



SLOVENSKI STANDARD
oSIST prEN 50491-4-1:2011
01-maj-2011

Nadomešča:
SIST EN 50090-2-3:2005

Splošne zahteve za stanovanjske in stavbne elektronske sisteme (HBES) in stavbne sisteme avtomatizacije in nadzora (BACS) - 4-1. del: Sistemski pregled - Zahteve splošne funkcionalne varnosti za proizvode, ki so namenjeni za vgradnjo v HBES in BACS

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

Allgemeine Anforderungen an die Elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA) - Teil 4-1: Anforderungen an die funktionale Sicherheit für Produkte, die für den Einbau in ESHG / GA vorgesehen sind

Exigences générales relatives aux systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) et aux Systèmes de Gestion Technique du Bâtiment (SGTB) - Partie 4-1: Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les systèmes HBES/SGTB

Ta slovenski standard je istoveten z: prEN 50491-4-1:2011

ICS:

97.120 Avtomatske krmilne naprave Automatic controls for
za dom household use

oSIST prEN 50491-4-1:2011

en,de

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 50491-4-1

February 2011

ICS 97.120

Will supersede EN 50090-2-3:2005

English version

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

Exigences générales relatives aux systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) et aux Systèmes de Gestion Technique du Bâtiment (SGTB) -
Partie 4-1: Exigences générales de sécurité fonctionnelle pour les produits destinés à être intégrés dans les systèmes HBES/SGTB

Allgemeine Anforderungen an die Elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA) -
Teil 4-1: Anforderungen an die funktionale Sicherheit für Produkte, die für den Einbau in ESHG / GA vorgesehen sind

This draft European Standard is submitted to CENELEC members for CENELEC enquiry.
Deadline for CENELEC: 2011-07-22.

It has been drawn up by CLC/TC 205.

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

1 **Foreword**

2 This draft European Standard has been prepared by the Technical Committee CENELEC TC 205, Home and
3 Building Electronic Systems (HBES). It is submitted to the CENELEC enquiry.

4 This document will supersede EN 50090-2-3:2005.

5 EN 50491-4-1 is part of the EN 50491 series, which will comprise the following parts under the generic title
6 *General requirements for Home and Building Electronic Systems (HBES) and Building Automation and*
7 *Control Systems (BACS):*

- 8 - Part 1: general requirements and overview
- 9 - Part 2: Environmental conditions
- 10 - Part 3: Electrical Safety requirements
- 11 - Part 4-1: General functional safety requirements for products intended to be integrated in Building
12 Electronic Systems (HBES) and Building Automation and Control Systems (BACS)
- 13 - Part 5-1: EMC requirements, conditions and test set-up
- 14 - Part 5-2: EMC requirements for HBES/BACS used in residential, commercial and light industry
15 environment
- 16 - Part 5-3: EMC requirements for HBES/BACS used in industry environment

(standards.iteh.ai)

[SIST EN 50491-4-1:2012](https://standards.iteh.ai/catalog/standards/sist/2debbd6b-e3df-434d-ad91-74aaffac6bc7/sist-en-50491-4-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/2debbd6b-e3df-434d-ad91-74aaffac6bc7/sist-en-50491-4-1-2012>

Contents

17			
18	Introduction		4
19	1 Scope		5
20	2 Normative references		5
21	3 Definitions		5
22	4 General requirements		8
23	4.1 General		8
24	4.2 Method of establishment for the requirements		8
25	5 Requirements for functional safety		10
26	5.1 General		10
27	5.2 Power feeding		10
28	5.3 Environment		11
29	5.4 Life time		11
30	5.5 Reasonably foreseeable misuse		11
31	5.6 Software and communication		12
32	5.7 Remote operations		13
33	Annex A (informative) Example of a method for the determination of safety integrity levels		15
34	Annex B (informative) Hazards and development of necessary functional safety requirements		17
35	Annex C (informative) Some examples of non safety related HBES /BACS applications		23
36	Bibliography		25
37	Figure		
38	Figure A.1 - Risk reduction - General concept		15
39	Tables		
40	Table 1 – Requirements for avoiding inadvertent operations and possible ways to achieve them		14
41	Table A.1 – Example of risk classification of accidents		16
42	Table A.2 – Interpretation of risk classes		16
43			

44 Introduction

45 Homes buildings and similar environments require various electronic devices for several application. These
46 devices when linked via a digital transmission network are called Home and Building Electronic System,
47 (HBES) or Building automation controll system (BACS).

