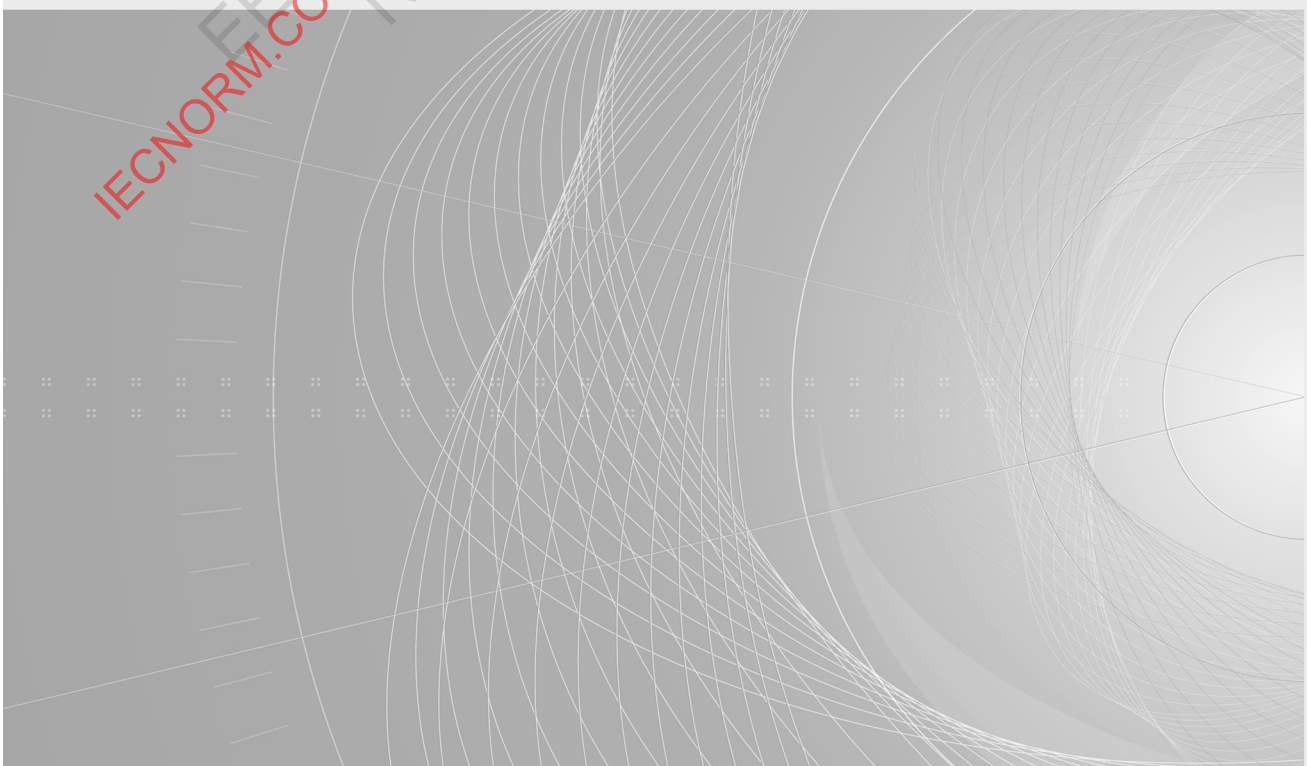
IEC TS 62933-5-1

Edition 1.0 2017-07

TECHNICAL SPECIFICATION

colour inside

Electrical energy storage (EES) systems – Part 5-1: Safety considerations for grid-integrated EES systems – General specification



IEC TS 62933-5-1:2017-07(en)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 - www.iec.ch/searchpub
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 It also gives information on projects, replaced and withdrawn publications.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 20 000 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
65 000 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: csc@iec.ch.

IEC TS 62933-5-1

Edition 1.0 2017-07

TECHNICAL SPECIFICATION

Electrical energy storage (EES) systems – Part 5-1: Safety considerations for grid-integrated EES systems – General specification

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 13.020.30

ISBN 978-2-8322-4565-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

ELECTRICAL ENERGY STORAGE (EES) SYSTEMS –

Part 5-1: Safety considerations for grid-integrated EES systems – General specification

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC TS 62933-5-1, which is a technical specification, has been prepared by IEC technical committee TC 120: Electrical Energy Storage (EES) Systems.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
120/89/DTS	120/100/RVC

Full information on the voting for the approval of this technical specification 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 62933 series, published under the general title *Electrical energy storage (EES) systems*, can be found on the IEC website.

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.

A bilingual version of this publication may be issued at a later date.

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.

INTRODUCTION

Many governments' plans for how electricity will be generated and managed in the future have been determined. Such current plans cannot be implemented without long-term storage with capacities in the multi-MWh range.

There are a number of types of storage technologies that have emerged. Examples of these technologies are pumped hydro storage (PHS), electrochemical batteries, flywheel storage systems and hydrogen and synthetic natural gas (SNG). Pumped hydro storage has been widely used in terms of the total amount of the stored energy. A flywheel is a model of kinetic energy storage with a high power density, excellent cycle stability and long life. While some flywheels are intended for short term operation, others can operate over longer periods of time of up to a few hours. Batteries require development primarily to decrease cost, and for some technologies to increase energy density as well. Hydrogen and synthetic natural gas (SNG) added to natural gas are likely to be essential elements of future electric grids because of their energy storage duration and capacity. Hydrogen and SNG should be further researched and developed across a broad front, including physical facilities, interactions with existing uses of gas for supply and distribution network, optimal chemical processes, safety, reliability and efficiency. The IEC White Paper “Electrical Energy Storage” (2011-12) may provide further background information on concerned EES systems.

The IEC expects to keep pace, as in other areas in the past, with the need for international consensus standards for the safety of new storage technologies. It encourages regulators to anticipate the requirement to guarantee the safety of these technologies, and to contribute to shaping suitable international standards upon which harmonized regulations may be based.

For mature EES systems various IEC standards exist covering technical features, testing and system integration. For other technologies there are only a few standards, covering special topics.

Up to now no general standard addressing safety for EES system integration into an electrical grid has been developed.

The rapid growth and the new technologies involved in electrical energy storage in the near future, as well as their installation by consumers will impose particular requirements for safety. At the same time, society and governments will need assurance of safety before the much-needed systems can be deployed.

This document stands as a decisive step towards the gradual alignment with specific technologies and applications concerning the safety of packaged or site-assembled grid-integrated EES system.

ELECTRICAL ENERGY STORAGE (EES) SYSTEMS –

Part 5-1: Safety considerations for grid-integrated EES systems – General specification

1 Scope

This part of IEC 62933, which is a Technical Specification, specifies safety considerations (e.g. hazards identification, risk assessment, risk mitigation) applicable to EES systems integrated with the electrical grid.

This document provides criteria to foster the safe application and use of electric energy storage systems of any type or size intended for grid-integrated applications.

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.

IEC 62933-1[1], *Electrical energy storage (EES) systems – Part 1: Terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62933-1 and the following 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
accumulation subsystem
storage subsystem
EESS subsystem, comprising at least one electrical energy storage, where the energy is stored in some form

Note 1 to entry: Mechanical energy, electrochemical energy, electromagnetic energy are frequent forms of stored energy.

Note 2 to entry: Generally (see Figure 8), the accumulation subsystem is connected to the power conversion subsystem that performs the necessary power conversion to electrical energy; however, in some cases, a power conversion is embedded in the accumulation subsystem (e.g. in electrochemical secondary cells the energy is directly available in the electrical form).

[1] Under preparation. Stage at the time of publication: IEC CDV 62933-1:2017.

3.2
auxiliary POC
EES system point of connection (POC) with the electric power system used to feed the auxiliary subsystem, only if the primary POC is not used to feed each subsystem

Note 1 to entry: Generally, an auxiliary POC can be replaced with another source of electrical energy (e.g. a diesel generator).

Note 2 to entry: The control subsystem is normally fed by the auxiliary subsystem and, therefore, by the auxiliary POC.

3.3
auxiliary subsystem
EESS subsystem containing equipment intended to perform particular functions additional to storing/extracting electrical energy which is done in the primary subsystem

Note 1 to entry: Generally (see Figure 8) the auxiliary subsystem is connected to the auxiliary POC through the auxiliary connection terminal.

Note 2 to entry: The equipment of the auxiliary subsystem (auxiliary equipment) is normally indispensable for setting up all the EESS operational states and assessing the correct performance (operation) of the primary and control subsystems during any operating mode.

Note 3 to entry: The auxiliary subsystem can be configured to take the energy from the primary subsystem (see Figure 8).

3.4
auxiliary subsystem de-energized
condition of service in which an auxiliary subsystem of the EES system does not have any energy source within the subsystem to feed the auxiliary equipment and is not connected to an external source of energy

Note 1 to entry: In this state the auxiliary subsystem is not fed by a possible UPS.

Note 2 to entry: "UPS" is defined in IEC 62040-1:2008, 3.1.1.

3.5
communication subsystem
EESS subsystem containing an arrangement of hardware, software, and propagation media to allow the transfer of messages from one EESS component/subsystem to another, including the data interface with external links

[SOURCE: IEC TS 62443-1-1:2009, 3.2.25, modified – the original definition has been particularized for the EES system.]

3.6
control subsystem
EESS subsystem serving for monitoring and controlling the EESS, by including all equipment and functions for acquisition, processing, transmission, and display of the necessary process information

Note 1 to entry: Generally (see Figure 8) the control subsystem may be connected to the communication interface and it comprises at least the management subsystem, the communication subsystem and the protection subsystem.

Note 2 to entry: The control subsystem is normally fed by the auxiliary subsystem.

[SOURCE: IEC TS 62351-2:2008, 2.2.195, modified – the second part of the original definition has been particularized for the EES system architecture, the first part of the original definition and notes to entry have been deleted.]

3.7
dead, adj.
DEPRECATED: de-energized, adj.
at an electric potential equal to or not significantly different from that of earth at the worksite

Note 1 to entry: This entry was numbered 651-01-15 in IEC 60050-651:1999.

[SOURCE: IEC 60050-651:2014, 651-21-09]

3.8
duty-cycle of the EES system
combination of controlled phases (charge phase, pause, discharge phase, etc.) starting from an initial state of charge and ending at a final state of charge, used in the EES system characterization, specification and testing for a certain operating mode

3.9
EESS module
EESS unit
part of an EES system, which is itself an EES system

Note 1 to entry: The EESS module is a specific EESS subsystem.

Note 2 to entry: In an EESS module the terminals, auxiliary and control subsystems may be absent; they may be centralized at EES system level.

3.10
EESS subsystem
part of an EES system, which is itself a system

Note 1 to entry: A subsystem is normally at a lower indenture level than the EES system of which it is a part.

[SOURCE: IEC 60050-192:2015, 192-01-04, modified – the original definition has been particularized for the EES system.]

3.11
electrical energy storage
EES
installation able to absorb electrical energy, to store it for a certain amount of time and to release electrical energy during which energy conversion processes may be included

EXAMPLE A device that absorbs AC electrical energy to produce hydrogen by electrolysis, stores the hydrogen, and uses that gas to produce AC electrical energy, is an electrical energy storage.

