TECHNICAL REPORT

ISO/TR 9968

First edition
2023-06

Road vehicles — Functional safety — Application to generic rechargeable energy storage systems for new energy vehicle

Véhicules routiers — Sécurité fonctionnelle — Application des systèmes génériques rechargeables de stockage d'énergie aux véhicules utilisant les énergies nouvelles

Reference number
ISO/TR 9968:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The rechargeable energy storage systems (RESS) (e.g. lithium-ion battery systems) used for new energy vehicles can introduce specific hazards like thermal runaway, toxic chemical release, high voltage electric shock, etc.

To prevent and mitigate the risk of RESS related hazards, E/E related technology, such as battery management systems (BMS), are integrated into the RESS. However, based on accident investigations and statistics, a large proportion of RESS safety-related incidents are caused by faults within the E/E systems (e.g. BMS), elements of other technologies (e.g. battery cells) or both[15]. Due to the possibility of the mechanical and electrochemical characteristics of the battery changing constantly over the lifecycle [e.g. state of health (SOH), state of health energy (SOHE), direct current resistance (DCR) for electrochemistry, and mechanical stress, air-dust tightness, resistance to chemicals for mechanical parts] the correlated safety threshold parameters of the battery can also change accordingly which can lead to reduced or even incorrect monitoring and control of the BMS.

Effective safety design and management of RESS relies on system capability to adaptively adjust the logic and control according to the alteration of mechanical and electrochemical related characteristics of the battery. The ISO 26262 series is focused on the malfunctioning behaviour of E/E systems. An item (as well as external measures) can include systems or elements of other technologies. Malfunctioning behaviour can be caused by failures of systems or elements of other technologies. However, the ISO 26262 series includes limited guidance concerning such failures, for example, sudden failures or wear out of other technologies.

The purpose of this document is to present a case study of functional safety for RESS considering E/E systems (e.g. BMS) and mechanical, electrical and electrochemical factors for elements of other technologies (e.g. battery cells) according to the methodology of the ISO 26262 series, and to show examples of functional safety development for E/E systems (e.g. BMS) and systems of other technologies as a reference.

Based on the ISO 26262:2018 series, the case study in this document provides an additional methodology to cover the strong interaction between E/E systems (e.g. BMS) and systems of other technologies (e.g. battery cells) by considering E/E, mechanical and electrochemical related factors. This document follows the V model framework defined in the ISO 26262 series and provides corresponding functional safety strategies, and verification and validation methods for the development of a functionally safe RESS.

All the technical information and the associated data in this document are combined with the state-of-the-art technologies of current automotive battery industry, which will be updated with the development of battery cell technology and other related technology.

Road vehicles — Functional safety — Application to generic rechargeable energy storage systems for new energy vehicle

1 Scope

This document is intended to be applied to the usage of ISO 26262 methodology for rechargeable energy storage systems (RESS), for example, lithium-ion battery systems, that are installed in series-production road vehicles, excluding mopeds.

This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

This document provides:

a) a generic informative framework regarding the interaction of E/E systems with elements of other technologies with respect to the ISO 26262 series aspects of item definition, hazard analysis and risk assessment (HARA), functional safety concept (FSC), verification and validation (V&V), and production, operation, service and decommissioning (POSD);

b) various examples elaborating the generic framework;

c) topics which could be considered in future editions of the ISO 26262 series.

RESS includes BMS, cells, harnesses, connectivity, etc. In order to achieve product safety non-E/E functional safety requirements need to be fulfilled by the other technology itself without the support of E/E technology. These requirements are not in scope of this document.

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.

ISO 26262-1, *Road vehicles — Functional safety — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 26262-1 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
RESS
rechargeable energy storage system
system that stores energy for delivery of electrical energy and which is rechargeable

EXAMPLE RESS including batteries, capacitors, *battery management system (BMS)* (3.2), etc.

3.2
BMS
battery management system
E/E system with the intended functionality being to measure battery status, exchanges information (e.g. voltage, current, temperature, fault information, etc.) with external E/E components, and support/ control managing battery electrical energy storage and delivery

Note 1 to entry: Managing the battery includes monitoring of safety-related properties and conditions and to appropriately react to these if necessary.

Note 2 to entry: It monitors and/or manages its state, calculates secondary data, reports that data and/or controls its environment to influence the battery's safety, performance and/or service life.

Note 3 to entry: The BMS is sometimes also referred to as a BMU (battery management unit).

3.3
hazardous condition
condition causing the occurrence of a hazard

EXAMPLE 1 Over temperature can lead to a thermal event of a lithium-ion battery cell. In this case the over temperature is considered to be a hazardous condition.

EXAMPLE 2 For some lithium-ion battery technologies, repeated charging at sub-zero temperatures can cause lithium plating, dendrite growth and ultimately a cell short circuit leading to a thermal event. In this case charging at sub-zero temperatures is considered to be a hazardous condition.

3.4
protection function
intended E/E functionality to control a malfunctioning behaviour of another item, a failure of an element external to the item, to prevent the occurrence of a *non-E/E-functional hazard* (3.6), to control non-E/E-functional hazard or to prevent the occurrence of harm due to non-E/E-functional hazards

3.5
hazard
potential source of harm

[SOURCE: ISO 26262-1:2018, 3.75, modified — The phrase "caused by malfunctioning behaviour of the item" as well as the Note 1 to entry were deleted.]

3.6
non-E/E-functional hazard
hazard not in scope of the ISO 26262 series

EXAMPLE Hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of safety-related E/E systems.

3.7
E/E-functional hazard
hazard caused by the malfunctioning behaviour of the item

Note 1 to entry: This hazard is within scope of the ISO 26262 series.

