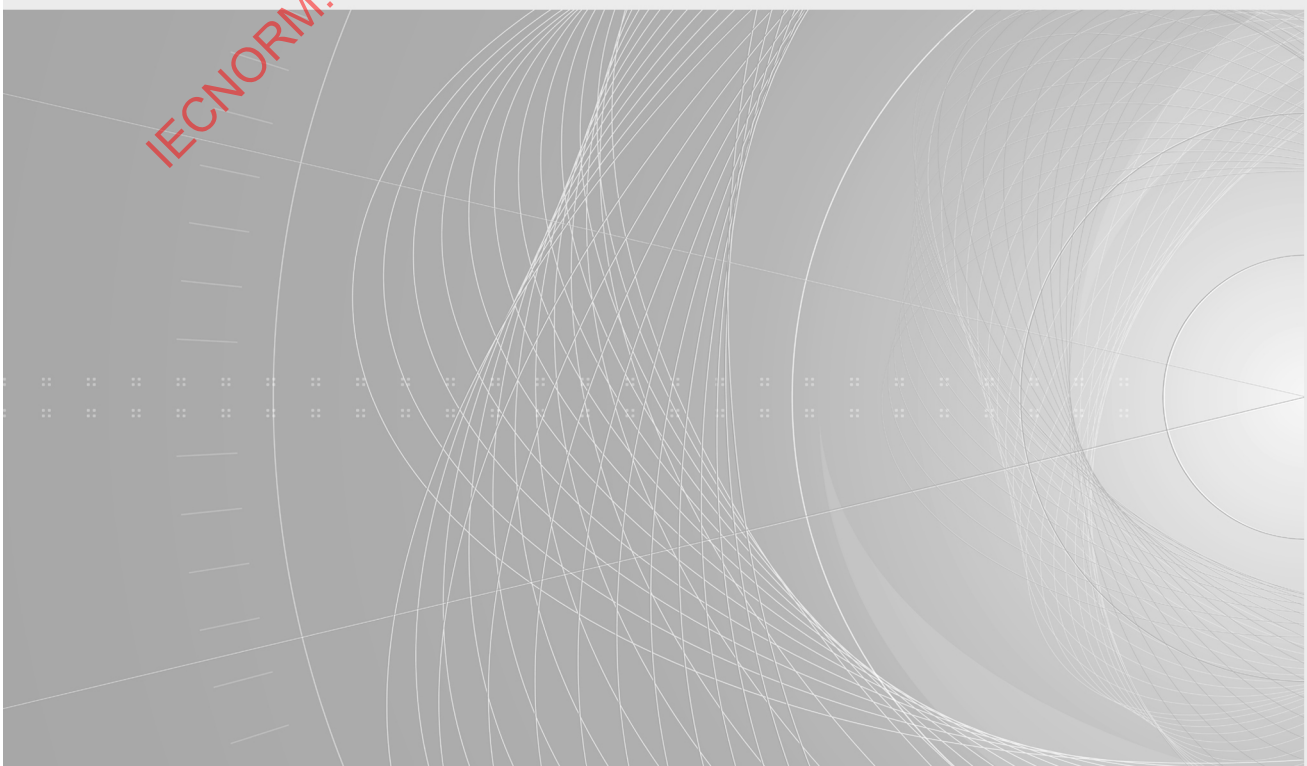
IEC PAS 63325

Edition 1.0 2020-12

PUBLICLY AVAILABLE SPECIFICATION

colour inside

Lifecycle requirements for functional safety and security for IACS



IEC PAS 63325:2020-12(en)

IEC Central Office
3, rue de Varembé
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 corrigendum or an amendment might have been published.

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 It also gives information on projects, replaced and withdrawn publications.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 once a month by email.

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.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries 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 PAS 63325

Edition 1.0 2020-12

PUBLICLY AVAILABLE SPECIFICATION

colour inside

Lifecycle requirements for functional safety and security for IACS

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040

ISBN 978-2-8322-8861-0

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

LIFECYCLE REQUIREMENTS FOR FUNCTIONAL SAFETY AND SECURITY FOR IACS

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.