Note 1 to entry: The term “electrical energy storage” may also be used to indicate the activity of an apparatus described in the definition of this term during the performance of its own functionality.

Note 2 to entry: The term “electrical energy storage” should not be used to designate a grid-connected installation; "electrical energy storage system" is the appropriate term.

3.12
electrical energy storage system
EES system
EESS
grid-connected installation with defined electrical boundaries, comprising at least one electrical energy storage, which extracts electrical energy from an electric power system, stores this energy internally in some manner and injects electrical energy into an electrical power system and which includes civil engineering works, energy conversion equipment and related ancillary equipment

Note 1 to entry: The EES system is controlled and coordinated to provide services to the electric power system operators or to the electric power system users.

Note 2 to entry: In some cases, an EES system may require an additional energy source (non electrical) during its discharge, providing more energy to the electric power system than the energy it stored (compressed air energy storage is a typical example where thermal energy is requested).

3.13
electrical installation
assembly of electrical equipment which is used for the generation, transmission, conversion, distribution and/or use of electric energy

Note 1 to entry: The electrical installation includes energy sources such as batteries, capacitors and all other sources of stored electric energy.

Note 2 to entry: This entry was numbered 651-01-04 in IEC 60050-651:1999.

[SOURCE: IEC 60050-651:2014, 651-26-01]

3.14
emergency stop
operating procedure intended to stop, as quickly as possible, an operation which has become dangerous

3.15
end of service life
life cycle stage of the EES system starting when it is removed from its intended use stage

Note 1 to entry: According to ISO Guide 64:2008, the sentence “removed from its intended use stage” does not mean “dismantled”. In fact, at the end of the service life, the EES system can either be reused/recovered or disposed of (after treatment, whenever necessary), possibly after dismantling and further processes.

Note 2 to entry: The term ”life-cycle” is defined in ISO Guide 64:2008, 2.5, and in IEC 60050-901:2013, 901-07-12, as “life cycle”.

[SOURCE: IEC 60050-904:2014, 904-01-17, modified – the original definition has been particularized for the EES system and notes to entry have been added]

3.16
end of service life values
value of unit parameters of an EES system that designate the end of service life

Note 1 to entry: EES system unit parameters, such as rated energy capacity, step response performances, rated powers, are generally determined by consensus between the user and the supplier.

3.17
energized, adj.
live, adj.
at an electric potential different from that of earth at the worksite and which presents an electrical hazard

Note 1 to entry: A part is energized when it is electrically connected to a source of electric energy. It can also be energized when it is electrically charged and/or under the influence of an electric or magnetic field.

Note 2 to entry: This entry was numbered 651-01-14 in IEC 60050-651:1999. It has been modified as follows: The word “significant” has been removed as it could not be quantified.

[SOURCE: IEC 60050-651:2014, 651-21-08]

3.18
expected service life
T_{SL}
design duration for which the EES system unit parameters are greater than end of service life values at continuous operating conditions

Note 1 to entry: Generally this duration is expressed in years or in duty-cycles.

[SOURCE: IEC 62477-1:2012, 3.14, modified – the original definition has been particularized for the EES system and the note to entry has been added]

3.19
explosion hazard
condition of an EES system with a potential for an undesirable consequence from explosion

Note 1 to entry: Explosion hazard is a condition where danger exists because hazardous substances that are present may react (e.g., detonate, deflagrate) in a mishap with potential unacceptable effects (e.g., death, injury, damage) to people, property, operational capability, or the environment.

3.20
failure mode
DEPRECATED: fault mode
manner in which failure occurs

Note 1 to entry: A failure mode may be defined by the function lost or other state transition that occurred.

[SOURCE: IEC 60050-192:2015, 192-03-17]

3.21
failure modes and effects analysis
FMEA
DEPRECATED: fault mode and effects analysis
qualitative method of analysis that involves the study of possible failure modes and faults in sub items, and their effects at various indenture levels

Note 1 to entry: The term "fault mode and effects analysis" in IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) is deprecated, since a fault (192-04-01) is a state and cannot logically have a mode, whereas a failure mode (192-03-17) is a change of state.

[SOURCE: IEC 60050-192:2015, 192-11-05]

3.22
failure modes, effects and criticality analysis
FMECA
DEPRECATED: fault mode, effects and criticality analysis
quantitative or qualitative method of analysis that involves failure modes and effects analysis together with a consideration of the probability of the failure mode occurrence and the severity of the effects

Note 1 to entry: The term "fault mode, effects and criticality analysis" in IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) is deprecated, since a fault (192-04-01) is a state and cannot logically have a mode, whereas a failure mode (192-03-17) is a change of state.

[SOURCE: IEC 60050-192:2015, 192-11-06]

3.23
fault tree analysis
FTA
deductive analysis using fault trees

Note 1 to entry: See also fault tree (192-11-07).

[SOURCE: IEC 60050-192:2015, 192-11-08]

3.24
fire hazard
condition of an EES system with a potential for an undesirable consequence from fire

Note 1 to entry: Fire hazard is a condition where danger exists because flammable solids, liquids, gases or their mixture are present in quantities/concentrations that may result in uncontrolled combustion with potential for death, injury, or damage to people, property, operational capability, or the environment.

[SOURCE: ISO 13943:2008, 4.112, modified – the original definition has been particularized for the EES system and note 1 to entry has been added.]

3.25
grid-connected state
operating state in which the EES system is connected to the primary POC

3.26
grid-disconnected state
operating state in which the EES system is disconnected from the primary POC

3.27
harm
physical injury or damage to persons, property, and livestock

[SOURCE: IEC 60050-903:2013, 903-01-01]

3.28
hazard
potential source of harm

Note 1 to entry: In English, the term “hazard” can be qualified in order to define the origin of the hazard or the nature of the expected harm (e.g. “electric shock hazard”, “crushing hazard”, “cutting hazard”, “toxic hazard”, “fire hazard”, “drowning hazard”).

Note 2 to entry: In French, the synonym “risque” is used together with a qualifier or a complement to define the origin of the hazard or the nature of the expected harm (e.g. “risque de choc électrique”, “risque d'écrasement”, “risque de coupure”, “risque toxique”, “risque d'incendie”, “risque de noyade”).

Note 3 to entry: In French, the term “risque” also denotes the combination of the probability of occurrence of harm and the severity of that harm, in English “risk” (see 903-01-07).

[SOURCE: IEC 60050-903:2013, 903-01-02]

3.29
hazard and operability studies
HAZOP studies
structured and systematic technique for examining a defined system with the objective of: identifying potential hazards in the system (the hazards involved may include both those essentially relevant only to the immediate area of the system and those with a much wider sphere of influence, for example some environmental hazards) and identifying potential operability problems with the system and in particular identifying causes of operational disturbances and production deviations likely to lead to non conforming products

3.30
hazardous substance
hazardous material
substance which can affect human health or the environment with an immediate or retarded effect or is capable of posing an unacceptable risk to health, safety, property or to the environment

Note 1 to entry: It may concern other substances than those officially recognized as such in existing hazardous material classification systems, for example, Global Harmonized System (GHS), Transport of Dangerous Goods (TDG).

3.31
intentional islanding
intentional island
island that is intentionally created, usually to restore or maintain power to a section of the utility grid affected by a fault

Note 1 to entry: The generation and loads may be any combination of customer-owned and utility-owned, but there is an implicit or explicit agreement between the controlling utility and the operators of customer-owned generation for this situation.

Note 2 to entry: The term "island" is defined in IEC 60050-617:2009, 617-04-12.

[SOURCE: IEC 62116:2014, 3.6, modified – the note 2 to entry has been added.]

3.32
life cycle
consecutive and interlinked stages of a product system, from raw material acquisition or generation from natural resources to the final disposal

[SOURCE: IEC 60050-901:2013, 901-07-12]

3.33
long duration application
long term application
energy intensive application
EES system application generally not very demanding in terms of step response performances but with long charge and discharge phases at variable powers

Note 1 to entry: Reactive power exchange with the electric power system may be present along with the active power exchange

Note 2 to entry: The term "electric power system" is defined in IEC 60050-601:1985, 601-01-01.

3.34
management subsystem
EESS subsystem providing the functionality needed for the safe, effective and efficient EES system operation

3.35
mechanical hazard
condition of an EES system with a potential for an undesirable consequence from physical force

Note 1 to entry: Mechanical hazard is a condition where physical factors may give rise to injury due to the mechanical properties of products/product parts.

Note 2 to entry: The definition has been formulated along the same lines as that in ISO 13943:2008, 4.112.

3.36
modularity
property of an EES system that specifies the extent to which it has been composed out of separate parts called EESS modules

[SOURCE: ISO/IEC 14543-2-1:2006, 3.2.9, modified – the original definition has been particularized for the EES system]

3.37
operating state
particular combination of EESS element states bound to a specific operation of an EES system during a required time

3.38
personal protective equipment
PPE
any device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards whilst performing live working

Note 1 to entry: This entry was numbered 651-07-01 in IEC 60050-651:1999. It has been modified for greater clarity on the role of PPE.

[SOURCE: IEC 60050-651:2014, 651-23-01]

3.39
point of connection
POC
reference point on the electric power system where an EES system is connected

Note 1 to entry: An EES system may have several POCs arranged in two different classes: primary POC and auxiliary POC. From an auxiliary POC it is not possible to charge electrical energy in order to store it internally and, finally, to discharge it to the electric power system, but a primary POC can be used to feed the auxiliary subsystem and the control subsystem. In the absence of an auxiliary POC, the primary POC can be named simply as POC.

Note 2 to entry: The term ”electric power system” is defined in IEC 60050-601: 1985, 601-01-01.

[SOURCE: IEC 60050-617:2009, 617-04-01, modified – the original definition has been particularized for the EES system and notes to entry have been added.]

3.40
power conversion subsystem
EESS subsystem where energy is converted from the available form at the output of the accumulation subsystem of the EES system to electrical energy with the same characteristics (voltage, frequency etc.) present at the primary POC

Note 1 to entry: Generally (see Figure 8) the power conversion subsystem is connected to the accumulation subsystem and to the primary POC through the primary connection terminal.

3.41
primary POC
point of connection where the EES system charges electrical energy from the electric power system, in order to store it internally and, finally, discharge it to the electric power system

Note 1 to entry: Generally, the primary POC is connected with the EES system's primary subsystem through the primary connection terminal.

Note 2 to entry: The term ”electric power system” is defined in IEC 60050-601:1985, 601-01-01.

3.42
primary subsystem
EESS subsystem consisting of the components/subsystems that are directly responsible for storing electrical energy and extracting electrical energy

Note 1 to entry: Generally the primary subsystem is connected to the primary POC and comprises at least the accumulation subsystem and the power conversion subsystem (see Figure 8).

3.43
protection subsystem
EESS subsystem containing an arrangement of one or more protection equipment, and other devices intended to perform one or more specified protection functions

Note 1 to entry: The protection subsystem includes one or more protection equipment, instrument transformer(s), transducers, wiring, tripping circuit(s), auxiliary supply(ies). Depending upon the principle(s) of the protection subsystem, it may include one end or all ends of the protected section and, possibly, automatic reclosing equipment.

Note 2 to entry: The switches and fuses are excluded.