3.8
risk mitigation effectiveness
risk reduction due to the safety measure for the safety concern under consideration

Note 1 to entry: The safety measure effectiveness can be assessed in a quantitative way as well as in a qualitative way.

Note 2 to entry: Safety concerns include, but are not limited to, hazards and failure modes.

EXAMPLE 1 Due to mechanical overdesign the expected failure rate is reduced by a factor of 1 000.

EXAMPLE 2 The failure mode coverage of a safety mechanism.

EXAMPLE 3 The *diagnostic coverage* (3.9) of a safety mechanism.

EXAMPLE 4 Expert judgement rating the risk mitigation effectiveness as low, medium or high.

3.9
diagnostic coverage
percentage of the failure rate of a hardware or *other technology* (3.10) element, or percentage of the failure rate of a failure mode of a hardware or other technology element that is detected or controlled by the implemented safety mechanism or *protection function* (3.4)

[SOURCE: ISO 26262-1:2018, 3.33, modified — The phrases "or other technology" and "or protection function" were added and Notes 1 to 3 to entry were deleted.]

3.10
OT
other technology
technology different from E/E technologies that are within the scope of the ISO 26262 series

EXAMPLE Mechanical technology; hydraulic technology; chemical technology.

[SOURCE: ISO 26262-1:2018, 3.105 modified —Note 1 to entry was deleted and "chemical technology" was added to the example.]

3.11
OT safety
other technology safety
absence of unreasonable risk due to *non-E/E-functional hazards* (3.6) caused by fault, failures or properties of the *other technology* (3.10)

4 Abbreviated terms

BMS Battery management system

BOL Beginning of life

CB Circuit breaker

DCR Direct current resistance

EOL End of life

FSC Functional safety concept

HARA Hazard analysis and risk assessment

HVIL High voltage interlock loop

MOL Middle of life

OT Other technology

OVP Overvoltage protection

RESS Rechargeable energy storage system

SOC State of charge

SOH State of health

SOHE State of health energy

UVP Undervoltage protection

V&V Verification and validation

5 Item definition

5.1 Objectives

The objectives of this clause are:

a) to provide a generic framework for the item definition regarding the interaction of E/E systems with elements of OT;

b) to provide examples of "item definitions" illustrating the proposed "generic framework", especially the interactions of E/E systems with elements of OT.

5.2 General

The ISO 26262 series allows significant degrees of freedom regarding the definition of item and its boundary. Hence for a given system there are multiple ways to define the item compliant with the ISO 26262 series. In the context of RESS two kinds of item definition approaches can be distinguished:

a) the OT is part of the item;

b) the OT is external to the item.

The different two approaches are elaborated with the help of a simplified RESS example as shown in 5.3 and 5.4. Regardless of which approach is used, the common point is:

1) to define the item itself and interior of the item:
   - defining the functionality of the item, and the assumptions of the item;
   - defining the functionality of internal elements;
   - defining interfaces and interactions between the internal elements.
2) to define relationship between the item and other objects:
   - defining expected behaviour of other objects (environment, other items, external elements, etc.);
   - defining the functionality of the item under consideration required by other objects and constraints resulting from other objects;
   - defining the functionality and constraints of other objects required by the item under consideration;
   - defining external interface.

These points are shown in Figure 1.

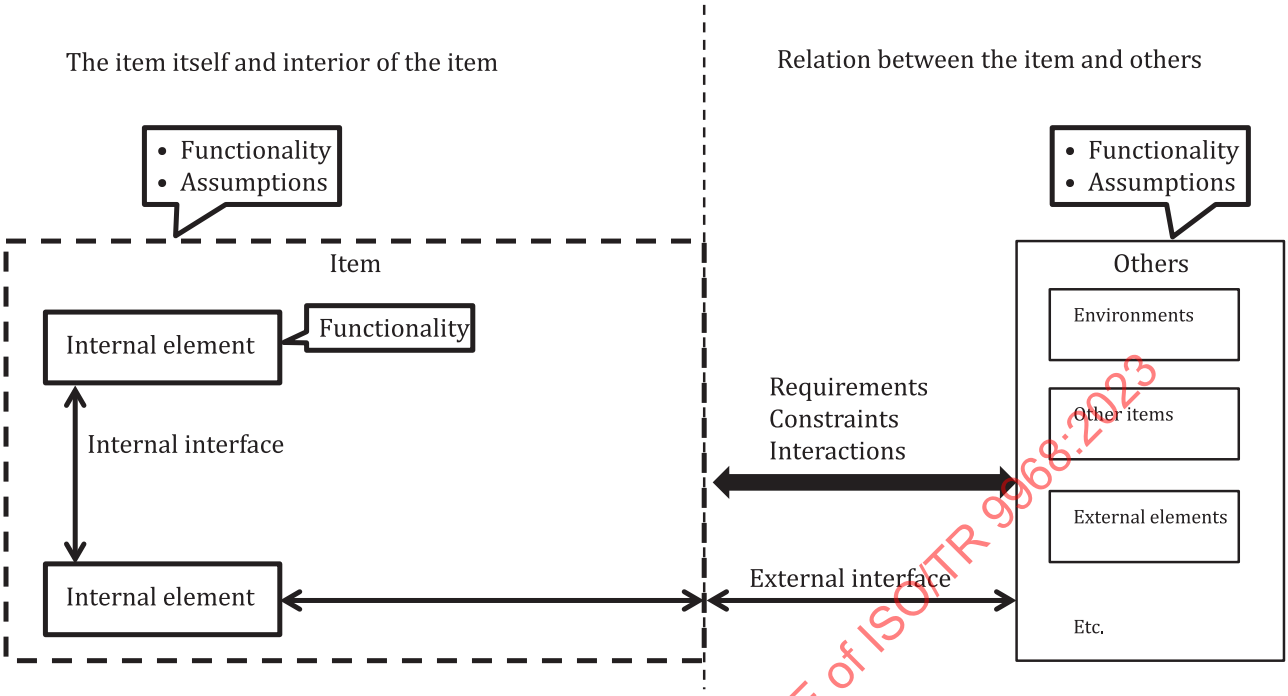


Figure 1 — Visualization of the task of the item definition

5.3 OT is part of the item

5.3.1 General

In this case the item corresponds with RESS in Figure 2.

