1), modified]

3.22

natural person

data subject

one who may be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

[SOURCE: Article 4 of the EU Data Protection Regulation, (1), modified]

3.23

personally identifiable information

PII

information that can be used to establish a link between the information and the natural person to whom such information relates, or is or can be directly or indirectly linked to a natural person

Note 1 to entry: The “natural person” in the definition is the PII principal (3.23). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: EN ISO/IEC 29100:2020, 2.9, modified]

3.24

PII principal

natural person to whom the personally identifiable information (PII) relates

[SOURCE: EN ISO/IEC 29100:2020, 2.11, modified]

3.25

privacy

right of an entity (normally a person or an organization), acting on its own behalf, to determine the degree to which the confidentiality of their private information is maintained

3.26

unmanaged network

network installed in a building and commissioned by an organization or private owner but not managed by any organization during operation

Note 1 to entry: E.g. network made of plug and play devices.

3.27**security level**

level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit

Note 1 to entry: Also defined as a measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner.

Note 2 to entry: Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

[SOURCE: EN IEC 62443-3-3:2019, 3.1.38, and EN IEC 62443-4-2:2019, 3.1.37, modified]

3.28**security zone**

grouping of logical or physical assets that share common security requirements

Note 1 to entry: All unqualified uses of the term “zone” in this document should be assumed to refer to a security zone.

Note 2 to entry: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical in the sense that they can be comprised of a collection of sub-zones

3.29**sensitive personally identifiable information****sensitive PII****linked data**

PII that can be directly tied to a person's identity, and of which the misuse could cause potential harm to a person

Note 1 to entry: First and last name or credit card number are also referred to as sensitive personally identifiable information, or linked data. This is because this information is directly or almost directly linked to, and can reveal, an individual's identity.

Note 2 to entry: The potential harm its misuse could do to a person ranges from public embarrassment to criminal victimization, if the information is lost, stolen, or disclosed without authorization.

Examples:

- one-to-one voice conversation;
- geo location;
- first and last name;
- home address;
- email address;
- telephone number;
- passport number;
- driver's license number;
- Social Security Number;
- photo of a face;

- credit card number;
- account username;
- fingerprints;
- financial records;
- medical records.

3.30

service provider

organization that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

Note 2 to entry: An organization can be an internal or external organization, manufacturer, etc.

[SOURCE: EN IEC 62443-2-4:2024, 3.1.19, modified]

3.31

system integrator

person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

[SOURCE: EN IEC 62443-4-1:2018, 3.1.34]

3.32

system responsible person

user who has been authorized to manage security policies/capabilities for a product or system

3.33

trusted zone

all devices that are completely under control by the system responsible person in terms of physical access, security updates, user access, user account credentials

3.34

untrusted zone

untrusted devices where the system responsible person has no control in terms of physical access and/or security updates

3.35

zone

collection of entities that represents partitioning of a system under consideration based on their functional, logical, and physical (including location) relationship

Note 1 to entry: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

[SOURCE: EN IEC 62443-4-2:2019, 3.1.49]