[SOURCE: IEC 60050-448:1995, 448-11-04,modified – the original definition has been particularized for the EES system, and note 2 to entry has been generalized to exclude all the switches and fuses and not only the circuit breakers.]

3.44
protective measure
measure intended to achieve adequate risk reduction, implemented by the designer (inherent design, safeguarding and complementary protective measures, information for use) and by the user (organization: safe working procedures, supervision, training; permit-to-work systems; provision and use of additional safeguards; use of personal protective equipment)

[SOURCE: IEC 60050-903:2013, 903-01-17]

3.45
reasonably foreseeable misuse
use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behaviour

[SOURCE: IEC 60050-903:2013, 903-01-14]

3.46
risk
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: In French, the term “risque” also denotes the potential source of harm, in English “hazard” (see 903-01-02).

[SOURCE: IEC 60050-903:2013, 903-01-07]

3.47
risk analysis
systematic use of available information to identify hazards and to estimate the risk

[SOURCE: IEC 60050-903:2013, 903-01-08]

3.48
risk assessment
overall process comprising a risk analysis and a risk evaluation

[SOURCE: IEC 60050-903:2013, 903-01-10]

3.49
risk evaluation
procedure based on the risk analysis to determine whether the tolerable risk has been achieved

[SOURCE: IEC 60050-903:2013, 903-01-09]

3.50
safety
EES system freedom from unacceptable risk

Note 1 to entry: In standardization the safety of products, processes and services is generally considered with a view to achieve the optimum balance of a number of factors, including non-technical factors such as human behaviour, that will eliminate or reduce avoidable risks of harm to persons and goods to an acceptable degree.

Note 2 to entry: Unacceptable risk should be defined case by case.

Note 3 to entry: If no conditions that might lead to unacceptable risk can occur, then the EES system is in safe state, otherwise the EES system is in unsafe state.

[SOURCE: IEC 60050-903:2013, 903-01-19, modified – inclusion of note 2 from IEC 60050-351:2013, 351-57-05.]

3.51
self-contained EES system
EES system whose components have been matched and assembled at the factory and that is shipped in one or more containers that are ready to be installed in the field

Note 1 to entry: The term ”container” is defined in IEC TS 62686-1:2015, 3.1.2

3.52
service life
duration from the EES system commissioning test to the end of service life

Note 1 to entry: Generally this duration is expressed in years or in duty-cycles.

Note 2 to entry: Commissioning test is defined in IEC 60050-411:1996, 411-53-06.

3.53
short duration application
short term application
power intensive application
EES system application generally demanding in terms of step response performances and with frequent charge and discharge phase transitions or with reactive power exchange with the electric power system

Note 1 to entry: The term “electric power system” is defined in IEC 60050-601:1985, 601-01-01.

3.54
shutdown
command to move the EES system to the stopped state from another operating state

Note 1 to entry: This command may also be a consequence of an emergency condition.

3.55
skilled person
qualified person
person with relevant education, training, knowledge and experience to enable him or her to perceive risks and to avoid danger which electricity can create

Note 1 to entry: This entry was numbered 651-01-33 in IEC 60050-651:1999. It has been modified as follows: Use of more appropriate English to provide greater clarity to the definition.

[SOURCE: IEC 60050-651:2014, 651-26-11]

3.56
stopped state
operating state in which the EES system is in a grid-disconnected state and the accumulation subsystem is not connected with the power conversion subsystem

Note 1 to entry: Where no switches are available between the accumulation subsystem and the power conversion subsystem other solutions may ensure the galvanic separation (for example extractable batteries).

Note 2 to entry: In this state the auxiliary subsystem is energized.

3.57
thermal hazard
condition of an EES system with a potential for an undesirable consequence from thermal effect

Note 1 to entry: Thermal hazard is a condition which presents an unacceptable risk of personal injury or illness because of heat from heated parts, substances, or surfaces and due to internal short, operation at excessive current and self-heating.

3.58
tolerable risk
risk which is accepted in a given context based on the current values of society

[SOURCE: IEC 60050-903:2013, 903-01-12]

3.59
unintentional islanding
unintentional island
islanding condition in which the generation within the island that is supposed to cease energizing the utility grid instead continues to energize the utility grid

Note 1 to entry: "Island" is defined in IEC 60050-617:2009, 617-04-12.

[SOURCE: IEC 62116:2014, 3.6, modified – "unintentional islanding" added as preferred term and "unintentional island" maintained as admitted term.]

4 Basic guidelines for safety aspects of EES systems

This document is based on IEC Guide 104 which defines procedures for the preparation of safety publications in addition to ISO/IEC Guide 51, including the preparation and use of basic safety publications. IEC Guide 104 has been prepared by ACOS (Advisory Committee on Safety).

The approach taken in this document is shown in Figure 1. The first aspects covered in Clause 5, are the different hazards associated with an EES based on system type, location, size and how it can impact or be impacted by its surroundings. The second aspect, covered in Clause 6, is the conduct of a risk assessment given what is found under Clause 5, according to operational use. The third aspect covered in Clause 7 deals with measures to implement to reduce the risk based on the assessment conducted under Clause 6.

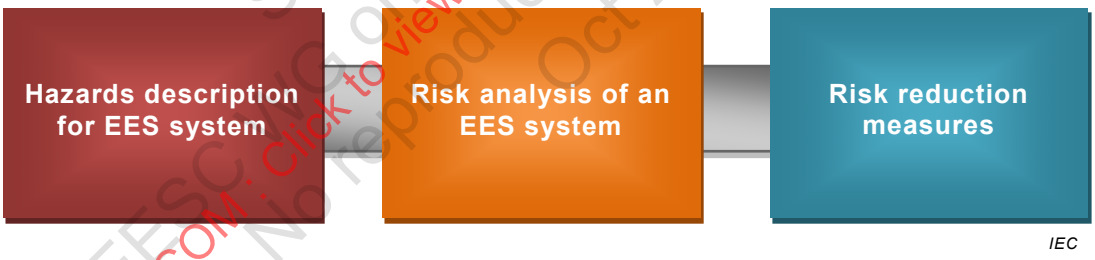


Figure 1 – General description of the approach to address hazards in EES systems

5 Hazard considerations for EES systems

5.1 Electrical hazards

Electricity travels in closed circuits, normally through a conductor. But sometimes a human body and, when proximate, water and even air can be conductors of electricity and inadvertently become part of the electric circuit.

Electrically-caused pain or injury (electric shock) may occur when electrical energy capable of causing pain or injury is transferred to a body part.

Electrical energy transfer occurs when there are two or more electrical contacts to the body:

- between a body part and a conductive part of the equipment;

- between another body part and earth and water or another conductive part of the equipment.

When a person receives a shock, electricity flows between parts of the body or through the body to the ground or the earth.

Depending on the magnitude, duration, wave shape, and frequency of the current, the effect to the human body varies from undetectable to detectable to painful to injurious. Burns are the most common shock-related injury but electric shock may also cause ventricular fibrillation.

In addition to shock and burn hazards, electricity poses other dangers. For example, arcs that result from short circuits during work on energized systems, referred to as “arc flash”, can cause injury or start a fire.

Thermal burns can also be caused when clothing catches fire, as may occur when an electric arc is produced. Arc flash boundaries should be determined to establish appropriate levels of personal protective equipment for workers involved in maintenance and other actions on energized equipment.

Extremely high-energy arcs can damage equipment, causing fragmented metal to fly in all directions. Even low-energy arcs can cause violent explosions in atmospheres that contain flammable gases, vapors, or combustible dusts.

Static electricity can also cause shocks or can just discharge to an object with serious consequences, as when friction causes a high level of static electricity to build up at a specific spot on an object. This can happen simply through handling plastic pipes and materials or during normal operation of rubberized drives or machine belts found in many worksites. In these cases, for example, static electricity can potentially discharge when sufficient amounts of flammable or combustible substances are located nearby and cause an explosion.

Electric hazards can also arise from inappropriate electric fire fighting procedures.

5.2 Mechanical hazards

Mechanically-caused injury is due to kinetic energy transfer to a body part when a collision occurs between a body part and an equipment part. The kinetic energy is a function of the relative motion between a body part and accessible parts of the equipment, including parts ejected from the equipment that collide with a body part.

Examples of kinetic energy sources are:

- body motion relative to sharp edges and corners;
- part motion due to rotating or other moving parts, including pinch points;
- part motion due to loosening, exploding, or imploding parts;
- equipment motion due to instability;
- equipment motion due to wall, ceiling, or rack mounting means failure;
- equipment motion due to handling failure;
- part motion due to an exploding battery;
- equipment motion due to cart or stand instability or failure;
- displacement due to mechanical vibration;
- equipment motion due to interaction with natural risks (flood, earthquake).

Mechanical trauma includes friction, pressure, abrasions, lacerations and contusions causing more or less serious injuries.

5.3 Other hazards

5.3.1 Explosion hazards

An explosion is a rapid expansion of gases resulting in a rapidly moving pressure or shockwave. Explosions are classified according to the nature of the system “transformation”, and usually explosions of physical origin and chemical origin are distinguished.

Physical explosions include BLEVE (boiling liquid expanding vapour explosion) which is a violent explosive vaporization leading to the rupture of a tank containing a liquid at a temperature significantly above its normal boiling point at atmospheric pressure. In this case the "transformation" is a variation of internal energy.

Chemical explosion can result from the runaway of exothermic chemical reaction or from the decomposition of unstable substances. The burning of a fuel/air mixture’s combustible vapours (gas explosions) and burning of a suspension’s air/fuel particles (dust explosions) are also involved, and the transformation is a combustion reaction of an explosive atmosphere. The potential hazards associated with explosive atmosphere are released when ignited by an effective ignition source.

In general explosions of solids, liquids or gases are divided into two types: deflagrations and detonations. In both types a reaction zone propagates through the reactant(s). Owing to the density difference, the energy release per unit of volume is much higher for liquids and solids than for gaseous reactants.

Explosions endanger the lives and health of those exposed as a result of the uncontrolled effects of flame and pressure, the presence of noxious reaction products, the discharge of projectiles, and the consumption of the oxygen in the ambient air.

5.3.2 Hazards arising from electrical, magnetic, and electromagnetic fields

In addition to the conventional electrical hazards described in 5.1, high-level electromagnetic energy produced by radio frequency radiation (RFR) can also induce electrical currents or voltages that may be a source of disturbance on other equipment, cause electrical arcs that may ignite flammable materials, or act as an ignition source in explosive atmospheres' hazardous areas. Radiation-caused injury is out of the scope of this document.

5.3.3 Fire hazards

A fire hazard occurs if combustible materials, oxidizer and ignition energy are available in sufficient quantities at the same place and at the same time. The fire hazard depends on the interaction of these three items.

Certain materials are inherently unstable, or have extraordinary oxidizing properties, or are capable of self-heating. This affects the fire hazard.

Variation in the oxygen concentration (e.g. oxygen enrichment) can also significantly affect the fire hazard.

The fire hazard can arise from the materials used or released by the EES system, from materials in the vicinity of the EES system, or from materials used in the construction of the EES system.

Combustible materials can occur as solids, liquids or gases of organic or inorganic nature. It should be determined whether combustible materials exist or can exist and in what quantity and distribution.

