

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Building intercom systems –
Part 3-2: Application guidelines – Advanced security building intercom systems
(ASBIS)**

**Systèmes d'interphone de bâtiment –
Partie 3-2: Lignes directrices d'application – Systèmes d'interphone de bâtiment
à sécurité avancée (ASBIS)**

IECNORM.COM : Click to view the full PDF of IEC 62820-3-2:2018



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2018 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Building intercom systems –
Part 3-2: Application guidelines – Advanced security building intercom systems
(ASBIS)**

**Systèmes d'interphone de bâtiment –
Partie 3-2: Lignes directrices d'application – Systèmes d'interphone de bâtiment
à sécurité avancée (ASBIS)**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.320

ISBN 978-2-8322-5357-1

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references	9
3 Terms, definitions and abbreviated terms	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	18
4 Requirements for the ASBIS and ranges of application	18
4.1 General.....	18
4.2 Selected examples for ASBIS applications	19
4.2.1 General	19
4.2.2 ASBIS for access communication	19
4.2.3 ASBIS in schools and other education institutions.....	19
4.2.4 ASBIS in authorities and offices.....	19
4.2.5 ASBIS in the legal system.....	19
4.2.6 ASBIS at railway stations and airports	20
4.2.7 ASBIS in shopping centres	20
4.2.8 ASBIS in Public residential buildings	20
4.2.9 Other examples	20
4.3 ASBIS operational flow chart for emergency and danger communication.....	20
4.4 System structure.....	21
4.5 Tasks of an ASBIS.....	22
4.5.1 General	22
4.5.2 Safety / security tasks.....	22
4.5.3 Tasks for improving day-to-day processes (schools, universities, etc. in the example here).....	22
4.5.4 Day-to-day communication	22
4.6 Safety / security grades	22
4.7 Components of an ASBIS.....	25
4.7.1 Electronic measures	25
4.7.2 Mechanical protection measures.....	26
4.7.3 Other options.....	26
4.8 Requirements for system components and interfaces.....	26
4.8.1 Basic requirements	26
4.8.2 Requirements for the system networks	30
4.8.3 System control centre (ASBIS-server).....	30
4.8.4 Intercom unit as source (VCU, URU)	31
4.8.5 Intercom unit as receiver (SMU, URU)	31
4.8.6 Intercom unit as source and receiver (URU, SMU).....	31
4.8.7 Emergency and danger warning equipment (ASBIS warning equipment).....	31
4.8.8 Operational indicators and alarms	33
4.8.9 Power supply.....	34
4.8.10 Electrical cables	35
4.8.11 Interface to to other safety/security systems	35
4.9 Other requirements	36
4.9.1 Implementation of services	36

4.9.2	Arrangement and distribution of call terminals	36
4.9.3	Distinguishing between a call and an emergency call.....	36
4.9.4	Alarm groups	36
4.9.5	Internal alarm and instructions on how to proceed	36
4.10	General device and system requirements.....	37
4.10.1	General requirements	37
4.10.2	Protection against environmental influences	37
4.10.3	Onsite Influences.....	37
4.10.4	Functional safe guard	37
4.10.5	Operating safety/security	38
4.10.6	Indicators	39
4.10.7	Messages	39
4.10.8	Structure	39
4.10.9	Processing messages.....	40
5	Commissioning / delivery	40
5.1	General.....	40
5.2	General information	40
5.2.1	Documentation	40
5.2.2	Commissioning	41
5.3	Functional interaction of the system components	41
5.4	Options	41
6	Operation and maintenance	41
6.1	General.....	41
6.2	Operational test	42
6.3	Commissioning/repairs.....	42
6.4	Replacing the battery and rechargeable battery	42
6.5	Software updates	42
7	Tasks and responsibilities.....	42
7.1	General information	42
7.2	Organization in charge (responsible organization).....	44
7.3	Top tier of management	44
7.4	Technical Risk Management	44
7.4.1	General	44
7.4.2	Specifications in the TRM file	45
7.5	ASBIS-user	46
7.6	Trained person.....	46
7.7	Planner (technical planners, architect, consultant, general planners)	46
7.8	Installer.....	47
7.9	Maintenance staff	47
7.10	Manufacturer of the system components and the IT network	48
8	Change management.....	48
8.1	General information	48
8.2	Change process	48
Annex A (informative)	Information on voice announcements	50
A.1	General information	50
A.2	Examples of announcement texts.....	50
Annex B (informative)	Advanced security building intercom systems (ASBIS)	51

Annex C (informative) Relationship between TRM and ORM as part of an overall risk management related to an ASBIS application	52
C.1 General information	52
C.2 Graphical description	52
Annex D (informative) Table: Help-tables for risk assessment.....	53
D.1 Risk identification related to ASBIS applications	53
D.2 Example table for assessing the likelihood of an emergency / dangerous situation	54
D.3 Protection target definitions as part of the planning for an ASBIS.....	55
D.4 Classification of the protections demanded	55
Annex E (informative) Assisting organizational issues to reduce emergency, danger and hazard event duration	56
E.1 Labelling doors and buildings.....	56
E.2 Training	56
Bibliography.....	57
Figure 1 – Interdependence between human/organizational and technical level at an ASBIS used for emergency and danger reaction purposes	20
Figure 2 – System structure of an ASBIS	21
Figure 3 – Classification of the grade.....	24
Figure 4 – Example of an emergency and danger warning equipment as a single module.....	32
Figure 5 – General information of interrelationships and responsibilities	43
Figure C.1 – Overview of interrelationship between TRM and ORM as parts of the overall risk management	52
Table 1 – Requirements for the ASBIS and its intercom units depending on the grade.....	27
Table 2 – Requirements for the ASBIS power supply	35
Table D.1 – Risk identification related to typical dangers	53
Table D.2 – Table to identify environmental conditions for assessing the likelihood of an emergency / dangerous situation	54
Table D.3 – List of typical protection targets to identify the risk relevance.....	55

INTERNATIONAL ELECTROTECHNICAL COMMISSION

BUILDING INTERCOM SYSTEMS –**Part 3-2: Application guidelines –
Advanced security building intercom systems (ASBIS)****FOREWORD**

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62820-3-2 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
79/601/FDIS	79/605/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62820 series, published under the general title *Building intercom systems*, can be found on the IEC website.

This International Standard is to be used in conjunction with IEC 62820-3-1.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC 62820-3-2:2018

INTRODUCTION

This document has become necessary because

- Both the application fields and importance of Advanced Security Building Intercom Systems (ASBIS) have increased;
- different events, emergencies, dangers and hazards needs various responses and reactions, which have to be verified by voice communication in advance;
- a detailed guide is needed for companies and operators with no previous knowledge of ASBIS.

In particular, this document is targeted at police, insurance companies, planners, architects, manufacturers and specialist security system companies, construction clients, owners, operators, ASBIS-users and residents of all kind of buildings.

This document covers applications for higher risks such as accidents, emergencies, dangers, mass attack, terror, school shootings, terrorist attacks, bombs threats, earthquakes, floods, etc.

An ASBIS is used to receive advanced access communication events (visitor-calls, user-receiver-calls, security-management-calls) as well other events (emergency, danger and hazard alarms), forward them to a technical receiver and present them appropriately at a support agency (e.g. Security Management Unit). On acknowledging receipt, the support agency assumes responsibility for verifying and initiating measures defined in accordance with the Technical Risk Management file. The acknowledgement is displayed at the point where action is initiated.

A daily use of other ASBIS applications (e.g. Annex B) is suggested for ASBIS-users training as well as system availability in grade 1 of IEC 62820-3-2. The frequency of daily use is a kind of system check to indicate the system availability.

IECNORM.COM : Click to view the full pdf of IEC 62820-3-2:2018

BUILDING INTERCOM SYSTEMS –

Part 3-2: Application guidelines – Advanced security building intercom systems (ASBIS)

1 Scope

This part of IEC 62820 describes the basic application requirements for Advanced Security Building Intercom Systems (ASBIS) in public and private buildings with advanced safety and security needs. ASBIS are also used to meet the requirements of the Local Regulations of Workplace Safety and/or other relevant local regulations, in particular, protecting the life and limb of employees and all persons in the building, taking into account the inclusion of people with disabilities (e.g. to achieve barrier-free access or calls for help) where required by local applicable law.

This document applies for planning, installation, commissioning, handover, operation and maintenance of ASBIS, for the transmission of emergency, danger and hazard audio messages and/or other operational indications to an assisting authority for remote assessment and for implementing suitable intervention-, protection- and rescue measures. Additional information can also be transmitted and the system can be used in day-to-day work for all communication needs. ASBIS also feature in high availability for end unit monitoring and system monitoring.

Advanced Security Building Intercom Systems (ASBIS) are used for rapid emergency, danger and hazard calls, verification by voice communication, warning of a danger, rapid notification of the responsible emergency / intervention services and for sending voice instructions and/or other operational indications on how to proceed. Requirements for a suitable concept are a prior risk assessment and a definition of the protection target. The Technical-Risk Management (TRM) and Organizational Risk-Management (ORM) have to work out a common workflow strategy in conjunction with the corresponding system requirements, to achieve the residual risks. This document provides requirements for the technical risk-management as well as comments and recommendations for the organizational risk-management.

The present application document for an ASBIS describes among others, the technological processes and responsibilities involved in supporting all processes, from detecting an event (visitor-call, emergency, danger, hazard) until that event is finally dealt with. It includes TRM, the defining protection goals and organizational procedures, and the necessary requirements for a TRM file. This document defines three different safety/security grades, with the product requirements for each. Selecting products which can be deployed as technical resources as part of an ASBIS is the responsibility of the TRM to be employed.

This document, taken together with an ASBIS, also defines the associated tasks, responsibilities, and activities. These are elements of a holistic TRM process to meet the protection goals for personnel safety/security, efficiency and effectiveness, data- and system security. This document does not specify any risk levels. In particular, it does not define any acceptable residual risks. The TRM and ORM are of equal importance in the overall risk management (see Annex C).

This document defines the technical requirement profiles for ASBIS for three safety/security grades. It is the TRM responsibility to determine the grade involved, based on their risk assessment, selecting whichever grade best matches the risk identified, allowing for an acceptable residual risk. The annexes to this document will assist in assessing risks.

This document also describes the process for creating, maintaining and updating a TRM file. The risks are listed, assessed and residual risks are defined in this document. The analysed results define the extent and the structure of the ASBIS. An ASBIS is a part of a whole solution for managing certain events, such as emergencies or crises.

The structure and operation of an ASBIS demands TRM over the entire life cycle of the ASBIS. The monitoring of an ASBIS over its life cycle is a part of the TRM file.

This document is intended to aid implementation of legal and miscellaneous requirements.

Depending on the requirements of the Local Disabilities Act, or the relevant regulation for people with disabilities, an ASBIS can be used for the implementation of such local regulations, which means, communication in two different formats such as light and sound (two-meaning principle).

This document applies in its entire scope for other remote signalling and information technology systems if they include the functions of Advanced Security Building Intercom Systems (ASBIS).

This document does not replace any relevant standards for safety/security systems or other relevant systems. Such systems can however be integrated within an ASBIS taking these standards into account.

If the regulations in standards for such systems contradict this document, the TRM weighs up the regulations with each other, assesses them, and documents them in the decision as a deviation from the standard in the TRM file.

The recommendations and requirements of IEC 62820-3-1 are mandatory for this document. Exceptions are to be decided by the TRM and to be documented in the TRM file.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE The following standards are named as known. If standards in the following list are not named IEC or ISO, the relevant relevant IEC/ISO standards are unknown; use available local standards instead.

IEC 60268-16:2011, *Sound system equipment – Part 16: Objective rating of speech intelligibility by speech transmission index*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 60839-5-1:2014, *Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements*

IEC 60839-5-2:2016, *Alarm and electronic security systems – Part 5-2: Alarm transmission systems – Requirements for supervised premises transceiver (SPT)*

IEC 60839-5-3:2016, *Alarm and electronic security systems – Part 5-3: Alarm transmission systems – Requirements for receiving centre transceiver (RCT)*

IEC 60839-7-12:2001, *Alarm systems – Part 7-12: Message formats and protocols for serial data interfaces in alarm transmission systems – PTT interfaces for dedicated communications channels using ITU-T Recommendation V.23 signalling*

IEC 61000-6-1, *Electromagnetic compatibility (EMC) – Part 6-1: Generic standards – Immunity for residential, commercial and light-industrial environments*

IEC 61000-6-3, *Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments*

IEC 62262:2002, *Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)*

IEC 62599-1:2010, *Alarm systems – Part 1: Environmental test methods*

IEC 62599-2, *Alarm systems – Part 2: Electromagnetic compatibility – Immunity requirements for components of fire and security alarm systems*

IEC 62642-1:2010, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

IEC 62820-1-1:2016, *Building intercom systems – Part 1-1: System requirements – General*

IEC 62820-1-2:2017, *Building intercom systems – Part 1-2: System requirements – Building intercom systems using the internet protocol (IP)*

IEC 62820-2, *Building intercom systems – Part 2: Requirements for advanced security building intercom systems (ASBIS)*

IEC 62820-3-1, *Building intercom systems – Part 3-1: Application guidelines – General*

IEC 62851-2, *Alarm and electronic security systems – Social alarm systems – Part 2: Trigger devices*

IEC 62851-3, *Alarm and electronic security systems – Social alarm systems – Part 3: Local unit and controller*

ISO/IEC 17065, *Conformity assessment – Requirements for bodies certifying products, processes and services*

ISO 31000, *Risk management – Principles and guidelines*

ISO/IEC 31010, *Risk management – Risk assessment techniques*

ISO 7240-11:2011, *Fire detection and alarm systems – Part 11: Manual call points*

ITU-T P.800, *TELEPHONE TRANSMISSION QUALITY: Methods for objective and subjective assessment of quality*

EN 50134-2:2016, *Alarm systems. Social alarm systems. Part 2: Trigger devices (or equivalent IEC standard)*

EN 50134-3:2012, *Alarm systems – Social alarm systems – Part 3: Local unit and controller (or equivalent IEC standard)*

DIN VDE 0833-1 (VDE 0833-1):2009-09, *Alarm systems for fire, intrusion and hold-up – Part 1: General provisions (or equivalent IEC standard)*

3 Terms, definitions and abbreviated terms

NOTE In the following, instead of repeating “emergency, danger and hazard”, only the word “danger” is used to represent all three terms.

3.1 Terms and definitions

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

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

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

3.1.1

acceptance test

documented joint inspection of the ASBIS by ASBIS qualified person/operator/ manager with highest level of management of the ASBIS TRM, in the form of a visual and functional check and a check on the completeness of the documents, as a prerequisite for subsequent handover to the operator and commissioning

3.1.2

alarm equipment

item of equipment which is used to warn persons or call up help to avert the danger

Note 1 to entry: The alarm equipment may be a part or an item of additional equipment in an ASBIS.

3.1.3

alarm signal

local alarm for danger avoidance

EXAMPLE Acoustic and/or optical and/or haptic signals and/or vocal announcements and/or text operational indicators.

3.1.4

alarm transmission system

alarm transmission device or network used to send information concerning the state of one or more alarm systems and ASBIS's in a monitored building to one or more operating- and displaying device(s) from one or more alarm receiving centres

Note 1 to entry: An alarm transmission system may comprise more than one alarm transmission path.

3.1.5

alarm precheck

checking an alert to see whether it was the result of a dangerous situation (e.g. by means of a pre-check on-site, remote testing through voice communication and/or transmission of situation images)

3.1.6

alternative power source

energy source which is in the position to supply the ASBIS in advance for a specific amount of time when the main power source is not available

3.1.7

ASBIS alarm

warning of an existing danger to persons, property, or the environment, triggered by an alarm state, as well as the demand to call up help to avert the danger

3.1.8

ASBIS alarm condition

status when a potentially or acutely dangerous situation exists which requires the attention or response from an intervention service

3.1.9

ASBIS-user

person with the entitlement to use the ASBIS

3.1.10

ASBIS qualified person

ASBIS specialist

person who can assess the allocated work or identify potential dangers due to their technical training, knowledge and experience and familiarity with relevant equipment, standards, requirements and guidelines.

Note 1 to entry: Operation of the ASBIS requires persons to be qualified in electrical engineering in the area of message-, information-, microprocessor-, measurement- and control- or general electrical engineering; evidence shall be provided of the other areas and knowledge of the danger alarm systems. Knowledge on the assessment of building prerequisites, fire protection in buildings or mechanical safety/security systems, the affect of room usage, and the limits to the use of notification capture.

Note 2 to entry: A position in a relevant work area lasting several years can be applied to the assessment of the specialist training

3.1.11

assisting authority

person commissioned by the operator of the ASBIS or a centre manned at all times (e.g. emergency and service control centre as the assisting authority), which receives the alarms, alerts and information from the building, checking this information before passing it on and instructs others to take appropriate action, e.g. to monitor or conduct a search of the building

3.1.12

back-up duration

length of time for which the alternative power source can maintain full functionality of the ASBIS

3.1.13

commissioning

final test, signing off and activation of ASBIS by the owner, the organization in charge or the TRM

3.1.14

communication

switching or sending of signals or information between system components and persons

Note 1 to entry: For an ASBIS system this will include but not be limited to:

- a) the transfer of useful signals from the source to the receiver and between all technical components / functions;
- b) the transfer of check and acknowledgement signals from the source to the receiver via all necessary system components;
- c) the transmission of voice, text and/or image(s) between source and receiver;
- d) a voice communication (voice dialogue) from the trigger to the assisting authority. via all necessary system components;
- e) a voice communication (voice dialogue) from the assisting authority to the trigger and the intervention service via all necessary system components.

3.1.15

data and system security

operating state of an ASBIS, in which important information (data and systems) have adequate protection against impairments to confidentiality, integrity, and availability

Note 1 to entry: Data- and system security shall be ensured by guidelines, manuals, infrastructure and services which have been developed to protect important information and systems, that are used to record, transmit, save and apply information in order to best meet the goals of the organization.

3.1.16**emergency call**

call for help or information in case of an emergency (e.g. first aid)

3.1.17**emergency and service control centre**

continuously manned location commissioned by the operator which receives remote alarms, alerts, and information from a monitored building, checking them before passing them on, and taking and instructing others to take necessary action, such as monitoring the building and/or instructing an intervention, and documenting it

3.1.18**evaluation**

checking of equipment or a procedure by qualified personnel to assess its suitability for the desired purpose

3.1.19**false alarm****unwanted alarm**

alarm which is not indicative of danger

3.1.20**fault**

state of a unit, e.g. an ASBIS or an individual system component, characterised by its inability to meet a required function, for whatever reason

3.1.21**fault message**

message indicating that there is a deviation from the specified functionality of an ASBIS or an ASBIS system component

3.1.22**emergency conference****help call conference**

calling appropriate persons which are required to mitigate or end conflicts between persons

3.1.23**integrator****ASBIS server**

system component used to meet a technical function of an ASBIS which is used as a control unit including distribution unit (e.g. switch) for the processing, transfer, diversion and documentation between source and receiver, which can be integrated split, centrally or distributed or in the source or recipient

3.1.24**internal alarm**

alarm signal in the building after ASBIS functions are triggered for warning those present in the affected area with the aim of putting in process the required actions (e.g. self-help, self-rescue) and to notify an assisting authority where applicable

3.1.25**intervention**

action used to avoid or limit personal injury, damage to property or assets

3.1.26

intervention service

person or persons who instigate measures to avert danger after an alert or an alarm to prevent or limit personal injury and/or damage to property or assets

3.1.27

inspection

measures used to establish and assess the actual state of an ASBIS including determining the causes of increased wear and devising preventative measures for future use

3.1.28

installer

specialist, organization, company with ASBIS-qualified personal which is responsible for the proper installation, commissioning and documentation of the ASBIS and for instructing ASBIS-users

3.1.29

immediate

carried out without an intentional delay, e.g. an inspection or repair

3.1.30

main power source

energy source which supplies the ASBIS under normal operating conditions

3.1.31

maintenance staff

specialist company with ASBIS qualified persons which can carry out all maintenance work, inspections, extensions and modifications and which provide acceptable cover 365 days a year including holding necessary spares

3.1.32

maintenance

combination of all technical and administrative measures and measures by management during the life cycle of an ASBIS to ensure its 100 % availability in either a fully functional or agreed fall-back state

3.1.33

call terminal

any Intercom Terminal, URU, SMU, VCU and any other Intercom unit and single call buttons, etc.

3.1.34

network

system(s), comprising communication networks and communication connections used to enable transmissions between two or more specific transmission nodes via cables, fibres or wireless or any other suitable medium

3.1.35

mass attack

act of violence when a perpetrator- either randomly or with intent- has injured or killed a number of persons (usually not known initially) in particular with weapons, explosives, dangerous tools or through the extraordinary use of force, or when such an event is anticipated and can impact on other people

3.1.36

operational indicators

information (in acoustic, visual or any other form) which helps the ASBIS-user operate the ASBIS

3.1.37**operational test**

activity to be carried out after installing, expanding, modifying or after repair work as a means of confirmation that the ASBIS is able to meet the required function

3.1.38**organization in charge****responsible organization**

organization (or staff employed by an organization) which carries legal responsibility for the ASBIS and which may bear one, more or all the costs of installing, operating and maintaining same

EXAMPLES A ministry, war cabinet, municipal authority, municipal executive board, or employees or contractors commissioned as appropriate.

3.1.39**process**

set of interdependent activities which, when activated, lead to the desired result(s)

Note 1 to entry: The term 'activities' comprises the application of resources.

[SOURCE: ISO 14971:2007, 2.13, modified – The phrase "transforms inputs into outputs" has been replaced by "when activated, lead to the desired result(s)".]

3.1.40**protection goals**

target safety/security level with kinds of measures with respect to expected dangers taking personnel safety/security, effectiveness/efficacy, data and system security into account, whereby the goals meet the targeted final state, though leave the means of achieving this goal open

3.1.41**receiver****recipient**

system component or satisfying a technical function of an ASBIS which receives alarm signals from the integrator, displays them and passes them on to an assisting authority and also passes on responses received from this authority to the integrator with control and communication signals

3.1.42**reminder signal**

signal, e.g. an acoustic signal which draws the ASBIS-users attention to the limited functionality of the ASBIS at regular intervals, e.g. to a shut-down function, to warning devices which have been switched off, etc.

3.1.43**remote alarm**

alarm from an assisting authority not present on site, e.g. fire brigade, police, or safety/security company

3.1.44**remote alarm forwarding device**

device for passing on (forwarding) remote alarm, alerts and information to a commissioned assisting authority

3.1.45**repairs**

step taken to return a faulty ASBIS system to full functionality, not to include modifications or additions to the system

3.1.46

residual risk

risk which remains after carrying out measures to manage the risk

[SOURCE: ISO 14971:2007, 2.15, modified – The definition has been redrafted.]

3.1.47

risk

combination of the probability of the occurrence of damage and the severity of this damage

[SOURCE: ISO 14971:2007, 2.16, modified – "harm" has been replaced by "damage".]

3.1.48

risk analysis

systematic use of available information for identifying any kind of danger and to assess resulting risks

[SOURCE: ISO 14971:2007, 2.17, modified – "hazards" and "the risk" have been replaced by "any kind of danger" and "resulting risks" respectively.]

3.1.49

risk assessment

part of a TRM process according to ISO 31000 which contains risk identification, risk analysis and risk evaluation

3.1.50

risk control

process in which decisions are made and action taken to reduce the risks to specified areas or are held to it

[SOURCE: ISO 14971:2007, 2.19, modified – The definition has been redrafted.]

3.1.51

specialist company

firm responsible for planning, installing and commissioning of the ASBIS which has at least one employee qualified in ASBIS (ASBIS qualified person)

3.1.52

sabotage

intentional physical, cyber or other damage to an ASBIS or its system components

3.1.53

safety concept

security concept

the overall, pre-defined basis on which organizational, personnel, technical and constructional steps are taken towards providing building protection or to avert dangers

Note 1 to entry: The safety/security concept shall contain -at a minimum -information, about the use of the building, the risk for the building, the protection goals of the ASBIS, such as to prevent personal injury and/or damage to property, the areas to be monitored with automatic alarm systems, the non-automatic alarms to be activated by persons, to any existing control functions, personnel protection measures, alarm equipment, and alarm zones and assisting centres.

3.1.54

signal transducer

device which generates and issues acoustic and/or visual signals

3.1.55**source**

system component which can automatically or manually trigger an ASBIS-alarm condition, and receive and display acknowledgements, issuing signals or enabling voice communication

3.1.56**system component**

individual items of equipment which together make up an ASBIS

3.1.57**TRM file**

set of records and other documents created during TRM

[SOURCE: ISO 14971:2007, 2.23, modified – The main term "risk management file" has been replaced by "TRM file" and the definition has been redrafted.]

3.1.58**technical risk manager**

person responsible for the TRM of an ASBIS (e.g. Certified Security Manager or similar)

3.1.59**transmission device**

part of an alarm transmission system for danger alerts; used to pass on notifications

3.1.60**transmission path**

external connection of system components used to send information or send messages from an ASBIS

Note 1 to entry: The transmission path may also be used as a means of energy supply.

3.1.61**technical risk management****TRM**

systematic application of management strategies, procedures and practical experience to the tasks of analysis, evaluation, management and monitoring of risks

[SOURCE: ISO 14971:2007, 2.22, modified – The main term "risk management" has been replaced by "technical risk management" and the definition has been redrafted]

3.1.62**top tier of management**

person or group of persons appointed by the organization in charge to be the overall management and client who is responsible for the ASBIS at the highest level and shall approve the TRM file and the residual risk resulting from it (e.g. the local authority/office leader, director/school head or employer with relevant employees, general manager, senior manager)

3.1.63**trained person**

person who has been given training by a qualified specialist of the ASBIS (ASBIS qualified person) in tasks needed to operate an ASBIS and who is in the position to carry out the operation of the ASBIS independently

Note 1 to entry: These tasks include the execution or instructing others to execute protective measures to avert danger by shutting down or disrupting system components and instructing others to remedy faults or repair impairments.

3.1.64

transmission of images

in the case of alarm, sending images of the area from which it was generated with the specified transmission procedure and the specified file format (image and, where applicable, control) in order to validate the alarm, confirm the exact location, and to enable/support measures by intervention services

3.1.65

verification

proof on the accuracy, facts, cause of an alarm (establishment of the truth), by observing, checking the cause of the trigger/process of an alarm, by means of a personnel visual review, communication or by transmitting images of the situation, in cases of doubt, also by working out the triggering process, to make a distinction between a false alarm and a genuine dangerous situation

3.1.66

voice alarm system

system used to issue alarms and instructions through tone signals and voice announcements and which allows live announcements after automatic control by a different danger warning

3.1.67

workday

day on which work is performed

3.2 Abbreviated terms

The following abbreviations are used:

TRM	Technical Risk Management
ORM	Organizational Risk Management
GRM	General Risk Management
RM	Risk Management
VSS	Video Surveillance System
ASBIS	Advanced Security Building Intercom Systems
SMU	Security Management Unit
VCU	Visitor Call Unit
URU	User Receiver Unit

4 Requirements for the ASBIS and ranges of application

4.1 General

The recommendations and requirements of IEC 62820-3-1 are mandatory for this document. Exceptions are to be decided by the TRM and to be documented in the TRM file.