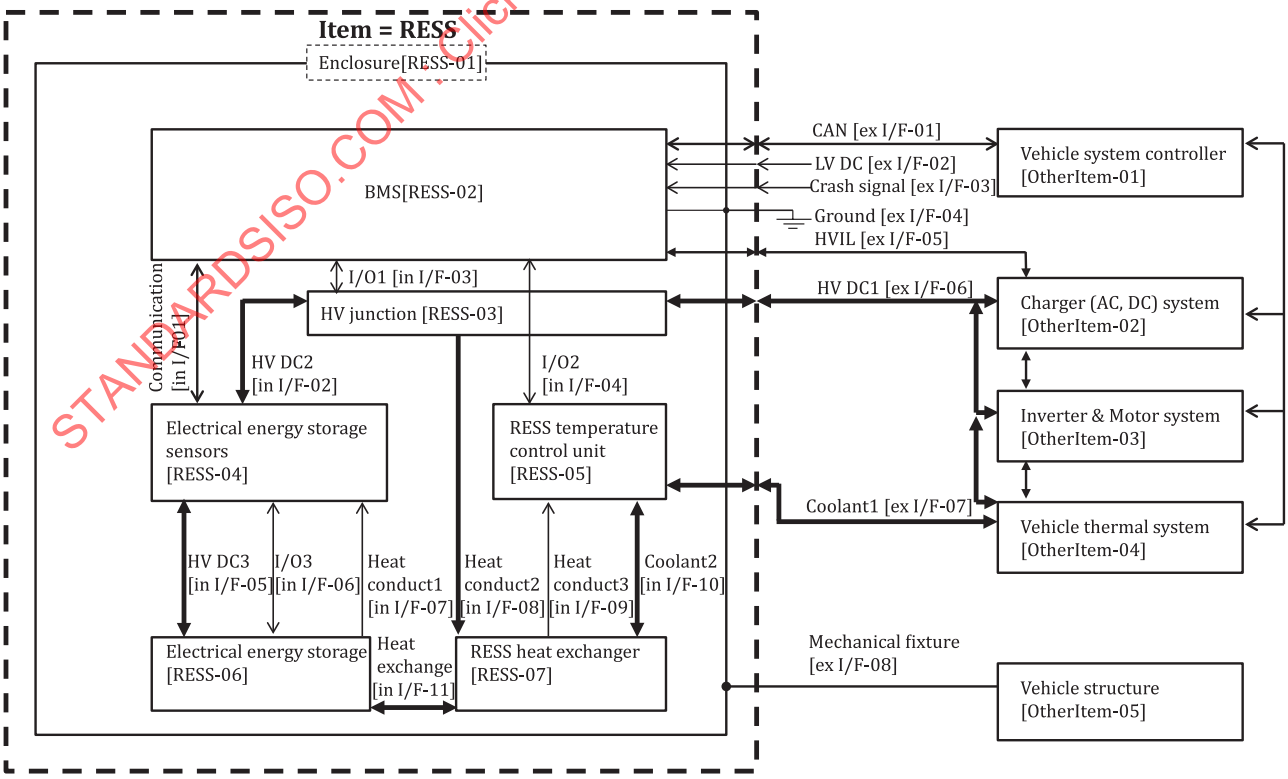


Figure 2 — OT is part of the item – Example

5.3.2 Assumptions

The assumptions for the item are:

a) electrical energy storage [RESS-06] consists of several lithium-ion cells;

b) each cell has specifications for use (e.g. cell voltage, temperature, must be within operating limits);

NOTE Usually, these specifications are provided from the lithium-ion cell manufacturer.

c) the total voltage of the RESS-06 is greater or equal to 240 V.

5.3.3 Functionality

The functionality of the item is:

a) to cooperate with other HV DC systems to provide the required RESS energy level, input / output current and temperature within operating limits;

b) to connect/disconnect RESS and other HV DC systems;

c) to store electrical energy within itself, providing electrical energy for other HV systems, and receiving electrical energy from other HV DC systems.

5.3.4 Internal elements and their functionality

Internal elements and their functionality are as follows, including their classification as E/E or OT:

a) enclosure [RESS-01]: OT

- to provide structural protection for the RESS and separation from the external environment that could affect the internal RESS;
- to ensure pressure balancing and limit the pressure with the venting device;

b) BMS [RESS-02]: E/E

- to estimate state of charge (SOC);
- to estimate state of health (SOH);
- to send information to other systems, e.g.
  - SOC, SOH, charging/discharging current limit, cooling/warming request;
- to receive information from other systems, e.g.
  - HV junction connecting/disconnecting request;
- to monitor current, voltage and temperature;
- to perform emergency electrical disconnection during crash;
- to monitor ground isolation;
- to perform cell balancing;
- etc.

c) HV junction [RESS-03]: E/E

- to connect/disconnect RESS and other HV DC systems;
- to provide an electrical controlled fuse to protect from overcurrent;

d) electrical energy storage sensors [RESS-04]: E/E

- to measure all cell voltages;
- to measure electrical storage temperature;
- to measure current into and out of electrical storage;

e) RESS temperature control unit [RESS-05]: E/E

- to measure RESS heat exchanger temperature;
- to open/close coolant path;

f) electrical energy storage [RESS-06]: E/E and OT

- to store electrical energy;

g) RESS heat exchanger [RESS-07]: OT

- to cool HV junction, and exchange heat (cooling or warming) between electrical storage and itself.