The ease of combustion of materials is affected by the size, shape and deposition of the materials. For example, small pieces of a material loosely collected together can be more

easily ignited than a large piece of that material. The combination of materials can also have an influence on the ignitability and the burning behaviour. Consideration should be given as to whether the properties of the materials can change over time or with use. Such changes can include the possibility of decomposition of the material releasing combustible gases and vapours. This can lead to an increased fire hazard.

In assessing the fire hazard, the existence and quantity of fire supporting substances, for example oxygen producing substances, and the probability of their occurrence should be determined. The most common oxidizer is air but there are other oxidizers which support combustion, for example potassium nitrate (KNO_3), potassium permanganate ($KMnO_4$), perchloric acid ($HClO_4$), hydrogen peroxide (H_2O_2), and nitrous oxide (N_2O).

It should be determined which ignition sources exist or can occur. Possible ignition sources can arise due to the influence of:

a) heat energy;

b) electrical energy;

c) mechanical energy;

d) chemical energy.

Electrically-caused fire is due to conversion of electrical energy to thermal energy where the thermal energy heats a fuel material followed by ignition and combustion. Electrical energy is converted to thermal energy either in a resistance or in an arc and is transferred to a fuel material.

Fire initiation is produced when sufficient energy release allows the heating of a fuel element by conduction, convection, or thermal radiation to a temperature such that a combustion reaction starts. It should be noted that the combustion reaction will always occur between the oxygen and the gaseous fuel.

Depending on the nature of the fuel (gas, liquid or solid), the ignition process will be different.

For gases, the initiation occurs in a fuel oxidizer mixture with proportions between the lower flammability limit (LFL) and the upper flammability limit (UFL). The energy input to initiate combustion mixture is often very low. This energy is commonly measured in the stoichiometric proportions of the combustion reaction. Hence it is called low energy flammability (LEF). This energy is often of the order of a few milliJoules. A spark may be enough to ignite the mixture.

For liquids, combustion occurs from the vapor emitted, provided that the vapor emission rate is sufficient to create a flammable mixture with the ambient air. In addition, ignition of the mixture will only occur if enough energy (≥ LEF) is provided when the temperature of the liquid is higher than its temperature flash point.

For solid fuels, the initiation phenomenon is more complex because it is governed by heat transfer within the material. The energy received by the fuel increase the temperature of the solid until the sublimation or decomposition temperature is reached. This process is called the pyrolysis phenomenon. The initiation time depends on the intensity of the thermal flow, of the thermal properties, of the ignition temperature and of the water content.

The propagation phase corresponds to the rise of fire related to the path of combustion of the flammable items. During this phase the position of the fuel elements plays an important role as a criterion that enables or impedes the development of the fire.

The fire hazard can result for example from the fire itself, the thermal radiation, the fire effluent, or the escaping materials. An explosion hazard may exist in addition to the fire hazard.

Thermal and chemical fire-induced hazards threaten people and the environment. These fires may vary highly in nature and intensity according to the material that is burning (nature, geometry, quantity) and burning conditions.

5.3.4 Temperature hazards

Thermal energy transfer occurs when a body touches a hot equipment part or hot liquids. The extent of injury depends on the temperature difference, the thermal mass of the object, rate of thermal energy transfer to the skin, and duration of contact. The perception of the human body varies from warmth to heat that may result in pain or injury (burn).

Hot smoke inhalation can cause burn injury. In fact, 60 % to 80 % of burn fatalities come from major smoke inhalation. The immediate effects can include fainting, blockages of airways, singed facial and/or nose hair, and burns around the face and neck. Smoke inhalation can also lead to pulmonary (lung) injury.

Exposure to thermal radiation can cause burns to the skin. The radiation types of greatest concern are thermal radiation issued from open flames and explosions.

Exposure to extreme cold temperatures could also generate some injury to skin and body parts.

Normal operations as well as abuse conditions can both generate dissipation of heat and therefore potential thermal hazards

5.3.5 Chemical hazards

Injury caused by hazardous substances is due to a chemical reaction with a body part. The extent of injury by a given substance depends on both the magnitude and duration of exposure and on the body part's susceptibility to that substance.

A worker’s skin and eyes may be exposed to hazardous chemicals through direct contact with contaminated surfaces, deposition of aerosols, immersion, or splashes.

Chemical agents are divided into two types: primary irritants and sensitizers. Primary or direct irritants act directly on the skin though chemical reactions. Sensitizers may not cause immediate skin reactions, but repeated exposure can result in allergic reactions.

Contact with strong acids or alkaloids or other corrosive or caustic materials can eat away or “burn” skin and deeper tissue. These can be caused by various chemicals used in workplaces.

There are also the immediate and long-term dangers from inhaling, swallowing or absorbing toxic chemicals through the skin.

Chemical effect may be fire induced (e.g. fire gases toxicity) or not (release of effluents during normal operations) or may be induced through heating chemicals beyond decomposition temperature in either normal or abuse conditions.

Chemical effect may also encompass creating an explosive atmosphere by production of flammable gases (e.g. hydrogen).

Discharge of previously accumulated toxic gas can generate serious hazards in terms of massive exposure to humans in the area. In addition, severe corrosion issues may be triggered.

5.3.6 Unsuitable working conditions

All EES systems that are located indoors or are located outdoors in an enclosure should be arranged to facilitate access to and egress from the area in which the system is installed or enclosed to prevent persons from becoming trapped. Working space and conditions shall be adapted to the risk of musculoskeletal disorders (MSD) injury which depends on work positions and postures, how often the task is performed, the level of required effort and how long the task lasts. Risk factors that may lead to the development of MSDs include:

- exerting excessive force by lifting heavy objects, pushing or pulling heavy loads, manually pouring materials, or maintaining control of equipment or tools;
- performing the same or similar tasks repetitively. Performing the same motion or series of motions continually or frequently for an extended period of time;
- working in awkward postures or being in the same posture for long periods of time;
- pressing the body or part of the body (such as the hand) against hard or sharp edges, or using the hand as a hammer.

Cold temperatures in combination with any one of the above risk factors may also increase the potential for MSDs to develop through

– excessive noise that is continuous and can damage hearing over time for persons in the vicinity that are not using protective hearing equipment;
– exposure to radio frequency energy of sufficient intensity at frequencies between 3 kHz and 300 GHz that can adversely affect personnel.

6 EES system risk assessment

6.1 EES system structure

6.1.1 General characteristics

To conduct the risk assessment study, a description of the EES system is required. The following general characteristics shall be noted:

- type, power, energy, rated life according to calendar or cycling ageing (guaranteed life time, number of cycles),
- application type,
- hazardous materials contained (formulas, physical state, quantities, safety data sheets),
- general functions, security functions, programming functions,
- self-test functions, remote control, staff presence,
- auxiliary devices included in the system,
- measures taken to ensure the design safety and the reliability of the system,
- measures available to mitigate the risks,
- operating parameters,
- known hazards associated with any components of the EES system,
- instructions for use.

6.1.2 Specific characteristics

The main types of EES systems, according to the energy form, are mechanical, electrochemical, thermal and chemical, as noted below:

- mechanical
  – pumped hydro (PHS)

  - compressed air (CAES)
  - flywheel (FES)
- electrochemical
  - secondary batteries
  - flow batteries
- thermal
- chemical
  - hydrogen

Annex A gives a short description of the main risks of different mechanical, electrochemical and chemical storage technologies.

6.2 Description of storage conditions

6.2.1 Types of grids

EES includes any type of grid-connected energy storage which can both store electrical energy from a grid or any other source and provide electrical energy to a grid. “Grid” includes:

a) transmission grids
b) distribution grids
c) commercial grids
d) industrial grids
e) residential grids
f) islanded grids

6.2.2 Type of applications

The following are some EES system applications:

a) peak shaving (long duration application)
b) load levelling (long duration application)
c) frequency regulation (short duration application)
d) stabilizing renewable energy (short duration application)
e) backup power

6.2.3 Location

The following are EES system locations:

a) residential including group of households
b) commercial and public access buildings
c) industrial
d) utility

Physical storage locations also should be considered. Examples of the physical storage locations are:

- outdoor enclosed and/or unenclosed
- indoor enclosed and/or unenclosed
- underground

6.2.4 Vulnerable elements

To assess the severity of a potential accident or incident, it is essential to clearly identify the elements of the environment that could be affected. Generally the following elements have to be considered:

- people (e.g. site staff concerned, resident populations or people working around the site, including number, time of presence, distance from the plant and type of persons and their limitations);
- facilities and equipment not directly in the field of study;
- some essential safety equipment;
- devices relying on the EES system;
- properties and structures;
- natural environment (e.g. groundwater, rivers, soil, atmosphere, wind direction, seismic levels, lightning levels, and altitude).

6.2.5 Special provisions for EES systems in generally accessible locations

With residential grids, there is the added concern with regard to exposure of the system to the untrained public. Equipment located in residential grids may be located where the general public may have direct contact, so the design of the system should take this into consideration. These include preventing access to hazardous parts through the use of enclosures and guards with limited openings, insulation to prevent thermal hazards, and preventing access to controls to prevent tampering or misoperation. Controls will need to be designed to be automated as well as inaccessible to some level as there are no skilled operators on site. Equipment for use with residential grids may need to be provided with protection to prevent damage from inadvertent impact from vehicles if located in garages or near roadways. If located within residences, EES systems will need to meet local residential building code criteria. Use of EES systems in residential grids may limit some technologies, where hazards cannot be sufficiently mitigated in a residential setting.

6.2.6 Sources of external aggression

Some sources of aggression should generally be identified:

- on site sources: other facilities and hazardous equipment, vehicles and other moving objects, work, utility losses, malicious acts;
- natural sources: extreme weather conditions (frost, wind, snow, fog, etc), landslides and earthquakes, lightning, flooding with fresh or salt water.

6.2.7 Unattended operation

An unattended operation EES system may undergo a variety of external aggressions and internal trouble during its operation. Often the system may emit vibration, sounds or odours, which often cannot be detected by humans. A remote monitoring system may send a fault signal to the operator control station. The operator takes the necessary actions remotely, and the operating signals are delivered to the system. Both the risks associated with wrong signals back and forth and the risks associated with human errors should be considered.

6.2.8 Unintentional islanding

In general, a distribution line is at no-voltage during the system blackout because the distribution line circuit breakers are opened (see Figure 2). In the distribution lines which are connected to the EES system, the area which should be originally at no-voltage, however, is energized and in that case the EES system continues to operate and is not separated from the power networks. The state in which distribution lines are energized only by the electric power supplied from the EES system is called unintentional islanding.

With an EES system designed for intentional islanding, in case a circuit breaker opens in the distribution line, the disconnected part can be supplied by the EES systems and possible local energy production.

Unintentional islanding is in danger of having considerable impact on the safety of human bodies and facilities. The public as well as technical staff might be at risk of electric shock during incident investigation or during equipment removal operations.

There is a requirement that unless designed for intentional islanding, measures are to be taken to prevent the islanding operation by detecting it directly or indirectly using the protection relay or other methods and swiftly disconnecting the EES system from the distributing network.