ASBIS shall be planned, installed, operated, modified, and maintained according to the specifications in IEC 62820-2 and this document.

With different alarm organizations, a situation inquiry is needed after an alarm message in order to verify the cause of the alarm and to implement the various intervention-, rescue- and protection measures as quickly as possible, depending on the cause (e.g. in the case of a fire or a mass attack). As a result, there is the need for a quick situation inquiry to implement the correct intervention-, protection and rescue measures. A situation inquiry can also uncover mistakes and false alarms. It avoids taking unnecessary measures. ASBIS, described in this document, are designed especially for the task of situation inquiry. The assisting authority can

use these systems to clarify and get information about the situation with the persons affected on site who triggered the call or emergency call to take suitable measures.

ASBIS are designed to cover most of all advanced security communication needs in all kinds of buildings. Examples of the range of all possible advanced security communications for the applications are described in Annex B.

- All security communication applications in a dedicated building can be realized by an ASBIS individually or in a common, integrated, ASBIS solution. The integration of security applications for daily use (e.g. access communication) and security applications for use in very seldom situations (e.g. terror acts) together in only one ASBIS, is very helpful.
- The frequency of daily use is a kind of system check to indicate the system availability
- The daily use can avoid training for system operation in seldom emergency situations
- An ASBIS for 2 or more different security applications needs only one common data cable network.

4.2 Selected examples for ASBIS applications

4.2.1 General

All functionalities of the following examples are typically integrated in one ASBIS application.

4.2.2 ASBIS for access communication

Typical building locations for daily communication needs shall be equipped with intercom units which are part of the overall security concept, (e.g. doors, gates, parking entrances and exits, vending machines, interlocking doors, information terminals, internal communication points, assembly points).

ASBIS shall be capable of full integration to or incorporation of other disciplines such as access control systems, video Surveillance systems, public address systems, fire alarm systems and disabled refuge systems, etc.

4.2.3 ASBIS in schools and other education institutions

For instance, use of an alarm system, as per the school construction guidelines with the depiction of all phases in the process chain from the (alarm-) message to rescue (inclusion/evacuation) and use of an emergency and danger response system (specially for mass attacks and other situations) with emergency monitoring and emergency conference and for day-to-day use in school, e.g. for interjections, paging, break signal communication and school communication.

4.2.4 ASBIS in authorities and offices

Communication, in the event of an emergency or danger, to allow assistance by internal personnel via an internal alarm (here without an acoustic alarm at the trigger location) or assistance by external intervention services via a remote alarm with emergency monitoring and emergency conference.

4.2.5 ASBIS in the legal system

Communication in the event of an emergency or danger, to allow assistance by internal personnel via an internal alarm (here without an acoustic alarm at the trigger location) or assistance by external intervention services via a remote alarm with emergency monitoring and emergency conference. Also calling witnesses and the cell communication.

4.2.6 ASBIS at railway stations and airports

Emergency and emergency call devices with wheelchair access (in particular, note the following: volume, voice intelligibility and barrier-free access).

4.2.7 ASBIS in shopping centres

Help-point Intercom with service-centres, emergency-intercom in rest rooms for persons with disabilities. Terror-Alarm-Intercom with direct connection to, and communication with intervention forces. Emergency-help-point intercom with direct connection to, and communication with ambulance. Interface to public address system. Elevator Emergency communication.

4.2.8 ASBIS in Public residential buildings

Depending on the use of the building, a combination of the functionalities and applications mentioned in the examples above can be efficient solutions for Emergency and dangerous situations as well as in combination with the use for fast inhouse communication and silent alarm messaging in individual dangerous situations.

4.2.9 Other examples

Annex B is showing a list of typical ASBIS applications for different buildings. The more different applications and functions that are integrated in one system, the higher the degree of utilization of the system. A higher degree of utilization can lead to lower residual risks.

4.3 ASBIS operational flow chart for emergency and danger communication

The workflow of a danger event reported from an intercom unit can be split into two levels: the "human/organizational level" and the "technical level"; these are interdependent. Figure 1 shows the different measures taking the duration of the event into account. Each human/organizational measure requires a corresponding technical measure and vice versa.

All human / organizational workflow (upper level of the arrow) shall be specified by the organization in charge and/or by the top tier of management.

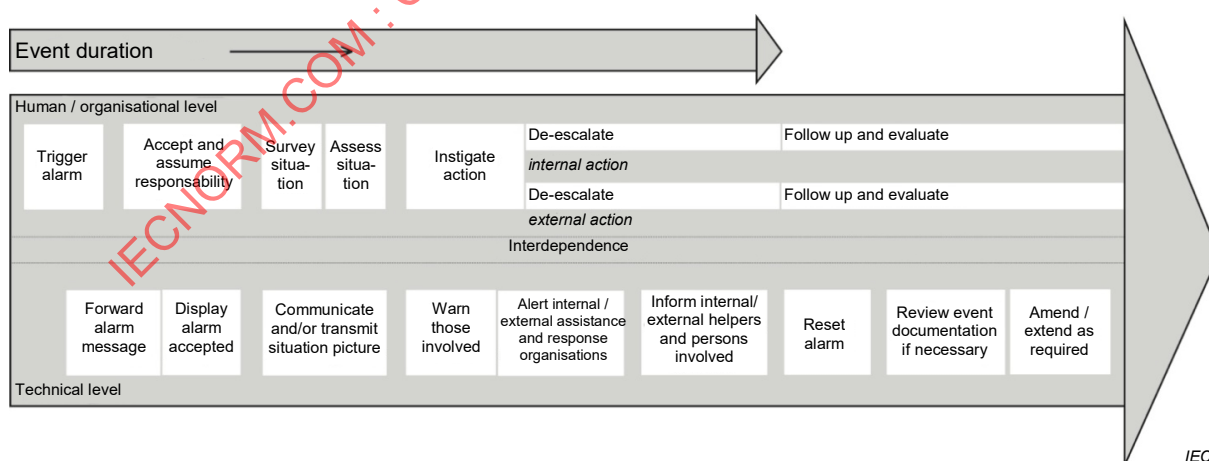
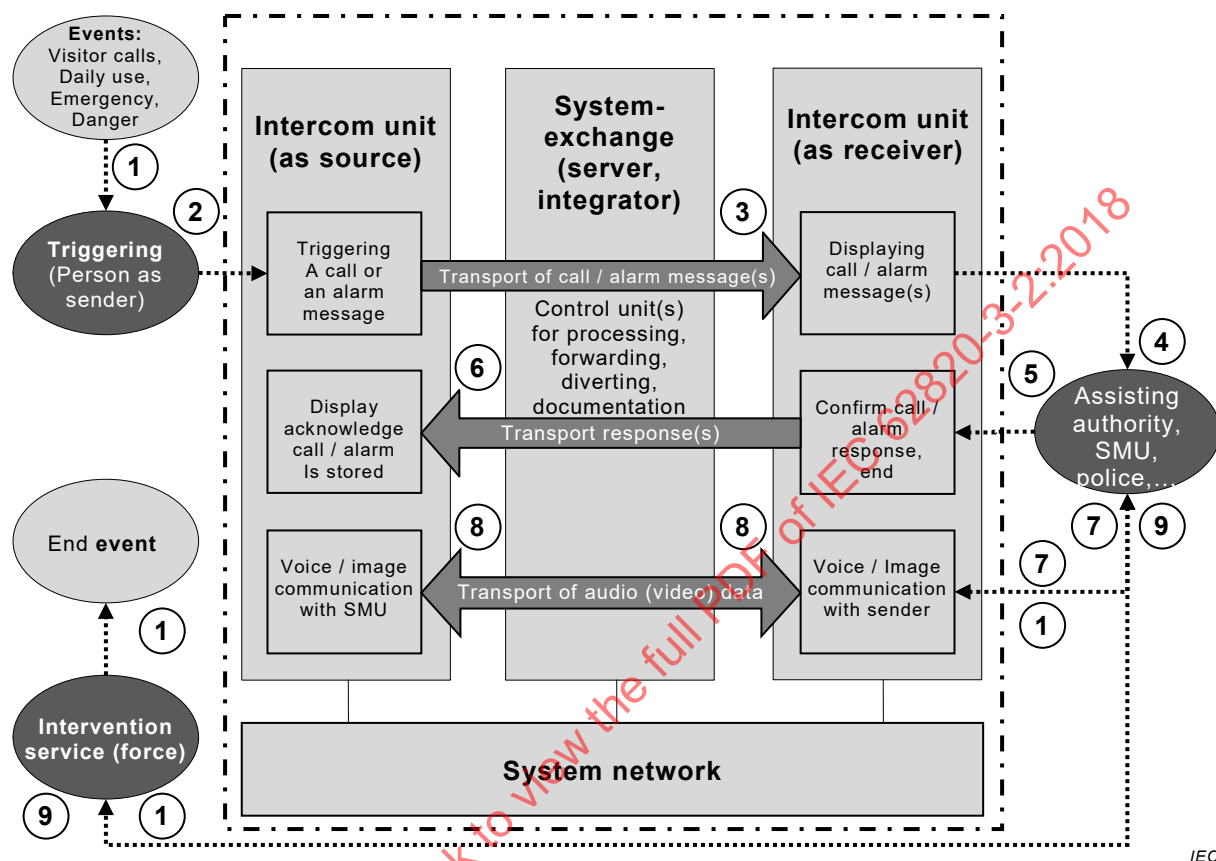


Figure 1 – Interdependence between human/organizational and technical level at an ASBIS used for emergency and danger reaction purposes

4.4 System structure

ASBISs are security/safety-technical devices and shall be a part of the whole security/safety concept for security protection and personal protection in the application area. They shall meet the requirements based on use and the protection requirement in terms of efficacy, operational reliability and availability.



IEC

Figure 2 – System structure of an ASBIS

Figure 2 represents the system structure of an ASBIS and describes the functions and devices. These individual functions in the figure are split from each other for clarification. The various functions can be combined in one device/housing however. These functions and the workflow are described as follows:

- 1) An event (visitor, emergency situation, danger) is observed by a triggering party (person).
- 2) The triggering party (person) reports an event by actuating an ASBIS messaging/warning device (e.g. by pushing a button on VCU / URU).
- 3) The call / alarm message is sent to the relevant receiver (SMU / URU) for this purpose via the system control unit (electronic exchange device) where it is displayed visually/acoustically.
- 4) The assisting authority (SMU) observes the operational indicators of the call / alarm message.
- 5) The receiver (SMU) acknowledges the receipt of the call-request or alarm message.
- 6) Sending a receipt confirmation (acknowledgement for the call request / alarm message) triggering call terminal for visual/acoustic operational indicators there (e.g. reassurance announcement) (VCU / URU).
- 7) Establish the connection for an audio transmission by the assisting authority for a location inquiry (possibly with the transmission of video of the situation) (SMU / URU).

- 8) Voice dialogue with the trigger for determining and verifying the type and scope of the event (possibly with transmission of video of the location) (SMU-URU, SMU-VCU, URU-VCU).
- 9) Alarming the intervention services by the assisting authority (SMU) via voice communication (possibly with additional data transmission) and, where applicable, the triggering of a suitable internal alarm.
- 10) Intervention service assumes responsibility and where applicable triggers a suitable internal alarm.
- 11) Intervention service ends the event.

4.5 Tasks of an ASBIS

4.5.1 General

Emergency and danger intercoms shall meet several tasks in the area of application. These are described as follows.

4.5.2 Safety / security tasks

- a) Report emergency cases and dangers to an assisting authority.
- b) Location inquiry (verification) by the assisting authority via voice communication with persons at the triggering location.
- c) Emergency monitoring of the emergency/danger location by intervention services.
- d) Transmission of warning information and information about how to proceed (live announcements/speed storage) in the affected area (individual rooms, groups of rooms, select building rooms or the entire building) with suitable announcements.
- e) Search calls with auto-response (e.g. first aid, mediators).
- f) Remote-controllability of other safety/security/monitoring techniques (e.g. voice alarm system (VAS), Video, access control) via interface.

4.5.3 Tasks for improving day-to-day processes (schools, universities, etc. in the example here)

- a) Search calls with personal response (e.g. headmaster, teachers, janitor, students are searched for).
- b) General area- or group announcements of general importance (e.g. timetable change, event admissions, general information).
- c) Inquiries and clarifications via one-to-one discussions (e.g. with the administration).
- d) Transmission of signal announcements.

4.5.4 Day-to-day communication

Since the basic operation workflow is identical for day-to-day use and emergency and danger management, the use for internal communication on a day-to-day basis automatically also practices operation in the event of emergency or danger. The system is so familiar through day-to-day use that in most cases, regular exercises can be avoided.

In addition, the day-to-day use of the system may act as an availability check for the necessary technical inspections (e.g. for signal announcements transmission every 45 min) in a school. If the break signal is missing, this can mean the system is not working either in full or in part and requires a technical service.

4.6 Safety / security grades

An ASBIS may be provided for applications of different kinds, such as access communication, panic alarms, threat alarms, building alarms, stand-down calls, calls for assistance, containment alarms, voice communication and information purposes. The nature, scope and level of the applications involved govern how the ASBIS is configured in technical terms. The TRM will make the determinations required as part of the planning and evaluation process.

During planning, installation, operation and extension of the ASBIS as part of the scope of the TRM process, data protection concerns and the relevant legal situation and other official documents or documents legally required for insurance purposes (e.g. fire protection, escape routes/emergency escape routes) and other standards shall be taken into account.

In particular, the responsible authorities (e.g. fire brigade, police) are already involved in the planning phase or when devising the total protection concept within the scope of the TRM process. In particular, forwarding the alarm and intervention measures including the required plans for the intervention shall be agreed for the intervention. This shall be documented in the TRM file.

During planning, installation, operation and extensions of the ASBIS, the minimisation of false alarms shall always be taken into account and implemented using suitable measures.

The degree of the safety/security level to be achieved is dependent on

- the systematic analysis of the individual risk situation (risk assessment),
- the agreed application of safety/security measures (e.g. constructional and mechanical protection measures), and electronic measures (electronic, visual and other devices) within the scope of an integral ASBIS,
- the targeted interaction of all technical devices with clear organizational and administrative steps (e.g. access controls, codes of conduct, voice communication) and instructions,

which shall be verified in terms of their ability to function, their efficacy and compliance at regular intervals

ASBIS systems are divided into three safety/security grades, as follows:

Grade 1:

Low-risk application requirements. The application's technical requirements are met by checking the system to ensure it is working as intended every working day. This system check can be performed manually or automatically. If the application is also used for regular operating procedures every working day, this is considered equivalent. Either way, it is important to ensure appropriate measures are taken in accordance with the TRM file in the event of a fault, and initiator and assisting agency shall also be able to communicate orally to verify matters.

Grade 2:

Medium-risk application requirements. The application's technical requirements are met by checking the system to ensure it is working as intended multiple times daily (every day). The system check shall be automatic to eliminate human error if the testing is performed manually. It is important to ensure that appropriate measures are taken in accordance with the TRM file in the event of a fault; and the initiator and the assisting agency shall also be able to communicate orally to verify matters.

Grade 3:

High-risk application requirements. The application's technical requirements are met by checking the system automatically daily at least to ensure it is working as intended; and all application components and transmission channels shall be monitored continuously. Monitoring transmission channels implicitly by checking all active components (source, integrator and receiver) are operational at all times is considered equivalent. All sources and receivers shall indicate actively at all times that the application can be used as intended. It is important to ensure appropriate measures are taken in accordance with the TRM file in the event of a fault and, that the initiator and assisting agency able to communicate orally (real time voice dialog) to verify matters rapidly.

Further technical requirements for the different grades are shown in Table 1.

The information in Figure 3 shall be accounted for when classifying the grade.

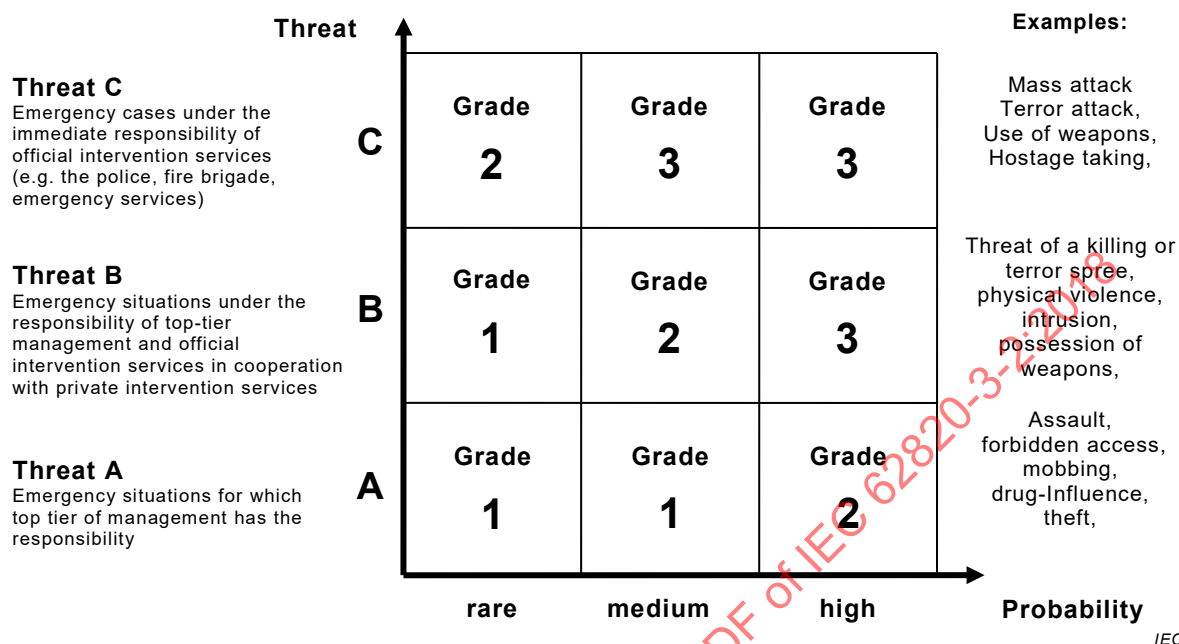


Figure 3 – Classification of the grade

Taking Figure 3 into account and when establishing the grade, the following points in particular shall be taken into account, classified, and the relevant monitors defined:

- the threat(s);
- central component and other system parts in need of protection;
- philosophy of the protection measures;
- operation of the ASBIS under fault conditions (e. g. when an emergency power supply is needed, equipment- or cable errors, communication breakdowns, redundancies);
- safety/security requirements (e.g. emergency exits, escape routes, fire protection) taking the local used building product act into account;
- environmental and EMC conditions at the location;
- assembly locations for the system components;
- collaboration of ASBIS-users (e.g. operation, instruction);
- cable ducts, cable types, maximum cable lengths;
- communication connections (availability, reliability, safety/security, efficiency);
- tamper detection;
- verification, issue and treatment (intervention measures) of different alarms.

Depending on the grade required, the requirements described in Table 1 shall be met completely by a suitable application

The evaluation and the result, in which level the application was set, shall be documented in the TRM file.

Central components and an alarm-transmission-unit shall be housed in a restricted access room for ASBIS with sabotage protection where possible.

Jointly used system components shall meet the requirements of the highest grade in each case.

All standard-relevant applications shall meet the requirements of the lowest grade at least. Other applications which do not meet this document can be integrated provided that they are without interference with the standard-relevant application. The TRM makes the decision and is responsible for the integration and necessary priorities of such applications.

4.7 Components of an ASBIS

4.7.1 Electronic measures

Where signal transducers for other alarm types, (e.g. evacuation alarm, fire alarm), as well as, where applicable, loudspeaker, similar other signals, (e.g. chime signals), or voice alarm systems are existing in buildings, these should work only with differing tones and/or sequences.

In particular, to protect against threats by persons (e.g. persons running amok, terrorists, school shooter) can be implemented with the agreement of the security authorities, a specific signalisation system can be implemented which prevents a perpetrator from being able to access secured areas unimpeded (containment alarm). However, this alarm shall clearly differ from the other signals in a classifiable way.

Note that persons in extreme stress situations can make a clear distinction between signals with an adequate degree of reliability. The rarity of the event is an aggravating factor which makes it harder to have a sufficient reminder to the meaning of the different signals. In addition, depending on the position development, a signal output may not apply to the entire property/building. The corresponding areas affected shall be stipulated and documented for this purpose.

To avoid misinterpretation, alarm messages shall be distributed in clear spoken voice messages. These messages shall be announced by a warning tone. The benefits are as follows:

- direct influence on persons present as to how they shall act,
- the ability to apply differing procedures especially in large building complexes,
- the ability to impart significantly more information which could help calm those present,
- the ability to announce the cessation of the dangerous situation.

The announcements shall be audible in all parts of the building and free areas of the affected areas. In addition responsible persons shall be defined including instructions/trainings and information about defined helper staff.

Enquiries by phone shall be possible for the assisting authority and the intervention force, depending on the extent and type of danger involved to establish the situation and where applicable for tactical control by intervention services (for example, ASBIS interface to: telephone system, mobile phone, voice-alarm system).

As a part of the TRM process, an assessment shall be made to determine whether, depending on the case concerned, (for example, if an 'amok or terror alarm' is triggered), code words or clear instructions on how to proceed shall be communicated via loudspeaker and/or voice communication system (ASBIS). Depending on the design, a threat system requires completely contrary behaviours, (e.g., 'please remain where you are' or 'please leave the building immediately') as the correct ones. This shows that it depends on analysing the situation appropriately as quickly as possible and it makes sense to give out situational-specific, concrete operating procedures instead of code words, which are appropriate to the local situation (see also Clause A.2).

For offences such as vandalism and personal injury, an information via video image transfer can serve to increase the ability to quickly implement the necessary intervention.

The installation and/or Integration of such systems shall be assessed within the scope of the TRM process taking data protection into account and the specifications of the related standard.

4.7.2 Mechanical protection measures

Especially with higher risks and to provide protection for threats from people (e.g. in mass attack), the possibility of locking doors automatically, manually and with mechanical or electronic locks, shall be provided as an important protection measure. For other events which are to be expected, this capability shall be assessed as a part of the TRM process.

Where applicable, the doors shall be lockable from both sides – it shall be possible for anyone to open a door from the outside only when the door is not locked. Doors shall default to the secured position on closure. Otherwise, only authorized persons with the key shall be able to open the door from the outside.

The relevant standards shall be taken into account when choosing the individual elements. The safety/security components shall be inspected and certified by a testing/certification authority accredited to IEC 17065.

4.7.3 Other options

Other protection-, monitoring-, communication- and information measures can be evaluated as part of the TRM process and where applicable, implemented taking relevant standards and specifications into account.

4.8 Requirements for system components and interfaces

4.8.1 Basic requirements

The basic requirements for an ASBIS are as follows:

- displaying the fault message at the location(s) determined by the TRM;
- displaying the operating states of the system (e.g. maintenance, inspection, alarm state, etc.) at the location(s) determined by the TRM;
- the possibility to put alternative pre-defined alarm and rescue plans into force in the event of a safety/security-relevant fault message in order to ensure safety/security. The TRM shall provide the plans before system commissioning;
- Table 1 has the requirements which shall be accounted for in full depending on the grade.

Table 1 – Requirements for the ASBIS and its intercom units depending on the grade

Requirements	Grade		
	1	2	3
System monitoring (communication paths, messaging call terminal (source), system control centre (integrator) and receiver call terminal (receiver) (e.g. by monitoring the operational readiness))			
Monitoring interval of the communication path (e.g. network) internal	$t \leq 25 \text{ h}^{1)}$	$t \leq 5 \text{ h}$	$t \leq 180 \text{ s}$
Monitoring the system comprising source, integrator and receiver for operational readiness	$t \leq 25 \text{ h}^{1)}$	$t \leq 5 \text{ h}$	$t \leq 180 \text{ s}$
Displaying the fault messages at the location(s) determined by the TRM	For technical monitoring of the group operational indicators	Group operational indicators	Detailed fault message as plain text - operational indicators
Displaying the operating states of the system (e.g. alarm state, fault, etc.) or a maintenance/inspection or at the location(s) determined by the TRM	For technical monitoring of the group operational indicators	Group operational indicators	Detailed fault message as plain text operational indicators
Reporting the change to operational readiness (operating mode alarm state and non-alarm state) to all functionally connected system components (sources <> integrator, receiver <> integrator)		X	X
Notification/display of impaired sources with their identification at location(s) determined by the TRM	X ¹⁾	Detailed operational indicators, e.g. via LEDs	Detailed message in form of plain text operational indicators
Indication of operational readiness of all receivers as long as all the assigned sources are operationally ready	-	Continuous display	Continuous display
Indication of operational readiness at sources where at least one assigned recipient can be reached	-	In the event of an alarm, silent technical acknowledgement that the message reached the receiver	Continuous light display ²⁾
Display of missing operational readiness through clear light indication on sources and receiver within the affected area while the supply voltage remains available	-	If communication with the integrator is not possible	If communication with the integrator is not possible and the assigned sources/receivers cannot be reached
Power supply in implementation type A or B in accordance with 4.8.9 for the integrator and the remote alarm equipment so that a power supply failure is recognised, reported to the appropriate stations and appropriate actions can be taken	X	X	X
Power supply as per 4.8.9, Table 2 for the remaining components except the integrator and the remote alarm devices when using implementation type A or B	E	X	X
Maintenance (service and inspection)	1x per year	1x per year	1x per year
Start of repairs on site	within 48 h	within 24 h	within 12 h
Sending an alarm message and responses			

Requirements	Grade		
	1	2	3
Categories of the alarm transmission system (according to EN 50136-1 or equivalent IEC or local standard) with automatic alarm forwarding, e.g. to the fire brigade, police, emergency and service control centre.	at least SP2 or DP1	at least SP3 or DP2	at least SP5 or DP4
Report with acknowledgement on the correct transmission of data packets (technical acknowledgement).	-	X	X
Indication of the alarm signal on the receiver after the alarm message has been received.	X	X	X
It shall be possible to clearly distinguish between different alarm priorities given identical alarm events (technical prioritisation). The indication of alarm signals with a higher priority on the receiver shall have precedence over the indication of lower-priority alarm signals.	-	X	X
Verifications and assumptions of responsibility by the intervention service			
The ASBIS shall enable a voice communication between the trigger and the assisting authority. The trigger here can send and receive information but is not allowed to control or end the communication. In contrast, the intervention service also offers the possibility of controlling the communication.	X	X	X
The ASBIS shall enable a data and voice communication between the trigger and the assisting authority. The trigger here can send and receive information but is not allowed to control or end the communication. In contrast, the intervention service also offers the possibility of controlling the communication.		E	X
3 types of responses are possible: - responsibility taken - responsibility rejected - responsibility not clear (e.g. subscriber not reached)	-	X	X
In the event of "Responsibility taken", the alarm signal is responded to by the receiver and this response is forwarded to the source via the integrator (e.g. reassurance light).	-	X	X
In the event of "Responsibility rejected" or "Responsibility unclear", the integrator shall pass on the ASBIS-alarm condition to other receivers and/or increase the priority.	-	X	X
The integrator shall continue to forward an alarm notification to the receiver until the integrator has received the response "Responsibility taken". The TRM shall define a suitable course of action (e.g. internal alarm) if no response is received ≤ 180 s.	-	X	X
With ASBIS signalling equipment which use a mechanical hindrance above it with lasting change in form (e.g. push-button alarm with glass), the change in form shall be removed before putting the ASBIS back into service.	X	X	X
The ASBIS-alarm condition shall be reset at the source and/or integrator.	-	X	X
The integrator shall record information about ASBIS-alarm conditions which have been received and distributed, responses from intervention services and the presence of fault notifications and other events.	30 days	60 days	90 days
Recording images of the situation and voice communication (where present) in the event of an alarm.	-	Language	Language and image of the situation

Requirements	Grade		
	1	2	3
Performance characteristics			
Emergency conference between triggering party and crisis intervention team	-	Optional (functionality is to be assessed in TRM)	X
Search calls (to all or defined group) with auto-response (first aid, mediators, etc.)	X	X	X
Indicate trigger location on receiver call terminal	X	X	X
Queue	Yes (minimum for 10 calls, others get occupied)	Yes (minimum for 10 calls, others get occupied)	Yes (same number of all intercom call units)
Forward call internally by time, configurable, maximum 180 s.	-	X	X
Call forwarding internal	X	X	X
Call forwarding to external	-	X	X
Reassurance announcement	-	X	X
Emergency global call	X	X	X
Handsfree communication in open duplex	-	X	X
Simplex	X	X	X
Duplex, voice-switched and / or DSP-controlled	-	X	X
Initiation of warning messages and instructions on how to proceed from the internal assisting authority as a response to the verification	X	X	X
Initiation of warning messages and instructions on how to proceed from an external assisting authority as a response to the verification	-	X	X
System availability ²⁾	99,7 %	99,9 %	99,99 %
Emergency monitoring	-	X	X
Protection from unwanted tapping by defined maximum talk time, minute tone, and call operational indicators (tapping protection)	-	X	X
Minimum protection class of qualified person call devices as per IEC 60529 for publicly accessible signalling call terminals	IP 33	IP 54	IP 54 in special function rooms and for external use: IP 65
Minimum impact protection (vandalism) as per IEC 62262 for publicly accessible signalling call terminals	IK 05	IK 06	IK 07

Requirements	Grade		
	1	2	3
Voice transmission index (STI) of 0.5 according to IEC 60268-16	in 1 m distance from call terminal alternatively, a subjective test based on ITU-T P.800 shall have a result of at least 3 points	in 2 m distance from call terminal alternatively, a subjective test based on ITU-T P.800 shall have a result of at least: 4 points in rooms, 3 points in corridors, 3 points in halls	at each location in all relevant rooms, corridors and halls alternatively, a subjective test based on ITU-T P.800 shall have a result of at least: 4,9 points in rooms, 4 points in corridors, 3 points on halls
Volume (SPL) above the expected noise level according to the specifications of the TRM (measured at 1 kHz (alternative 1,1 kHz) in 1 m distance with 0,1 m ahead of the geometric center of the enclosed surface of the unit-loudspeaker).	6 dB	9 dB	12 dB
Microphone speaking distance with signalling call terminals (measured in a quiet environment with a maximum ambient noise level of 45 dB (A)), at least 3 points shall arise from the receiver terminals (to ITU-T P.800)	at least 3 m	at least 5 m	at least 7 m
(X) = Required (E) = Recommended (–) = Not required 1) Not required for grade 1 when a use in day-to-day operations is assured. The underlying functionality shall be assessed as part of TRM. Using organizational measures, it shall be ensured that a repair action is implemented, and the fault is entered in the operator's log. 2) The system availability indicates within what time (in %) an ASBIS shall be available – as a minimum – when used as intended and operated all the year round. With the ASBIS, this applies for system control centre, at least one receiver call terminal, 80 % of the signalling call terminals and the transmission routes. Announced maintenance times planned with the agreement of the ASBIS-user are kept out of the calculation. The system availability can be assured purely technically (e.g. redundancies, two receiver call centres), technically and organizationally (technical personnel and material on-site), by experience (proven performance) or using manufacturer's instructions from the manufacturer QA system.			