5.3.5 Internal interfaces

The internal interfaces are as follows, including their classification as E/E or OT:

a) communication [in I/F-01]: E/E

- communication of measured values (all cell voltages, electrical storage temperature, current) from electrical energy storage sensors to BMS;
- communication of cell balancing instructions from BMS to electrical energy storage sensors;

b) HV DC2 [in I/F-02]: E/E

- transferring electrical power between HV junction and electrical energy storage sensors;

c) I/O1 [in I/F-03]: E/E

- transferring drive signals from BMS to HV junction. This signal is able to connect/disconnect RESS and other HV DC systems;

d) I/O2 [in I/F-04]: E/E

- transferring measured temperature value of heat exchanger from RESS temperature control unit to BMS;
- transferring drive signals from BMS to RESS temperature control unit. This signal is able to open/close coolant path;

e) HV DC3 [in I/F-05]: E/E

- transferring electrical power between electrical energy storage sensors and electrical storage;

f) I/O3 [in I/F-06]: E/E

- connecting electrical energy storage and electrical energy storage sensors for monitoring cell voltage;
- transferring charge to balance cell voltage;

g) heat conduct1 [in I/F-07]: OT

— conducting electrical storage heat to electrical energy storage sensors;

h) heat conduct2 [in I/F-08]: OT

— conducting HV junction heat to RESS heat exchanger;

i) heat conduct3 [in I/F-09]: OT

— conducting RESS heat exchanger heat to RESS temperature control unit;

j) Coolant2 [in I/F-10]: OT

— transferring heat between RESS temperature control unit and RESS heat exchanger;

k) heat exchange [in I/F-11]: OT

— exchanging heat between electrical storage and RESS heat exchanger.

5.3.6 Other objects

Other objects are as follows, including their classification as E/E or OT.

a) vehicle system controller [OtherItem-01]: E/E

— controlling the drive of a vehicle;

b) charger (AC, DC) system [OtherItem-02]: E/E and OT

— controlling charging power or charging constant current or charging constant voltage into RESS;

c) inverter and motor system [OtherItem-03]: E/E and OT

— controlling power to traction motors and power from regenerative braking;

d) vehicle thermal system [OtherItem-04]: E/E and OT

— controlling RESS to the proper temperature;

e) vehicle structure [OtherItem-05]: OT

5.3.7 External interfaces

External interfaces are as follows, including their classification as E/E or OT:

a) CAN [ex I/F-01]: E/E

— exchanging information between RESS to other systems;

b) LV DC [ex I/F-02]: E/E

— supplying power to RESS E/E systems;

c) crash signal [ex I/F-03]: E/E

— sending signal to RESS that a vehicle crash has occurred;

d) ground [ex I/F-04]: E/E

— supplying power ground to RESS;

e) HVIL [ex I/F-05]: E/E

— high voltage interlock loop – monitors high-voltage isolation with a low voltage circuit;

f) HV DC1 [ex I/F-06]: E/E

— transferring electrical power between RESS and other HV systems;

g) Coolant1 [ex I/F-07]: OT

— transferring heat between RESS and vehicle thermal system;

h) mechanical fixture [ex I/F-08]: OT

— fixing RESS to vehicle structure.

Additional functionalities and constraints are omitted for the sake of simplicity.

5.4 OT is not part of the item

In this case the item corresponds with the BMS (battery management system) of Figure 3. The relationship between the item and the OT, which belongs now to the other objects, is described as functionalities and constraints. These include the identified hazards of the OT, the hazardous conditions of the OT or both.

NOTE The identified hazards and the hazardous conditions are a result of the safety analysis of the OT.

EXAMPLE If one of the OT is a lithium-ion cell a possible hazard is thermal runaway. A hazardous condition for this cell is too high temperature. One possible functionality required by the OT from the item is a temperature supervision of the lithium-ion cells and to disconnect the cells in case the lithium-ion temperature rises above a certain threshold value. This would be part of the item definition as required in ISO 26262-3:2018, 5.4.2.