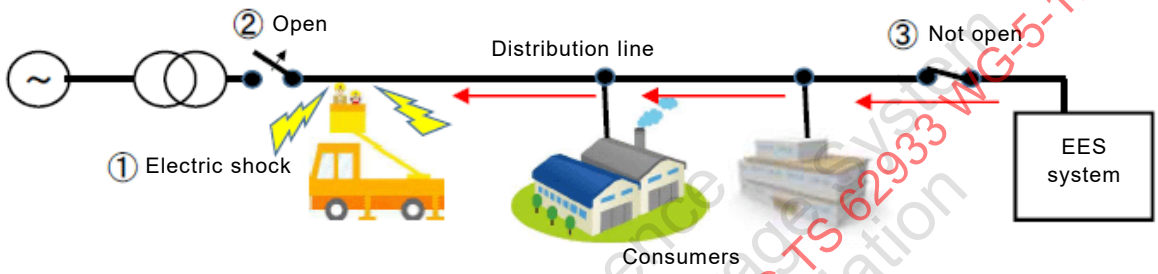


Figure 2 – Islanding of the EES system

6.3 Risk analysis

6.3.1 General

During the risk assessment the impact of the hazards should be considered for all stages of the life cycle (design and planning, transport, installation, commissioning, operation, maintenance and repair, and end of service life).

All EES system components such as power conversion subsystems, generators, hydro turbines and pumps, energy storage devices (battery, dam, etc.), transformers, system controllers, breakers, fuses, wiring, filters, tanks, pipes, blowers, control power sources, etc., are, in principle, designed, manufactured and tested based on relevant international standards for their safety compliance.

For the operation of those components, the EES system has a lot of connections between components, such as main circuit connections, control signal wiring, communication signal wiring, pipes, control power lines, fasteners to buildings, trenches, etc.

Additionally, components may be produced or supplied by different manufacturers for an EES system. The combination of those components should not be considered as safe per se and therefore further risk assessment due to the integration is needed. In particular, the risk of incompatibility of some components resulting from the integration shall be assessed by appropriate risk assessment methods. Furthermore, the total energy stored in the EES system and the potentially exposed population in the area should be considered.

6.3.2 Risk considerations

6.3.2.1 Issues raised from unauthorised or unsafe access resulting from inadequate protection

Ineffective access control or lack of access control (e.g. for security reasons) or unsafe access provisions (e.g. lack of space ergonomy for maintenance operations), inadequate design, size of emergency exits or other shortcomings of protection may trigger special causes of hazards.

6.3.2.2 Ineffective protection coordination of total system

Ineffective protection coordination can possibly cause a fire or electric hazards. For example, when the protection device cannot interrupt high current in case of accidental short circuit, some part of the system is overheated and fire can result.

6.3.2.3 Malfunction detection

The absence or ineffective operation of malfunction detection can give rise to electrical hazards, mechanical hazards, explosion, fire, etc. For example, when an electrical fault gives rise to leakage or earth fault current and is not detected, electric shock hazards can result. When the malfunction is not detected, the EES system may be operable beyond the safety limit. Explosion or fire may result.

6.3.2.4 System control malfunction

System control malfunction and operation beyond the safety limit of the EES system can cause electrical hazards, mechanical hazards, explosion, fire, etc. System control malfunction and operation beyond the safety limits of the EES system can possibly be caused by lost external communication, communication lost between equipment, short or open circuiting of the control signal line, control signal error, malfunction of equipment, control power lost, etc. When large energy, material or chemical quantities, stored in the EES system are released, explosion or fire can be caused.

6.3.2.5 Auxiliary subsystem malfunction

Auxiliary subsystem malfunctions can cause various hazards such as temperature hazards, chemical hazards, explosion hazards and fire hazards. For example, an air conditioner malfunction could cause the operating temperature of some components to be exceeded. A ventilation malfunction could cause chemical poisoning.

6.3.2.6 Safety policies

Safety policies should be in place in order to minimize hazards due to human error, improper design or installation, insufficient inspection or maintenance, and inadequate training and signage.

6.3.2.7 Improper working environment, conditions, and equipment

Improper working environment, conditions and equipment could cause many hazards. The EES system should be designed and constructed to ensure that it is suitable for the environment in which it is to be used. Factors such as humidity, temperature and flooding amongst many others should be addressed in the design criteria.

6.3.2.8 Guidelines and indications for extinguishing fires, evacuation plan, route and indications

Ineffective guidelines and indications for extinguishing fires, ineffective evacuation plan, route, and indications could extend fire and explosion hazard results.

6.3.2.9 Serious hazard risks

Significant failure of some EES system could result in fire, explosion, or toxic gas release. In addition projectiles could be expelled during an explosion. Such hazards may have the capacity to cause serious injury or death. Consideration of these serious hazard risks is necessary for the appropriate design of the EES system.

6.3.2.10 Risks from maintenance

Lack of suitable maintenance procedures or unskilled/poorly trained service personnel can introduce risks. The risk analysis should consider maintenance as a potential source of hazards.

6.3.3 System level risk analysis

One key action to keep an EES system safe is to efficiently use analysis techniques for system reliability such as the procedures for failure mode and effects analysis (FMEA) described in IEC 60812. In the system level FMEA, if all component functions and all connecting points between those components are defined correctly, then the malfunction effects of components and connecting point functions are analyzed. Also, workers' roles can be defined and human error effects can be taken into account.

For low-risk and low-complexity systems, failure modes, effects and criticality analysis (FMECA) may be a very cost-effective and appropriate method. If during the FMECA the likelihood of high-risk effects is recognized it is recommended that a probabilistic risk analysis (PRA) should be used in preference to a FMECA.

The other risk analysis tools defined in IEC standards such as fault tree analysis (FTA) described in IEC 61025, and the hazard operational process (HAZOP) described in IEC 61882, can be used as an alternative. The result of risk analysis is documented and the study will be kept available for the organizations responsible for operating the EES system.

When FMEA, FTA or HAZOP show the possibility of fire, explosion or toxic gas discharge, functional safety management should be conducted following IEC 61508 (all parts) or one of its derivative standards.

In case the public communication line is employed, cyber security is also to be considered even when it is employed only partially. Risk analysis for cyber security could be made and described separately from the analysis described here.

7 Requirements necessary to reduce risks

7.1 General measures to reduce risks

As a result of the system level FMEA or risk analysis conclusions, the necessary prevention and protection measures shall be taken to prevent accidents and limit their consequences. This means that for all the scenarios for which the probability and/or the severity of consequences is too high, measures of risk reduction shall be proposed according to Figure 3. Subclause 7.1 is intended to describe guidance for reducing risks. Details should be separately discussed for each technology.

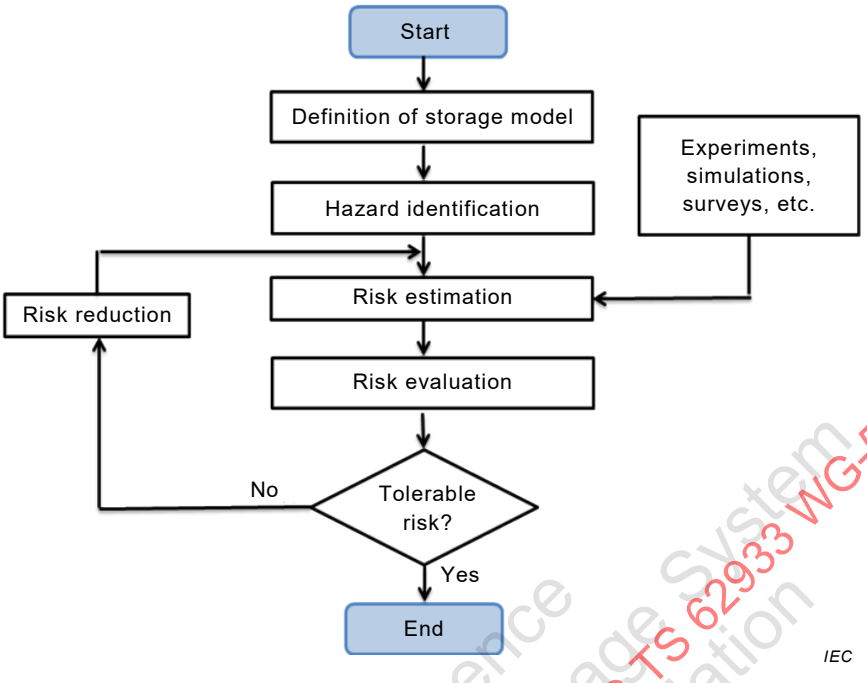


Figure 3 – Iterative checking sequence in general risk assessment procedures

The scenarios considered in the risk analysis shall include catastrophic external effects on the system of both severe natural disasters and severe social/human impact. Natural disasters include all kinds of natural disasters, some of which are seasonal and some of which come with little forewarning such as earthquake, flooding and tsunami. Social/human impact includes sabotage by a single person, social turmoil, and terrorism.

Preventive measures heavily depend on the location of the system but measures should be identified even for rare external events that may have significant impact on the EES system. Preventive measures to be identified here are the measures to avoid the impact, to minimize the impact to limited system damage and to mitigate the catastrophic system damage.

In spite of the preventive measures, in the event that partial damage could take place, measures to suppress the propagation of the damage should be immediately taken. Proven firefighting, internal propagation reduction means, emergency fire extinguishers and emergency shutdown are also part of this prevention. Further call-up of the emergency team is included depending upon the level of damage.

Figure 4 indicates general risk reduction measures for an EES system. When a hazardous incident occurs, measures to control the propagation of the damage should be considered in the layers of prevention and mitigation. Additionally, plant emergency responses and area emergency responses should be planned and prepared in advance to minimize the magnitude of the hazard.

Figure 5 indicates damage propagation from an incident to hazards, and layered measures to minimize damage. A minor incident such as external impact, hardware/software and system malfunction, reasonably foreseeable misuse, can cause partial damage to the system. If the partial damage propagates to a wider area of the system, a big accident could happen. The necessity of layered measures to control the damage propagation should be considered apart from the normal control and monitoring.