4.8.2 Requirements for the system networks

In general, no exclusive ASBIS network is necessary, if it can be assured that there will be no negative Influence (cross-talk, interference, delay, etc.) from other network users; this also applies when using existing IP networks, e.g. when setting up a VLAN with the necessary bandwidth reservation (QoS).

4.8.3 System control centre (ASBIS-server)

The system-exchange, server, integrator, (centrally, distributed or as a software implementation) shall also support all the requirements on the call terminals, in use in full and in a suitable manner.

The location and protection capability of the system control centre shall be configured according to the TRM and safety/security grade.

Taking tapping protection (data protection) into account, in normal mode, tapping should not be possible at all of the signalling and receiver call terminals which are connected. The necessary workflows and functions are supported for the various operating modes (e.g. normal mode, alarm mode).

The remaining signal tones shall be available for all operational modes as well as for day-to-day communication.

4.8.4 Intercom unit as source (VCU, URU)

The ASBIS signaling call terminals are used to signal emergency- and danger situations on and in a property. They shall consist of a minimum of:

- loudspeakers;
- microphone;
- visual/acoustic operational indicators;
- one or more call button(s) for day-to-day communication;
- indication that the emergency and danger report was sent and saved (acknowledgement);
- indication that a call connection exists;
- indication that there is a fault;
- indication that at least one receiver call terminal can be reached (only required for grade 3).

ASBIS signalling call terminals are also used for voice communication for verification and location inquiry by the assisting authority as well as for the receipt and issue of warning messages and instructions on how to proceed. These instructions shall be broadcast visually/acoustically by means of an attention signal (2-meaning principle) and shall differ significantly from the signals for the day-to-day communication (e.g. alarm tone according to local standard).

4.8.5 Intercom unit as receiver (SMU, URU)

Receiver call terminals are used to display messages, voice communication after receiving calls, message verification and location inquiry and the performance of suitable measures. These include warnings and instructions on how to proceed to persons on and in the property. They shall be broadcast visually/acoustically by means of an attention signal (2-meaning principle) and shall differ significantly from the signals for the day-to-day communication (e.g. local standard alarm tone, followed by live announcements or announcements from a voice memory).

They shall contain the following at a minimum:

- loudspeakers;
- microphone;
- visual/acoustic operational indicators;
- optional ASBIS connectible signalling equipment;
- full command keyboard.

4.8.6 Intercom unit as source and receiver (URU, SMU)

Intercom units for both functions shall use the requirements of both intercom unit types.

4.8.7 Emergency and danger warning equipment (ASBIS warning equipment)

Emergency and danger warning equipment for ASBIS is used for manual triggering of an alarm message in the event of an acute emergency or a danger (e.g. a mass attack). ASBIS warning equipment shall be implemented so that in all cases, only a targeted manual triggering by a person as an intentional actuation leads to an actual triggering of the alarm. An automatic alarm trigger, e.g. as a result of the lack of a so-called plain text message is not authorized.

Depending on the group of persons needed for the property concerned, it shall be evaluated as part of the TRM process and documented in the TRM file whether to use ASBIS warning equipment which can be actuated by anyone, or only by a specified group of persons (e.g. designated staff, security force, the police etc.).).

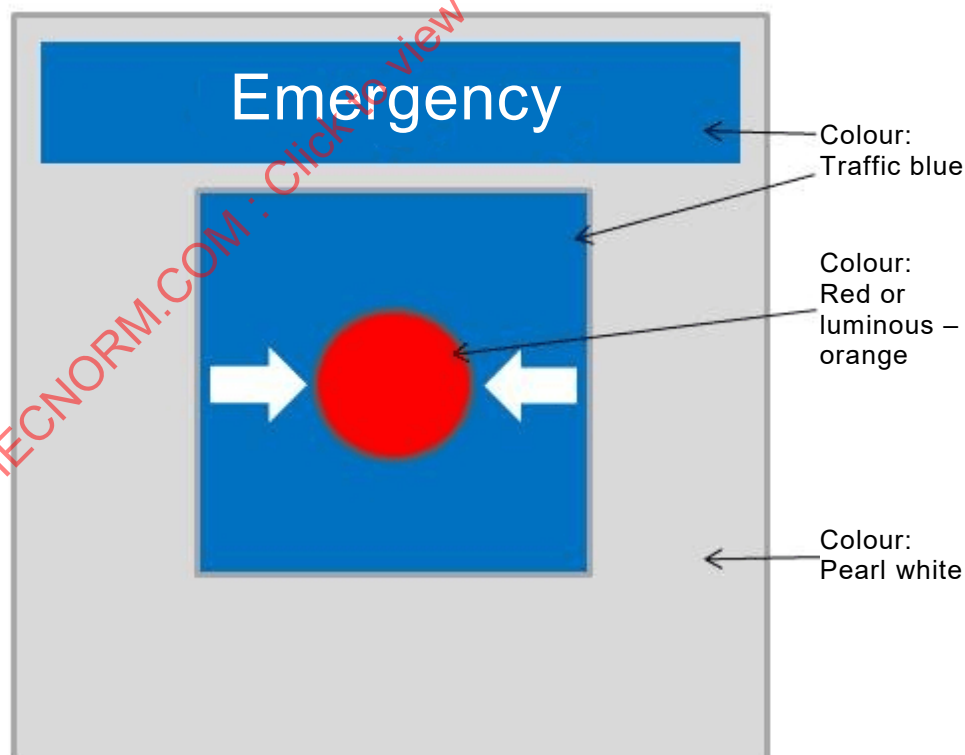
If it is not possible to allow anyone to trigger the alarm due to official regulations (e.g. from the police) or in particular, to avoid unauthorized alarms or the misuse of alarms, the ASBIS warning equipment or parts thereof shall be structured such that the triggering party or operators shall identify themselves beforehand with means of identification (e.g. transponders), or triggering requires a means of identification.

Where applicable, triggering of alarms by anyone can be minimised by choosing the places of installation and thus minimise the triggering of false alarms (e.g. beneath a desk – the cables shall be secured against breaks).

ASBIS warning equipment shall be identified clearly by EMERGENCY signage. The identifier POLICE EMERGENCY shall be used if the trigger has a direct connection to the police with the agreement of the police. This specification shall be documented in the TRM file.

An ASBIS signaling equipment which can be operated by anyone generally comprises a button with a mechanical hindrance in front of it (e.g. a 'break glass' or similar), see Figure 4. The button shall be with appropriate identification by use of the following colors:

- a) button (press button) in red (e.g. RAL 3000) or luminous orange (e.g. RAL 2005) or similar;
- b) surface around the button and background colour in traffic blue (e.g. RAL 5017);
- c) font in pearl white (e.g. RAL 1013);
- d) housing in pearl white (e.g. RAL 1013) where single module.



IEC

Figure 4 – Example of an emergency and danger warning equipment as a single module

An item of ASBIS warning equipment can also be integrated functionally into other units (e.g. call terminals)- above colours a) to c) are to be implemented. The mechanical hindrance with lasting change in form, the designation and the colour of the surface around the button and the colour of the button are to be implemented analogously.

In particular, it shall be possible for the intervention services to establish which item of warning equipment was triggered and its exact location.

Other basic requirements for ASBIS warning equipment:

- The warning equipment shall be implemented so that it cannot be confused with other installation.
- The actuation shall be clearly identifiable by the ASBIS-user (e.g. by a unique pressure point).
- The items of warning equipment shall be designed for at least 100 000 operations (quality feature).
- Safe actuation shall be ensured (e.g. by use of a raised button).

Single modules and the fragile element (e.g. glass panel) as a mechanical obstacle shall be implemented analogously to the requirements of ISO 7240-11:2011.

Additional warning equipment for low-priority messages (e.g. internal alarm, emergency call, de-escalation call) may be connected to the ASBIS for triggering corresponding messages at a local assisting authority. This shall be designed to prevent confusion with ASBIS warning equipment. In addition, a unique identification shall be carried out using other colors and labels.

4.8.8 Operational indicators and alarms

4.8.8.1 Operational indicators

All of the visual alarm operational indicators required shall remain active until they were reset by a person authorized in the TRM file. It shall only be possible to reset the operational indicators when the cause on which the operational indicators is based no longer applies.

All of the information required shall be displayed such that it can be interpreted unambiguously by persons (e.g. unique and distinguishable visual and acoustic operational indicators). When using operational indicators elements (e.g. text/graphical operational indicators) in which it is not possible to display all of the information at the same time, it shall be possible to identify when additional information is present (e.g. scroll capability).

ASBIS-users/operators/specialist companies shall be able to reset the acoustic operational indicators (e.g. status/fault operational indicators).

4.8.8.2 Internal alarm

The internal alarm is used to warn persons present within an affected area as per the specifications in the TRM file.

The acoustic signal for internal alarm shall have a nominal sound pressure level (measured at a spacing of 1 m) of 85 dB(A) at a minimum and 120 dB(A) at a maximum.

The acoustic signals which are issued via the signal transducer for the internal alarm shall be distinguishable based on their separate functions in terms of volume and the frequency of the signal and shall be easily identifiable by a person present in the property.

It shall be possible to restrict the duration of internal acoustic alarms automatically. The limitation on the duration shall be adjustable in the range of at least 180 s to a maximum of 10 min. The warnings which vary according to the risk and depending on the event or the specified times are to be documented in the TRM file.

Appropriate texts shall be stipulated for alarm announcements and shall be documented in the TRM file. The texts shall be formulated clearly, briefly and uniquely (see Annex A). The duration and the number of repetitions of the voice announcements shall be stipulated in the TRM file.

4.8.8.3 Remote alarm

Remote alarm devices forward the ASBIS messages to an assisting authority (e.g. emergency and service control centre).

All of the usual communication procedures based on IEC 60839-5-1, -5-2, -5-3, -7-12 for communicating messages from ASBIS can be used taking into account the connections specified in Table 2.

Generally, remote alarms shall be sent to an instructed assisting authority (e.g. qualified emergency and service control centre). In justified cases, and with the agreement of the police, a direct connection between the ASBIS and the police can also be employed.

If a direct connection to the police shall be executed, the police shall be involved in the planning of the ASBIS throughout the entire process. Note the local guidelines for alarm transmission to the police or other response forces.

Due to a diversity of communications formats in sending messages between the ASBIS and an instructed assisting authority or an instructed/responsible person, it shall be ensured that this instructed authority/person is in the position to receive information from the ASBIS and to assign it as appropriate.

Message types shall be transferred and displayed so that they can be uniquely identified by the instructed service.

4.8.8.4 Alarm precheck

The necessary alarm pre-checks and measures shall be specified between operator and the assisting authority in detail and shall be documented in the TRM file. Police/fire brigade shall be involved in the specification.

Whether and where applicable, the duration of an alarm trigger -forwarding should be extended in order to carry out an alarm pre-check, shall be evaluated as part of the TRM process.

As a general rule, an alarm may only be passed onto the police/fire brigade when the result of an alarm pre-check (e.g. per voice communication, image of the situation) is positive or an item of signalling equipment provided especially for this purpose, e.g. for police emergency, is triggered intentionally by a person (e.g. in the event of a mass attack).

NOTE In the event of false alarms, high fines can be imposed by the police/fire brigade for misuse. Additional costs can also arise for medical treatment of traumatized persons.

4.8.9 Power supply

It shall be ensured that energy supplies used in the ASBIS are designed for stresses both under usual conditions and for alarms, warning, and voice communication.

ASBIS and their component parts (also components in internal communication paths) shall be supplied with one of the following energy supplies:

- Implementation type A: A main source of energy, e.g. a mains supply, and an alternative power source which is recharged by the ASBIS or the mains supply, e.g. a rechargeable battery.

- Implementation type B: A main source of energy and an alternative power source which is not recharged by the ASBIS or the mains supply, e.g. a battery with a higher back-up time capacity.

The power supply of the ASBIS shall meet the requirements according to Table 2.

Table 2 – Requirements for the ASBIS power supply

Power supply Implementation type	Main power source Mains supply	Duration of the back-up time of alternative power source	Duration for recharging alternative energy supply
A	x	12 h	72 h
B	x	24 h ¹⁾	./.
x required; ./ not applicable; h hours; ¹⁾ The residual bridging duration of ≤ 12 h shall be displayed.			

In the TRM process, an assessment is made whether the minimum times required according to Table 1 in grade 1 and grade 2 may vary from the minimum times required in Table 2 for implementation of types A and B. In this case, a failure to the power supply shall be detected immediately and reported to the assisting authority(s) to ensure that the power supply can be restored as quickly as possible. This assessment and specifications shall be documented in the TRM file.

If, after a failure to the main power source, power is taken from an alternative power source or a remaining power source as a bypass, make sure that the capacity of this power source is sufficient, to supply the ASBIS with signal transducer(s) for the length of the alarm state as well as, where applicable, for a voice communication of least at least 15 min talk time. This shall be assured until the end of the monitoring period.

Switching between the main power source and the alternative power source and back, shall not generate an alarm state or have a negative effect on the condition of an ASBIS.

ASBIS power supplies shall not be used to supply other power supplies or system components.

4.8.10 Electrical cables

The cable specifications of the manufacturer of the system components shall be followed. If the manufacturer has not made any entries, the cable installation should comply with national or local standards. The “cross section” shall be specified taking into account the power consumption and the range of the operating voltage of the connected system components and the length of the cable.

Cable installation and distribution (e.g. cable distributors, switches) for the ASBIS shall be given appropriate protection against manipulation (e.g. not visible for everyone).

4.8.11 Interface to to other safety/security systems

ASBIS are able to be linked to other Safety/security systems by optional interfaces (e.g. mobile radio, mobile phone, public address systems, video surveillance systems, access control system, fire alarm system, Intrusion and hold-up system, etc.). The kind of interface depends on the solution and the security grade, which shall be achieved.

NOTE There is no standard about any interface to ASBIS defined.

4.9 Other requirements

4.9.1 Implementation of services

With ASBIS required under the construction ordinance, the documents named in the construction decision shall be accounted for and taken into account in the planning/configuration.

The client assumes responsibility for the implementation of the ASBIS and the order-specific implementation of this document.

All specifications of the manufacturer are binding provided that they do not contradict this document, relative national or local standards.

4.9.2 Arrangement and distribution of call terminals

Note the following points for the arrangement and distribution of call terminals depending on the organizational concept and its application requirements:

- good visibility;
- free accessibility (e.g. also for "barrier-free construction" according to local standards or other relative local standards);
- good accessibility to ASBIS signalling equipment as per used as intended;
- when using wall-assembly, accessibility of the trigger buttons shall be assured for the expected ASBIS-users;
- easy to view and in sufficient quantity in open spaces and corridors;
- in sports halls, assembly and event rooms in the escape route, next to the rescue doors.

In especially dangerous areas and along escape and rescue routes or depending on the use and quality of a building, the maximum distance at all relevant locations to the next call terminal has to be defined by the risk management.

4.9.3 Distinguishing between a call and an emergency call

A call is a day-to-day communication while an emergency call relates to a safety/security-critical situation. A distinction shall be made between calls and emergency calls. They can have different call destinations. The emergency call has a higher priority. Emergency calls shall be indicated differently from calls at receiver terminals.

4.9.4 Alarm groups

In combination with a loudspeaker system, alarm and group call areas shall be brought into harmony in an evacuation and barricading scenario.

4.9.5 Internal alarm and instructions on how to proceed

Instructions on how to proceed shall be given as verbal messages as all calls or group calls. The group size and group distribution shall be freely definable. Escape and emergency routes shall be accounted for the classification.

The size of the groups (building areas) are based on local situations and the specification in the TRM file. All persons within a group shall be able to receive the instructions as to how to proceed. Information shall be transmitted synchronously within a group. This also applies when information is sent in parallel via the loudspeaker and call terminals.

Nature and extent of behavioral instructions shall be specified and documented with the TRM and those involved according to the use of the building.

The signals, warning information and procedural instructions shall be distinguishable from operating signals and exceed the general noise level (interference noise level) by 10 dB(A) in rooms at any time. The minimum sound pressure level shall not be lower than 65 dB (A). The measurement shall be done at the same locations as for STI-Test, specified in IEC 60268-16.

In larger rooms, measures may need to be taken to increase the volume/better audio distribution.

4.10 General device and system requirements

4.10.1 General requirements

All of the system components used in the ASBIS shall meet the requirements on planning, installation, commissioning, delivery, operation and-maintenance-described in Clauses 4 and 5 as well as the requirements listed below.

4.10.2 Protection against environmental influences

As a rule, the protection against environmental influences of the device and system shall comply with the following standards:

- IEC 60529
- IEC 62599-2
- IEC 62599-1
- EN 50134-2, or the corresponding IEC-standard or, if not available, the local standard
- EN 50134-3, or the corresponding IEC-standard or, if not available, the local standard

Environmental classes are grouped based on standards IEC 62599-2 and IEC 62599-1.

4.10.3 Onsite Influences

System components of the ASBIS shall not be negatively influenced by environmental influence in its functioning. Depending on the type of the functional principle in application, environmental influences may have differing effects on the operational behavior. Therefore, the onsite influences (e.g. temperature, air humidity, EMC, noise) shall be indicated by the manufacturer as well as by the system designer and installer according to the situation onsite and comply with IEC 62820-1-1:2016.

4.10.4 Functional safe guard

4.10.4.1 Technical data

Technical data shall exist for the system components (e.g. performance characteristics, application boundaries). This shall include all of the parameters needed to ensure safe operation of the system components and the complete system. It shall be available in English and/or in the local language.

4.10.4.2 Assembly and installation guide

Assembly and installation guides written in English and/or local language shall be available for system components. These shall provide a clear depiction of the assembly and installation procedure and information on applications for which the system components are suitable, including information on environmental classes (e.g IP and IK ratings). Instructions on setting (e.g. volume adjustments, parametric programming, etc.) and maintenance shall also be supplied.

4.10.4.3 Operating manual

Operating manuals written in English and/or local language shall be available for manual operated system components. The guides shall have a clear depiction and explanation of all of the operating and operational indicators elements important for the operator/ASBIS-user and unique instructions for all operating states of the system.

4.10.4.4 Reliability

Construction elements for system components on the ASBIS shall be chosen such that they correspond to its intended purpose in the chosen environmental category (e.g. suitable IP and IK ratings).

4.10.4.5 Access to assemblies and construction elements

System parts and system components in the ASBIS shall be designed such that assemblies and construction elements are only accessible for the specialist company.

4.10.4.6 Connection and setting elements

Connection and setting elements shall be identified and shall be only accessible for the specialist company.

4.10.5 Operating safety/security

4.10.5.1 Control

These operations shall be designed intuitively to the operator\ASBIS-user such that a simple and accurate operation is possible after a person has been trained. Operational indicators shall be clear and intuitive in use.

4.10.5.2 Label

The function of the operational indicators and operating elements shall be clearly understood from the labels of the system components. All ASBIS indications and abbreviations, in particular alphanumeric ones, shall be arranged logically and easily interpreted.

4.10.5.3 Degree of protection

In the assembled state, system components in the ASBIS shall achieve the degree of protection IP 3x (or according to higher grade) as stated in IEC 60529.

4.10.5.4 Access protection

Parts of system components in the ASBIS which can affect the functionality, connectivity and settings of system shall be tamper protected (e.g. by use of covers).

4.10.5.5 Error tolerance

System components of the ASBIS shall be installed such that there is no negative affect on the functionality of the system by erroneous or incorrect operating procedures.

4.10.5.6 Parameterisation of the machine

The device for parametrization of the system components of the ASBIS shall be designed such that, after commissioning, each parameterization may only be changed with the operator's consent by authorized personal.

4.10.6 Indicators

Visual indicators – with the exception of concentrated indicators (e.g. summary error indicator) – shall be identifiable by different colors and, if their meaning cannot thus be clearly identified, by the use of clear, unambiguous labelling. Abbreviations, in particular alphanumeric ones, shall be arranged logically and easily interpreted.

4.10.7 Messages

4.10.7.1 Identifying messages

Messages shall be designed such that forwarding as intended is assured.

4.10.7.2 Issuing messages

The messages shall be issued in accordance with the type of the fault and the relevant state of the ASBIS. The messages shall be identified, issued and displayed within 10 s.

Fault message shall be issued in accordance with the type of the fault and the relevant state of the ASBIS. Fault messages shall be identified, issued and displayed within 100 s.

4.10.7.3 Message loss

Inputs/input functions for messages shall be designed such that no messages or information is lost and/or can be changed without appropriate authorization.

4.10.7.4 Test functions (test)

ASBIS shall have test functions for the ASBIS-user (for example, for checking warning equipment). The kind of test function, the procedure and the result documentation shall be decided by the TRM.

4.10.7.5 Switch-off functions

ASBIS shall have switch-off functions, e.g. for groups for warning equipment. It shall be possible to switch off the functions of an ASBIS individually or in a group by means of an intended action by means of an authorized ASBIS-user (at least access level 2 as per IEC 62642-1:2010). Critical functions which can be switched off shall be fitted with a "reminder signal" so that shut-downs shall not remain undiscovered for a longer period of time.

4.10.8 Structure

4.10.8.1 Stability

The housings for system components in the ASBIS shall have sufficient material strength according to meet the requirements from the TRM. Accessible elements which serve as an interface for the communication paths, (e.g. aerials, patch cables, etc.) shall be stable and secured.

4.10.8.2 Fixed mounting

System components in the ASBIS shall be designed to allow fixed mounting. This excludes system components which are not intended to be fixed (e.g. portable ASBIS warning equipment).

4.10.8.3 Potential-free, insulation resistance

Housing and housing parts belonging to system components in the ASBIS shall be potential-free (where necessary) – this excludes electrical protective measures and/or EMC protection measures. The insulation resistance shall be at least 500 kΩ.

4.10.8.4 Shielded cable conduit

System components in the ASBIS shall be designed such that the shields can be installed in an operationally reliable way with the shielded cables in the specifications. If system components shall be connected to the equipotential bonding conductor, a terminal shall be provided with a cross-section of 1,5 mm² to 4 mm².

4.10.8.5 Strain relief

Connection- and coupling sites for patch cables and lines shall be provided with relief from mechanical loads when such loads can be expected.

4.10.9 Processing messages

4.10.9.1 General information

Messages shall be processed and displayed and/or forwarded depending on the condition of the system.

4.10.9.2 Response time, loss of messages

After identifying a message, a report shall be sent to the specified points or the outputs for messages shall be controlled. No messages are allowed to go missing when using the system as intended.

5 Commissioning / delivery

5.1 General

The recommendations and requirements of IEC 62820-3-1 are mandatory for this standard. Exceptions are to be decided by the TRM and to be documented in the TRM file.

5.2 General information

5.2.1 Documentation

Documentation on ASBIS, including all system components, shall be exact, complete and unambiguous. Information on orderly installation, operation and maintenance shall be delivered to the operator who shall keep it available on site. An example shall be recorded in the TRM file.

For all of the parameters needed for safe operation of the machine parts belonging to the system and also information about standards-compliant system construction (e.g. the minimum required system components, maximum disassembly, restrictions, etc.) shall be documents available.

The documentation shall include the following:

- guides in English and/or the local language for the operation, installation and control of the devices including the following information listed to be delivered to the manufacturer;
- system description with a list of system components;
- installation plans (e.g. position-, switching-, wiring-, distribution-, network- and patch plans);
- deviations from the standards (where applicable, already included in the offer/order confirmation);
- acceptance test(s) and handover(s).