48 Examples of HBES /BACS /BACS applications are the management, of lighting, heating, energy water , fire
49 alarms, blinds , different forms of security , etc.

50 A HBES /BACS network may be based on different communication media as power line, twisted pair, coax
51 cable, radio frequency or infrared and may be connected to external networks like telephone, broad band,
52 television, power supply networks and alarm networks.

53 Several standards of this series serve to implement public interest matters, primarily as reflected in European
54 Commission Directives.

55 HBES products integrated in a HBES /BACS should be safe for the use in intended applications.

56 This European Standard specifies the general functional safety requirements for HBES /BACS following the
57 principles of the basic standard for functional safety EN 61508 and Technical Report R205-012 in particular.

58 This European Standard identifies functional safety issues related to products and their installation. The
59 requirements are based on a risk analysis in accordance with EN 61508.

60 The intention of this European Standard is to allocate, as far as possible, all safety requirements for HBES
61 /BACS products in there life cycle.

62 This European Standard only addresses HBES /BACS /BACS products.

63 This European Standard is addressed to committees that develops or modify HBES /BACS product/system
64 standards or, where not suitable HBES /BACS product standards addressing functional safety exist, to
65 product manufacturer.

SIST EN 50491-4-1:2012

66 HBES /BACS products in this European Standard are for non-safety related applications.7Additional
67 requirements for safety related HBES /BACS will be described, according to EN 61508, in Part 4-1 of the
68 EN 50491 series (under consideration).

69 1 Scope

70 This European Standard sets the requirements for functional safety for HBES /BACS products and systems,
71 a multi-application bus system where the functions are decentralised, distributed and linked through a
72 common communication process. The requirements may also apply to the distributed functions of any
73 equipment connected in a home or building control system if no specific functional safety standard exist for
74 this equipment or system.

75 The functional safety requirements of this European Standard apply together with the relevant product
76 standard for the device if any.

77 This European Standard is used as a product family standard. It is not intended to be used as a stand-alone
78 standard.

79 This European Standard does not provide functional safety requirements for safety-related systems.

80 2 Normative references

81 The following referenced documents are indispensable for the application of this document. For dated
82 references, only the edition cited applies. For undated references, the latest edition of the referenced
83 document (including any amendments) applies.

84	EN 50491-3	General requirements for Home and Building Electronic Systems (HBES) and
85		Building Automation and Control Systems (BACS) - Part 3: Electrical safety
86		requirements
87	EN 61508-4:2001	Functional safety of electrical/electronic/programmable electronic safety-related
88		systems – Part 4: Definitions and abbreviations
89		(IEC 61508-4:1998 + corrigendum 1999)
90	EN 61508-5:2001	Functional safety of electrical/electronic/programmable electronic safety-related
91		systems – Part 5: Examples of methods for the determination of safety integrity
92		levels (IEC 61508-5:1998 + corrigendum 1999)
93	EN 61709:1998	Electronic components - Reliability - Reference conditions for failure rates and stress
94		models for conversion (IEC 61709:1996)
95	CEN/CLC Guide 9	Guidelines for the inclusion of safety aspects in standards (ISO/IEC Guide 51)
96	EN ISO 9000 series	Quality management systems (9000 series)

97 3 Definitions

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

99 3.1

100 architecture

101 specific configuration of hardware and software elements in a system

102 [EN 61508-4:2001, definition 3.3.5]

103 3.2

104 authentication

105 means for certifying that the entity sending a message is what or who it purports to be and confirmation that
106 the message is identical to that which was sent

107 3.3

108 authorisation

109 mechanism to ensure that the entity or person accessing information, functions or services has the authority
110 to do so