A PAS is an intermediate specification made available to the public and needing a lower level of consensus than an International Standard to be approved by vote (simple majority).

IEC PAS 63325 has been processed by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
65/813/DPAS	65/826/RVDPAS

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

This PAS shall remain valid for an initial maximum period of 2 years starting from the publication date. The validity may be extended for a single period up to a maximum of 2 years, at the end of which it shall be published as another type of normative document, or shall be withdrawn.

IMPORTANT – The "colour inside" logo on the cover page of this document 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.

INTRODUCTION

Safety and security are becoming increasingly interdependent. Traditional safety-related systems are not isolated any more, as required by connectivity and inter-operability, and threats and vulnerabilities can increase the probability of attacks to safety-related systems. IEC TR 63069 gives some top-level framework recommendations for functional safety and security.

This specification concentrates on how to consider the lifecycles for functional safety and security in different stages, optimizing risk assessment, improving efficiency of safety and security related activities included in engineering processes, avoiding conflicts between safety functions and security countermeasures. This document also will give some safety and security co-engineering guidelines to make the implications to systems more safe, more secure, and cost efficient.

LIFECYCLE REQUIREMENTS FOR FUNCTIONAL SAFETY AND SECURITY FOR IACS

1 Scope

This PAS provides requirements and guidance for ensuring and assuring functional safety and security in different stages of the lifecycle. It will help the coordination of risk assessment, design and management and operation processes, avoiding conflicts between functional safety and security.

This specification does not aim to define a completely new lifecycle, but based on the functional safety lifecycle, security lifecycle and other state of the art engineering processes, it aims to provide requirements and suggestions to support coordination between functional safety and security.

The objective of this document is Industrial Automation Control Systems (IACS), including the Equipment Under Control (EUC) system and the safety-related system.

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.

There are no normative references in this document.

3 Terms, definitions and abbreviated 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:

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

More definitions could refer to the IEC 62443 series and the IEC 61508 series.

3.1.1
conflict
situation when one or several safety measures and one or several security countermeasures are not in coordination with each other and one or several safety measures cannot achieve its required target performance

Note 1 to entry: This conflict definition is in the context of this document.

3.1.2
safety
freedom from unacceptable risk

[SOURCE: IEC 61508-4:2010, 3.1.11 and IEC 62443-1-1:2009, 3.2.94]

3.1.3
functional safety
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12]

3.1.4
security
a) measures taken to protect a system

b) condition of a system that results from the establishment and maintenance of measures to protect the system

c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems

e) prevention of illegal or unwanted penetration of, or interference with the proper and intended operation of an industrial automation and control system

Note 1 to entry: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

[SOURCE: IEC 62443-1-1:2009, 3.2.99]

3.1.5
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC 62443-1-1:2009, 3.2.125]

3.1.6
vulnerability
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy

[SOURCE: IEC 62443-1-1:2009, 3.2.135]

3.1.7
asset
physical or logical object which has a perceived or a defined value for an IACS combined safety and operational functionality

Note 1 to entry: This asset definition is in the context of this document.

3.1.8
coordination
activity of the IACS, which means:

– all risk-related factors have been considered and are controlled;

– risk management process is reasonably implemented;

– no conflict exists between safety measures and security countermeasures.

3.2 Abbreviated terms

EUC Equipment under control

IACS Industrial automation control system

SOI System of interest

SIL Safety integrity level

4 Lifecycle stages

Cross-communication and interaction between the functional safety and security shall be implemented throughout the whole lifecycle to ensure that:

– all reasonably foreseeable attacks and misuse are identified and are controlled;

– all risk reduction requirements are achieved;

– when there is a conflict between safety measures and security countermeasures, risk can also increase, so while striving for compatibility, the appropriate design compromise ensuring that the tolerable risk is achieved shall be found.

Typically, the following stages need to be considered during the whole lifecycle:

– concept and scope;

– risk assessment;

– development and implementation;

– operation and maintenance;

– decommission and disposal.

NOTE Different standards have different lifecycle requirements (IEC 61508, IEC 61511, IEC 62443, etc.); this document just extracts some typical and important stages. Those stages also are very critical to achieve safety and security compatibility.