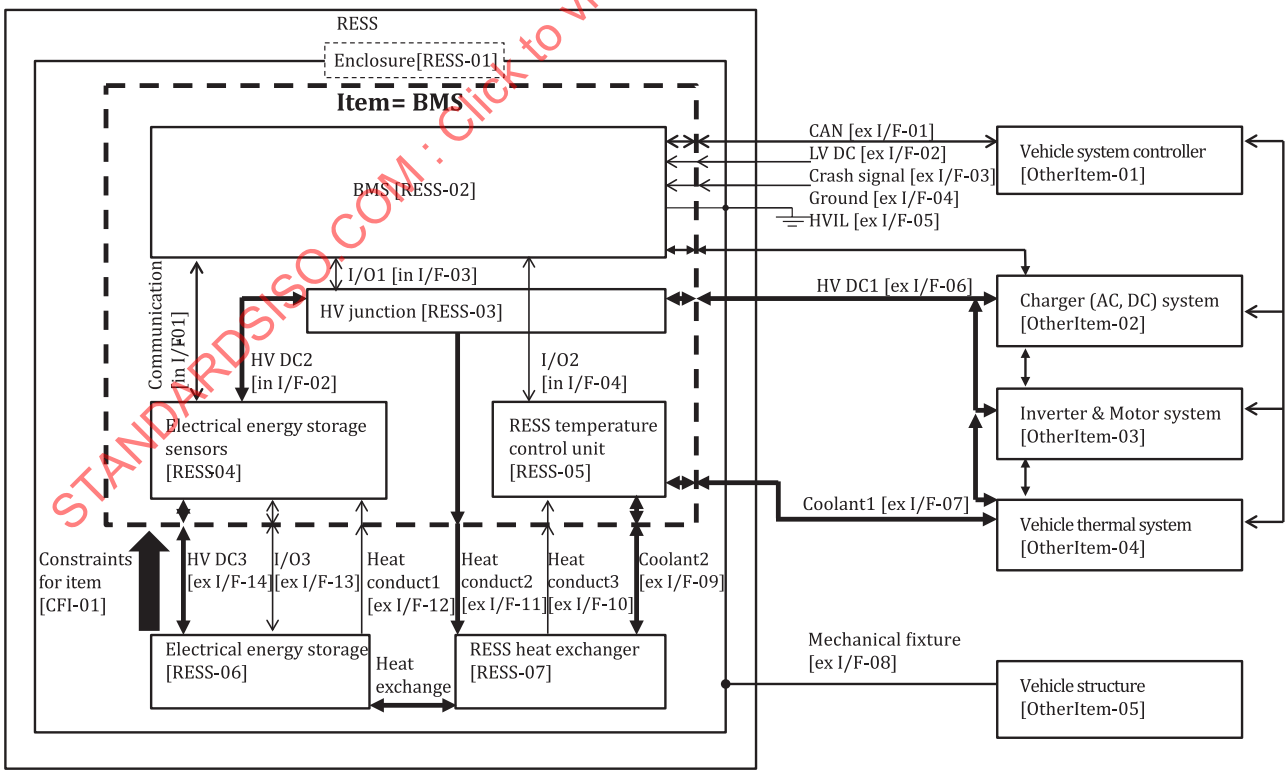


Figure 3 — Example of the OT is not part of the item

The functionality of BMS is:

a) to cooperate with other HV DC systems to keep electrical storage's amount of electrical energy, input / output current and temperature within operating limits;

b) to cooperate with the vehicle thermal system to keep internal BMS temperature within operating limits;

c) to connect/disconnect electrical storage and other HV DC systems.

The item definition determines which interface and which elements are considered to be internal elements and interfaces or external interfaces and other objects, for example, additional other objects for the BMS item can be:

— electrical energy storage [RESS-06]: OT;

— RESS heat exchanger [RESS-07]: OT.

For a case when OT is not part of the system there can be additional constraints for the BMS item originating from the OT object. For example, from the OT object electrical energy storage [RESS-06].

— Constraints for BMS item [CFI-01]:

  — cell voltage, temperature, SOC must be within operating limits;

  — current limit, that depends on cell temperature, must be within operating limits.

5.5 Safe intended functionality of the item

Even though the ISO 26262 series does not address the nominal performance of E/E systems, the implicit assumption is, that the intended functionality itself is free from unreasonable risk, i.e. safe. In the context of RESS one aspect to evaluate if the intended functionality can be regarded as safe, is to evaluate if the intended functionality can cause hazardous conditions of the OT or hazards of the OT. If this is the case, the resulting risk is evaluated and, if deemed necessary, the intended functionality is modified accordingly.

NOTE 1 It is possible that at the point of the initial item definition the OT is not yet defined or the OT related hazards and hazardous conditions are not yet known. In this case, the evaluation of the possibility of the intended behaviour causing hazards or hazardous conditions of the OT is executed when the OT is defined and its hazards and hazardous conditions have been identified. If a change of the E/E functionality is deemed necessary, the change is executed in compliance with ISO 26262-8:2018, Clause 8 and can result in a reiteration of the HARA.

EXAMPLE For some lithium-ion battery technologies, repeated charging at sub-zero temperatures can cause lithium plating, dendrite growth and ultimately a cell short circuit leading to a thermal event. To prevent this from happening the intended functionality can limit the charging current depending on the temperature.

In this document it is assumed that the intended behaviour is safe. Hence only a malfunctioning behaviour of the item can lead to hazards, not the intended behaviour of the item itself.

NOTE 2 The malfunctioning behaviour of the item causing hazards related to the OT is represented in case 1 in 6.2.

6 HARA and safety concepts

6.1 Objectives

The objectives of this clause are:

a) to identify the hazards related with the interaction of E/E systems and OT elements;

b) to illustrate a possible safety concept and safety requirements allocation specific to the interactions of E/E and OT.

6.2 General

The following subclauses assume that the item contains the OT elements, i.e. that the item corresponds with the RESS.

NOTE 1 See Annex A for an example of a HARA and the functional safety concept.

If not already given as part of the item definition, a safety analysis of the OT identifies OT-related hazards and their hazardous conditions. The hazards and the corresponding hazardous conditions of the OT can depend on the technology used, e.g. some cells can be more robust against overheating than others and it is possible that OT safety measures are present already minimizing certain risks to a reasonable level (e.g. dendrite proof separators preventing cell short circuits). The newly identified hazards and hazardous conditions are evaluated, e.g. in accordance with ISO 26262-4:2018, 6.4.4.7 or ISO 26262-5:2018, 7.4.3.6, typically requiring a reiteration of the HARA in accordance with ISO 26262-3:2018.

NOTE 2 The hazardous condition of OT elements can change during the life cycle.

EXAMPLE 1 During the life cycle (e.g. BOL, MOL and EOL) of the battery, the chemical characteristics of the battery changes (e.g. direct current resistance (DCR) increase, capacity decrease), thus hazardous conditions of the battery change accordingly. For instance, the maximum safe current that the battery can withstand will theoretically decrease along with SOH decrease.

The HARA of the OT-related hazards can be supported by corresponding tests in order to determine the S, E and C parameters.

EXAMPLE 2 Abuse testing according to EUCAR/SANDIA/UN-Test.

Regarding the interaction of functional safety and OT safety following cases can be distinguished.

— **Case 1**: the malfunctioning behaviour of the E/E systems can cause hazards related to the OT (see 6.3).