The information to be delivered by the device manufacturers shall contain the following details:

- a) name and address of the manufacturer;
- b) type designation;
- c) list of technical data;
- d) complete operating manual and operating instructions, all maintenance instructions and the applicable precautionary measures;
- e) maintenance requirements;
- f) the instructions for use and operating. The manual shall contain all information needed for use of all user and operator relevant system components, as intended. This includes explanations on the workings of control devices, display devices and signals, sequence of operation, connection and the disconnection of removable parts and removable accessories;
- g) the meaning of images, captions, warning information and abbreviations on devices shall be explained in the relevant manuals.

5.2.2 Commissioning

The operator and ASBIS-users shall be trained using the operating and instruction manuals with information about preventing false alarms and what to do in the case of alarms and false triggers. The specialist company shall notify the operator about the rules for operation and maintenance listed as follows.

5.3 Functional interaction of the system components

All of the system components which make up the system shall be executed and joined functionally so that the intended function of the system is ensured within the limits specified by the manufacturer to minimise of false alarms.

5.4 Options

Functionality and component options shall not have a negative influence on the required functions of the system. The properties of options shall be specified by the manufacturer.

6 Operation and maintenance

6.1 General

The recommendations and requirements of IEC 62820-3-1 are mandatory for this standard. Exceptions are to be decided by the TRM and to be documented in the TRM file.

All system components parts shall be regularly checked by the operator or its officers at the intervals set out in the TRM file for external damage and faulty components. Portable trigger devices shall be checked for mechanical integrity and the condition of the battery.

In addition to the visual inspection by the operator or a person (e.g. ASBIS users) commissioned by them, an inspection/maintenance of the component parts shall be carried out by an approved specialist company order to maintain the full functionality of the system. This inspection shall take place once per year as a minimum.

Where work on the system which can induce false alarms, e.g. renovation, triggering for inspection/test purposes is to be carried out, appropriate precautions shall be taken to avoid such alarms being passed on or interventions being instigated. After concluding work, the original operational readiness shall be restored and checked.

6.2 Operational test

All non-destructive functionality testing of component parts shall be carried out at least once per year according to the requirements of the manufacturer's operating manual. For component parts in electronic monitoring devices, special attention shall be paid to the prevention of false alarms.

Portable operating devices shall be checked for correct function in all the stipulated areas.

If a remote alarm system is provided, this shall be checked with the agreement of the instructed assisting authority and checked according to the functions.

6.3 Commissioning/repairs

If defects are found during the visual and/or functionality tests (e.g. faulty system component), these shall be replaced or repaired by a specialist firm without delay.

6.4 Replacing the battery and rechargeable battery

The batteries of the devices shall be replaced at least once per year or within the manufacturer's warranty period. A battery shall be replaced immediately when the devices indicate that a battery replacement is required.

Rechargeable batteries shall be replaced at least every four years or within the manufacturer's warranty period.

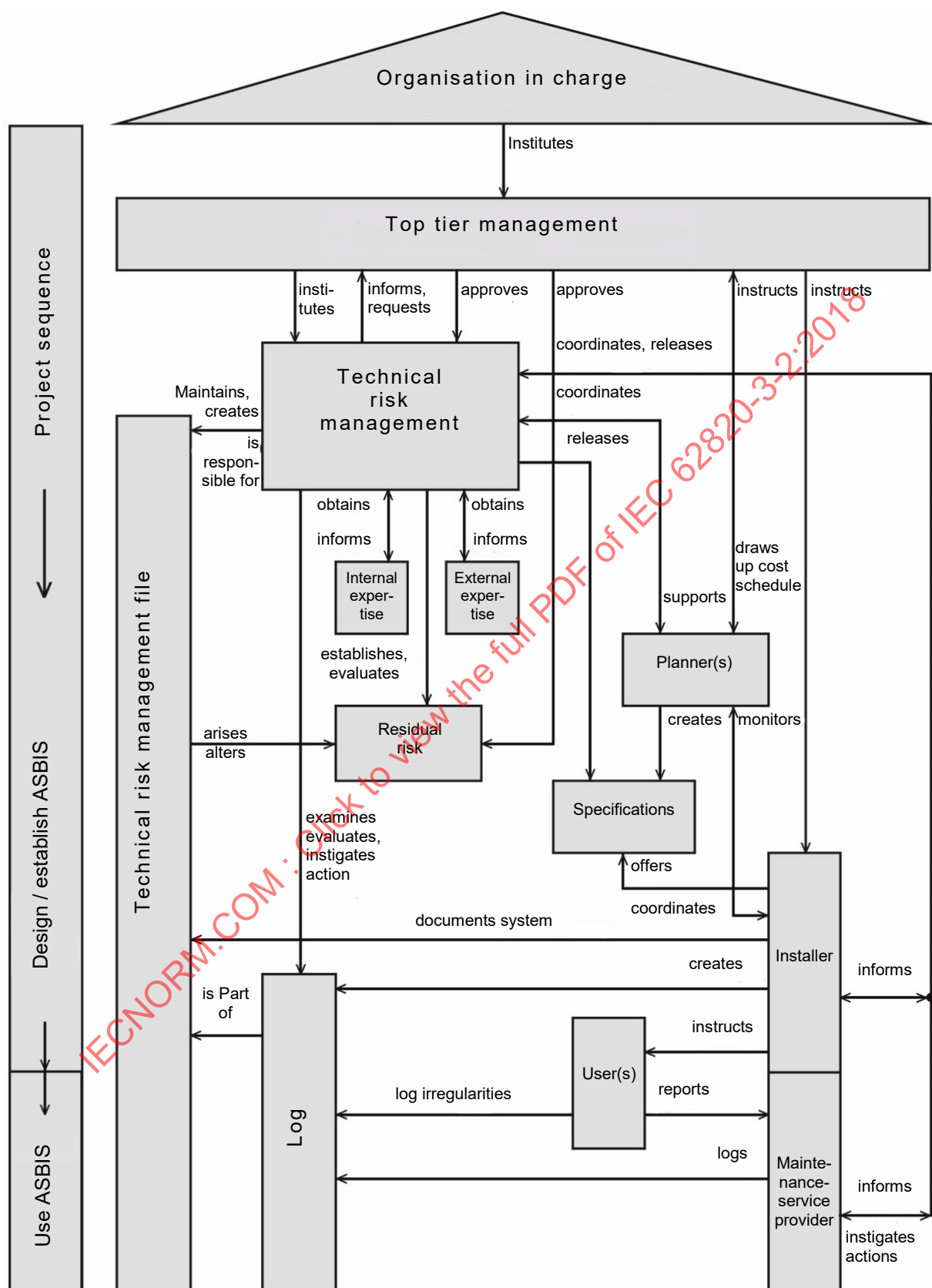
6.5 Software updates

Software updates shall be carried out as per the manufacturer's specifications. Every upgrade of the software version of the system and any modification to the required functionality shall be registered in an event memory in the system and/or to be entered into the operating log. After every such software upgrade or modification to the required functionality, all component parts shall be checked for the required functions, and finally, the complete system shall be checked for the required functions.

7 Tasks and responsibilities

7.1 General information

Figure 5 shows the typical decision-takers and actors for an ASBIS with their tasks and responsibilities and the relation between each other. It is important to understand, that this Figure shows a permanent process of a project (building) live time.



IEC

Figure 5 – General information of interrelationships and responsibilities

7.2 Organization in charge (responsible organization)

The organization in charge has the overall responsibility for overall risk management for an ASBIS. The organization in charge is also responsible for the TRM process of the ASBIS. This process extends to the planning, development, installation, equipment connection, configuration, application, maintenance and the putting out of service of equipment.

The organization in charge shall nominate a top tier of management which is to be documented in the TRM file.

The top tier of management ensures that the planners and specialist companies are instructed accordingly, and where applicable, with the agreement of the organization in charge.

7.3 Top tier of management

The top tier of management shall report to the organization in charge on all of the relevant activities of overall risk management.

The top tier of management shall do the following as part of the TRM of the ASBIS:

- a) Ensure that a specialist is nominated as a TRM and their representation for management, for creating and updating the TRM file, for planning, installation, operation and commissioning of the ASBIS and for technical risk assessment activities.
- b) All of the above-mentioned persons shall be informed of their responsibility according to this document. This includes their responsibility for the effectiveness of measures instigated overall risk control.
- c) The delegated tasks are maintained over the entire service life of the ASBIS.
- d) The delegated tasks shall be monitored for compliance.
- e) Define and/or approve the requirements for TRM in terms of the structure and operation of the ASBIS.
- f) Create and/or approve requirements how the defined protection targets in terms of personnel safety/security, efficacy and effectiveness and data and system security.
- g) Take care that the risk management process is carried out according to ISO/IEC 31010 and national standards if they are of higher importance.
- h) Provide the necessary resources.
- i) Check the results of TRM activities including regular evaluations in order to ensure continued suitability and the effectiveness of the overall risk management process.
- j) Accept and approve the residual risk under consideration of the interaction between technical and ORM.
- k) Commission and release planning and installation of the ASBIS.
- l) The entire planning, installation, operation, maintenance and repair of the ASBIS during the entire service life as per the TRM file.
- m) To carry out each year a management assessment taking the TRM and the ASBIS-user into consideration and write and/or approve a management report.

The above points shall be documented in the TRM file for the ASBIS.

7.4 Technical Risk Management

7.4.1 General

The TRM in the sense of this document does not, as a whole, relate to a TRM in the usual sense, but within the scope defined in Figure C.1.

The TRM is nominated by the top tier of management and is commissioned with the overall management of the TRM process as related to the ASBIS. The top tier of management can transfer authority to the TRM. He is responsible for constructing and maintaining the necessary communications between internal and external participants in the TRM process. In particular, these should be operators, ASBIS-users, planners, installers, maintenance staff, other service providers, building management, intervention services, authorities and where applicable others.

A TRM is a specialist staff member who can work with the elements of TRM, in a versatile, interdisciplinary, cross-functional, communicative, analytical and networked way. The TRM shall have an appropriate qualification (certified security manager, or comparable) and be able to demonstrate it by means of a certification as TRM to ISO 31000 or with practical experience. The purpose is to create a qualified risk assessment according to ISO/IEC 31010.

The TRM is responsible for the TRM process in the scope of the ASBIS. The TRM shall ensure that the assessment procedures in use are suitable for risk assessment and meet ISO/IEC 31010. The TRM shall create a TRM file and is responsible for the organization and implementation of the TRM process, to meet the protection goals (personnel security, efficacy and effectiveness and data and system-security).

Individual processes can also be delegated to persons with equivalent qualifications or companies. Responsibility for the proper execution of the delegated measure, however, remains with the TRM.

The tasks of the TRM as the central contact person include – as a minimum (including documentation in the TRM file):

- receiving messages from ASBIS-users (see 7.5 ASBIS-user), whose documentation and evaluation within the scope of TRM;
- collecting, analyzing, evaluating and storing information which are required for the TRM;
- project-related coordination of the requirements for the ASBIS with the technical planner;
- specifying the alarming types and -areas in cooperation with the ORM;
- specifying the alarm processes in cooperation with the ORM;
- approving the performance index that was created;
- inspecting and evaluating the operating log for up-to-dateness, proper management and implementation of suitable measures at their own discretion;
- informing the responsible organization of residual risks on the ASBIS and informing the operator about possible dangers caused by changes to the configuration;
- regularly reporting on the TRM process to the top tier of management;
- responsibility for training the ASBIS-user on using the ASBIS;
- implementing the TRM process when the ASBIS is changed;
- grouping all technical risk-relevant information, decisions and changes to the ASBIS in the TRM file;
- definition of exceptions from this document and its influence to the residual risk.

7.4.2 Specifications in the TRM file

The TRM file comprises the ongoing documentation of TRM which shall be kept up-to date at all times. The following shall be set out and documented in the technical risk management file as a minimum:

- specifications and the assignments made to individual functions and tasks (see Figure 5) such as organization in charge, top tier of management, TRM;
- technical risk assessment and specification of the grade, in cooperation with the ORM;

- specification and interaction of components and their function, operation and maintenance in the ASBIS;
- specification whether a receipt confirmation shall be displayed at the trigger site to prevent perpetrator responses;
- specification whether system features of a higher degree (e.g. voice and/or image recording) can minimize the residual risk of a lower degree;
- specification of system availability including inspection cycles;
- specification of the affected areas for each type of alarm;
- coordination and documentation of the intervention measures and creating corresponding plans for the intervention as part of the whole TRM;
- where applicable, set up an intervention team/crisis team for its own interventions on-site;
- description and release of residual risks;
- the content and results of approvals with the responsible authorities, e.g. fire brigade, police;
- specification and documentation of the alarm process (internal alarm, remote alarm, duration, type, scope of alarm and signals/announcement texts as well controls/intercom capabilities etc.) taking into account the accessibility of persons with disabilities (e.g. visual or – audio disability);
- specification of alternative measures in the event of a safety/security-relevant fault to the ASBIS;
- system documentation (plans, the position of warning equipment, accuracy of location detection after the triggering of portable ASBIS signalling equipment, detection of warning equipment operating manuals, operator's log, installers-/maintenance documents);
- amendment requests, with review and resulting actions and tasks;
- specifying the timetable for the checking and, if necessary, revising of the TRM;
- decided exceptions of this document and its influence to the residual risk.

7.5 ASBIS-user

The ASBIS-user is obliged to immediately notify the repair personnel and TRM in writing about special events, in particular technical and/or personnel attacks, the loss of system components (e.g. portable ASBIS warning equipment), missing functions or malfunctions, etc.

In addition, the ASBIS-user shall forward all information which may have an influence on TRM. These include e.g. new danger situations, unforeseeable events, constructional changes (changing the room use and -type).

7.6 Trained person

The trained person(s) who are commissioned by the operator/ASBIS-user with the operation of the ASBIS, he/she/they shall be trained by the ASBIS qualified person so that they are in the position to independently carry out operation of the ASBIS in the required scope.

Where a system functionality test is carried out manually on workdays (in grade 1), a trained person shall be responsible for documenting these system tests. Where faults are detected, measures shall be implemented according to the specifications in the TRM file.

7.7 Planner (technical planners, architect, consultant, general planners)

The planner shall design the ASBIS with the agreement of the technical risk manager or be a member of the technical risk management team. Several planners (or qualified specialist companies such as installers/maintenance staff) may work on an ASBIS. If this is the case, their duties and responsibilities shall be specified clearly and documented in the orders and in the TRM file.

Planners shall have the following knowledge and experience:

- verifiable knowledge of this document;
- verifiable specialist knowledge and experience in the area of the installed safety/security technology including the applicable standards.

The following special performances shall be carried out:

- technical concept design taking this document into account working together with the TRM;
- information and advising of the TRM over technical components, their operation, function and interaction, which is needed to implement the ASBIS;
- preparation of construction and tax documents;
- creating the performance index;
- monitoring the installation, acceptance of commissioning.

7.8 Installer

The installer is responsible for the installation, commissioning, documentation and training for the ASBIS as a specialist company.

Several installers may work on an ASBIS. In this case, the duties, interfaces and responsibilities shall be specified clearly and documented in the orders and in the TRM file.

The installer shall have a qualified ASBIS-person with the following knowledge and experience:

- verifiable knowledge of this document (where applicable, dependent on the grade);
- verifiable specialist knowledge and experience in the area of the installed safety/security technology including the applicable standards (where applicable depending on the grade).

The installer also has the following task:

- creating the operator's log;
- obligation to cooperate in TRM until the warranty matured.

7.9 Maintenance staff

As employees of a specialist company, the maintenance staff are responsible for the maintenance, inspection and improvement of the ASBIS.

Several maintenance staff may work on an ASBIS. In this case, the duties and responsibilities shall be specified clearly and documented in the orders and in the TRM file.

The maintenance staff shall have an ASBIS qualified person with the following knowledge and experience:

- verifiable knowledge of this document (where applicable, dependent on the grade);
- verifiable specialist knowledge and experience in the area of the installed safety/security technology including the applicable standards (where applicable depending on the grade).

Moreover, the maintenance staff shall guarantee the response times set out in this document for the start of maintenance (see Table 1).

The inspection and maintenance is to be carried out at least 1 time per year. An operator's log shall be maintained according to the specifications in this document. The operator's log is a part of the TRM file.

NOTE Examples about "how to inspect" can be found in the German Standard VDE 0833-1, see Bibliography.

As part of the maintenance and change management, the maintenance staff has a duty to collaborate with TRM.

7.10 Manufacturer of the system components and the IT network

Information about the intended purpose, as well as instructions for safe and effective operation and the using of the system components shall be in the manufacturer's information about components and interfaces.

The manufacturer's specifications shall contain the following, as a minimum:

- all of the technical information relevant for installation as intended and operations;
- the intended purpose of components;
- the necessary prerequisites of the system for operation of the components;
- the information about the configuration of the system for use of the components;
- the technical specification of the components for the system- and network connection.

The technical documentation of the components should be available for at least 10 years.

If there is a missing entry in the manufacturer's technical documentation which is of relevance to TRM, the TRM shall request this entry from the manufacturer.

An IT network is a part of the ASBIS. The interoperability of all components is to be checked by the planner. In addition, any opportunities for sabotage shall be minimised depending on the grade.

8 Change management

8.1 General information

Generally, change management in the implementation phase as well as in operation is necessary (e.g. owing to an evaluation). In the implementation phase, it may be that all significant developments may not be able to be predicted exactly at the start of the project. The challenge in change management in the implementation phase is to carry out as many changes as possible in a consistent way and to approve as few as possible. In the following subclause, only change management in operation is taken into account which is above all else a question of documentation and information.

The organization in charge bears general responsibility for change management involving the top tier of management and the TRM. They shall ensure that the defined processes are adhered to. The TRM is responsible for the control of the individual changes.

8.2 Change process

A change process shall be defined for operating the ASBIS in the TRM file. In this context, all of the necessary steps are evaluated, documented in a comprehensible way, the respective changes are set out, approved and implemented with all the affected locations. Process steps in the change process are:

a) Identify the change requirement

In the first step, it is about identifying a potential change. A change is always assumed when it has a technical or organizational effect on the ASBIS.

b) Formulate change request

If a change requirement is identified, this shall be documented.

c) Evaluate change request

If there is a change request, the TRM shall evaluate this. It is important that the planned change does not result in any impairments to the protection goals of the ASBIS and that they are included in the technical risk analysis, as well in the overall risk-calculation if the ORM is influenced.

d) Decide the change request

This shall be decided immediately after the evaluation of the change request. The responsibility for the decision is born by the top tier of management and/or TRM.

e) Carry out the change

After approving the change, all of the required measures shall be implemented and the affected documents updated right away.

f) Change evaluation

After a change was carried out, the organization in charge and/or TRM shall ensure that the change does in fact achieve the desired effect. If this is not the case, it shall be checked whether another change requirement applies.

IECNORM.COM : Click to view the full PDF of IEC 62820-3-2:2018

Annex A (informative)

Information on voice announcements

A.1 General information

In emergency situations, the following aspects shall be taken into account for arranging voice announcements with the presence of an electro-acoustic system.

- before the announcement, issue an attention signal (not too long, maximum 4 s);
- short, clear and understandable emergency announcements;
- adapt it to the expected public (e.g. foreign-language texts too);
- recorded emergency announcement texts shall be available to communicate them either right away or after a predefined delay automatically in the event of an emergency;
- make sure that the voice can be understood properly (e.g. female voice, acoustics properties of the space in the areas, complies with stated STI);
- coordinate the content of the emergency announcements with the responsible authorities;
- implement important behavioural instructions so that panic and unwanted reactions are avoided;
- set the time, number and the time sequence of the announcements;
- prevent the danger of confusing emergency announcements with other announcements, such as lunches, start of work, end of work, etc.
- use alerting sound levels and any other ASBIS sound level with a reasonable higher level than the predicted background noise levels into account;
- carry out the sound test;
- provide an announcement when the emergency situation has ended.

A.2 Examples of announcement texts

Since the texts are to be formulated clearly, briefly and uniquely, here are some examples of announcement texts for critical situations:

- Attention signal – "Fire alarm – Please leave the building using the escape routes"
- Attention signal – "General emergency – Remain in a room – close and lock doors and windows – wait for announcements"
- Attention signal – "Medical emergency – medics in room ..."

Annex B (informative)

Advanced security building intercom systems (ASBIS)

Examples of applications for all kinds of buildings as a part of an overall security concept.

No.	ASBIS – Safety/security applications	Definition / additional description
1	Building-Access-Intercom	Communication in case to assist access control. Door entry communication between VCU, URU and SMU with door lock control
2	Emergency-Intercom	Communication in case of an emergency. Mainly used in public areas, public-urban-transport-stations and highways
3	Elevator-Intercom	Elevator-Emergency communication according to EN 81 Standard
4	Alarm-Communication	Communication in case of an alarm. 2-Way communication in case of an Alarm-message to verify its kind and importance
5	Disabled-Help-Intercom	Communication in case of needed help. Mainly used in social rooms for people with handicaps to ask for any kind of help
6	Surgery-Intercom	Communication in case of urgent and critical situations. Especially used in hospital operational theatres
7	Emergency-Help-Intercom	Communication in case of needed help. Mainly used in parking garages and other lonesome areas
8	Acoustic-Escape-Routing	Directional sound transmission. Dynamic transmission of directional sound for very fast evacuation via single addressable unit-loudspeakers
9	Cell- Communication-Intercom	Communication for inmates and guards. Mainly in prisons, forensic-hospitals and police-stations for help-calls
10	School-Emergency-Intercom	Communication for personal safety and efficient education. For schools, universities to verify emergency situations and to reduce reaction time
11	Defibrillator-Intercom	Communication in case of personal safety. Mainly used where defibrillators are present, to call for additional help
12	Production-Warning-Intercom	Communication along production lines. Mainly used in industrial areas for danger warnings and to verify critical situations
13	Aggression-Detection	Communication with emergency and service centres. Automatic 2-way-communication with a SMU after detection of an aggression sound
14	Video-Intercom	Communication in case to assist Access control. 2-way voice-communication in addition to video-image transmission by interface between VSS and ASBIS

NOTE All applications can be part of a stand-alone ASBIS as well as be integrated in any combination in one ASBIS or with independent ASBIS, linked together by system interfaces to one functional ASBIS.

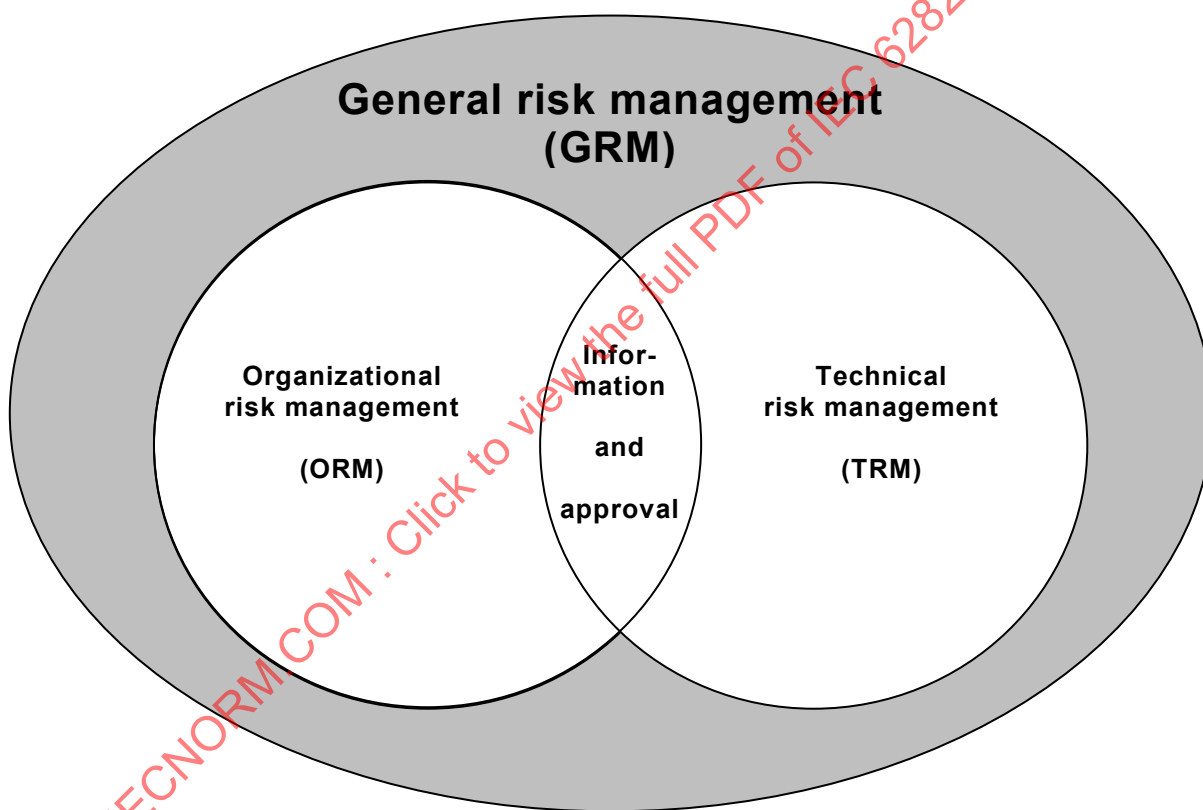
Annex C (informative)

Relationship between TRM and ORM as part of an overall risk management related to an ASBIS application

C.1 General information

Among other risk management aspects, the overall risk management consists of the TRM and the ORM. The ORM is not part of this document, but it has an influence on the TRM. Every change in the ORM shall be notified to the TRM and shall be approved to ensure that there is no impact to the technical residual risk and the overall residual risk. If there would be changes in the overall residual risk, a new technical risk assessment shall be done.

C.2 Graphical description



IEC

**Figure C.1 – Overview of interrelationship between TRM and ORM
as parts of the overall risk management**

Annex D (informative)

Table: Help-tables for risk assessment

D.1 Risk identification related to ASBIS applications

Table D.1 – Risk identification related to typical dangers

No.	Kind of emergency, danger, hazard for people in charge in a building	Frequency of occurrence per time interval	Weighting factor	Result	Comment
1	Amok threat				
2	School shooting				
3	Impaired building				
4	Insult				
5	Bomb threat				
6	Fire				
7	Arson				
8	Drug use				
9	Burglary				
10	Earthquake				
11	Explosion				
12	Hostages				
13	Poison gas				
14	Flood				
15	Inclusion				
16	Physical violence				
17	Mobbing				
18	Robbery / theft				
19	Snow				
20	Other dangers				
21	Storm, thunderstorm				
22	Unwanted behaviour				
23	Terror-attack				
24	Environmental alarm				
25	Accident by attack of other persons				
26	Accident, self-inflicted (injury)				
27	Vandalism				
28	Weapon in use				
29	Heavy rain				
30	Others				

D.2 Example table for assessing the likelihood of an emergency / dangerous situation

Table D.2 – Table to identify environmental conditions for assessing the likelihood of an emergency / dangerous situation

No.	Criterion for the following emergency / dangerous situation	Rating (points)	Weighting factor	Result	Comment
1	Number of persons in charge a) below average b) average c) above average				
2	Kind of buildings a) many floors, many levels b) low-rise building, low-rise level c) many buildings				
3	... a) ... b) ... c) ...				
4	... a) ... b) ... c) ...				
5	... a) ... b) ... c) ...				
6	... a) ... b) ... c) ...				
7	... a) ... b) ... c) ...				
8	... a) ... b) ... c) ...				