5 Management coordination requirement

5.1 General

Technical management processes shall be considered at the beginning of the lifecycle, for the specified organization, it is recommended to plan the overall technical management processes including safety and security people.

Technical management processes shall be implemented through the whole lifecycle. Except for the safety and security management requirements specific to a domain, if some crossover requirements between safety activities and security activities are identified, responsibilities should be clearly assigned to ensure that requirements are implemented.

The basic objectives for achieving safety and security should be to minimize the risk of human harm, major property losses, environmental damage and reputation effects.

Risk control concepts are used both for safety and security, safety measures and security countermeasures are designed to achieve the tolerable risk target. When there is a conflict between safety measures and security countermeasures, the appropriate design compromise ensuring that the tolerable risk is achieved shall be found.

5.2 Organization requirements

Responsibility:

– All people, related to common safety and security activities, shall be clearly aware of their responsibilities and tasks;

– communication mechanisms shall be set up, especially between safety-related people and security-related people;
– Special coordination procedures and mechanisms shall be established to deal with functional safety and security crossover work.

5.3 Management of change

An interrelated modification management shall be established.

Procedures should be developed to assess the potential for negative impact on safety and security, when changes are made to IACS (including configuration, execution status, etc.).

Changes due to functional safety should be cross-audited by security staff to confirm the validity and effectiveness of the security countermeasures.

Changes in functional safety-related systems often lead to new vulnerabilities. In this case, new information security measures are usually added, and a special risk assessment needs to be carried out if it is necessary to re-confirm the security capabilities.

When the security measures are changed (including patching), corresponding analysis (and if required, appropriate tests) shall be conducted to confirm that these changes will not negatively impact the safety function.

The changes may affect the integrity of safety and cannot immediately implement the security-driven change process, and its vulnerability should be tracked and managed. A special risk assessment may be conducted when necessary to identify compensation measures that do not affect the integrity of safety. The implementation of these compensation measures requires the approval of the security management person.

6 Lifecycle requirements

6.1 Concept and scope

It is necessary to identify the safety and security related systems, their scope and their perimeter, giving the list of the SOI (system of interest).

All the facilities, control systems and network environment shall be considered to achieve safety and security objectives, including but not limited to:

– types and application of the plant/workshop installation and its control system;
– physical transmission medium and communication protocol for data exchange between all devices, control systems and the public network;
– communication networks that need to be isolated;
– the boundaries of various virtual networks and physical areas should be clearly identified, including the functional boundaries of typical systems.

The system response or the response mechanism after a critical attack shall be determined. Response mechanisms may include:

– continue to maintain the original state of operation, remain unchanged in the short time;
– isolate the system until the fault is fixed or the threat is removed;
– directly shut down the production operation process and achieve a safe state.

EXAMPLE: if the operation station fails or is infected with a virus, it may only need to be temporarily isolated, and the failure of the safety controller may require immediate shutdown.

There shall be a classification of all the systems and devices, see an example for the process sector in Table 1; this table does not describe a generic classification, as different applications may have different classifications.

Table 1 – Example of classification of all the systems and devices

Systems or devices	Safety-related	Security-related
Non-electrical/digital instrument used for basic control	No	No
Electrical/digital instrument used for basic control	No	Yes
Non-electrical/digital instrument used for protection control	Yes	No
electrical/digital instrument used for protection control	Yes	Yes
Basic control unit	No	Yes
Safety control unit	Yes	Yes
HMI for basic control	No	Yes
HMI for protection control	Yes	Yes
Firewall, gateway	No	Yes

There shall be a documented architecture description including systems and network. This description shall consider:

– Completely isolated;
– End-to-end communication connection;
– Isolated monitoring layer network communication connection;
– Shared monitoring layer network communication connection;
– Fieldbus network connection;
– Safety / non-safety control hybrid system network connection.

6.2 Risk assessment

6.2.1 General requirement

There shall be a high-level risk assessment before traditional safety-related risk assessment and threat-vulnerability assessment.

There shall be a conflict resolution process after traditional safety-related risk assessment and threat-vulnerability assessment.

There should be one team to execute the whole risk assessment, or two teams to execute safety and security related risk assessment with enough cross-support or communication.

The general process is shown in Figure 1.