111 3.4**112 disturbed communication**

113 where for any reason a message being communicated is incomplete, truncated, contains errors or has the
114 correct format but delivers information which is outside the range of expected parameters for such a
115 message

116 3.5**117 functional safety**

118 freedom from unacceptable risk of harm due to the operation of an HBES /BACS , including that resulting
119 from

- 120 1) normal operation,
- 121 2) reasonably foreseeable misuse,
- 122 3) failure,
- 123 4) temporary disturbances

124 NOTE 1 Definition of EN 61508-4:2001, 3.1.9: part of the overall safety relating to the EUC (Equipment Under Control) and the EUC
125 control system which depends on the correct functioning of the Electrical/Electronic/Programmable Electronic (E/E/PE) safety related
126 systems, other technology safety related systems and external risk reduction facilities.

127 NOTE 2 Definition of IEC TR 61000-2-1 and IEC TS 61000-1-2 (IEC/TC 77) are taken into account.

128 3.6**129 Hamming distance**

130 numbers of bits in which two binary codes differ

131 3.7**132 harm**

133 physical injury or damage to the health of people either directly or indirectly as a result of damage to property
134 or to the environment

135 [EN 61508-4:2001, definition 3.1.1]

136 3.8**137 hazard**

138 a potential source of harm

139 [CEN/CLC Guide 9, respectively ISO/IEC Guide 51:1990]

140 NOTE The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that
141 have a long-term effect on a person's health (for example, release of a toxic substance).

142 [EN 61508-4:2001, definition 3.1.2]

143 3.9**144 hazardous event**

145 situation which results in harm on normal operation or abnormal condition

146 NOTE Definition of EN 61508-4:2001, 3.1.3 and 3.1.4: circumstance in which a person is exposed to hazard(s) which results in harm

147 3.10**148 HBES /BACS Home and Building Electronic Systems**

149 a multi-application bus system where the functions are decentrally distributed and linked through a common
150 communication process

151 NOTE HBES is used in homes and buildings plus their surroundings. Functions of the system are e.g: switching, open loop controlling,
152 closed loop controlling, monitoring and supervising.

153 3.11**154 HBES /BACS product**

155 products consist of devices in the form of hardware, firmware, their associated software and configuration
156 tools, intended to be used in an HBES /BACS

157 **3.12**
 158 **product**
 159 devices in the form of hardware, firmware, their associated software and configuration tools

160 **3.13**
 161 **product documentation**
 162 – the manufacturer's installation and operations literature
 163 – as manufacturer's catalogue, leaflet and other printed or electronic product information
 164

165 **3.14**
 166 **safety related system**
 167 designated system that both
 168 – implements the required safety functions necessary to achieve or maintain a safe state for the EUC, and
 169 – is intended to achieve on its own or with other E/E/PE safety related systems, other technology safety-
 170 related systems or external risk reduction facilities, the necessary safety integrity for the required safety
 171 functions.

172 NOTE 1 The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the
 173 external risk reduction facilities (see EN 61508-4:2001, definition 3.4.3), the necessary risk reduction in order to meet the required
 174 tolerable risk (see EN 61508-4:2001, definition 3.1.6). See also Annex A of EN 61508-5:2001.

175 NOTE 2 The safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action
 176 on receipt of commands. The failure of a safety-related system would be included in the events leading to the determined hazard or
 177 hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to
 178 achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems
 179 and safety-related protection systems, and have two modes of operation (EN 61508-4:2001, definition 3.5.12).

180 NOTE 3 Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or
 181 actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system
 182 (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and
 183 independent systems dedicated to safety.

184 NOTE 4 A safety-related system may
 185 a) be designed to prevent the hazardous event (i.e. if the safety-related systems perform their safety functions then no hazardous
 186 event arises),
 187 b) be designed to mitigate the effects of the hazardous event, thereby reducing the risk by reducing the consequences,
 188 c) be designed to achieve a combination of a) and b).

189 NOTE 5 A person can be part of a safety-related system (EN 61508-4:2001, definition 3.3.1). For example, a person could receive
 190 information from a programmable electronic device and perform a safety action based on this information, or perform a safety action
 191 through a programmable electronic device.