D.3 Protection target definitions as part of the planning for an ASBIS

Table D.3 – List of typical protection targets to identify the risk relevance

No.	Protection targets	Yes / no 1 / 0	Weighting factor	Result / ranking	Comment
1	Deterrence				
2	Reduce aggression				
3	Acceptance of technology				
4	Present Persons shall be informed				
5	Observance of human with disabilities				
6	Reduce threats				
7	Receive operation to continue				
8	Secure evidence				
9	Data protection				
10	Inform external assisting agencies				
11	Inform internal assisting agencies				
12	Ensure communication in an emergency				
13	Protect people				
14	Open atmosphere				
15	Prevention				
16	Protect property				
17	Increase security				
18	...				

D.4 Classification of the protections demanded

Protection target	Specification
Grade 1	– The result values in all 3 Tables (D.1 to D.3) are relatively low compared with similar buildings and applications. – Low protection requirements: Expected simple protective measures in compliance with the ASBIS standard grade level 1 should be sufficient.
Grade 2	– The result values in all 3 Tables (D.1 to D.3) are relatively the same compared with similar buildings and applications. – Medium protection requirements, Expected allows existing inventory systems combined use with suitable equipment and an adapted crisis organization and network to an overall solution in accordance with the ASBIS standard, grade level 2 is recommended.
Grade 3	– The result values in all 3 Tables (D.1 to D.3) are relatively high compared with similar buildings and applications. – High protection requirements, expected a complex system solution of possible standard-compliant and available on the state of the art security systems in combination with an adapted crisis organization in compliance with the ASBIS standard grade level 3 is required.

Annex E (informative)

Assisting organizational issues to reduce emergency, danger and hazard event duration

E.1 Labelling doors and buildings

Depending on the risk grade, doors and building parts can be labelled

- for reliable control by intervention services,
- with unique designations for steering and orientation of persons,
- with unambiguous identification of the escape route,
- based on the actual situation,
- clear and free of stress,

especially for high risks. A colour guidance system can be of huge benefit. This shall be evaluated as part of the TRM process.

E.2 Training

Depending on the risk grade, the General-Risk-Management shall initiate emergency-trainings for all kinds of staff and public in the building.

- The Training shall be done min. 1 time per year
- Both, TRM and ORM shall workout the emergency-training event
- Training of emergency situations with the highest grade shall prioritized

Training results shall be used to improve the organisational and technical concept.

Bibliography

General: The following standards are named as known. If the relevant IEC Standards are unknown, use available local standards instead.

IEC 61907:2009, *Communication network dependability engineering*

IEC 62642-1, *Alarm systems – Intrusion and hold-up systems – Part 1: System requirements*

IEC 62676 (all parts), *Video surveillance systems for use in security applications*

ISO/IEC 17065, *Conformity assessment – Requirements for bodies certifying products, processes and services*

ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

ISO 11801:2010, *Information technology – Generic cabling for customer premises*

ISO 14971:2007, *Medical devices – Application of risk management to medical devices*

DIN VDE 0100, *Installing low-voltage systems*

DIN VDE 0100-200 (VDE 0100-200), *Erection of power installations with rated voltages below 1000- Part 200: Terms*

DIN VDE 0815 (VDE 0815), *Wiring cables for telecommunications and IT systems*

DIN VDE V 0826-1 (VDE V 0826-1):2013-09, *Monitoring systems – Part 1: Hazard warning systems (GWA) for use in residential buildings, apartments and rooms with similar purposes – Planning, installation, operation, maintenance, devices and system requirements*

DIN VDE 0833-1 (VDE 0833-1):2009-09, *Alarm systems for fire, intrusion and hold-up – Part 1: General provisions*

DIN VDE 0833-3 (VDE 0833-3):2009-09, *Alarm systems for fire, intrusion and hold-up – Part 3: Requirements for intrusion and hold-up alarm systems*

DIN 33404-3, *Danger signals for workplaces; auditory danger signals; unified emergency signal; technical requirements of safety/security, testing*

EN 54-11, *Fire alarm systems – Part 11: Manual fire alarms*

EN 81-28, *Safety rules for the construction and installation of lifts – Part 28: Remote alarms on passenger and goods passenger lifts*

EN 81-70, *Safety rules for the construction and installation of lifts – Part 70: Accessibility to lifts for persons including persons with disability*

EN 50136-1 (VDE 0830-5-1):2012-08, *Alarm systems – Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems*

EN 50173-1:2011, *Information technology – Generic cabling systems – Part 1: General requirements*

EN 50173-2:2007/A1:2010, *Information technology – Generic cabling systems – Part 2: Office premises*

EN 50173-3:2007/A1:2010, *Information technology – Generic cabling systems – Part 3: Industrial premises*

EN 50173-4:2007/A2:2012, *Information technology – Generic cabling systems – Part 4: Home*

EN 50173-5:2007/A2:2012, *Information technology – Generic cabling systems – Part 5: Data Centres*

EN 50173-6:2014, *Information technology – Generic cabling systems – Part 6: Distributed building services*

EN 50174-1:2009/A1:2011, *Information technology – Cabling installation – Part 1: Specification and Quality*

EN 50174-2:2009/A1:2011, *Information technology – Cabling installation – Part 2: Installation planning and practices inside buildings*

EN 50174-3:2013, *Information technology – Cabling installation – Part 3: Installation planning and practices outside buildings*

EN 50310:2010, *Application of equipotential bonding and earthing in buildings with information technology equipment*

EN 50346:2002/A2:2009, *Information technology – Generic cabling systems – Testing of installed cabling*

EN 50600-1:2012, *Information technology – Data centre facilities and infrastructures – Part 1: General concepts*

EN 50600-2-1:2013, *Information technology – Data centre facilities and infrastructures – Part 2-1: Building construction*

EN 50600-2-2:2013, *Information technology – Data centre facilities and infrastructures – Part 2-2: Power distribution*

EN 50600-2-3:2013, *Information technology – Data centre facilities and infrastructures – Part 2-3: Environmental control*

EN 50600-2-4, *Draft Information technology – Data centre facilities and infrastructures – Part 2-4: Telecommunications cabling infrastructure*

EN 50600-2-5, *Draft Information technology – Data centre facilities and infrastructures – Part 2-5: Security systems*

EN 50600-2-6, *Draft Information technology – Data centre facilities and infrastructures – Part 2-6: Management and operational information*

IECNORM.COM : Click to view the full PDF of IEC 62820-3-2:2018

SOMMAIRE

AVANT-PROPOS	63
INTRODUCTION	65
1 Domaine d'application	66
2 Références normatives	67
3 Termes, définitions et abréviations	69
3.1 Termes et définitions	69
3.2 Abréviations	77
4 Exigences relatives au système ASBIS et domaines d'application	77
4.1 Généralités	77
4.2 Exemples choisis d'applications ASBIS	78
4.2.1 General	78
4.2.2 ASBIS pour la communication d'accès	78
4.2.3 ASBIS dans les écoles et autres établissements d'enseignement	78
4.2.4 ASBIS dans les administrations et les bureaux	78
4.2.5 ASBIS dans le système juridique	78
4.2.6 ASBIS dans les gares et les aéroports	78
4.2.7 ASBIS dans les centres commerciaux	79
4.2.8 ASBIS dans les bâtiments résidentiels publics	79
4.2.9 Autres exemples	79
4.3 Organigramme opérationnel ASBIS pour la communication d'urgence et de danger	79
4.4 Structure du système	79
4.5 Tâches d'un système ASBIS	81
4.5.1 Généralités	81
4.5.2 Tâches de sûreté/sécurité	81
4.5.3 Tâches visant à améliorer les processus quotidiens (écoles, universités, etc. dans l'exemple)	81
4.5.4 Communication quotidienne	81
4.6 Niveaux de sûreté/sécurité	82
4.7 Composants d'un système ASBIS	84
4.7.1 Mesures électroniques	84
4.7.2 Mesures de protection mécanique	85
4.7.3 Autres options	86
4.8 Exigences relatives aux composants et interfaces du système	86
4.8.1 Exigences de base	86
4.8.2 Exigences relatives aux réseaux du système	90
4.8.3 Poste de commande du système (serveur ASBIS)	90
4.8.4 Unité d'interphone en tant que source (VCU, URU)	91
4.8.5 Unité d'interphone en tant que récepteur (SMU, URU)	91
4.8.6 Unité d'interphone en tant que source et récepteur (URU, SMU)	91
4.8.7 Matériel de mise en garde d'urgence et de danger (matériel de mise en garde ASBIS)	92
4.8.8 Indicateurs opérationnels et alarmes	94
4.8.9 Alimentation électrique	95
4.8.10 Câbles électriques	96
4.8.11 Interface avec d'autres systèmes de sûreté/sécurité	96

4.9	Autres exigences	96
4.9.1	Mise en œuvre de services	96
4.9.2	Disposition et répartition des postes d'appel	97
4.9.3	Distinction entre un appel et un appel d'urgence	97
4.9.4	Groupes d'alarmes	97
4.9.5	Alarme interne et instructions sur la manière de procéder	97
4.10	Exigences générales relatives au dispositif et au système	98
4.10.1	Exigences générales	98
4.10.2	Protection contre les influences environnementales	98
4.10.3	Influences sur site	98
4.10.4	Moyen de protection fonctionnelle	98
4.10.5	Sûreté/sécurité de fonctionnement	99
4.10.6	Indicateurs	99
4.10.7	Messages	100
4.10.8	Structure	100
4.10.9	Messages de traitement	101
5	Mise en service/livraison	101
5.1	Généralités	101
5.2	Informations générales	101
5.2.1	Documentation	101
5.2.2	Mise en service	102
5.3	Interaction fonctionnelle des composants du système	102
5.4	Options	102
6	Fonctionnement et entretien	102
6.1	Généralités	102
6.2	Essai opérationnel	103
6.3	Mise en service/réparations	103
6.4	Remplacement de la batterie et de la batterie rechargeable	103
6.5	Mises à jour logicielles	103
7	Tâches et responsabilités	103
7.1	Informations générales	103
7.2	Organisation en charge (organisation responsable)	105
7.3	Échelon supérieur de gestion	105
7.4	Gestion des risques techniques	106
7.4.1	Généralités	106
7.4.2	Spécifications dans le dossier TRM	107
7.5	Utilisateur ASBIS	107
7.6	Personne formée	108
7.7	Planificateur (planificateurs techniques, architectes, consultants, planificateurs généraux)	108
7.8	Installateur	108
7.9	Personnel d'entretien	109
7.10	Fabricant des composants du système et du réseau IT	109
8	Gestion des modifications	110
8.1	Informations générales	110
8.2	Processus de modification	110
Annexe A (informative)	Informations relatives aux annonces vocales	111
A.1	Informations générales	111

A.2 Exemples de textes d'annonce	111
Annexe B (informative) Systèmes d'interphone de bâtiment à sécurité avancée (ASBIS)	112
Annexe C (informative) Relations entre la TRM et l'ORM dans le cadre d'une gestion globale des risques liée à une application ASBIS	113
C.1 Informations générales	113
C.2 Description graphique	113
Annexe D (informative) Tableau: tableaux d'aide pour l'évaluation des risques	114
D.1 Identification des risques liés aux applications ASBIS	114
D.2 Exemple de tableau d'évaluation de la probabilité d'une situation d'urgence/dangereuse	115
D.3 Définitions des objectifs de protection dans le cadre de la planification d'un système ASBIS	116
D.4 Classification des protections demandées	117
Annexe E (informative) Réponses aux questions organisationnelles afin de réduire la durée des événements d'urgence, de danger et de phénomène dangereux	118
E.1 Étiquetages des portes et des bâtiments	118
E.2 Formation	118
Bibliographie	119
Figure 1 – Interdépendance entre le niveau humain/organisationnel et le niveau technique d'un système ASBIS utilisé pour réagir en cas d'urgence et de danger	79
Figure 2 – Structure d'un système ASBIS	80
Figure 3 – Classification du niveau	83
Figure 4 – Exemple de matériel de mise en garde d'urgence et de danger en tant que module simple	93
Figure 5 – Informations générales des interdépendances et des responsabilités	104
Figure C.1 – Aperçu des relations entre la TRM et l'ORM dans le cadre de la gestion globale des risques	113
Tableau 1 – Exigences relatives au système ASBIS et ses unités d'interphone en fonction du niveau	87
Tableau 2 – Exigences relatives à l'alimentation électrique du système ASBIS	95
Tableau D.1 – Identification des risques liés à des dangers classiques	114
Tableau D.2 – Tableau d'identification des conditions environnementales pour l'évaluation de la probabilité d'une situation d'urgence/dangereuse	115
Tableau D.3 – Liste des objectifs de protection classiques pour identifier la pertinence du risque	116

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SYSTÈMES D'INTERPHONE DE BÂTIMENT –

Partie 3-2: Lignes directrices d'application –
Systèmes d'interphone de bâtiment à sécurité avancée (ASBIS)

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62820-3-2 a été établie par le comité d'études 79 de l'IEC: Systèmes d'alarme et de sécurité électroniques.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/601/FDIS	79/605/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62820, publiées sous le titre général *Systèmes d'interphone de bâtiment*, peut être consultée sur le site web de l'IEC.

La présente Norme internationale doit être utilisée conjointement avec l'IEC 62820-3-1.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 62820-3-2:2018

INTRODUCTION

Le présent document est devenu nécessaire pour les raisons suivantes:

- Les champs d'application et l'importance des systèmes d'interphone de bâtiment à sécurité avancée (ASBIS) ont augmenté;
- il est nécessaire que des événements, des urgences, des dangers et des phénomènes dangereux différents fassent l'objet de réponses et de réactions adaptées, qui doivent au préalable être vérifiées par voie de communication vocale;
- les sociétés et les opérateurs néophytes en matière de système ASBIS ont besoin d'un guide détaillé.

Le présent document s'adresse en particulier à la police, aux compagnies d'assurance, aux planificateurs, aux architectes, aux fabricants et aux sociétés spécialisées dans les systèmes de sécurité, aux maîtres d'œuvre, aux propriétaires, aux opérateurs, aux utilisateurs du système ASBIS et aux résidents de tous types de bâtiments.

Le présent document couvre les applications correspondant à des risques de niveau plutôt élevé, comme les accidents, les urgences, les dangers, les attentats, les menaces terroristes, les fusillades en milieu scolaire, les attaques terroristes, les menaces d'attentat à la bombe, les séismes, les inondations, etc.

Un système ASBIS permet de recevoir des événements de communication d'accès avancée (appels visiteur, appels de réception d'utilisateur, appels de gestion de la sécurité) ainsi que d'autres événements (alarmes d'urgence, de danger et de phénomènes dangereux), de les transférer vers un destinataire technique et de les présenter de manière appropriée à un organisme de soutien (une unité de gestion de la sécurité, par exemple). Après avoir accusé réception, l'organisme de soutien prend la responsabilité de vérifier et de prendre les mesures définies conformément au fichier de gestion du risque technique. L'accusé de réception s'affiche au moment où l'action est déclenchée.

Une utilisation quotidienne d'autres applications ASBIS (Annexe B, par exemple) est suggérée pour former les utilisateurs ASBIS et pour la disponibilité du système au niveau 1 de l'IEC 62820-3-2. La fréquence d'utilisation quotidienne est un moyen de contrôle du système permettant d'indiquer sa disponibilité.

SYSTÈMES D'INTERPHONE DE BÂTIMENT –

Partie 3-2: Lignes directrices d'application – Systèmes d'interphone de bâtiment à sécurité avancée (ASBIS)

1 Domaine d'application

La présente partie de l'IEC 62820 décrit les exigences d'application de base des systèmes d'interphone de bâtiment à sécurité avancée (ASBIS) installés dans les bâtiments publics ou privés ayant des besoins en matière de sûreté et de sécurité avancées. Les systèmes ASBIS sont également utilisés pour satisfaire aux exigences des règlements locaux en matière de sécurité au travail et/ou d'autres règlements locaux pertinents, en particulier, la protection de la vie et de l'intégrité physique des employés et de toutes les personnes présentes dans le bâtiment, sans oublier les personnes handicapées (pour prévoir un accès sans obstacle ou des moyens d'appeler à l'aide, par exemple) si cela est exigé par la loi locale applicable.

Le présent document s'applique pour la planification, l'installation, la mise en service, la réception, le fonctionnement et la maintenance du système ASBIS, pour la transmission des messages audio d'urgence, de danger et de phénomène dangereux et/ou d'autres indications opérationnelles à une autorité chargée de l'assistance dans le cadre d'une évaluation à distance, et pour la mise en œuvre de mesures d'intervention, de protection et de secours adaptées. Des informations supplémentaires peuvent également être transmises et le système peut être utilisé dans le travail quotidien pour répondre à tous les besoins de communication. Le système ASBIS assure également une haute disponibilité pour la surveillance de l'unité d'extrémité et la surveillance du système.

Les systèmes d'interphone de bâtiment à sécurité avancée (ASBIS) sont utilisés pour les appels rapides pour signaler une urgence, un danger et un phénomène dangereux, la vérification par communication vocale, la mise en garde en cas de danger, la notification rapide des services d'urgence/intervention responsables et l'envoi d'instructions vocales et/ou d'autres indications pratiques quant à la manière de procéder. Les exigences relatives à un concept adapté portent sur l'appréciation préalable du risque et la définition de l'objectif de protection. La TRM (Technical-Risk Management – gestion des risques techniques) et l'ORM (Organizational Risk-Management – gestion des risques organisationnels) doivent permettre de mettre en place une stratégie de flux de travaux commune associée aux exigences système correspondantes, afin de parvenir à des risques résiduels. Le présent document donne les exigences relatives à la gestion des risques techniques, ainsi que des commentaires et recommandations en matière de gestion des risques organisationnels.

Le présent document d'application concernant un système ASBIS décrit, entre autres, les processus technologiques et les responsabilités engagées dans leur prise en charge, de la détection d'un événement (appel visiteur, urgence, danger, phénomène dangereux) jusqu'à son traitement. Il inclut la TRM, la définition des objectifs de protection et des procédures organisationnelles, et les exigences nécessaires relatives à un dossier TRM. Le présent document définit trois niveaux différents de sûreté/sécurité, chacun faisant l'objet d'exigences concernant les produits. Le choix des produits qui peuvent être déployés en tant que ressources techniques dans le cadre d'un système ASBIS relève de la responsabilité de la TRM à utiliser.

Le présent document, accompagné d'un système ASBIS, définit également les tâches, responsabilités et activités associées. Il s'agit d'éléments d'un processus TRM holistique visant à atteindre les objectifs en matière de protection de la sûreté/sécurité du personnel, de rendement et d'efficacité, de sécurité des données et du système. Le présent document ne spécifie aucun niveau de risque. En particulier, il ne définit aucun risque résiduel acceptable. La TRM et l'ORM sont d'une importance égale dans l'ensemble de la gestion des risques (voir l'Annexe C).

Le présent document définit les profils d'exigences techniques d'un système ASBIS pour trois niveaux de sûreté/sécurité. Il revient au gestionnaire des risques techniques de déterminer le niveau concerné, en s'appuyant sur son appréciation du risque, en choisissant le niveau correspondant le mieux au risque identifié et en permettant un risque résiduel acceptable. Les annexes au présent document aident à l'évaluation des risques.

Le présent document décrit également le processus de création, d'entretien et de mise à jour d'un dossier TRM. Les risques sont répertoriés et évalués, et les risques résiduels sont définis dans le présent document. Les résultats analysés définissent l'étendue et la structure du système ASBIS. Un système ASBIS fait partie intégrante d'une solution globale de gestion de certains événements (des urgences ou des crises, par exemple).

La structure et le fonctionnement d'un système ASBIS font appel à la TRM sur l'ensemble du cycle de vie du système ASBIS. La surveillance d'un système ASBIS sur son cycle de vie entre dans le cadre du dossier TRM.

Le présent document vise à faciliter la mise en œuvre d'exigences juridiques et autres.

En fonction des exigences des lois locales en matière d'invalidité ou de la réglementation correspondante concernant les personnes handicapées, un système ASBIS peut être utilisé pour la mise en œuvre de ce type de règlements locaux, à savoir une communication sous deux formes différentes, comme la lumière et le son, par exemple (principe à deux significations).

Le domaine d'application du présent document s'applique dans son ensemble pour d'autres systèmes de signalisation à distance et de technologie de l'information s'ils incluent les fonctions des systèmes d'interphone de bâtiment à sécurité avancée (ASBIS).

Le présent document ne remplace pas les normes correspondantes relatives aux systèmes de sûreté/sécurité ou autres systèmes pertinents. Ces systèmes peuvent toutefois être intégrés dans un système ASBIS en prenant ces normes en compte.

Si les règlements indiqués dans les normes pour ce type de systèmes contredisent le présent document, le gestionnaire des risques techniques met les règlements en balance les uns par rapport aux autres, les évalue et les documente dans la décision comme une dérogation à la norme dans le dossier TRM.

Les recommandations et exigences de l'IEC 62820-3-1 sont obligatoires pour la présente norme. Les exceptions doivent être décidées par le TRM et être documentées dans le fichier TRM.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

NOTE Les normes ci-dessous sont indiquées telles qu'elles sont connues. Si les normes figurant dans la liste ci-dessous ne sont pas nommées IEC ou ISO, les normes IEC/ISO correspondantes sont inconnues; utiliser à la place la norme locale disponible.

IEC 60268-16:2011, *Équipements pour systèmes électroacoustiques – Partie 16: évaluation objective de l'intelligibilité de la parole au moyen de l'indice de transmission de la parole*

IEC 60529, *Degrés de protection procurés par les enveloppes (code IP)*

IEC 60839-5-1:2014, *Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements* (disponible en anglais seulement)

IEC 60839-5-2:2016, *Alarm and electronic security systems – Part 5-2: Alarm transmission systems – Requirements for supervised premises transceiver (SPT)* (disponible en anglais seulement)

IEC 60839-5-3:2016, *Alarm and electronic security systems – Part 5-3: Alarm transmission systems – Requirements for receiving centre transceiver (RCT)* (disponible en anglais seulement)

IEC 60839-7-12:2001, *Systèmes d'alarme – Partie 7-12: Formats de message et protocoles pour les interfaces de données série dans les systèmes de transmission d'alarme – Interfaces PTT pour les voies de communication dédiées utilisant la recommandation UIT-T V.23 pour la signalisation*

IEC 61000-6-1, *Compatibilité électromagnétique (CEM) – Partie 6-1: Normes génériques – Immunité pour les environnements résidentiels, commerciaux et de l'industrie légère*

IEC 61000-6-3, *Compatibilité électromagnétique (CEM) – Partie 6-3: Normes génériques – Norme sur l'émission pour les environnements résidentiels, commerciaux et de l'industrie légère*

IEC 62262:2002, *Degrés de protection procurés par les enveloppes de matériels électriques contre les impacts mécaniques externes (code IK)*

IEC 62599-1:2010, *Systèmes d'alarme – Partie 1: Méthodes d'essais d'environnement*

IEC 62599-2, *Systèmes d'alarme – Partie 2: Compatibilité électromagnétique – Exigences relatives à l'immunité des composants des systèmes d'alarme de détection d'incendie et de sécurité*

IEC 62642-1:2010, *Systèmes d'alarme – Systèmes d'alarme contre l'intrusion et les hold-up – Partie 1: Exigences système*

IEC 62820-1-1:2016, *Systèmes d'interphone de bâtiment – Partie 1-1: Exigences du système – Généralités*

IEC 62820-1-2:2017, *Systèmes d'interphone de bâtiment – Partie 1-2: Exigences du système – Systèmes d'interphone de bâtiment utilisant le protocole internet (IP)*

IEC 62820-2, *Systèmes d'interphone de bâtiment – Partie 2: Exigences pour les systèmes d'interphone de bâtiment à sécurité avancée*

IEC 62820-3-1, *Building intercom systems – Part 3-1: Application guidelines – General* (disponible en anglais seulement)

IEC 62851-2, *Systèmes d'alarme et de sécurité électroniques – Systèmes d'alarme sociale – Partie 2: Déclencheurs*

IEC 62851-3, *Systèmes d'alarme et de sécurité électroniques – Systèmes d'alarme sociale – Partie 3: Unité locale et contrôleur*

ISO/IEC 17065, *Évaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services*

ISO 31000, *Management du risque – Principes et lignes directrices*

ISO/IEC 31010, *Gestion des risques – Techniques d'évaluation des risques*

ISO 7240-11:2011, *Systèmes de détection et d'alarme d'incendie – Partie 11: Déclencheurs manuels d'alarme*

UIT-T P.800, *QUALITÉ DE TRANSMISSION TÉLÉPHONIQUE: Méthodes d'évaluation objective et subjective de la qualité*

EN 50134-2:2016, *Systèmes d'alarme. Systèmes d'alarme sociale. Partie 2: Déclencheurs* (ou norme IEC équivalente)

EN 50134-3:2012, *Systèmes d'alarme – Systèmes d'alarme sociale – Partie 3: Unité locale et contrôleur* (ou norme IEC équivalente)

DIN VDE 0833-1 (VDE 0833-1):2009-09, *Systèmes d'alarme d'incendie, d'intrusion et d'attaque – Partie 1: Règles générales* (ou norme IEC équivalente)

3 Termes, définitions et abréviations

NOTE Seul le terme "danger" est utilisé ci-après pour éviter de répéter les trois termes "urgence, danger et phénomène dangereux".

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>.

3.1.1

essai de réception

examen conjoint documenté du système ASBIS par une personne/un opérateur/un gestionnaire qualifié ASBIS avec le plus haut niveau de gestion de la TRM ASBIS, se présentant sous la forme d'un contrôle visuel et fonctionnel et d'une vérification de l'exhaustivité des documents, en tant que condition préalable à la réception subséquente par l'opérateur et à la mise en service

3.1.2

matériel d'alarme

élément du matériel utilisé pour mettre en garde les personnes ou demander de l'aide en cas de danger

Note 1 à l'article: le matériel d'alarme peut faire partie intégrante d'un élément de matériel supplémentaire dans un système ASBIS.

3.1.3

signal d'alarme

alarme locale pour écarter le danger

EXEMPLE Signaux sonores et/ou optiques et/ou haptiques et/ou annonces vocales et/ou indicateurs opérationnels textuels.

3.1.4

système de transmission d'alarme

dispositif ou réseau de transmission d'alarme utilisé pour envoyer des informations relatives à l'état d'un ou de plusieurs système(s) d'alarme et systèmes ASBIS dans un bâtiment surveillé à un ou plusieurs dispositif(s) de manœuvre et d'affichage à partir d'un ou de plusieurs centre(s) de réception des alarmes

Note 1 à l'article: un système de transmission d'alarme peut être composé de plusieurs chemins de transmission d'alarme.