  EXAMPLE 3 The malfunctioning behaviour “repeated charging at sub-zero temperatures” can cause lithium plating, dendrite growth and ultimately a cell short circuit leading to a thermal event.

  NOTE 3 The behaviour of the E/E system causing the OT related hazard can be part of the malfunctioning behaviour of the item.

— **Case 2**: failure of OT causes E/E failures (see 6.4).

  EXAMPLE 4 Incapability of the battery cells to provide power, leading to the loss of the E/E functionality.

— **Case 3**: non-E/E-functional hazards and related hazardous conditions are addressed by E/E protection functions (see 6.5).

  EXAMPLE 5 An E/E function monitoring the coolant fluid level.

— **Case 4**: safety measures of OT address functional safety requirements and safety goals (see 6.6).

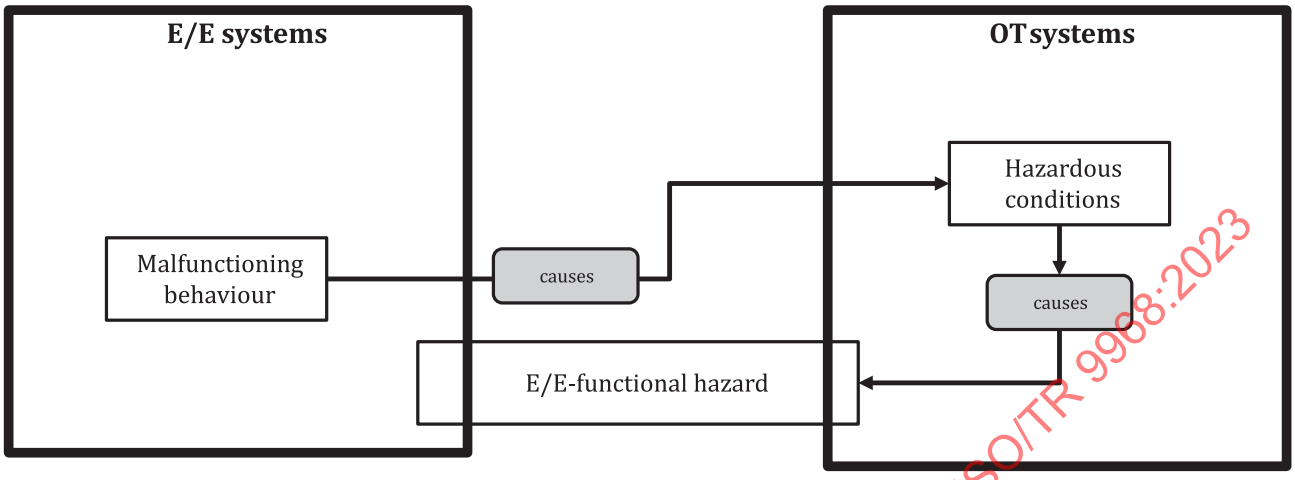
  EXAMPLE 6 The safety goal "Prevent explosion of the battery cells due to overheating by the E/E function" is allocated to the OT and realized by adding a pressure release vent, which releases the pressure before it can lead to an explosion of the cells.

— **Case 5**: a combination of OT and E/E safety measures implementing a given safety requirement (see 6.7). Case 3 and case 4 are special cases of case 5.

  EXAMPLE 7 Protection from high voltage shock by colour coded isolation, IPXXB/D connectors and E/E safety mechanism to monitor isolation integrity.

6.3 Case 1: Malfunctioning behaviour of the E/E systems can cause hazards related to the OT

This case is visualized in Figure 4.



NOTE The E/E-functional hazard is in this case an OT-related hazard.

Figure 4 — Visualization of an E/E behaviour causing an OT-related hazard

In this case the HARA is executed in compliance with ISO 26262-3:2018, Clause 6. As a result, safety goals are specified that will be implemented in compliance with the ISO 26262 series.

EXAMPLE The E/E malfunctioning behaviour "create overvoltage" can cause a lithium-ion cell to go into thermal runaway, leading to the hazard "fire". The S, E and C parameters of the hazard "fire" are evaluated for the different operational situations according to ISO 26262-3:2018, Clause 6. As a result, the ASIL of the hazard "fire" is determined and a corresponding safety goal is specified, e.g. "prevent applying voltage > X V for longer than y ms to the battery (ASIL Z)". This safety goal is then implemented in compliance with the complete ISO 26262 series.

6.4 Case 2: Failure of OT causes E/E failures

This case is visualized in Figure 5.