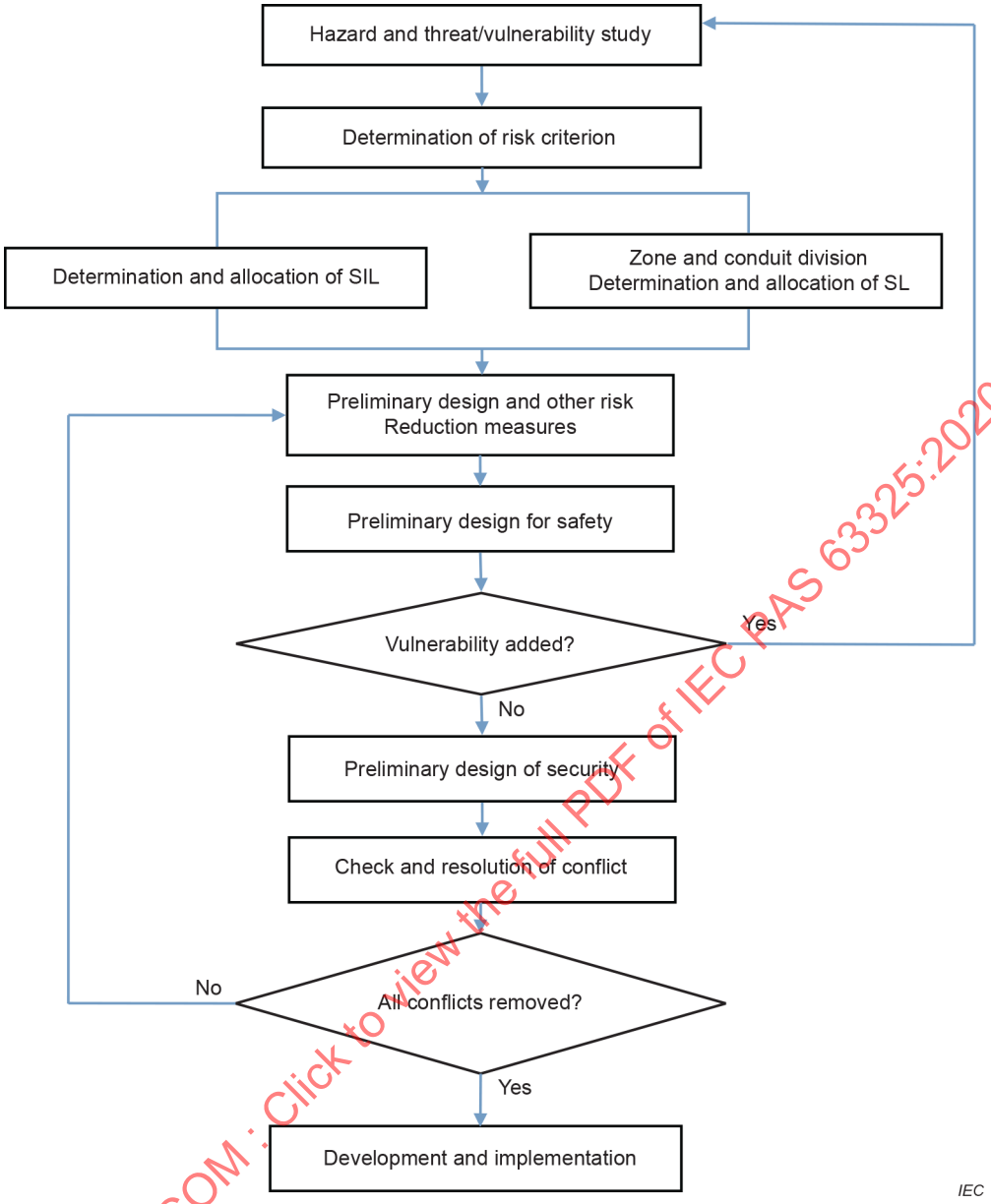


Figure 1 – General process of risk assessment

6.2.2 Hazard and risk analysis / threat-vulnerability assessment

Identify all potential hazardous events to defined domains of interest emerging from IACS, use and coordination of functional safety, security and other safety technical measures, comprehensively, to maintain the risk below a tolerable level.