3.1.5

précontrôle d'alarme

contrôle d'une alerte pour savoir si elle résulte d'une situation dangereuse (au moyen d'un précontrôle sur site, d'un essai à distance par communication vocale et/ou d'une transmission des images de la situation, par exemple)

3.1.6

source d'alimentation de secours

source d'énergie en mesure d'alimenter le système ASBIS à l'avance pendant une durée déterminée lorsque la source d'alimentation principale n'est pas disponible

3.1.7

alarme ASBIS

mise en garde d'un danger existant pour les personnes, les biens ou l'environnement, déclenchée par un état d'alarme, ainsi que l'appel à l'aide en cas de danger

3.1.8

condition d'alarme ASBIS

état dans lequel il existe une situation potentiellement ou excessivement dangereuse et qui exige l'attention ou une réponse de la part d'un service d'intervention

3.1.9

utilisateur ASBIS

personne habilitée à utiliser le système ASBIS

3.1.10

personne qualifiée ASBIS spécialiste ASBIS

personne qui peut évaluer le travail attribué ou identifier les dangers potentiels grâce à sa formation, ses connaissances et son expérience techniques, et à sa connaissance du matériel, des normes, des exigences et des lignes directrices

Note 1 à l'article: le fonctionnement du système ASBIS exige la présence de personnes qualifiées en génie électrique dans le domaine de la messagerie, de l'information, des microprocesseurs, des mesures, de la commande ou dans le domaine du génie électrique en général. Une preuve doit être apportée des autres domaines et connaissances des systèmes d'alarme de danger. Des connaissances sont nécessaires en matière d'évaluation des conditions préalables des bâtiments, des systèmes de protection incendie ou des systèmes mécaniques de sûreté/sécurité, des effets liés à la fréquentation des salles et des limites à l'utilisation des captures de notification.

Note 2 à l'article: un poste occupé pendant plusieurs années dans un domaine d'activité correspondant peut permettre d'évaluer la formation spécialisée.

3.1.11

autorité chargée de l'assistance

personne nommée par l'opérateur du système ASBIS ou centre dont la permanence est assurée vingt-quatre heures sur vingt-quatre (poste de commande d'urgence et de service, comme l'organisme d'assistance) qui reçoit des alarmes, des alertes et des informations provenant du bâtiment, qui vérifie ces informations avant de les transmettre et qui demande à d'autres personnes de prendre les mesures appropriées (surveiller ou fouiller le bâtiment, par exemple)

3.1.12**durée de la période de secours**

durée pendant laquelle la source d'alimentation de secours peut maintenir l'ensemble des fonctionnalités du système ASBIS

3.1.13**mise en service**

essai final, procédure de fin de traitement et activation du système ASBIS par le propriétaire, l'organisme en charge ou le TRM

3.1.14**communication**

commutation ou envoi de signaux ou d'informations entre des composants du système et des personnes

Note 1 à l'article: pour un système ASBIS, cela comprend, mais sans s'y limiter:

- a) le transfert de signaux utiles entre la source et le destinataire et entre l'ensemble des composants/fonctions techniques;
- b) le transfert de signaux de contrôle et d'accusé de réception entre la source et le destinataire par l'intermédiaire de tous les composants nécessaires du système;
- c) la transmission vocale, de texte et/ou d'image(s) entre la source et le destinataire;
- d) une communication vocale (dialogue vocal) entre le déclencheur et l'autorité chargée de l'assistance par l'intermédiaire de tous les composants nécessaires du système;
- e) une communication vocale (dialogue vocal) entre l'autorité chargée de l'assistance et le déclencheur et le service d'intervention par l'intermédiaire de tous les composants nécessaires du système.

3.1.15**sécurité des données et du système**

état de fonctionnement d'un système ASBIS, dans lequel les informations importantes (données et systèmes) font l'objet d'une protection adaptée contre les dégradations de la confidentialité, de l'intégrité et de la disponibilité

Note 1 à l'article: la sécurité des données et du système doit être assurée par des lignes directrices, des manuels, une infrastructure et des services qui ont été développés pour protéger les informations importantes et les systèmes, utilisés pour enregistrer, transmettre, sauvegarder et appliquer des informations afin de satisfaire au mieux aux objectifs de l'organisation.

3.1.16**appel d'urgence**

demande d'aide ou d'informations en cas d'urgence (premiers secours, par exemple)

3.1.17**poste de commande d'urgence et de service**

endroit occupé vingt-quatre heures sur vingt-quatre commandé par l'opérateur qui reçoit les alarmes, alertes et informations à distance provenant d'un bâtiment sous surveillance, qui les contrôle avant de les transmettre, qui demande à d'autres personnes de prendre les mesures nécessaires (comme la surveillance du bâtiment et/ou une demande d'intervention, par exemple) et qui en rend compte

3.1.18**évaluation**

contrôle du matériel ou procédure réalisée par du personnel qualifié pour évaluer son aptitude à atteindre les objectifs poursuivis

3.1.19**fausse alarme****alarme indésirable**

alarme qui n'est pas indicative d'un danger

3.1.20

défaut

état d'une unité (un système ASBIS ou un composant individuel du système, par exemple) qui se caractérise par son inaptitude à satisfaire à la fonction exigée, quelle qu'en soit la raison

3.1.21

message de défaut

message indiquant l'existence d'un écart par rapport à la fonctionnalité spécifiée d'un système ASBIS ou d'un composant du système ASBIS

3.1.22

conférence téléphonique

audioconférence

appel des personnes appropriées qui doivent atténuer ou mettre un terme aux conflits entre des personnes

3.1.23

intégrateur

serveur ASBIS

composant système utilisé pour satisfaire une fonction technique d'un système ASBIS utilisé comme unité de commande, y compris une boîte de dérivation (un commutateur, par exemple), pour le traitement, le transfert, la dérivation et la documentation entre la source et le récepteur, qui peut être un répartiteur intégré, de manière centralisée ou répartie, ou dans la source ou le destinataire

3.1.24

alarme interne

signal d'alarme dans le bâtiment, après le déclenchement des fonctions ASBIS, visant à mettre en garde les personnes présentes dans la zone concernée afin de mettre en place les actions exigées (auto assistance, auto sauvetage, par exemple) et d'informer une autorité chargée de l'assistance, le cas échéant

3.1.25

intervention

action permettant d'éviter ou de limiter les blessures corporelles et les dommages matériels

3.1.26

service d'intervention

personne qui prend des mesures visant à écarter un danger après une alerte ou une alarme afin d'empêcher ou de limiter les blessures corporelles et/ou les dommages matériels

3.1.27

examen

mesure permettant d'établir et d'évaluer l'état réel d'un système ASBIS, y compris la détermination des causes d'usure accrue et de prévoir des mesures préventives à usage ultérieur

3.1.28

installateur

spécialiste, organisme ou société disposant du personnel qualifié ASBIS, chargé(e) des bonnes installation, mise en service et documentation du système ASBIS et de la formation des utilisateurs ASBIS

3.1.29

immédiat

réalisé sans délai volontaire (un examen ou une réparation, par exemple)

3.1.30**source d'alimentation principale**

source d'énergie qui alimente le système ASBIS dans les conditions normales de fonctionnement

3.1.31**personnel d'entretien**

société spécialisée disposant des personnes qualifiées ASBIS qui peuvent réaliser tous les travaux d'entretien, tous les examens, toutes les extensions et toutes les modifications, et qui assure son service 365 jours par an, y compris la détention de pièces détachées

3.1.32**maintenance**

combinaison de toutes les mesures techniques et administratives et des mesures de gestion pendant le cycle de vie d'un système ASBIS, afin d'assurer 100 % de disponibilité dans un parfait état de fonctionnement ou à l'état dégradé convenu

3.1.33**poste d'appel**

Interphone, URU, SMU, VCU et toute autre unité d'interphone et simples boutons d'appel, etc.

3.1.34**réseau**

système(s), composé(s) de réseaux de communication et de connexions de communication, utilisé(s) pour assurer les transmissions entre au moins deux nœuds de transmission spécifiques grâce à des câbles, des fibres, sans fil ou tout autre moyen adapté

3.1.35**attentat de masse**

acte de violence perpétré de manière aléatoire ou préméditée, avec de nombreuses personnes blessées ou tuées (en général des anonymes), à l'aide d'armes, d'explosifs, d'outils dangereux ou en faisant usage de la force, ou lorsque ce type d'événement est anticipé et peut avoir un impact sur d'autres personnes

3.1.36**indicateurs opérationnels**

informations (acoustiques, visuelles ou sous toute autre forme) qui aident l'utilisateur à faire fonctionner le système ASBIS

3.1.37**essai opérationnel**

activité à réaliser après l'installation, l'extension, la modification ou après les travaux de réparation, afin de confirmer que le système ASBIS peut satisfaire à la fonction exigée

3.1.38**organisme en charge****organisme responsable**

organisme (ou personnel employé par un organisme) qui porte la responsabilité juridique du système ASBIS et qui peut supporter un, plusieurs ou tous les coûts d'installation, d'exploitation et d'entretien

EXEMPLES Un ministère, un conseil de guerre, une autorité municipale, un conseil municipal ou des employés ou sous-traitants, selon le cas.

3.1.39**processus**

ensemble d'activités corrélées ou interactives liées qui, lorsqu'elles sont activées, mène au(x) résultat(s) souhaité(s)

Note 1 à l'article: le terme "activités" comprend l'application des ressources.

[SOURCE: ISO 14971:2007, 2.13, modifiée – La phrase "transforme des éléments d'entrée en éléments de sortie" a été remplacée par "lorsqu'elles sont activées, mène au(x) résultat(s) souhaité(s)".]

3.1.40

objectifs de protection

niveau de sûreté/sécurité à atteindre avec différents types de mesures prises en fonction des dangers prévus, en prenant en considération la sûreté/sécurité du personnel, l'efficacité/le rendement, la sécurité des données et du système, et selon lequel les objectifs finaux visés sont atteints, même si les moyens d'atteindre ces objectifs restent ouverts

3.1.41

récepteur

destinataire

composant du système permettant de satisfaire une fonction technique d'un système ASBIS et qui reçoit des signaux d'alarme de la part de l'intégrateur, les affiche et les transmet à une autorité chargée de l'assistance, transmettant également à l'intégrateur les réponses reçues de cette autorité avec des signaux de commande et de communication

3.1.42

signal de rappel

signal (acoustique, par exemple) qui attire l'attention de l'utilisateur du système ASBIS sur la fonctionnalité limitée du système ASBIS à intervalle régulier (une fonction de mise hors tension, des dispositifs de mise en garde qui ont été mis hors tension, etc.)

3.1.43

téléalarme

alarme provenant d'une autorité chargée de l'assistance ne se trouvant pas sur le site (pompier, police ou compagnie de sûreté/sécurité, par exemple)

3.1.44

dispositif de transfert de téléalarme

dispositif de transmission (de transfert) de téléalarme, d'alertes et d'informations à une autorité mandatée chargée de l'assistance

3.1.45

réparations

procédure permettant de rétablir toutes les fonctionnalités d'un système ASBIS défaillant, sans modifications ni ajouts

3.1.46

risque résiduel

risque subsistant après avoir pris des mesures pour le gérer

[SOURCE: ISO 14971:2007, 2.15, modifiée – La définition a été remaniée.]

3.1.47

risque

combinaison de la probabilité d'un dommage et de sa gravité

[SOURCE: ISO 14971:2007, 2.16, modifiée – En anglais, "harm" a été remplacé par "damage".]

3.1.48

analyse du risque

utilisation des informations disponibles pour identifier tous les types de dangers et estimer les risques qui en découlent

[SOURCE: ISO 14971:2007, 2.17, modifiée – "phénomènes dangereux" et "le risque" ont été respectivement remplacés par "tous les types de danger" et "les risques qui en découlent".]

3.1.49

évaluation des risques

partie d'un processus TRM conforme à l'ISO 31000 portant sur l'identification, l'analyse et l'évaluation du risque

3.1.50

maîtrise du risque

processus au cours duquel les décisions sont prises et les mesures visant à réduire les risques ou à les maintenir dans les limites spécifiées sont mises en place

[SOURCE: ISO 14971:2007, 2.19, modifiée – La définition a été remaniée.]

3.1.51

société spécialisée

entreprise chargée de la planification, de l'installation et de la mise en service du système ASBIS et qui dispose d'au moins un employé qualifié (personne qualifiée ASBIS)

3.1.52

sabotage

dommages physiques, cyberdommages ou autres types de dommages volontaires dont fait l'objet un système ASBIS ou ses composants

3.1.53

concept de sûreté

concept de sécurité

base globale prédéfinie sur laquelle la procédure en matière d'organisation, de personnel, de technique et de construction est exécutée pour assurer la protection du bâtiment ou écarter tout danger

Note 1 à l'article: le concept de sûreté/sécurité doit au moins contenir des informations relatives à l'usage du bâtiment, au risque dont il fait l'objet, aux objectifs de protection du système ASBIS (de manière à éviter les blessures corporelles et/ou les dommages matériels), aux zones à surveiller avec des systèmes d'alarme automatiques, aux alarmes non automatiques que des personnes doivent activer, aux fonctions de commande existantes, aux mesures de protection des personnes et aux zones d'alarme et centres d'assistance.

3.1.54

transducteur de signal

dispositif qui génère et émet des signaux sonores et/ou visuels

3.1.55

source

composant du système qui peut déclencher automatiquement ou manuellement une condition d'alarme ASBIS, et recevoir et afficher des accusés de réception, en émettant des signaux ou en activant la communication vocale

3.1.56

composant du système

éléments individuels du matériel qui composent ensemble un système ASBIS

3.1.57

dossier TRM

ensemble des enregistrements et d'autres documents produits pendant la TRM

[SOURCE: ISO 14971:2007, 2.23, modifiée – Le terme "dossier de gestion des risques" a été remplacé par "dossier TRM" et la définition a été remaniée.]

3.1.58

gestionnaire des risques techniques

personne chargée de la TRM d'un système ASBIS (un gestionnaire de sécurité certifié ou similaire, par exemple)

3.1.59

dispositif de transmission

partie d'un système de transmission d'alarme pour les alertes de danger, utilisée pour transmettre des notifications

3.1.60

chemin de transmission

connexion externe des composants du système utilisée pour envoyer des informations ou des messages à partir d'un système ASBIS

Note 1 à l'article: le chemin de transmission peut également être utilisé comme moyen d'alimentation en énergie.

3.1.61

gestion des risques techniques

TRM

application systématique des politiques de gestion, des procédures et des expériences pratiques à des tâches d'analyse, d'évaluation, de gestion et de maîtrise des risques

[SOURCE: ISO 14971:2007, 2.22, modifiée – Le terme "gestion des risques" a été remplacé par "gestion des risques techniques" et la définition a été remaniée.]

3.1.62

échelon supérieur de gestion

personne ou groupe de personnes nommé(e) par l'organisation en charge de la gestion globale et par le client, chargé(e) du système ASBIS au plus haut niveau, et qui doit approuver le dossier TRM et le risque résiduel qui en découle (l'autorité locale/le chef de service, le directeur/directeur d'établissement scolaire ou l'employeur et ses employés, le directeur général, le cadre supérieur, par exemple)

3.1.63

personne formée

personne ayant reçu une formation dispensée par un spécialiste qualifié du système ASBIS (personne qualifiée ASBIS) sur les tâches nécessaires au fonctionnement d'un système ASBIS et qui est en mesure de prendre à son compte l'exploitation du système ASBIS

Note 1 à l'article: il s'agit d'exécuter ou de demander à d'autres personnes d'exécuter des mesures de protection pour écarter tout danger en mettant hors tension ou en interrompant les composants du système, et de demander à d'autres personnes de remédier aux défauts ou de procéder à des réparations.

3.1.64

transmission des images

dans le cas d'une alarme, envoi d'images de la zone dans laquelle elle a été générée avec la procédure de transmission et le format de fichier spécifiés (l'image et, le cas échéant, la commande) afin de valider l'alarme, confirmer l'endroit exact et permettre/prendre en charge les mesures par les services d'intervention

3.1.65

vérification

preuve de l'exactitude, des faits, de la cause d'une alarme (établissement de la vérité) en observant et en vérifiant la cause du déclencheur/processus d'une alarme, au moyen d'un examen visuel réalisé par le personnel, d'une communication ou de la transmission d'images de la situation, en cas de doute, en étudiant également le processus de déclenchement afin de faire la distinction entre une fausse alarme et une véritable situation dangereuse

3.1.66**systèmes d'alarme vocale**

système utilisé pour émettre des alarmes et des instructions grâce à des signaux sonores et des annonces vocales, et qui permet de faire des annonces en direct après une commande automatique par une mise en garde d'un danger différente

3.1.67**jour ouvrable**

jour où le travail est réalisé

3.2 Abréviations

Les abréviations suivantes sont utilisées:

TRM	Technical Risk Management (gestion des risques techniques)
ORM	Organizational Risk Management (gestion des risques organisationnels)
GRM	General Risk Management (gestion des risques généraux)
RM	Risk Management (gestion des risques)
VSS	Video Surveillance System (système de surveillance vidéo)
ASBIS	Advanced Security Building Intercom Systems (systèmes d'interphone de bâtiment à sécurité avancée)
SMU	Security Management Unit (unité de gestion de la sécurité)
VCU	Visitor Call Unit (unité d'appel du visiteur)
URU	User Receiver Unit (unité de réception d'utilisateur)

4 Exigences relatives au système ASBIS et domaines d'application**4.1 Généralités**

Les recommandations et exigences de l'IEC 62820-3-1 sont obligatoires pour le présent document. Les exceptions doivent être décidées par le TRM et être documentées dans le fichier TRM.

Le système ASBIS doit être planifié, installé, utilisé, modifié et entretenu selon les spécifications de l'IEC 62820-2 et du présent document.

Avec différentes organisations d'alarme, une enquête de situation est nécessaire après un message d'alarme afin de vérifier la cause de l'alarme et de mettre en œuvre aussi rapidement que possible les différentes mesures d'intervention, de sauvetage et de protection en fonction de la cause (en cas d'incendie ou d'attentat de masse, par exemple). Par conséquent, il est nécessaire de procéder à une enquête de situation rapide pour mettre en œuvre les bonnes mesures d'intervention, de protection et de sauvetage. Une enquête de situation peut également révéler des erreurs et de fausses alarmes. Elle évite de prendre des mesures inutiles. Les systèmes ASBIS, décrits dans le présent document, sont spécialement conçus pour ce type d'enquête de situation. L'autorité chargée de l'assistance peut utiliser ces systèmes pour clarifier et obtenir des informations relatives à la situation auprès des personnes sur site qui ont déclenché l'appel ou l'appel d'urgence, puis prendre les mesures adaptées.

Les systèmes ASBIS sont conçus pour répondre à la plupart des besoins en matière de communication de sécurité dans tous les types de bâtiments. Des exemples de tout l'éventail des communications de sécurité avancées possibles pour les applications sont donnés à l'Annexe B.

- Toutes les applications de communication de sécurité présentes dans un bâtiment dédié peuvent être réalisées par un système ASBIS individuel ou dans le cadre d'une solution ASBIS commune intégrée. L'intégration dans un seul système ASBIS d'applications de

sécurité à usage quotidien (communication d'accès, par exemple) et d'applications de sécurité utilisées dans de très rares situations (des actes terroristes, par exemple) est très utile.

- La fréquence d'utilisation quotidienne est un moyen de contrôle du système permettant d'indiquer sa disponibilité.
- L'utilisation quotidienne peut éviter de se former sur le fonctionnement du système dans les situations d'urgence rares.
- Un système ASBIS pour au moins 2 applications de sécurité différentes n'a besoin que d'un seul réseau câblé de données.

4.2 Exemples choisis d'applications ASBIS

4.2.1 General

Toutes les fonctionnalités suivantes des exemples donnés sont en général intégrées dans une application ASBIS.

4.2.2 ASBIS pour la communication d'accès

Pour répondre à leurs besoins de communication quotidiens, les bâtiments doivent être équipés d'unités d'interphone faisant partie intégrante du concept global de sécurité (portes, barrières, entrées et sorties de parking, distributeurs automatiques, portes à verrouillage, terminaux d'information, points de communication interne, points d'assemblage, par exemple).

Le système ASBIS doit être en mesure de s'intégrer totalement à d'autres disciplines ou d'en incorporer (les systèmes de contrôles d'accès, les systèmes de surveillance vidéo, les systèmes d'annonces passagers, les systèmes d'alarme incendie et les systèmes de refuges désactivés, par exemple).

4.2.3 ASBIS dans les écoles et autres établissements d'enseignement

Par exemple, l'utilisation d'un système d'alarme, conformément aux lignes directrices en matière de construction d'établissements scolaires, en décrivant toutes les phases de la chaîne de processus, du message (d'alarme) au sauvetage (inclusion/évacuation), et l'utilisation d'un système de réponse d'urgence et de danger (en particulier pour les attentats de masse et autres situations), avec surveillance et conférence d'urgence, et pour l'utilisation quotidienne dans les établissements scolaires (pour les interjections, la radiomessagerie, la communication de signal d'arrêt et la communication scolaire, par exemple).

4.2.4 ASBIS dans les administrations et les bureaux

Communication, en cas d'urgence ou de danger, permettant d'obtenir l'aide du personnel interne grâce à une alarme interne (ici sans alarme acoustique à l'emplacement du déclencheur) ou des services d'intervention externes grâce à une téléalarme avec surveillance d'urgence et conférence d'urgence.

4.2.5 ASBIS dans le système juridique

Communication en cas d'urgence ou de danger permettant d'obtenir l'aide du personnel interne grâce à une alarme interne (ici sans alarme acoustique à l'emplacement du déclencheur) ou des services d'intervention externes grâce à une téléalarme avec surveillance d'urgence et conférence d'urgence. De même, appel de témoins et communication cellulaire.

4.2.6 ASBIS dans les gares et les aéroports

Dispositifs d'urgence et d'appel d'urgence concernant les accès en fauteuil roulant (noter en particulier ce qui suit: volume, intelligibilité vocale et accès sans obstacle).

4.2.7 ASBIS dans les centres commerciaux

Interphone de point d'aide avec centres de service, interphone d'urgence dans les salles de repos pour les personnes handicapées. Interphone d'alarme terroriste avec connexion et communication directes avec les forces d'intervention. Interphone de point d'aide d'urgence avec connexion et communication directes avec l'ambulance. Interface avec l'installation de diffusion sonore. Communication d'urgence dans un ascenseur.

4.2.8 ASBIS dans les bâtiments résidentiels publics

En fonction de l'usage du bâtiment, une combinaison des fonctionnalités et des applications mentionnées dans les exemples ci-dessus peut s'avérer être une solution pertinente pour les situations d'urgence et les situations dangereuses, de même que la combinaison d'une communication interne rapide et d'une messagerie d'alerte restreinte dans des situations dangereuses particulières.

4.2.9 Autres exemples

L'Annexe B présente une liste des applications ASBIS classiques pour différents bâtiments. Plus les applications et fonctions intégrées dans un système sont différentes, plus le degré d'utilisation du système est élevé. Un degré plus élevé d'utilisation peut diminuer les risques résiduels.

4.3 Organigramme opérationnel ASBIS pour la communication d'urgence et de danger

Le flux de travaux d'un événement de danger signalé par une unité d'interphone peut être divisé en deux niveaux: le "niveau humain/organisationnel" et le "niveau technique". Ces deux niveaux sont interdépendants. La Figure 1 présente les différentes mesures prenant en compte la durée de l'événement. Chaque mesure humaine/organisationnelle exige une mesure technique correspondante, et inversement.

Tout le flux de travaux humain/organisationnel (niveau supérieur de la flèche) doit être spécifié par l'organisation en charge et/ou par l'échelon supérieur de gestion.

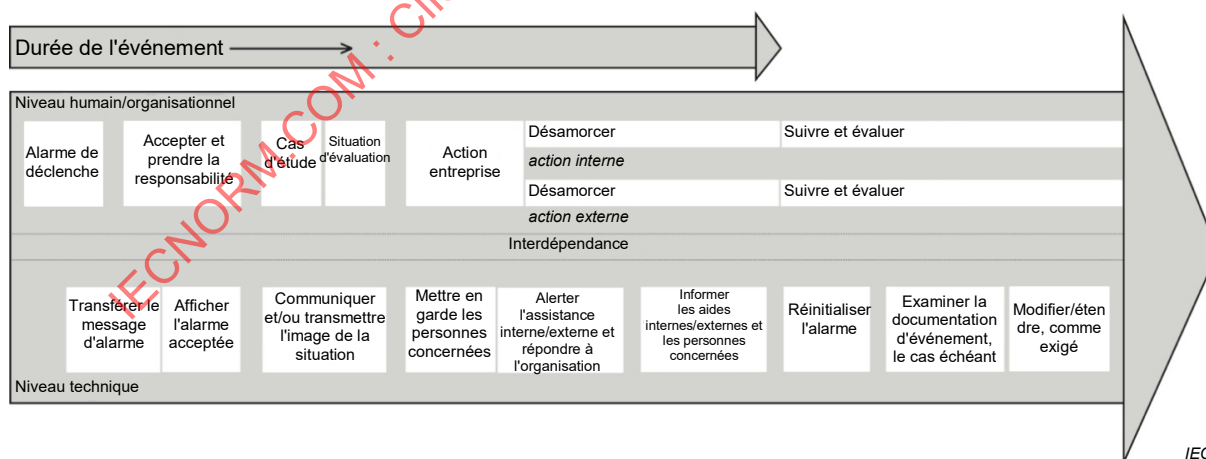
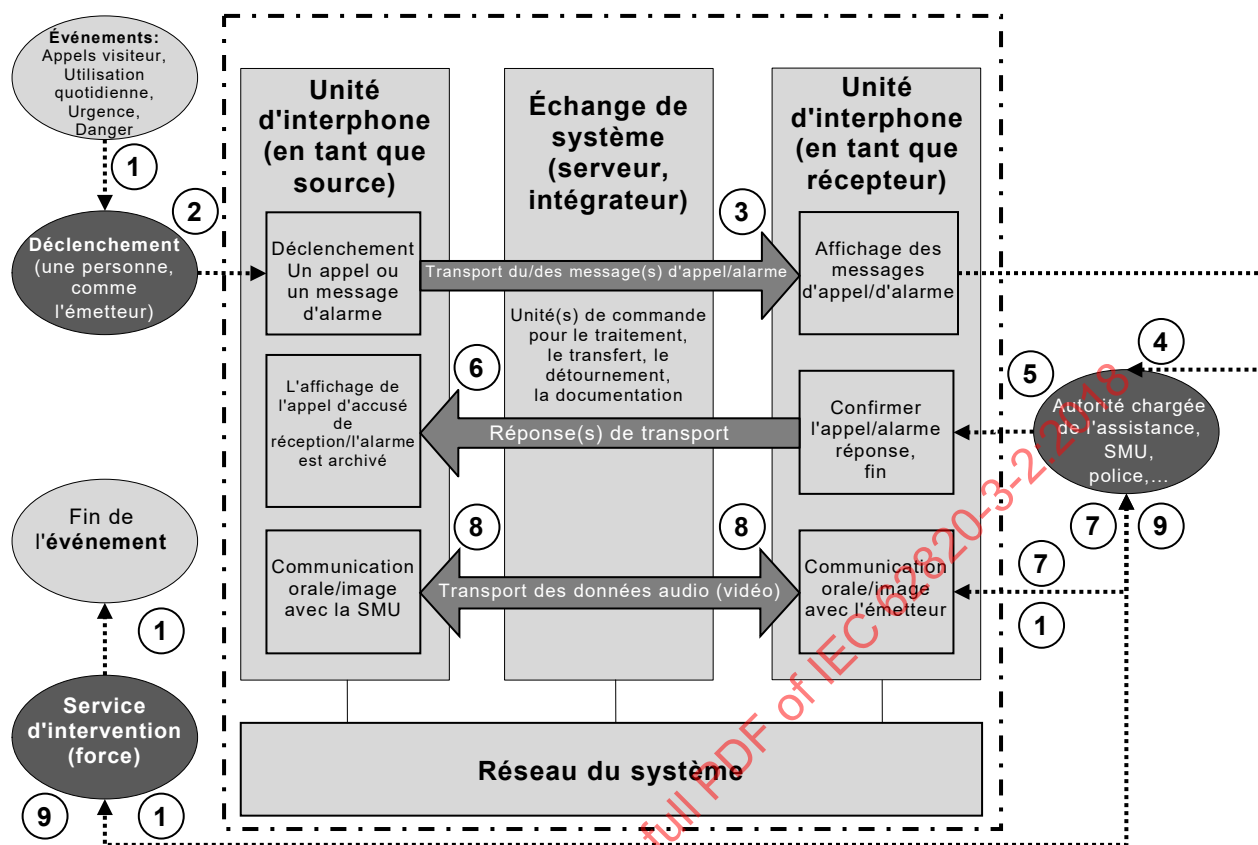


Figure 1 – Interdépendance entre le niveau humain/organisationnel et le niveau technique d'un système ASBIS utilisé pour réagir en cas d'urgence et de danger

4.4 Structure du système

Les systèmes ASBIS sont des dispositifs techniques de sûreté et de sécurité et doivent faire partie intégrante de l'ensemble du concept de sûreté/sécurité pour la protection de la sécurité et du personnel dans le champ d'application. Ils doivent satisfaire aux exigences en matière d'utilisation et de protection en termes de rendement, de fiabilité opérationnelle et de disponibilité.



