ICS 97.120 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA Február 2025

STN P	**Všeobecné požiadavky na bytové a domové elektronické systémy (HBES) a domové automatizačné a riadiace systémy (BACS) Časť 7: IT bezpečnosť a ochrana údajov Používateľská príručka**	**STN P CLC/TS 50491-7** 36 8055

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 01/25

Obsahuje: CLC/TS 50491-7:2024

obsahuje farebné strany

139859

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CLC/TS 50491-7

November 2024

ICS 97.120; 35.030

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

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.