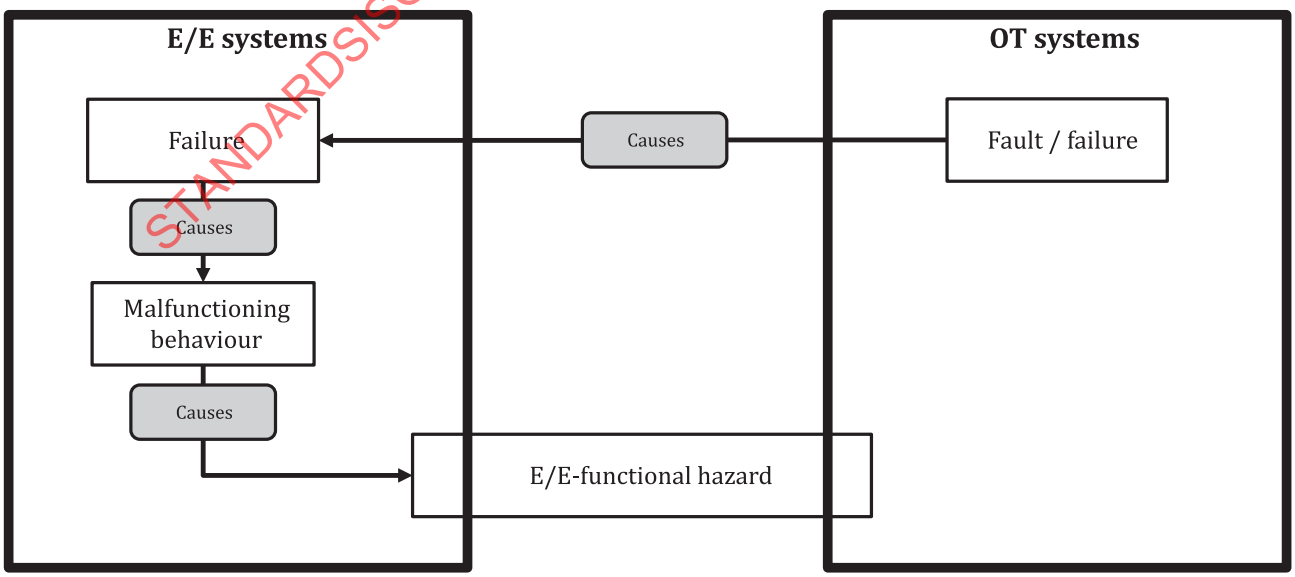


Figure 5 — Visualization of an OT fault or failure leading to an E/E failure

In this case the faults of the OT are evaluated within the safety analyses in compliance with ISO 26262-5. If necessary, corresponding safety measures are defined. The OT failure occurrence is determined and used for the calculation of the random hardware metrics in compliance with ISO 26262-5, Clause 8 and 9, if necessary.

EXAMPLE A steer-by-wire system has as a safety goal the safety-related availability requirement "prevent significant loss of steering capability for longer than x ms (ASIL Y)". The failure mode of the power supply system "loss of power" can lead to the violation of this safety goal. The fault of the lithium-ion cell "short to ground" can lead to this failure mode. A possible safety mechanism would be a redundant power supply (e.g. a redundant battery) in combination with a system with the capability to disconnect the faulty battery in order to prevent a cascading failure.

6.5 Case 3: Non-E/E-functional hazards and related hazardous conditions are addressed by E/E protection functions

This case is visualized in Figure 6 and Figure 7.

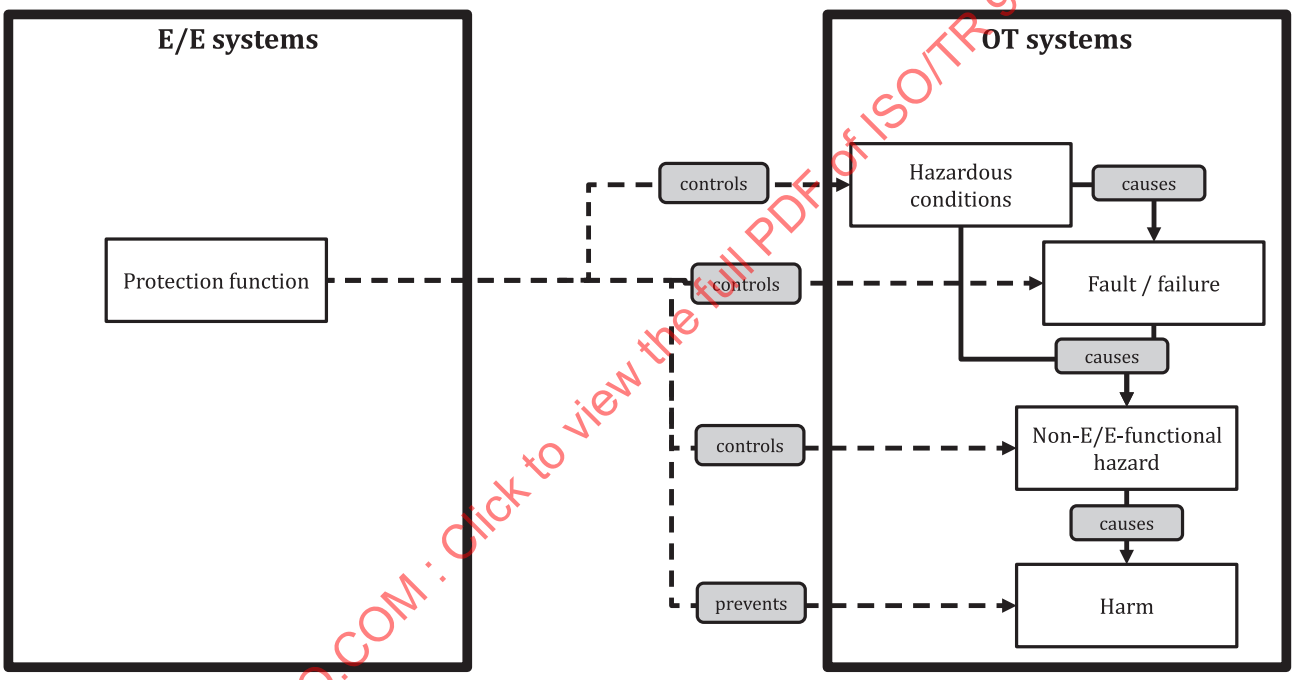


Figure 6 — Visualization of a protection function controlling OT faults or failures or preventing hazards due to OT faults or failures