IEC

Figure 2 – Structure d'un système ASBIS

La Figure 2 représente la structure d'un système ASBIS et décrit les fonctions et dispositifs. Ces fonctions individuelles présentées dans la figure sont séparées les unes des autres par souci de clarté. Toutefois, les différentes fonctions peuvent être combinées dans un dispositif/boîtier. Ces fonctions et le flux de travaux sont décrits ci-dessous :

- 1) Un événement (visiteur, situation d'urgence, danger) est observé par le déclencheur (une personne).
- 2) Le déclencheur (une personne) signale un événement en actionnant un dispositif de messagerie/mise en garde ASBIS (en appuyant sur un bouton de la VCU/URU).
- 3) Le message d'appel/alarme est envoyé au destinataire pertinent (SMU/URU) à cet effet par l'intermédiaire de l'unité de commande du système (dispositif d'échange électronique) dans laquelle il s'affiche de manière visuelle/acoustique.
- 4) L'autorité chargée de l'assistance (SMU) observe les indicateurs opérationnels du message d'appel/alarme.
- 5) Le destinataire (SMU) accuse réception de la demande d'appel ou du message d'alarme.
- 6) Envoi d'une confirmation de réception (accusé de réception correspondant à la demande d'appel/au message d'alarme) déclenchant les indicateurs opérationnels visuels/acoustiques du terminal d'appel (annonce pour rassurer, par exemple) (VCU / URU).
- 7) Établissement de la connexion pour une transmission audio par l'autorité chargée de l'assistance dans le cadre d'une demande de positionnement (éventuellement avec la transmission de la vidéo de la situation) (SMU/URU).
- 8) Dialogue vocal avec le déclencheur pour déterminer et vérifier le type et la portée de l'événement (éventuellement avec la transmission de la vidéo de l'emplacement) (SMU-URU, SMU-VCU, URU-VCU).
- 9) Fin de l'événement.

- 9) Alerte des services d'intervention par l'autorité chargée de l'assistance (SMU) par l'intermédiaire d'une communication vocale (éventuellement avec la transmission de données supplémentaires) et, le cas échéant, déclenchement d'une alarme interne adaptée.
- 10) Le service d'intervention prend la responsabilité et, le cas échéant, déclenche une alarme interne adaptée.
- 11) Le service d'intervention met fin à l'événement.

4.5 Tâches d'un système ASBIS

4.5.1 Généralités

Les interphones d'urgence et de danger doivent exécuter plusieurs tâches dans le domaine d'application. Elles sont décrites ci-dessous.

4.5.2 Tâches de sûreté/sécurité

- a) Signaler les cas d'urgence et les dangers à une autorité chargée de l'assistance.
- b) Demande de positionnement (vérification) par l'autorité chargée de l'assistance par l'intermédiaire d'une communication vocale avec les personnes se trouvant sur le site de déclenchement.
- c) Surveillance d'urgence des lieux d'urgence/de danger par les services d'intervention.
- d) Transmission des informations de mise en garde et des informations relatives à la manière de procéder (annonce en direct/stockage de vitesse) dans la zone concernée (pièces individuelles, groupes de pièces, choisir les pièces du bâtiment ou tout le bâtiment) avec des annonces adaptées.
- e) Chercher les appels avec réponse automatique (premiers secours, médiateurs, par exemple).
- f) Possibilité de télécommander d'autres techniques de sûreté/sécurité/surveillance (système d'alarme vocale [VAS – Voice Alarm System], vidéo, commande d'accès) via l'interface.

4.5.3 Tâches visant à améliorer les processus quotidiens (écoles, universités, etc. dans l'exemple)

- a) Rechercher les appels avec des réponses personnelles (directeur, enseignants, concierge, étudiants font l'objet d'une recherche, par exemple).
- b) Annonces générales d'importance générale au niveau de la zone ou du groupe (changement de planning, admissions à un événement, informations générales).
- c) Enquêtes et clarifications dans le cadre de discussions individuelles (avec l'administration, par exemple).
- d) Transmission des annonces de signal.

4.5.4 Communication quotidienne

Le flux de travaux opérationnel de base étant identique qu'il s'agisse d'une utilisation quotidienne ou d'une gestion des urgences et des dangers, son utilisation quotidienne pour la communication interne entraîne automatiquement le déclenchement d'une opération en cas d'urgence ou de danger. Le système est tellement utilisé quotidiennement que, dans la plupart des cas, des exercices réguliers peuvent être évités.

De plus, l'utilisation quotidienne du système peut s'apparenter à un contrôle de disponibilité dans le cadre des examens techniques nécessaires (pour la transmission des annonces de signal toutes les 45 min, par exemple) dans un établissement scolaire. Si le signal d'arrêt manque, cela peut signifier que le système ne fonctionne pas en totalité ou en partie et qu'il exige l'intervention du service technique.

4.6 Niveaux de sûreté/sécurité

Un système ASBIS peut être composé de différents types d'applications pour la communication d'accès, les alarmes en cas de danger, les alarmes en cas de menace, les alarmes de bâtiment, les appels de retrait, les appels à l'aide, les alarmes de confinement, la communication et les informations vocales, par exemple. La nature, la portée et le niveau des applications concernées régissent la manière de configurer le système ASBIS en termes techniques. Le gestionnaire des risques techniques prend les décisions exigées dans le cadre du processus de planification et d'évaluation.

Pendant la planification, l'installation, l'exploitation et l'extension du système ASBIS dans le cadre du domaine d'application du processus TRM, les problèmes liés à la protection des données, la situation juridique correspondante et d'autres documents officiels ou exigés d'un point de vue juridique pour les assurances (protection incendie, chemins d'évacuation/chemins d'évacuation d'urgence) ainsi que d'autres normes doivent être pris en compte.

En particulier, les autorités responsables (pompiers, police, par exemple) participent déjà à la phase de planification ou à l'élaboration du concept de protection global dans le cadre du processus TRM. En particulier, le transfert de l'alarme et les mesures d'intervention, y compris les plans exigés pour l'intervention, doivent faire l'objet d'un accord d'intervention. Cela doit être documenté dans le dossier TRM.

Pendant la planification, l'installation, l'exploitation et les extensions du système ASBIS, la minimisation des fausses alarmes doit toujours être prise en compte et mise en œuvre à l'aide de mesures adaptées.

Le degré du niveau de sûreté/sécurité à atteindre dépend

- de l'analyse des risques liés à la situation de risque individuelle (évaluation des risques),
- de l'application convenue des mesures de sûreté/sécurité (mesures de protection de la construction et de protection mécanique, par exemple) et des mesures électroniques (dispositifs électroniques, visuels ou autres) dans le domaine d'application d'un système ASBIS intégral,
- de l'interaction ciblée de tous les dispositifs techniques avec des procédures organisationnelles et administratives (contrôles des accès, codes de conduite, communication vocale) et des instructions claires,

de ce qui doit être vérifié à intervalles réguliers en termes d'aptitude à la fonction, de rendement et de conformité.

Les systèmes ASBIS sont divisés en trois niveaux de sûreté/sécurité, comme suit:

Niveau 1:

exigences d'application à risque faible. Les exigences techniques de l'application sont satisfaites en contrôlant le système afin de s'assurer qu'il fonctionne comme prévu chaque jour ouvrable. Le système peut être contrôlé manuellement ou automatiquement. Si l'application est également utilisée pour les procédures d'exploitation normales tous les jours ouvrables, cela est considéré comme étant équivalent. Dans tous les cas, il est important de s'assurer que les mesures appropriées sont prises conformément au dossier TRM en cas de défaut, l'initiateur et l'autorité chargée de l'assistance devant également pouvoir communiquer oralement pour procéder à la vérification.

Niveau 2:

exigences d'application à risque moyen. Les exigences techniques de l'application sont satisfaites en contrôlant le système afin de s'assurer qu'il fonctionne comme prévu plusieurs fois par jour (tous les jours). Le contrôle du système doit être automatique pour éliminer les erreurs humaines si l'essai est réalisé manuellement. Il est important de s'assurer que les

mesures appropriées sont prises conformément au dossier TRM en cas de défaut, l'initiateur et l'autorité chargée de l'assistance devant également pouvoir communiquer oralement pour procéder à la vérification.

Niveau 3:

exigences d'application à risque élevé. Les exigences techniques de l'application sont satisfaites en contrôlant automatiquement le système tous les jours, au moins pour s'assurer qu'il fonctionne comme prévu. Tous les composants d'application et les voies de transmission doivent être surveillés en permanence. La surveillance implicite des voies de transmission en vérifiant que tous les composants actifs (source, intégrateur et récepteur) sont opérationnels à tout moment est considérée comme étant une opération équivalente. Toutes les sources et tous les récepteurs doivent indiquer à tout moment de manière active que l'application peut être utilisée comme prévu. Il est important de s'assurer que les mesures appropriées sont prises conformément au dossier TRM en cas de défaut, et que l'initiateur et l'autorité chargée de l'assistance sont en mesure de communiquer oralement (dialogue vocal en temps réel) pour procéder rapidement à la vérification.

D'autres exigences techniques correspondant aux différents niveaux sont présentées au Table 1.

Les informations du Figure 3 doivent être prises en compte lors de la classification du niveau.

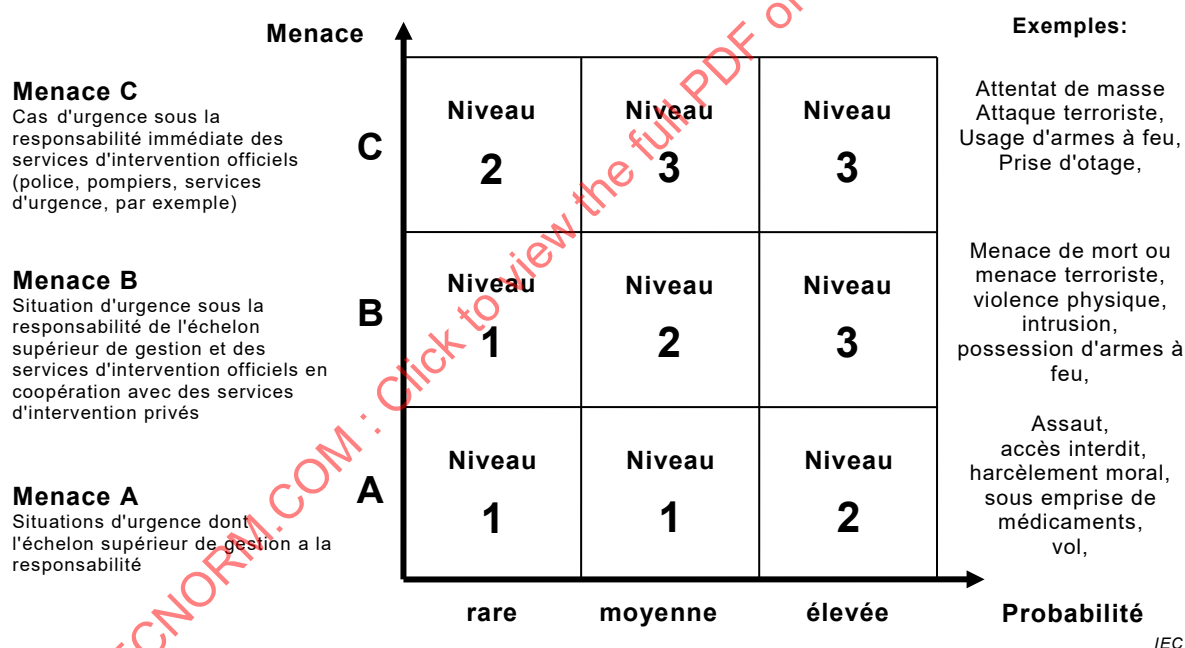


Figure 3 – Classification du niveau

En prenant en compte la Figure 3 et dans le cadre de la détermination du niveau, les points suivants en particulier doivent être pris en compte, classés et les moniteurs pertinents définis:

- la/les menace(s);
- le composant central et d'autres parties du système nécessitant une protection;
- la philosophie des mesures de protection;
- le fonctionnement du système ASBIS dans des conditions de défaut (lorsqu'une alimentation de secours est nécessaire, en cas d'erreurs de matériel ou de câble, de rupture de communication, de redondances);
- les exigences de sûreté/sécurité (sorties de secours, chemins d'évacuation, protection incendie) prenant en compte la loi locale en vigueur sur les produits du bâtiment;

- les conditions d'environnement et CEM sur le site;
- les sites d'assemblage des composants du système;
- la collaboration des utilisateurs ASBIS (exploitation, instruction, par exemple);
- les gaines de câble, les types de câbles, les longueurs maximales de câble;
- les connexions de communication (disponibilité, fiabilité, sûreté/sécurité, rendement);
- la détection d'effraction;
- la vérification, l'émission et le traitement (mesures d'intervention) des différentes alarmes.

En fonction du niveau exigé, les exigences du Tableau 1 doivent être intégralement satisfaites par une application adaptée.

L'évaluation et le résultat, en fonction desquels le niveau de l'application a été défini, doivent être documentés dans le dossier TRM.

Les composants centraux et une unité de transmission d'alarme doivent être hébergés dans une salle à accès limité pour le système ASBIS, avec une protection contre les actes de sabotage, dans la mesure du possible.

Les composants du système utilisés conjointement doivent dans tous les cas satisfaire aux exigences du niveau le plus élevé.

Toutes les applications normatives doivent satisfaire au moins aux exigences du niveau le plus bas. Les autres applications qui ne satisfont pas au présent document peuvent être intégrées, à condition qu'elles n'aient pas d'impact sur l'application normalisée. Le gestionnaire des risques techniques prend la décision et est chargé d'assurer l'intégration et de définir les priorités nécessaires de ce type d'applications.

4.7 Composants d'un système ASBIS

4.7.1 Mesures électroniques

Si les bâtiments sont équipés de transducteurs de signaux pour d'autres types d'alarmes (alarme d'évacuation, alarme incendie, par exemple) et, dans la mesure du possible, de haut-parleurs, d'autres signaux similaires (signaux sonores, par exemple) ou de systèmes d'alarme vocale, il convient que tous ces systèmes fonctionnent selon différentes tonalités et/ou séquences.

En particulier, une protection contre les menaces par des personnes (des personnes prises de folie furieuse, des terroristes, un tireur en milieu scolaire, par exemple) peut être mise en place avec l'accord des autorités de sécurité, un système de signalisation spécifique pouvant l'être également pour empêcher un intrus d'accéder librement aux zones sécurisées (alarme de confinement). Toutefois, cette alarme doit se distinguer clairement des autres signaux de manière classifiable.

Noter que les personnes dans un état de stress extrême peuvent faire clairement la distinction entre les signaux selon un degré de fiabilité adapté. La rareté de l'événement est un facteur aggravant qui rend plus difficile le rappel suffisant de la signification des différents signaux. De plus, en fonction de la position, une sortie de signal peut ne pas s'appliquer à l'ensemble de la propriété/du bâtiment. Les zones correspondantes concernées doivent être stipulées et documentées à cet effet.

Pour éviter toute mauvaise interprétation, les messages d'alarme doivent être énoncés avec une voix parlée claire. Ces messages doivent être précédés d'une tonalité de mise en garde. Les avantages sont les suivants:

- impact direct sur les personnes présentes quant à la manière dont elles doivent agir,

- aptitude à appliquer différentes procédures, particulièrement dans des ensembles immobiliers étendus,
- aptitude à communiquer un plus grand nombre d'informations qui peuvent aider à calmer les personnes présentes,
- aptitude à annoncer la fin de la situation dangereuse.

Les annonces doivent être audibles dans toutes les pièces du bâtiment et les zones libres de parties concernées. De plus, les personnes responsables doivent être nommées, avec leurs instructions/formations et les informations relatives au personnel d'assistance défini.

L'autorité chargée de l'assistance et la force d'intervention doivent pouvoir procéder à des enquêtes par téléphone, selon l'étendue et le type de danger en présence, afin de dresser un état de la situation et, dans la mesure du possible, pour permettre aux services d'intervention d'assurer un contrôle tactique (par exemple, interface ASBIS avec: le système téléphonique, le système de téléphonie mobile, le système d'alarme vocale).

Dans le cadre du processus TRM, une évaluation doit être réalisée pour déterminer si, selon le cas (le déclenchement d'une "alarme de présence d'un forcené ou d'un terroriste", par exemple), des mots codés ou des instructions claires relatives à la manière de procéder doivent communiqué(e)s par l'intermédiaire de haut-parleurs et/ou d'un système de communication vocale (ASBIS). Selon la conception, un système de menace exige des comportements allant complètement à l'encontre ("restez où vous êtes" ou "quittez le bâtiment immédiatement", par exemple) des comportements corrects. Cela montre que tout dépend de l'analyse appropriée et aussi rapide que possible de la situation, et qu'il est judicieux de prévoir des procédures de fonctionnement concrètes en fonction des situations au lieu d'utiliser des mots codés, lesquels sont adaptés à une situation locale (voir également l'Article A.2).

Pour les délits comme le vandalisme et les blessures corporelles, des informations apportées par transfert d'images vidéo peuvent permettre de renforcer la capacité à mettre rapidement en place les mesures d'intervention nécessaires.

L'installation et/ou l'intégration de ce type de systèmes doi(ven)t être évaluée(s) dans le domaine d'application du processus TRM en prenant en compte la protection des données et les spécifications de la norme associée.

4.7.2 Mesures de protection mécanique

Particulièrement en cas de risques plus élevés et afin d'assurer la protection contre les menaces de personnes (un attentat de masse, par exemple), la possibilité de verrouiller les portes automatiquement, manuellement et à l'aide de verrous mécaniques ou électroniques doit être prévue comme étant une mesure de protection importante. Pour les autres événements qui doivent être prévus, cette fonctionnalité doit être évaluée dans le cadre du processus TRM.

Dans la mesure du possible, les portes doivent être verrouillables des deux côtés. Une personne doit pouvoir ouvrir une porte depuis l'extérieur uniquement si elle n'est pas verrouillée. Par défaut, les portes doivent passer en position sécurisée à leur fermeture. Sinon, seules les personnes autorisées détenant la clé doivent pouvoir ouvrir la porte depuis l'extérieur.

Les normes pertinentes doivent être prises en considération au moment du choix des éléments individuels. Les composants de sûreté/sécurité doivent être examinés et certifiés par une autorité d'essai/de certification agréée conformément à l'IEC 17065.

4.7.3 Autres options

Les autres mesures de protection, de surveillance, de communication et d'information peuvent être évaluées dans le cadre du processus TRM et, dans la mesure du possible, mises en œuvre en prenant en considération les normes et spécifications pertinentes.

4.8 Exigences relatives aux composants et interfaces du système

4.8.1 Exigences de base

Les exigences de base relatives à un système ASBIS sont les suivantes:

- affichage du message de défaut à/aux emplacement(s) déterminé(s) par la TRM;
- affichage des états de fonctionnement du système (entretien, examen, état d'alarme, etc.) à/aux emplacement(s) déterminé(s) par la TRM;
- possibilité de mettre en vigueur une alarme prédéfinie et des plans de sauvetage alternatifs en cas de message de défaut relatif à la sûreté/sécurité, à cet effet. Le gestionnaire des risques techniques doit fournir les plans avant la mise en service du système;
- Le Tableau 1 contient les exigences qui doivent être intégralement prises en compte en fonction du niveau.

IECNORM.COM : Click to view the full PDF of IEC 62820-3-2:2018

Tableau 1 – Exigences relatives au système ASBIS et ses unités d'interphone en fonction du niveau

Exigences	Niveau		
	1	2	3
Surveillance du système (chemins de communication, poste d'appel de messagerie [source], poste de commande du système [intégrateur] et poste d'appel du récepteur [récepteur] [en surveillant la disponibilité opérationnelle, par exemple])			
Intervalle de surveillance du chemin de communication (le réseau, par exemple) interne	$t \leq 25 \text{ h } ^{1)}$	$t \leq 5 \text{ h}$	$t \leq 180 \text{ s}$
Surveillance du système contenant la source, l'intégrateur et le récepteur pour connaître la disponibilité opérationnelle	$t \leq 25 \text{ h } ^{1)}$	$t \leq 5 \text{ h}$	$t \leq 180 \text{ s}$
Affichage des messages de défaut à/aux emplacement(s) déterminé(s) par la TRM	Pour la surveillance technique des indicateurs opérationnels de groupe	Indicateurs opérationnels de groupe	Message de défaut détaillé sous la forme d'indicateurs opérationnels en texte clair
affichage des états de fonctionnement du système (alarme d'état, défaut, etc.) ou entretien/examen à/aux emplacement(s) déterminé(s) par la TRM	Pour la surveillance technique des indicateurs opérationnels de groupe	Indicateurs opérationnels de groupe	Message de défaut détaillé sous la forme d'indicateurs opérationnels en texte clair
Indication du passage à la disponibilité opérationnelle (état d'alarme de mode de fonctionnement et état sans alarme) à tous les composants du système connectés d'un point de vue fonctionnel (sources <> intégrateur, récepteur <> intégrateur)	–	X	X
Notification/affichage des sources détériorées avec leur identification à/aux emplacement(s) déterminé(s) par la TRM	X ¹⁾	Indicateurs opérationnels détaillés (par l'intermédiaire de diodes électroluminescentes, par exemple)	Message détaillé sous la forme d'indicateurs opérationnels en texte clair
Indication de la disponibilité opérationnelle de tous les récepteurs tant que toutes les sources attribuées sont prêtes d'un point de vue opérationnel	-	Affichage continu	Affichage continu
Indication de la disponibilité opérationnelle au niveau des sources si au moins un destinataire attribué peut être atteint	-	En cas d'alarme, mettre sous silence l'accusé de réception technique selon lequel le message a atteint le récepteur	Affichage lumineux continu ²⁾
Affichage de la disponibilité opérationnelle manquante par l'intermédiaire d'une indication lumineuse claire sur les sources et le récepteur dans la zone concernée alors que la tension d'alimentation reste disponible	-	Si la communication avec l'intégrateur n'est pas possible	Si la communication avec l'intégrateur n'est pas possible et que les sources/récepteurs attribué(e)s ne peuvent pas être atteint(e)s
Alimentation électrique dans la mise en œuvre de type A ou B selon 4.8.9 pour l'intégrateur et le matériel d'alarme à distance, de manière à détecter une défaillance d'alimentation et à la signaler aux postes concernés, puis à pouvoir exécuter les actions appropriées	X	X	X

Exigences	Niveau		
	1	2	3
Alimentation électrique selon 4.8.9, Tableau 2, pour les autres composants, à l'exception de l'intégrateur et des dispositifs de téléalarme lors de l'utilisation de la mise en œuvre de type A ou B	E	X	X
Entretien (service et examen)	1 fois par an	1 fois par an	1 fois par an
Début des réparations sur site	dans les 48 h	dans les 24 h	dans les 12 h
Envoi d'un message d'alarme et réponses			
Catégories de système de transmission d'alarme (selon l'EN 50136-1 ou une norme IEC ou locale équivalente) avec transfert d'alarme automatique (aux pompiers, à la police, au poste de commande d'urgence ou de service, par exemple).	au moins SP2 ou DP1	au moins SP3 ou DP2	au moins SP5 ou DP4
Rapport avec accusé de réception relatif à la transmission correcte des paquets de données (accusé de réception technique).	-	X	X
Indication du signal d'alarme sur le récepteur après la réception du message d'alarme.	X	X	X
Il doit être possible de faire clairement la distinction entre les différentes priorités d'alarme en présence d'événements d'alarme identiques (hiérarchisation technique). L'indication de signaux d'alarme de priorité supérieure sur le récepteur doit l'emporter sur l'indication des signaux d'alarme de priorité inférieure.		X	X
Vérifications et hypothèses de responsabilité par le service d'intervention			
Le système ASBIS doit assurer une communication vocale entre le déclencheur et l'autorité chargée de l'assistance. Le déclencheur peut ici envoyer et recevoir des informations mais il n'est pas autorisé à contrôler la communication ou à y mettre fin. À l'inverse, le service d'intervention offre également la possibilité de contrôler la communication.	X	X	X
Le système ASBIS doit assurer une communication des données et une communication vocale entre le déclencheur et l'autorité chargée de l'assistance. Le déclencheur peut ici envoyer et recevoir des informations, mais il n'est pas autorisé à contrôler la communication ou à y mettre fin. À l'inverse, le service d'intervention offre également la possibilité de contrôler la communication.	-	E	X
3 types de réponses sont possibles: - responsabilité prise - responsabilité refusée - responsabilité pas claire (un abonné qui n'a pas été atteint par exemple)	-	X	X
Si le type de réponse est "Responsabilité prise", le signal d'alarme obtient une réponse de la part du récepteur, cette réponse étant transférée à la source par l'intermédiaire de l'intégrateur (un voyant de tranquillisation, par exemple).	-	X	X
En cas de "Responsabilité refusée" ou de "Responsabilité pas claire", l'intégrateur doit transmettre la condition d'alarme ASBIS aux autres récepteurs et/ou augmenter la priorité.	-	X	X
L'intégrateur doit continuer à transférer une notification d'alarme au récepteur tant qu'il n'a pas reçu la réponse "Responsabilité prise". Le gestionnaire des risques techniques doit définir une façon de procéder adaptée (alarme interne, par exemple) si aucune réponse n'est reçue ≤ 180 s.	-	X	X
Avec le matériel de signalisation ASBIS surmonté d'un obstacle mécanique à changement de forme durable (un bouton-poussoir sous verre, par exemple), le changement de forme doit disparaître avant de remettre le système ASBIS en service.	X	X	X
La condition d'alarme ASBIS doit être réinitialisée au niveau de la source et/ou de l'intégrateur.	-	X	X