All relevant hazard factors and threat possibilities shall be considered, including people, devices, regulation, material. The following situations need be identified:

– systems operations mode;
– complexity of systems;
– human competence.

6.2.3 Risk criterion

Safety measures are used to reduce the risk of human harm, environment damage, and property damage. To achieve functional safety and security objective, the relevant safety criteria shall be defined for the specified application.

For different applications, different measures could be chosen, the stake holder of specified applications shall make sure the risk is maintained below the risk criteria.

Risk criteria could be coming from:

– regulation;
– standards;
– society situation;
– others.

6.2.4 Conflict resolution

Conflicts shall be resolved at each hazard and risk assessment iteration, including the specification of compensation measures if judged necessary.

If some conflicts exist, changes should be made:

– in safety design, to achieve the overall risk reduction, different safety protection measures can be adopted; safety design should take into account from the very beginning that this may introduce new vulnerabilities, and seek alternatives to avoid the conflict, or
– in security design, some alternative security measures could be used (provided that information security personnel are aware of or are notified of such a conflict; for example, they may introduce an alternative fingerprint identification to allow an operator that forgot the password to send a critical command to safety systems), or
– compensation measures, through improving the risk reduction capacity of compensation measures, some of the security measures could be reduced.

6.3 Development and implementation

6.3.1 General

If some security countermeasures are integrated in the safety-related systems but not properly segregated, all those security countermeasures elements shall comply with IEC 61508 parts 1, 2 and 3.

After development and implementation, testing must be done to prove that there are no adverse impacts between safety and security.

In case testing is done on production systems, it has to be ensured that there is no impact from the testing activities on the desired system performance.

Testing could be done at the product level or at the system level. Tests should show that:

a) Safety functions can be executed, without blocked or prevented safety signals that need to be transmitted;
b) Reliable operation and maintenance are possible under normal conditions;
c) Fault response is as designed, and a safety state can be achieved;
d) Response times are acceptable for the application.

6.3.2 Response to system failures or security events

When any failure is detected in the safety-related system, maintenance procedures shall be performed following the maintenance plan including response to the diagnostic information, repair and re-validation after repair.

If any security event occurs during operation and a dedicated security countermeasure responds to it, the event and the response of the countermeasure shall be logged and monitored.

Additionally, since some response to security events may indirectly cause a safety system trip, an emergency mechanism shall be in place to avoid undesirable trips.

6.4 Operation and maintenance

There shall be a management system as mentioned in clause 5 also for operation and maintenance.

During the proof test for safety-related systems, tests must be done to prove there are no adverse effects between safety and security. Tests are very dependent on the application, for example an attack can be simulated offline to trigger the security measures and then a check can be made to see if the safety function can still work.

NOTE IEC 62443-4-2:2019 in subclause 7.5.3 mentions that security functionality verification during normal operation needs to be carefully implemented to avoid detrimental effects and it may not be suitable for safety systems. Here the situation is different: a) The proof test for functional safety is normally done offline, while for 7.5.3 it is online. That is the key reason 7.5.3 is not suitable for safety system, because it may cause spurious trip; and b) 7.5.3 is just functionality verification, while here the focus is more about the potential conflict.

Realization of both functional safety and security in the stage of operation and maintenance could be closely related and interwoven. Therefore, the security activities should be enhancements to the mature operation and maintenance procedures for functional safety in a plant, and security risks should be considered as part of the organization's risk management processes. In general, these activities involve normal operation and maintenance, response to safety/security events and possible modification to safety-related systems. The measures in Annex A for monitoring, logging and response to both safety and security events should be considered.

6.5 Decommission

decommission of any part in the safety-related system shall be analyzed for its possible impact to functional safety. Normally this is covered by a mature safety management procedure for functional safety. When security is considered, additional management requirements for security countermeasures shall be included. This includes monitoring, test and release of updates/ patches of security countermeasure software as well as re-validation after modification.