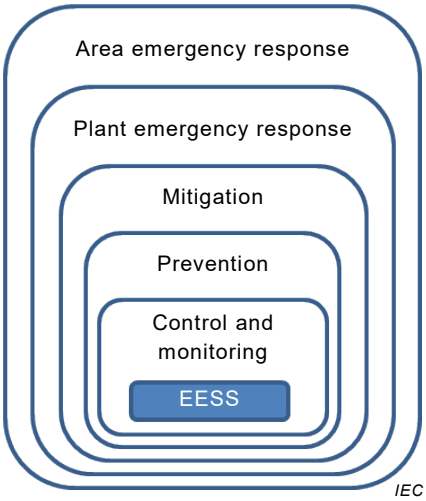


Figure 4 – General risk reduction measures to minimize hazards

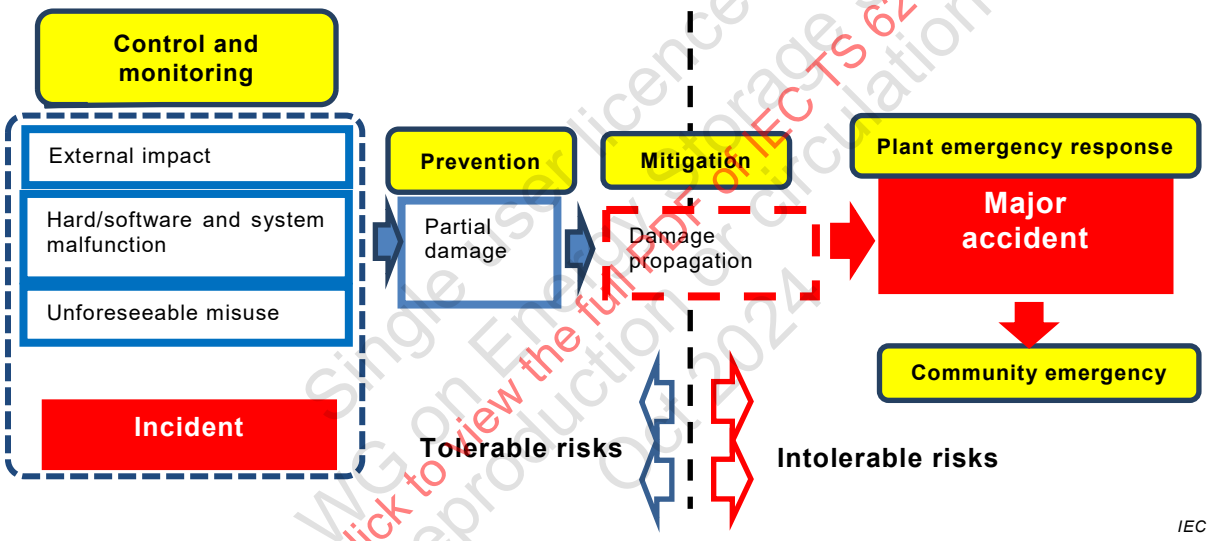


Figure 5 – Damage propagation from an incident to a big accident, and layered measures to minimize damages

7.2 Preventive measures against damage to neighbouring inhabitants

Attention should be paid to accidental phenomena causing effects likely to affect neighbouring inhabitants (e.g. explosion, fire, dispersion of toxics).

“Major accident” means an occurrence such as a major emission, fire or explosion resulting from uncontrolled developments in the course of the operation of the ESS system and leading to serious danger to human health or the environment, immediate or delayed inside or outside the establishment, and involving one or more dangerous substances.

Operators should have a general obligation to take all necessary measures to prevent major accidents, to mitigate their consequences and to take recovery measures.

When the risk assessment concerning fire, explosion or toxic gas discharge shows intolerable hazard possibility, the EES system should have a safety related system (SRS) preferably in accordance with IEC 61508 (all parts) to decrease the hazard risk to tolerable levels. It is recommended to use simple reliable hardware SRS which is independent and separated from the EES system control subsystem.

7.3 Preventive measures against damage to workers and residents

7.3.1 Protection from electrical hazards

All sources of electrical energy in the EES system should be controlled in such a way as to minimize human exposure to electrical hazards and prevent access to the EES system by fauna and flora. Live parts of EES systems that have hazardous voltage circuits should be guarded against accidental contact by an enclosure or by other means such as fencing, guarding, etc., to prevent inadvertent access to the live parts.

Operating and maintenance instructions shall include information on safe working practices. Wherever possible, work should commence only when conductors normally energised at a dangerous voltage have been securely isolated and earthed. Areas within and around the energy storage system requiring special protection measures against arc flash and shock hazards shall be provided with cautionary signage to identify the hazards and necessary precautions. Where isolation is not possible, for example work on battery terminals, instruction shall be provided on the appropriate personal protective equipment (PPE) required to perform the task.

The EES and associated electrical equipment that is likely to require examination, adjustment, servicing, or maintenance while energised should be designed to minimise the risk of electric shock or burn injury. In circumstances where it is impractical to prevent access to dangerous live parts, warning notices should be fixed to warn qualified persons of the hazards.

When wire and cable products are exposed to fresh or salt water or excessive moisture, the components may be damaged due to mildew or corrosion. This damage can result in insulation or termination failures and can generate additional electrical hazards.

Examples of preventive measures for electrical hazards need to consider the following:

- earth fault detection,
- over/under voltage detection,
- over/under current detection,
- over/under temperature,
- lightning protection,
- electrostatic dissipation,
- fusing.

Supplementary information is provided in IEC 60364-4-41 which deals with protection against electric shock as applied to low voltage electrical installations.

In case of unintentional islanding, the following two methods for island detection should be used in combination when the EES system is connected to a grid to decrease electrical risks:

a) Passive type method

The phenomena in which the voltage phase and the frequency are changed suddenly by the unbalance of the output of power generation and the load at the time of shifting to islanding.

b) Active type method

The phenomena in which the fluctuation of the voltage, frequency and line impedance, resulting in grid disconnection, becomes noticeable are an indication of islanding.

Unless the system is specifically designed and allowed to operate in intentional islanding, when islanding is detected, the EES system shall be automatically disconnected from the grid.

When maintenance operations are planned, appropriate analysis of the electric isolation of the concerned parts of the grid should be performed and documented before any intervention operation.

7.3.2 Protection from mechanical hazards

The basic safeguard against mechanically caused injury is a function of the specific EES system. Basic safeguards may include:

- enclosure structural requirements (rounded edges and corners; enclosure to prevent a moving part from being accessible);
- safety interlock to control access to an otherwise moving part;
- means to stop the motion of a moving part;
- means to stabilize the equipment;
- robust handles;
- robust mounting means;
- means to contain parts expelled during explosion or mechanical failure.

7.3.3 Protection from other hazards

7.3.3.1 Protection from explosion

The combination of an explosive atmosphere and an effective ignition source as a potential source of an explosion requires application of the basic principles of explosion prevention and protection in the following order:

a) Prevention:
   – avoid or reduce explosive atmospheres; this objective can mainly be achieved by modifying either the concentration of the flammable substance to a value below the explosion range or the concentration of oxygen to a value below the limiting oxygen concentration (LOC);
   – avoid any possible effective ignition source.

b) Protection:
   – halting the explosion and/or limiting the range to a sufficient level through protection methods, for example isolation, venting, suppression and containment; in contrast to the two measures described in a), here the occurrence of an explosion is accepted.

The risk reduction could be achieved by applying only one of the above prevention or protection principles. A combination of these principles can also be applied.

The avoidance of an explosive atmosphere shall always be the first choice.

The more likely the occurrence of an explosive atmosphere, the greater the extent of measures taken to prevent likely sources of ignition.

To allow selection of the appropriate measures, risk reduction assessment shall be developed for each individual case.

In the planning of explosion prevention and protection measures, consideration shall be given to normal operation, which includes start-up and shut-down. Moreover, possible technical malfunctions as well as reasonably foreseeable misuse shall be taken into account. Application of explosion prevention and protection measures requires a thorough knowledge of the facts and sufficient experience. It is thus advisable to seek guidance from competent persons.

7.3.3.2 Protection from hazards arising from electric, magnetic, and electromagnetic fields

EES systems should be integrated with equipment that satisfies relevant IEC documents such as IEC 61000 (all parts) so that they have sufficient immunity against electric, magnetic and electromagnetic disturbances to prevent hazards from arising. Moreover, any potential disturbances induced by the integration level should be taken into account.

Sufficient EMC immunity of the components is confirmed in the single component EMC immunity testing, but it should be considered that system interactions could amplify the magnetic and electromagnetic disturbances and can cause malfunction of individual components and communications between those components. In order to achieve essential safety, EES system protection controls should be designed and tested considering the existence of EMC disturbances that may occur in the environment in which the EES system is located.

7.3.3.3 Protection from fire hazards

The basic safeguard against electrically-caused fire is that the temperature of a material, under normal operating conditions and abnormal operating conditions, does not cause the material to ignite. The supplementary safeguard against electrically-caused fire reduces the likelihood of ignition or, in the case of ignition, reduces the likelihood of spread of fire.

Examples of prevention and protection measures include the following:

- use of materials in the construction of the system which are non combustible, non flammable and/or have reduced combustibility/flammability, for example flame retardant materials;
- elimination or minimization of the risk of overheating by analyzing the process deviations which might lead to overheating;
- where the possibility of a fire cannot be eliminated, the effects of that fire, including flames, heat and smoke etc., shall be limited for example by shielding or enclosure of the storage to eliminate or minimize the risk of injury to persons and/or damage to property and/or the environment;
- risk reduction may be achieved by appropriate use of integrated fire detection and fire fighting systems (safety components), which comprise devices for the detection, control, alarm and extinguishing functions;
- programmed shutdown or emergency stop of the storage and/or of auxiliary equipments;
- isolation of the protected area covered by the fire fighting system, for example by an enclosure or water curtain;
- supplying comprehensive and understandable documentation to the users in order to ensure that they can keep the installations and the technical fire protection equipment in proper condition and ready for operation and, where necessary, initiating the required fire fighting measures.

The level of fire detection and suppression required for an energy storage system is dependent upon the size, technology and location of the installation of the system as well as the quantity and geometry of hazardous substances. The protection may be as basic as instructions regarding the appropriate fire extinguishing materials to maintain within the location, installation instructions and basic housekeeping and safety procedures to follow, to installation of fire suppression systems at the location of installation of the EES system.

To determine the level and type of fire detection and fire suppression systems required, a fire risk assessment is to be conducted for energy storage system installations to ensure that suitable fire prevention and fire protection requirements for protecting persons and property are met in accordance with local codes and regulations.

Energy storage system installations required to be provided with fire suppression shall be provided with a means for fire detection and suppression in accordance with the siting of the system (i.e. indoors, etc.), the energy storage technology and the applicable installation, building and fire safety codes and regulations. If not provided as part of the energy storage system, guidance for choosing and installing suitable fire detection and suppression systems shall be provided in the installation and maintenance instructions for the energy storage system.

Supplementary information is provided in IEC 60364-4-42 which deals with protection against thermal effects, including combustion and flames caused by electrical installations.

7.3.3.4 Protection from temperature hazards

In the system which contains hot parts, thermal insulation or appropriate protection means to guard the hot parts is to be provided.

Regardless of whether the system contains hot parts or not in normal operation, in the case where the system deviates from normal operation, parts of the system may undergo temperature rise. Such parts are to be identified in the designing stage. Protection and/or appropriate signage is to be provided.

Temperature rise due to deviation from normal operation is to be continuously monitored by thermal sensors, and alarms for worker safety are to be provided according to the level of hazard to the worker.

7.3.3.5 Protection from chemical effects

The basic safeguard against injury caused by hazardous substances is containment of the material.

Supplementary safeguards against injury caused by hazardous substances may include:

- a second container or a spill-resistant container with sufficient capacity to store the fluid within the EES system;
- containment trays;
- tamper-proof screws to prevent unauthorized access;
- instructional safeguards;
- sensors and alarms;
- material resistance to chemicals contained.

If the possibility of toxic gas discharge exists, measures to avoid toxic gas accumulation should be considered. Toxic gas accumulation measures should consider the landform, the building design and the physical characteristics of the gas. Toxic gas detection and alarm may be a part of those measures. Also, use of appropriate personal protection equipment (PPE) should be considered.