Exigences	Niveau		
	1	2	3
L'intégrateur doit consigner les informations relatives aux conditions d'alarme ASBIS qui ont été reçues et réparties, les réponses provenant des services d'intervention et la présence de notifications de défaut et d'autres événements.	30 jours	60 jours	90 jours
Enregistrement d'images de la situation et communication vocale (le cas échéant) en cas d'alarme.	-	Langue	Langue et image de la situation
Caractéristiques de performances			
Conférence d'urgence entre la partie à l'origine du déclenchement et l'équipe de gestion de crise	-	Facultatif (la fonctionnalité doit être évaluée dans le cadre de la TRM)	X
Rechercher des appels (à tous ou à un groupe défini) avec réponses automatiques (premiers secours, médiateurs, etc.)	X	X	X
Indiquer le lieu de déclenchement sur le poste d'appel du récepteur	X	X	X
File d'attente	Oui (pour au moins 10 appels, les autres étant occupés)	Oui (pour au moins 10 appels, les autres étant occupés)	Oui (même nombre d'unités d'appel d'interphone)
Transférer l'appel en interne par durée, configurable, de 180 s maximum.	-	X	X
Transfert d'appel en interne	X	X	X
Transfert d'appel en externe	-	X	X
Annonce de tranquillisation	-	X	X
Appel d'urgence global	X	X	X
Communication mains libres en simultané (open duplex)	-	X	X
Simplex	X	X	X
Duplex, à commutation vocale et/ou contrôlé par processeur de signal numérique (DSP)	-	X	X
Initiation de messages de mise en garde et instructions sur la manière de procéder provenant de l'autorité chargée de l'assistance interne en réponse à la vérification	X	X	X
Initiation de messages de mise en garde et instructions sur la manière de procéder provenant de l'autorité chargée de l'assistance externe en réponse à la vérification	-	X	X
Disponibilité du système ²⁾	99,7 %	99,9 %	99,99 %
Surveillance d'urgence	-	X	X
Protection contre les écoutes indésirables par un temps de conversation maximal défini, une tonalité par minute, et des indicateurs opérationnels d'appel (protection contre les connexions)	-	X	X
Classe de protection minimale des dispositifs d'appel de la personne qualifiée conformément à l'IEC 60529 pour les postes de signalisation d'appels accessibles au public	IP 33	IP 54	IP 54 dans les salles de réception particulières et pour une utilisation extérieure: IP 65

Exigences	Niveau		
	1	2	3
Protection minimale contre les chocs (vandalisme) conformément à l'IEC 62262 pour les postes de signalisation d'appels accessibles au public	IK 05	IK 06	IK 07
Indice de transmission de la parole (STI) de 0,5 conformément à l'IEC 60268-16	à 1 m du poste d'appel par ailleurs, un essai subjectif reposant sur l'UIT-T P.800 doit donner un résultat d'au moins 3 points	à 2 m du poste d'appel par ailleurs, un essai subjectif reposant sur l'UIT-T P.800 doit donner un résultat d'au moins: 4 points dans les pièces, 3 points dans les couloirs, 3 points dans les entrées	à chaque endroit dans toutes les pièces, couloirs et entrées concernés par ailleurs, un essai subjectif reposant sur l'UIT-T P.800 doit donner un résultat d'au moins: 4,9 points dans les pièces, 4 points dans les couloirs, 3 points dans les entrées
Volume (SPL) au-dessus du niveau de bruit prévu selon les spécifications de la TRM (mesuré à 1 kHz [alternative 1,1 kHz] à une distance de 1 m, et à 0,1 m devant le centre géométrique de la surface close du haut-parleur de l'unité).	6 dB	9 dB	12 dB
Distance de conversation du microphone avec des postes de signalisation d'appels (mesurée dans un environnement calme avec un niveau de bruit ambiant maximal de 45 dB (A)), au moins 3 points devant être obtenus à partir des postes de récepteur (conformément à l'UIT-T P.800)	au moins 3 m	au moins 5 m	au moins 7 m
(X) = Exigé (E) = Recommandé (-) = Non exigé 1) Non exigé pour le niveau 1 si une utilisation quotidienne est assurée. La fonctionnalité sous-jacente doit être évaluée dans le cadre de la TRM. Des mesures organisationnelles doivent assurer la mise en œuvre d'une action de réparation et la consignation du défaut dans le journal de l'opérateur. 2) La disponibilité du système indique le délai (minimal) dans lequel un système ASBIS doit être disponible (en %) dans le cadre d'une utilisation prévue et toute de l'année. Avec le système ASBIS, cela s'applique au poste de commande du système, à au moins un poste d'appel du récepteur, à 80 % des postes de signalisation d'appels et aux chemins de transmission. Les durées de maintenance annoncées planifiées avec l'accord de l'utilisateur du système ASBIS ne sont pas prises en compte dans le calcul. La disponibilité du système peut être assurée de manière purement technique (redondances, deux postes d'appel du récepteur, par exemple), de manière technique et organisationnelle (personnel et matériel techniques sur site), par l'expérience (performances éprouvées) ou par l'utilisation des instructions du fabricant sur son système d'AQ.			

4.8.2 Exigences relatives aux réseaux du système

En règle générale, aucun réseau ASBIS n'est nécessaire si l'absence d'influences négatives (diaphonie, interférences, retard, etc.) provenant d'autres utilisateurs du réseau peut être démontrée. Cela s'applique également en cas d'utilisation de réseaux IP existants au moment, par exemple, de la configuration d'un réseau VLAN avec l'allocation de bande passante (QoS) nécessaire.

4.8.3 Poste de commande du système (serveur ASBIS)

La communication du système, le serveur, l'intégrateur (centraux, répartis ou en tant que mises en œuvre logicielles) doivent également satisfaire à toutes les exigences relatives aux postes d'appel, utilisés de manière complète et adaptée.

L'emplacement et la capacité de protection du poste de commande du système doivent être configurés conformément à la TRM et selon le niveau de sûreté/sécurité.

En prenant la protection contre les écoutes (protection des données) en considération, en mode normal, il convient que tous les postes de signalisation d'appel et postes d'appel du récepteur qui sont connectés ne puissent pas faire l'objet d'écoutes. Les flux de travaux et fonctions nécessaires sont pris en charge pour les différents modes de fonctionnement (mode normal, mode alarme, par exemple).

Les tonalités de signal restantes doivent être disponibles pour tous les modes opérationnels et pour la communication quotidienne.

4.8.4 Unité d'interphone en tant que source (VCU, URU)

Les postes de signalisation d'appels ASBIS sont utilisés pour signaler des situations d'urgence et de danger dans une propriété. Ils doivent être au moins composés des éléments suivants:

- haut-parleurs;
- microphone;
- indicateurs opérationnels visuels/acoustiques;
- au moins un bouton d'appel pour la communication quotidienne;
- indication de l'envoi et de la sauvegarde du compte rendu d'urgence et de danger (accusé de réception);
- indication de l'existence d'une connexion d'appel;
- indication d'un défaut;
- indication qu'au moins un poste d'appel du récepteur peut être atteint (exigé uniquement pour le niveau 3).

Les postes de signalisation d'appel ASBIS sont également utilisés pour la communication vocale dans le cadre d'une demande de vérification et de positionnement par l'autorité chargée de l'assistance, ainsi que pour la réception et l'émission de messages de mise en garde et d'instructions sur la manière de procéder. Ces instructions doivent être diffusées de manière visuelle/acoustique au moyen d'un signal d'attention (principe à 2 significations) qui doit différer de manière significative des signaux correspondant à la communication quotidienne (tonalité d'alarme en fonction de la norme locale, par exemple).

4.8.5 Unité d'interphone en tant que récepteur (SMU, URU)

Les postes d'appel du récepteur sont utilisés pour afficher les messages, la communication vocale après la réception d'appels, la demande de vérification et de positionnement du message et les performances des mesures adaptées. Cela inclut les mises en garde et les instructions sur la manière de procéder adressées aux personnes dans la propriété. Elles doivent être diffusées de manière visuelle/acoustique au moyen d'un signal d'attention (principe à 2 significations) qui doit différer de manière significative des signaux correspondant à la communication quotidienne (tonalité d'alarme normalisée locale, suivie d'annonces en direct ou d'annonces provenant d'une boîte vocale, par exemple).

Elles doivent au moins contenir les éléments suivants:

- haut-parleurs;
- microphone;
- indicateurs opérationnels visuels/acoustiques;
- matériel de signalisation connectable ASBIS facultatif;
- clavier à commande intégrale.

4.8.6 Unité d'interphone en tant que source et récepteur (URU, SMU)

Les unités d'interphone remplissant les deux fonctions doivent satisfaire aux exigences des deux types d'unités d'interphone.

4.8.7 Matériel de mise en garde d'urgence et de danger (matériel de mise en garde ASBIS)

Le matériel de mise en garde d'urgence et de danger ASBIS est utilisé pour le déclenchement manuel d'un message d'alarme en cas d'urgence ou de danger grave (un attentat de masse, par exemple). Le matériel de mise en garde ASBIS doit être mis en œuvre de sorte que, dans tous les cas, un seul déclenchement manuel volontaire ciblé par une personne se traduise par le déclenchement réel de l'alarme. Un déclencheur d'alarme automatique (en raison de l'absence d'un message en texte clair, par exemple) n'est pas autorisé.

Selon le groupe de personnes, nécessaire pour le bien concerné, et dans le cadre du processus TRM documenté dans le dossier TRM, il doit être déterminé si le matériel de mise en garde ASBIS peut être activé par quiconque ou uniquement par un groupe spécifié de personnes (le personnel désigné, les forces de sécurité, la police, etc.).

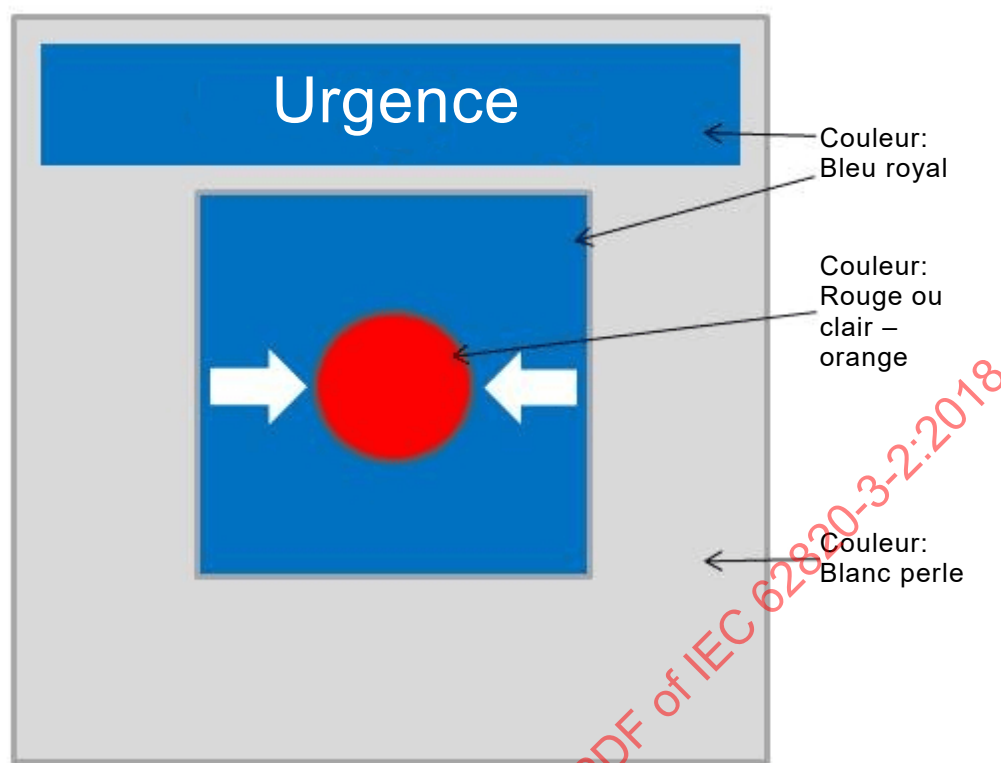
Si personne ne peut être autorisé à déclencher l'alarme en raison des règlements officiels (de la police, par exemple) ou en particulier pour éviter les alarmes non autorisées ou leur mauvais usage, la structure du matériel de mise en garde ASBIS ou de l'une de ses parties doit permettre à la partie déclencheuse ou aux opérateurs de s'identifier au préalable avec des moyens d'identification (des transpondeurs, par exemple) si le déclenchement l'exige.

Le cas échéant, le déclenchement d'alarmes par une personne peut être réduit le plus possible en choisissant les endroits d'installation ce qui, par conséquent, permet de réduire le plus possible le déclenchement de fausses alarmes (sous un bureau, par exemple, les câbles devant être protégés contre les ruptures).

Le matériel de mise en garde ASBIS doit être clairement identifié par la signalisation URGENCE. L'identifiant URGENCE – POLICE doit être utilisé si le déclencheur a une connexion directe avec la police, avec son accord. La présente spécification doit être documentée dans le dossier TRM.

Un matériel de signalisation ASBIS qui peut être utilisé par n'importe qui est en général composé d'un bouton faisant face à un blocage mécanique (une vitre à casser ou similaire, par exemple). Voir la Figure 4. Le bouton doit porter l'identification appropriée avec les couleurs suivantes:

- a) bouton (bouton-poussoir) en rouge (RAL 3000, par exemple) ou en orange clair (RAL 2005) ou analogue;
- b) surface autour du bouton et couleur de fond en bleu royal (RAL 5017, par exemple);
- c) police en blanc perle (RAL 1013, par exemple);
- d) boîtier en blanc perle (RAL 1013, par exemple) dans le cas d'un module simple.



IEC

Figure 4 – Exemple de matériel de mise en garde d'urgence et de danger en tant que module simple

Un élément d'un matériel de mise en garde ASBIS peut également faire l'objet d'une intégration fonctionnelle dans d'autres unités (des postes d'appel, par exemple). Les couleurs a) à c) ci-dessus doivent être mises en œuvre. Le blocage mécanique aux changements de forme durables, la désignation et la couleur de la surface autour du bouton et la couleur du bouton doivent être mis en œuvre de manière analogue.

En particulier, les services d'intervention doivent pouvoir déterminer quel élément du matériel de mise en garde a été déclenché et sa position exacte.

Autres exigences de base relatives au matériel de mise en garde ASBIS:

- Le matériel de mise en garde doit être mis en œuvre de manière à ne pas pouvoir le confondre avec une autre installation
- L'actionnement doit être clairement identifiable par l'utilisateur du système ASBIS (par un point de pression unique, par exemple)
- Les éléments du matériel de mise en garde doivent être conçus pour au moins 100 000 opérations (caractéristique de qualité)
- Un actionnement sûr doit être assuré (par l'utilisation d'un bouton surélevé, par exemple)

Les modules simples et l'élément fragile (le panneau en verre, par exemple) en tant qu'obstacle mécanique doivent être mis en œuvre selon les exigences de l'ISO 7240-11:2011.

Le matériel de mise en garde supplémentaire pour les messages de faible priorité (alarme interne, appel d'urgence, appel de désescalade) peut être connecté au système ASBIS pour le déclenchement des messages correspondants au niveau d'une autorité locale chargée de l'assistance. Cela doit permettre d'éviter toute confusion avec le matériel de mise en garde ASBIS. De plus, une identification unique doit être assurée grâce à d'autres couleurs et étiquettes.

4.8.8 Indicateurs opérationnels et alarmes

4.8.8.1 Indicateurs opérationnels

Tous les indicateurs opérationnels d'alarme visuelle exigés doivent rester actifs tant qu'ils n'ont pas été réinitialisés par une personne autorisée dans le dossier TRM. Les indicateurs opérationnels doivent pouvoir être réinitialisés lorsque la cause de leur déclenchement ne s'applique plus.

Toutes les informations exigées doivent s'afficher de manière à pouvoir être interprétées sans équivoque (indicateurs opérationnels visuels et sonores uniques et distinguables, par exemple). Lors de l'utilisation d'éléments d'indicateurs opérationnels (indicateurs opérationnels textuels/graphiques, par exemple) dans lesquels toutes les informations ne peuvent pas s'afficher en même temps, la présence d'informations supplémentaires doit pouvoir être identifiée (capacité de défilement, par exemple).

Les utilisateurs/opérateurs/sociétés spécialisées ASBIS doivent pouvoir réinitialiser les indicateurs opérationnels sonores (indicateurs opérationnels d'état/de défaut, par exemple).

4.8.8.2 Alarme interne

L'alarme interne est utilisée pour mettre en garde les personnes présentes dans une zone concernée conformément à la spécification du dossier TRM.

Le niveau nominal de pression acoustique du signal acoustique de l'alarme interne (mesuré à 1 m) doit être de 85 dB(A) au moins et de 120 dB(A) au maximum.

Les signaux acoustiques émis par l'intermédiaire du transducteur de signal pour l'alarme interne doivent se distinguer selon leurs fonctions séparées par le volume et la fréquence du signal, et doivent être aisément identifiables par une personne présente dans la propriété.

La durée des alarmes acoustiques internes doit pouvoir être automatiquement réduite. La limitation de la durée doit être réglable dans la plage comprise entre au moins 180 s et 10 min au maximum. Les mises en garde qui varient selon le risque et en fonction de l'événement ou des durées spécifiées doivent être documentées dans le dossier TRM.

Les textes appropriés des annonces d'alarme doivent être stipulés et être documentés dans le dossier TRM. Les textes doivent être formulés clairement, brièvement et une seule fois (voir l'Annexe A). La durée et le nombre de répétitions des annonces vocales doivent être stipulés dans le dossier TRM.

4.8.8.3 Téléalarme

Les dispositifs de téléalarme transfèrent les messages ASBIS à une autorité chargée de l'assistance (un poste de commande d'urgence et de service, par exemple).

Toutes les procédures de communication habituelles reposant sur l'IEC 60839-5-1, -5-2, -5-3, -7-12 pour communiquer des messages provenant du système ASBIS peuvent être utilisées en prenant en considération les connexions spécifiées au Tableau 2.

En règle générale, les téléalarmes doivent être envoyées à une autorité chargée de l'assistance informée (un poste de commande d'urgence et de service qualifié, par exemple). Dans des cas justifiés, et avec l'accord de la police, une connexion directe entre le système ASBIS et la police peut également être utilisée.

Si une connexion directe avec la police doit être établie, cette dernière doit être impliquée dans la planification du système ASBIS tout au long de l'ensemble du processus. Noter les lignes directrices locales concernant la transmission d'alarme à la police ou à d'autres forces de réaction.

Compte tenu de la diversité des formats de communication dans l'envoi de messages entre le système ASBIS et une autorité chargée de l'assistance informée ou une personne informée/responsable, il doit être garanti que ladite personne est en mesure de recevoir des informations provenant du système ASBIS et de les attribuer selon le cas.

Les types de messages doivent être transférés et affichés de façon à pouvoir être identifiés de manière unique par le service informé.

4.8.8.4 Précontrôle d'alarme

Les précontrôles d'alarme et mesures nécessaires doivent être spécifiés en détail entre l'opérateur et l'autorité chargée de l'assistance, et doivent être documentés dans le dossier TRM. La police/les pompiers doivent être impliqués dans la spécification.

Le cas échéant, il convient d'allonger la durée de transfert d'un déclencheur d'alarme afin de procéder à un précontrôle d'alarme, laquelle doit être évaluée dans le cadre du processus TRM.

En règle générale, une alarme peut uniquement être transmise à la police/aux pompiers lorsque le résultat d'un précontrôle d'alarme (par communication vocale, image de la situation, par exemple) est positif ou qu'un élément du matériel de signalisation fourni spécialement à cet effet (urgence de la police, par exemple) est volontairement déclenché par une personne (en cas d'attentat de masse, par exemple).

NOTE En cas de fausses alarmes, des amendes élevées peuvent être imposées par la police/les pompiers au motif d'usage abusif. Des frais supplémentaires peuvent également être liés au traitement médical des personnes traumatisées.

4.8.9 Alimentation électrique

Il doit être assuré que les alimentations en énergie utilisées dans le système ASBIS sont conçues pour répondre à des contraintes tant dans les conditions habituelles que pour les alarmes, les mises en garde et la communication vocale.

Le système ASBIS et ses parties de composant (également les composants des chemins de communication interne) doivent être accompagnés de l'une des alimentations en énergie suivantes:

- Type de mise en œuvre A: une source principale d'énergie (alimentation secteur, par exemple) et une autre source d'alimentation rechargée par le système ASBIS ou l'alimentation secteur (une batterie rechargeable, par exemple).
- Type de mise en œuvre B: une source principale d'énergie et une autre source d'alimentation qui n'est pas rechargée par le système ASBIS ou l'alimentation secteur (une batterie avec une période de secours plus longue, par exemple).

L'alimentation électrique du système ASBIS doit satisfaire aux exigences du Tableau 2.

Tableau 2 – Exigences relatives à l'alimentation électrique du système ASBIS

Alimentation électrique Type de mise en œuvre	Source d'alimentation principale Alimentation secteur	Durée de la période de secours de l'autre source d'alimentation	Durée de recharge de l'autre alimentation en énergie
A	x	12 h	72 h
B	x	24 h ¹⁾	./.
x exigé; ./ non applicable; h heures;			
¹⁾ La durée de chevauchement résiduel de ≤ 12 h doit s'afficher.			

Dans le processus TRM, une évaluation est réalisée pour savoir si les durées minimales exigées selon le Tableau 1 au niveau 1 et au niveau 2 peuvent varier par rapport à celles exigées au Tableau 2 pour les types de mises en œuvre A et B. Dans ce cas, une défaillance de l'alimentation électrique doit être détectée immédiatement et signalée à l'autorité chargée de l'assistance pour s'assurer que l'alimentation électrique peut être rétablie dans les plus brefs délais. Cette évaluation et les spécifications doivent être documentées dans le dossier TRM.

Si, après une défaillance de la source d'alimentation principale, la puissance provient d'une autre source d'alimentation ou d'une source d'alimentation restante (un shuntage, par exemple), vérifier que la capacité de cette source d'alimentation est suffisante pour alimenter le système ASBIS avec également un/des transducteur(s) de signal correspondant à la longueur de l'état d'alarme, le cas échéant, pour une communication vocale d'au moins 15 min de temps de conversation. Cela doit être assuré jusqu'à la fin de la période de surveillance.

Le passage de la source d'alimentation principale à l'autre source d'alimentation, et inversement, ne doit pas générer d'état d'alarme ni avoir d'impact négatif sur la condition d'un système ASBIS.

Les alimentations électriques du système ASBIS ne doivent pas être utilisées pour alimenter d'autres alimentations électriques ou composants du système.

4.8.10 Câbles électriques

Les spécifications de câble du fabricant des composants du système doivent être respectées. Si le fabricant n'en a formulé aucune, il convient que l'installation des câbles satisfasse aux normes nationales ou locales. La "section" doit être spécifiée en prenant en considération la consommation de puissance et la plage de tensions de service des composants du système connectés, ainsi que la longueur du câble.

L'installation et la répartition des câbles (distributeurs de câbles, commutateurs, par exemple) du système ASBIS doivent faire l'objet d'une protection appropriée contre toute manipulation (ne pas être visible à quiconque, par exemple).

4.8.11 Interface avec d'autres systèmes de sûreté/sécurité

Les systèmes ASBIS peuvent être associés à d'autres systèmes de sûreté/sécurité grâce à des interfaces optiques facultatives (radiocommunications mobiles, téléphones mobiles, installations de diffusion sonore, systèmes de surveillance vidéo, système de contrôle des accès, système d'alarme incendie, système de protection contre les intrusions et les hold-up, etc.). Le type d'interface dépend de la solution et du niveau de sécurité qui doit être atteint.

NOTE Il n'existe aucune norme relative aux interfaces définies pour ASBIS.

4.9 Autres exigences

4.9.1 Mise en œuvre de services

Selon les termes de la construction du système ASBIS, les documents indiqués dans la décision de construction doivent être considérés et pris en compte dans la planification/configuration.

Le client prend la responsabilité de la mise en œuvre du système ASBIS et de la mise en œuvre spécifique à la commande du présent document.

Toutes les spécifications du fabricant sont contraignantes, à condition qu'elles n'aillent pas à l'encontre du présent document et des normes nationales ou locales connexes.

4.9.2 Disposition et répartition des postes d'appel

Noter les points suivants concernant la disposition et la répartition des postes d'appel en fonction du concept organisationnel et de ses exigences d'application:

- bonne visibilité;
- accès libre (concerne également la "construction sans obstacle" conformément aux normes locales ou autres normes locales connexes, par exemple);
- bonne accessibilité au matériel de signalisation ASBIS selon l'usage prévu;
- si un assemblage mural est utilisé, l'accessibilité aux boutons de déclenchement doit être assurée pour les utilisateurs concernés du système ASBIS;
- facilité de visualisation et en quantité suffisante dans les espaces ouverts et les couloirs;
- dans les salles de sport, les salles de réunion et les salles des fêtes, dans le chemin d'évacuation, à proximité des sorties de secours.

Dans les zones particulièrement dangereuses et le long des chemins d'évacuation et les voies de secours ou en fonction de l'usage et de la qualité d'un bâtiment, la distance maximale entre les postes d'appel doit être définie dans le cadre de la gestion des risques.

4.9.3 Distinction entre un appel et un appel d'urgence

Un appel est une communication quotidienne, alors qu'un appel d'urgence concerne une situation critique de sûreté/sécurité. Une distinction doit être faite entre des appels et des appels d'urgence. Leurs destinations peuvent être différentes. L'appel d'urgence présente une priorité plus élevée. Les appels d'urgence doivent être indiqués différemment des appels au niveau des postes du récepteur.

4.9.4 Groupes d'alarmes

En combinaison avec un système de haut-parleurs, les zones d'appel d'alarme et d'appel de groupe doivent être adaptées dans un scénario d'évacuation et de barricade.

4.9.5 Alarme interne et instructions sur la manière de procéder

Les instructions sur la manière de procéder doivent être données sous la forme de messages vocaux (tous les appels ou appels de groupe). La taille et la répartition du groupe doivent être librement définissables. Les chemins d'évacuation et d'acheminement de secours doivent être pris en compte pour la classification.

La taille des groupes (zones de bâtiments) est fonction des situations locales et de la spécification dans le dossier TRM. Toutes les personnes dans un groupe doivent pouvoir recevoir les instructions sur la manière de procéder. Les informations doivent être transmises de manière synchrone à l'intérieur d'un groupe. Cela s'applique également lorsque les informations sont envoyées en parallèle par l'intermédiaire du haut-parleur et des postes d'appel.

La nature et l'étendue des instructions comportementales doivent être spécifiées et documentées avec la TRM et les personnes concernées en fonction de l'usage du bâtiment.

Les signaux, informations de mise en garde et instructions relatives à la procédure doivent se distinguer des signaux de manœuvre et dépasser le niveau général de bruit (niveau de bruit dû au brouillage) de 10 dB(A) dans les pièces et à tout moment. Le niveau minimal de pression acoustique ne doit pas être inférieur à 65 dB (A). Le mesurage doit être réalisé aux mêmes emplacements que pour l'essai STI (indice de transmission de la parole) spécifié dans l'IEC 60268-16.

Dans les pièces plus volumineuses, les mesurages peuvent être réalisés pour augmenter le volume/obtenir une meilleure répartition audio.