Annex A
(informative)

Measures that could be used in the coordination of safety and security in different stages

A.1 Risk assessment

An interrelated hazard and risk assessment that contains both safety and security aspects should be performed to identify potential hazard in the background of the factory. Generally, the safety risk is increased due to considerations of security threats. Possible security threats that could affect functional safety could be from human factors, from devices/systems connected to control system or safety-related system, or from the reaction/failure of a security countermeasure itself.

Malicious external hackers/insiders could attack the critical infrastructure or even the safety-related system directly. Well-meaning employees who have access privilege to the IACS could bring in security threats by unintentional operation.

These security threats could result in vulnerabilities including hardware failures and systematic failures, e.g. software bugs in control system and safety-related system.

A.2 Development and implementation

A.2.1 Physical compensation measures are necessary for access control

Key areas such as central control rooms, cabinet rooms, and engineer rooms are protected by physical access control (guards, access control, room locks), video surveillance, etc. Only certain types of known people are allowed to visit. Visitors need to be accompanied by authorized personnel, and registration.

Use a locked cabinet.

Unnecessary interfaces such as USB, optical drives, and wireless devices on the industrial host should be removed or closed. The user should clearly control the important security devices such as dongles for the engineer/operation station in the management system.

A.2.2 Segmentation into zones and perimeter protection

Safety networks are not completely segregated but may be connected to control system and corporate networks for the required interconnectivity and interoperability. This could induce more security attacking vectors than the traditional air-gapped solution, e.g. a security attack in the corporate network could propagate and affect safety-related systems. Additional boundary protections may be required on the network interfaces of safety-related system including dedicated firewall for safety-related systems, authentication and authorization on the access from networks, read-only access for the safety-related system, input validation/integrity check of data/commands sent to the safety-related system from networks.

A.2.3 Safety and security communication protocol

Traditional safety-related systems normally use proprietary communication protocols for safety communication. However, general communication protocol, e.g. Ethernet-based protocol could be widely used in the factory. This increases the risks for the safety communication, e.g. masquerading of safety messages and DoS attack. Security countermeasures dedicated for the data in transit should be enhanced especially.

A.2.4 Remote access control

Remote access is not common in traditional safety applications but could be widely supported in the factory. The situation increases the risk of eaves dropping and spoofing threats especially, e.g. man-in-the-middle attack. Security countermeasures for remote access control should be supported, and security could be improved by detailing policies and procedures for each deployment.

A.2.5 Wireless access control

Wireless could be a commonly-used technology for intelligent manufacturing, e.g. for IIoT and edge computing. Wireless may be used for future safety applications. Access control is particularly important when using wireless. The usage of Wireless is not discussed in this specification.

A.2.6 Device level

Device vendors need to take measures to enhance the security of their equipment and prevent the spread and operation of malicious code. Device vendors can enhance safety and security from operating system kernels, protocol stacks, and more.

The vulnerabilities in the device operating system and application software are the most direct threat to the device. The device vendors shall conduct vulnerability scans and mining of common equipment and devices, discover security vulnerabilities in operating systems and application software, and repair them in a timely manner.

Factory owners should pay close attention to the security vulnerabilities and patch releases of major field devices, take timely patch upgrade measures, and conduct strict security assessments and test of patches before patch installation.

For accessing field devices, unique identifiers based on hardware features are supported to provide hardware-identity-based identity authentication capabilities for upper-layer applications, including industrial Internet platforms. In addition, hardware-level components (chips or firmware) should be supported as a system root of trust to support the safety boot of field devices and data transmission confidentiality and integrity protection

A.2.7 Control level

The control environment in the factory is displayed by the convergence of information technology (IT) and operational technology (OT).

The traditional production control process is enclosed but credible, the change is more and more Interconnections, causing the impact of a security incident to increase substantially. Information security may affect functional safety and may have other consequences.

Identify possible hazard sources, hazardous conditions and incidents, and obtain information on identified hazards (e.g. duration, intensity, toxicity, exposure limits, mechanical forces, explosion conditions, reactivity, flammability, vulnerability, loss of information, etc.).

Determine the hazardous conditions or incidents that may occur between the control software and devices, include the cause of the accident and the types of events (such as component failures, program failures, human errors, and related failure mechanisms that can cause dangerous events).

Combine the characteristics of typical production processes, manufacturing processes, and quality control, analyze the safety impact.