7.3.3.6 Protection from unsuitable working environment

7.3.3.6.1 Remote controls and automatic controls

EES systems which have the ability to be controlled remotely should be provided with a means to disable the remote control in order to perform inspection or maintenance. The use of a remote control system should not lead to an unsafe condition as determined by the system hazard analysis and should not be able to override local safety controls. The same requirements apply for local automatic controls without human intervention, in response to the occurrence of predetermined conditions.

7.3.3.6.2 Working space

Sufficient working space for EES systems and equipment likely to require examination, adjustment, servicing, or maintenance while energized should be provided in compliance with local codes and regulations. Sufficient space shall be provided and maintained around EES systems to permit ready and safe operation and maintenance of such equipment.

7.3.3.6.3 Egress and protection from physical hazards

EES systems that are located indoors or are located outdoors in an enclosure should be provided with at least one entrance of sufficient size to give access to and egress from the working space in the system in accordance with local codes and regulations.

Doors provided for entrance into EES systems should open in the direction of egress and be equipped with panic bars, pressure plates, or other devices that are normally latched but open under simple pressure from the inside. Doors shall be equipped with locks to prevent access to unqualified persons. Sufficient precautions should be taken to ensure there is no one inside the door before locking it from the outside.

Entrances to EES systems should be marked with warning signs forbidding unqualified persons to enter.

Areas of access within the EES system should be designed to prevent tripping, slipping or falling when persons enter or exit, or while within the system. Surfaces and parts within a walk-in EES system should be designed to prevent inadvertent hazards to personnel within the enclosure (i.e. sharp edges, moving parts, hot surfaces, etc.) through appropriate guarding, electrical and thermal insulation methods and cautionary signage and warning labels.

7.3.3.6.4 Prevention of hazardous emissions and leaks

EES systems should not vent or leak hazardous or toxic materials within access areas of the EES system or into the surrounding environment in accordance with local codes and regulations.

EES systems that are installed indoors and enclosures associated with self-contained EES systems that can be fully entered by persons should have adequate ventilation for persons working on the indoor EES system or within an EES system.

If determined necessary by risk assessment, provisions are to be provided for liquid leakage detection, toxic gas detection and spill detection.

7.3.3.6.5 Task lighting within EES systems

Illumination should be provided for all working spaces within EES systems. The lighting outlets should be arranged so that persons changing lamps or making repairs on the lighting system are not endangered by live parts or other equipment.

Emergency lighting is to be provided in accordance with local regulations.

7.4 Over current protection design

Over current protection design which includes location, capacity and protection coordination should be confirmed by the calculation.

The calculation should be documented and maintained within the system documentation.

Relevant IEC documents should be referred to when applicable.

7.5 EES system disconnection and shutdown

7.5.1 General

Disconnection and shutdown procedures are important for ensuring safety during operation, routine maintenance or fault repair. They will depend on the design of the EESS, the technologies employed (see Figure 6), its size and the reason for the disconnection and shutdown. The EESS should be capable of being disconnected partially or totally to reflect the likely operation, routine maintenance and credible fault repair activities required. Emergency shutdown should also be addressed.

The main circumstances that may require conditions leading to the disconnection of the EES system or of some of its components are:

- regular maintenance;
- subsystem/component malfunction;
- external constraints;
- system upgrades;
- end of service life.

Disconnection or partial disconnection may be achieved at different parts of the EES system:

– point of connection to the grid;
– AC facility including transformer;
– switching device (SW);
– power conversion subsystem;
– alternator;
– storage subsystem;
– auxiliary subsystem;
– smaller parts in subsystems.

Where the EES system has high energy levels or high stored energy, special precautions may be required. The disconnection or shutdown procedure should not lead to the EES system becoming unsafe.

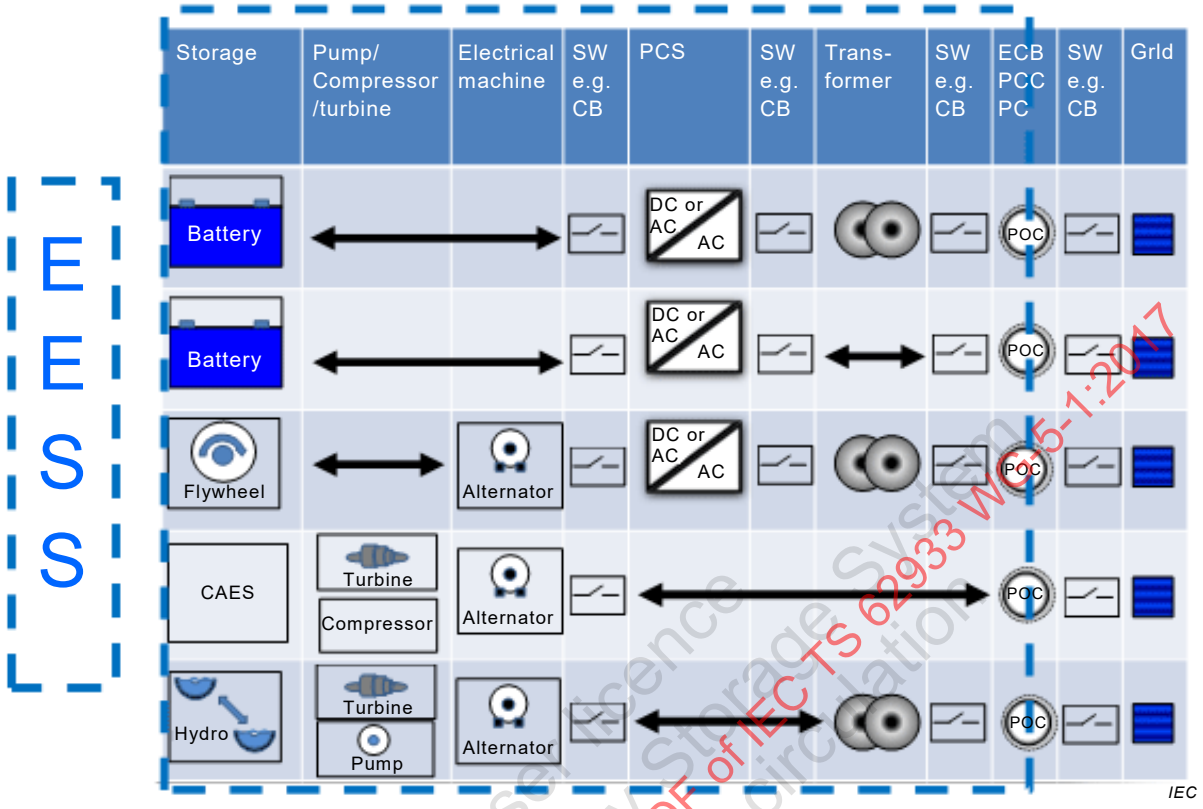


Figure 6 – Examples of different EES system architectures

As is shown in Figure 6, switching devices (SWs) are positioned differently for each technology. A detailed sequence of SW opening depends on the technology.

7.5.2 Grid-disconnected state

In the grid-disconnected state, the EES system will be electrically separated from the local grid connection. An EES system should be provided with a disconnection means that disconnects the unearthed conductors between the EES primary subsystem and the primary point of connection with the grid. If not installed on the EES system, information should be provided in the installation instructions to indicate:

- the type and rating of the disconnection means,
- that the disconnecting means should be located where it is accessible and in sight of the EES system, and
- that the disconnecting means should be provided with markings/signage to identify
  - the EES system ratings, and
  - the available short circuit current.

7.5.3 Stopped state

When the EES system is disconnected and the accumulation subsystem is not connected to the power conversion system, the EES system is considered to be in a stopped state. In this state the accumulation system may be energized and cannot generally be de-energized without serious damage. In the stopped state, part of the auxiliary subsystem remains powered as it contains critical subsystems for safety and monitoring.

7.5.4 EES system shutdown

EES system shutdown is the command to move the EES system to the stopped state.

As determined by the risk analysis of the system, an EES system should be provided with a means for both normal and emergency shutdown.

Conditions that can be safely controlled or that do not pose immediate hazard may be corrected with a normal shutdown of the EES system.

When voltage, current, temperature, pressure, or rotational speed, etc., exceed a safety limit, a hazardous event could be caused. It could be the result of the malfunction of a system component or communication error, etc. Abnormal operating conditions that may be liable to give rise to a hazardous event should be identified and processed to initiate an emergency shutdown. When actuated, the EES system is expected to return to a safe condition. The EES system shutdown function, including the emergency stop, should be provided with means to enable the coordinated shutdown of all necessary parts of the system as well as with equipment upstream and/or downstream of the system, if continued operation could be hazardous.

An EES system is disconnected by appropriate switching device(s) or other alternative measures.

7.5.5 Cyber security

Cyber security is important not only for remote monitoring but also for the system connected to the internet. Refer to international standards for additional guidance.

7.5.6 Partial disconnection

Where appropriate, the design of the EES system may permit disconnection of the constituent parts of the EES system separately. For those working on the EES system it may be possible to disconnect only the parts to be worked on to permit safe access. However, careful consideration should be given to risks posed by individual systems adjacent to those being worked on. In the case of appropriately designed multiple accumulation subsystems, individual subsystems can be disconnected for safe working while the EES system can remain operational.

Also in the case of a flywheel accumulator, it is allowed to stop it by providing energy to the grid or to other units in the system. This procedure will contribute to minimizing the time that the system is in a hazardous situation.

For certain EES systems where it is difficult to de-energize the accumulation subsystem (e.g. battery energy storage systems), care should be taken in the system design to minimize hazards.

7.5.7 Equipment guidelines for emergency shutdown

a) Emergency shutdown should be incorporated into an EES storage system to avoid hazardous situations that cannot be corrected by other controls, as determined by a risk analysis of the system. This function should:
   - stop the hazardous condition without creating additional hazards,
   - trigger or permit the triggering of certain safeguard actions where necessary,
   - override all other functions and operations in all modes,
   - prevent reset from initiating a restart,
   - be fitted with restart lock-outs in such a way that a new start command may take effect,
   - be on normal operation only after the restart lock-outs have been intentionally reset.

b) Manual emergency stops

   Manual emergency stops, if required by the risk analysis, should be identifiable, clearly visible and accessible in accordance with ISO 13850.

c) Control functions in the event of control system failure

In case of fault in the control system logic or failure of, or damage to, the control system hardware:

– once the emergency stop command has been given, the EES system should not allow its shutdown sequence to be interrupted,

– the protection devices should remain fully effective,

– the EES system should not re-connect/restart unexpectedly.

When a protective device or interlock causes an EES system safety shutdown, that condition should be signaled to the logic of the control system. The reset of the shutdown function should not initiate any hazardous condition. Control/monitoring systems that can operate safely in the hazardous situation may be left energized to provide system information.

7.6 Preventive maintenance

Preventive maintenance schemes to prevent unanticipated conditions are also important. In order to efficiently perform preventive maintenance, it is crucial to monitor the system regularly and it is in most cases done remotely.

Monitoring of the frequency of warnings of EES system parameters such as system efficiency or temperature could be an early indicator of malfunction of a subsystem and/or components.