192 NOTE 6 The term includes all the hardware, software and supporting services (for example, power supplies) necessary to carry out
 193 the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in
 194 the safety-related system).

195 NOTE 7 A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable
 196 electronic, hydraulic and pneumatic.

197 [EN 61508-4:2001, definition 3.4.1]

198 **3.15**
 199 **risk**
 200 combination of the probability of occurrence of a harm and the severity of that harm
 201 [CEN/CLC Guide 9, respectively ISO/IEC Guide 51:1990, modified]
 202 [EN 61508-4:2001, definition 3.1.5]

203 NOTE For risk classes see Annex A.

204 **3.16**
 205 **reasonably foreseeable misuse**
 206 the use of a product, process or service under conditions or for purposes not intended by the supplier, but
 207 which may happen, induced by the product, process or service in combination with, or as result of, common
 208 human behaviour
 209 [EN 61508-4:2001, definition 3.1.11]

210 **3.17**211 **safety function**

212 function to be implemented by an E/E/PE safety related system, other technology safety-related systems or
213 external risk reduction facilities, which is intended to achieve and maintain a safe state for the EUC, in
214 respect of a specific hazardous event (see EN 61508-4:2001, definition 3.4.1)

215 [EN 61508-4:2001, definition 3.5.1]

216 **4 General requirements**217 **4.1 General**

218 Functional safety of a system relies upon both the performance of the network, and upon the performance of
219 the connected HBES /BACS products:

- 220 1) failure of either the network or any other part of HBES /BACS system shall not cause the system, the
221 products, or the controlled equipment to become unsafe;
- 222 2) whilst in operation, individual HBES /BACS products shall not rely solely upon the system for their safe
223 operation;
- 224 3) while in operation, the systems interaction of any product(s) with any other product(s) shall not result in
225 unsafe operation of the system.

226 **4.2 Method of establishment for the requirements**

227 For specification of the functional safety requirements the life-cycle used in EN 61508 was followed:

- 228 1) concept phase of products;
- 229 2) application environment;
- 230 3) identification of hazards and hazard events;
- 231 4) hazard and risk analysis, risk reduction measures;
- 232 5) realisation of risk reduction measures;
- 233 6) validation;
- 234 7) maintenance;
- 235 8) installation and commissioning;
- 236 9) decommissioning.

237 The Product Technical Committees and/or developers shall take the requirements of this European Standard
238 into account in the product safety requirements, but it is not necessary to go into the EN 61508 process itself.

239 **4.2.1 HBES application environment**

240 The HBES /BACS application environment is taken into account.

241 4.2.2 Sources of hazards

242 The following sources of hazards have been considered:

- 243 1) material and construction;
- 244 2) reliability;
- 245 3) normal operation;
- 246 4) unintentional interaction with other products;
- 247 5) interaction with other HBES /BACS products;
- 248 6) abnormal conditions;
- 249 7) foreseeable misuse, including the download of unauthorised and malicious code;
- 250 NOTE This includes unintentional software modifications.
- 251 8) life time;
- 252 9) environment.

253 4.2.3 Hazardous events

254 The following hazardous events have been taken into account for the analysis (the bus and mains (230
255 V/400 V) have been considered):

- 256 1) power failure;
- 257 2) short circuit of bus line;
- 258 3) overvoltage on the bus line;
- 259 4) overvoltage on the mains;
- 260 5) insulation damage (temperature, surge, mechanical);
- 261 6) wrong connection;
- 262 7) over temperature;
- 263 8) fire;
- 264 9) mechanical shock, vibration;
- 265 10) corrosion;
- 266 11) electromagnetic disturbance;
- 267 12) disturbed communication;
- 268 13) pollution;
- 269 14) end of life time of a component/products;
- 270 15) reasonably foreseeable misuse;
- 271 16) software failure;
- 272 17) overload;
- 273 18) loss of reliability;
- 274 19) breakdown of material (mechanically);
- 275 20) inappropriate design/construction;
- 276 21) switching of damaged equipment and subsystems;
- 277 22) remote control;
- 278 23) command from two sources to one product (e.g. actuator);
- 279 24) system failures.