Remote monitoring system implementation should be considered in order to check if the system is operating safely. The data provided automatically by the EES system or through an EES system inquiry can help to evaluate its state of health and the remaining life of its components. Diagnosis is performed by monitoring change of capacity or changes in the evolution of measured parameters. This data can be transmitted through an information network in a timely manner.

In the case of remote monitoring, reliability of the monitored value is essential to keep the EES system safe. Detection of the measuring system malfunction and measured value error should be considered.

For unattended operation, the EESS should be capable of monitoring and detecting abnormal conditions and automatically entering a safe state without the need for operator interaction.

7.7 Staff training

Well-trained workers greatly increase safety at work. Any deviation from the desired process can be detected, and hence corrected, more quickly.

Workers shall be provided with training which informs them of the hazards at the workplace and the protective measures to be taken. This training shall explain how the different types of hazards arise and in what parts of the workplace they are present. The measures taken should be listed and their operation explained. The correct way of working with the available equipment shall be explained. Workers shall be instructed in safe work practices in or near hazardous places. This also involves explaining the meaning of any cautionary markings or markings of hazardous places, and specifying what mobile work equipment may be used there. Workers shall also be instructed in what PPE they shall wear to work in and around the EES system. The available operating instructions should be covered during the training.

Workers shall receive training:

- before initially starting work on the EES system;
- when work equipment is introduced for the first time or changed;
- when new technology is introduced.

Training of workers shall be repeated at suitable intervals. The workers' level of understanding shall be checked.

The duty to provide training also applies to the employees of outside contractors. Training shall be given by a competent person. Records should be kept in writing of the date and content of training activities and the participants.

7.8 Safety design

7.8.1 General

EES systems are expected to operate for a given life expectancy provided that they are properly maintained. During this life expectancy, the operation of the EES system is likely to be affected by a variety of factors, such as but not limited to:

- component technology changes
- local environmental factors
- market conditions
- new regulations

The effect of these factors on the EES system should not compromise its safe operation. For this to be achieved, a safety related design review may need to be carried out when changes occur. It may also be necessary to review the design of the EES system if other information becomes available, such as:

– operational experience
– component failure
– software failure
– inherent design issues

Figure 7 shows this process over the lifetime of the EES system.

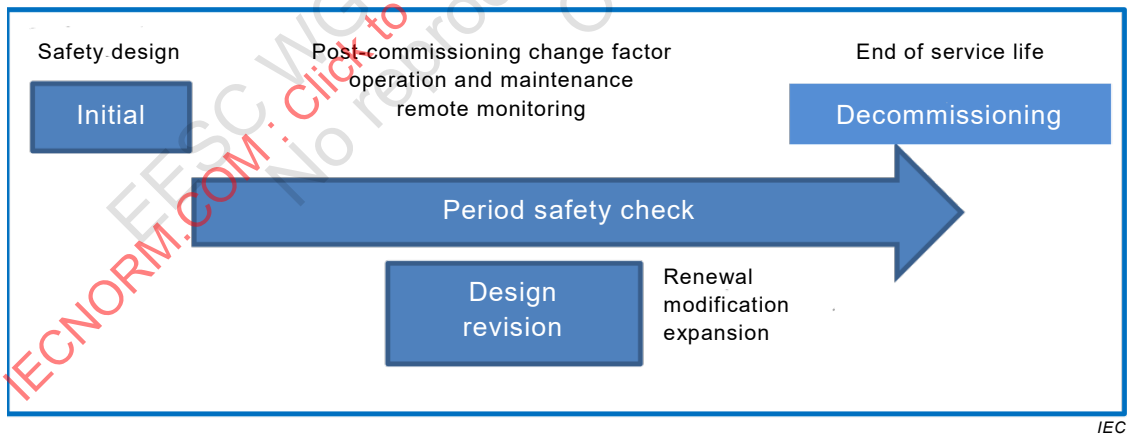


Figure 7 – Initial safety design and design revision

7.8.2 Initial safety design and subsequent design revision

Safety design is first done at the beginning of the whole system design. If the system undergoes a variety of changes, then, when necessary, a safety design should be conducted again. During the safety redesign, risk analysis and FMEA should be conducted again.

7.8.3 Design revision for minor and major system changes

When the system undergoes minor changes, risk analysis possibly integrating a limited FMEA is more practical. When major change takes place such as total storage capacity expansion and big changes in the surrounding environment, when conducting the FMEA, not only the whole system, but also the boundary region between the system and the surrounding environment should be taken into account.

8 System testing

8.1 General

In order to confirm the EES system design and the proper implementation and functionality of the safety mechanisms identified in the FMEA, the system response to potential malfunction conditions should be evaluated. Verification and validation of items should be determined based on the system level FMEA. In addition, the EES system should have a safety related system (SRS), for example IEC 61508-1.

An example of an EES system with a control subsystem is shown in Figure 8.

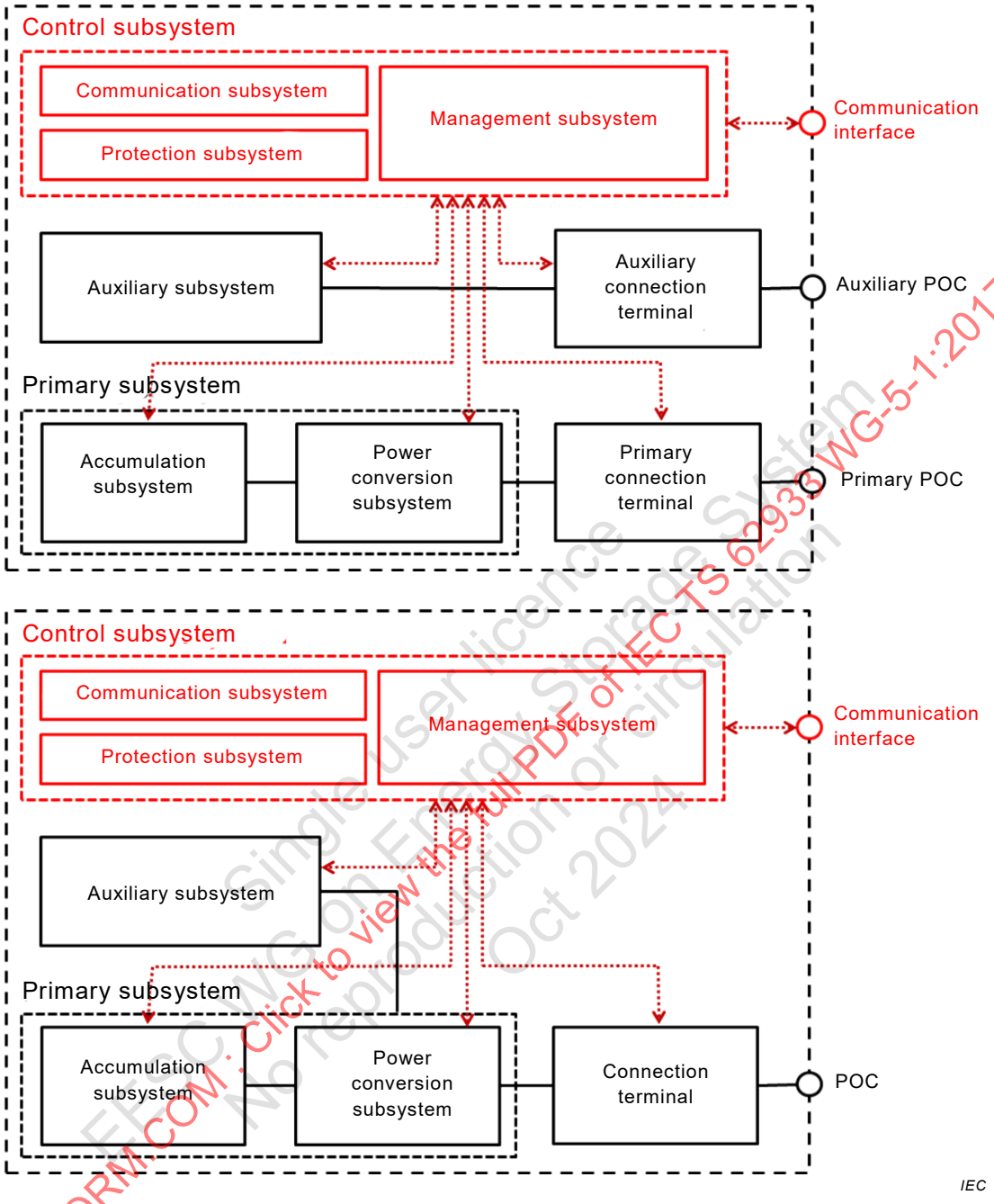


Figure 8 – EES system architecture in the two main EESS configurations

The EES system includes primary, auxiliary and control subsystems as shown in Figure 8. Each subsystem contains various components. Also, internal communication lines between those components, monitoring lines and control signal lines exist in the EES system.

Those EES system components may be designed, verified and validated based on other IEC standards. For example, a lithium ion battery energy storage system may satisfy IEC 62619, but it is considered that risks could be induced due to the system integration.

For example, electromagnetic noise induced by the power conversion system could cause the malfunction of the energy storage management central processing unit (CPU) and affect the energy storage device operation. The noise tolerance of the EES system components may satisfy IEC 61000 (all parts), but there is some possibility that one of the system components may fail because of the noise induced by the power conversion subsystem. Additionally, the accidental malfunction of the components can also occur. It should be verified that the system

components and communication malfunction do not affect the safety of people at the system level.

Test equipment, facilities or the on-site test environment should be appropriate for test purposes, possible test results, sample size and performance.

Appropriate personal protection equipment (PPE), standard operating procedures and facilities to protect personnel during testing should be provided.

Standard procedures for the safe storage, handling, operating, testing and disposal of test samples should be provided.

Samples used for testing should be representative of production samples. Testing may be conducted on subassemblies if demonstrated to be representative of the complete EES system to satisfy particular test purposes.

8.2 Auxiliary system malfunction

When the control power is lost, the protection mechanisms of the system may not work properly. Control power low or high voltage excursions above specified levels may affect the devices and components that ensure the system safety. The following items should be considered in the system level FMEA and testing. The FMEA auxiliary system fault conditions concerning safety, such as the items noted below, should be tested:

1) complete loss of control power
2) partial loss of control power
3) temporary loss of control power
4) control power voltage exceed a tolerable voltage level
5) control power voltage drops below a tolerable voltage level
6) cooling system malfunction
7) other auxiliary subsystem malfunction
8) temporary loss of control input

For all conditions tested, the system safety functionality should not be compromised and should react in accordance with the FMEA anticipated outcome.

8.3 EES control subsystem malfunction

When an EES control subsystem provides incorrect control information to the power conversion subsystem processing unit, the EES system could be damaged and put in an unsafe state. The FMEA system management fault conditions concerning safety, such as an EES system management control failure, should be tested.

For the conditions tested, the system safety functionality should not be compromised and the safety functions should operate in accordance with the FMEA anticipated outcome.

8.4 EES system internal communication malfunction

When the external communication line is short or open circuited, or when the external control signal is disturbed, the EES system might not work properly. The external communication fault conditions concerning safety that are identified by FMEA such as those items noted below should be tested:

1) internal communication line is opened
2) internal communication line is short circuited
3) internal communication line is disturbed