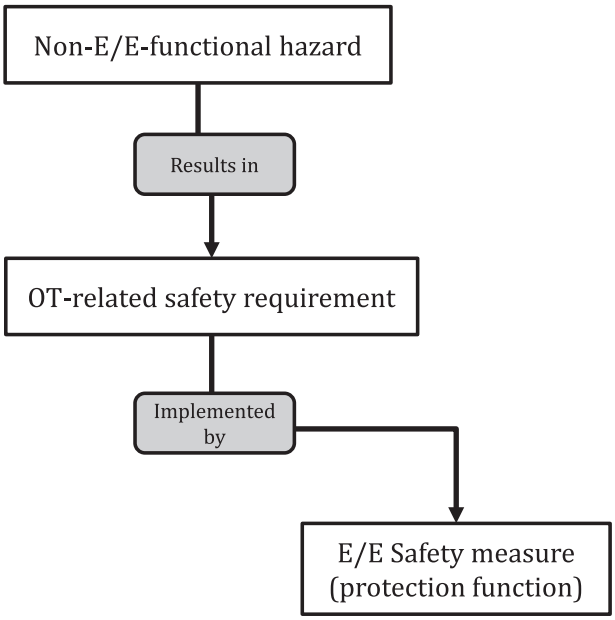


Figure 7 — Visualization of non-E/E-functional hazards and related hazardous conditions are addressed by E/E protection functions

In the context of non-E/E-functional hazards, the protection function can use different strategies:

— prevent the occurrence of the hazardous conditions;

— detect and control a fault of the OT; and

— detect the hazard and prevent the occurrence of harm, e.g. by warning the endangered persons.

EXAMPLE 1 A protection function monitoring the isolation status, requesting to disconnect the HV circuit in case of a detected isolation failure.

EXAMPLE 2 A protection function monitoring the level of coolant fluid. If the level is below a certain threshold the protection function initiates the transition into the safe state.

EXAMPLE 3 A protection function for thermal runaway detection of the battery. In case a thermal runaway of the cells is detected, it sends a warning to the vehicle occupants with sufficient time for the vehicle occupants to get to safety. See ECE R100 V3[21] for more details.

NOTE A protection function can also be used to address E/E-functional hazards of other items.

6.6 Case 4: Safety measures of elements of other technologies addressing functional safety requirements and safety goals

This case is visualized in Figure 8 and Figure 9.

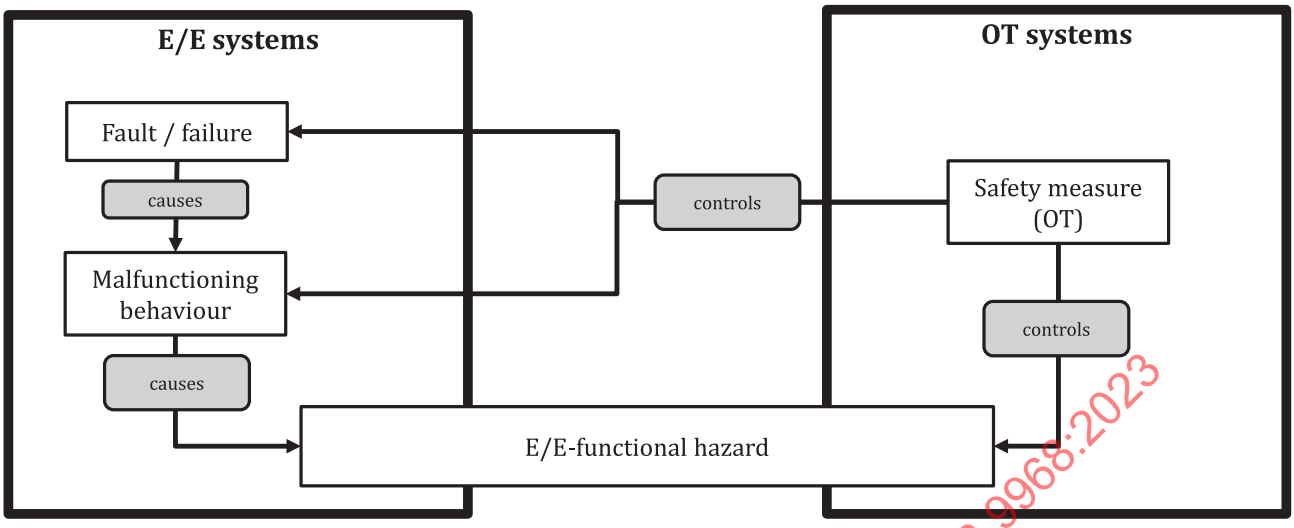


Figure 8 — Visualization of OT safety measure preventing the occurrence of harm due to E/E issues

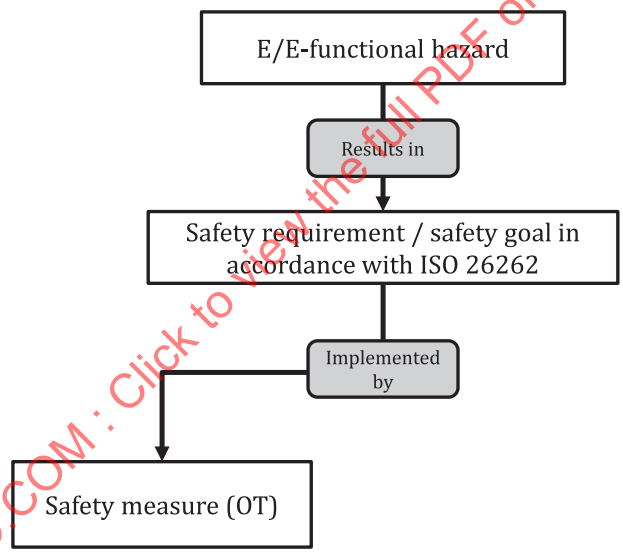


Figure 9 — Visualization of safety measures of elements of other technologies addressing functional safety requirements and safety goals

This case is mentioned in ISO 26262-3:2018, Clause 7. However, it can also be applied in later stages of the development, e.g. during system development (see 5.2) or hardware development (e.g. in form of a dedicated measure to address single-point faults).

6.7 Case 5: Combined OT and E/E safety measures implementing a safety requirement

This case is visualized in Figure 10.

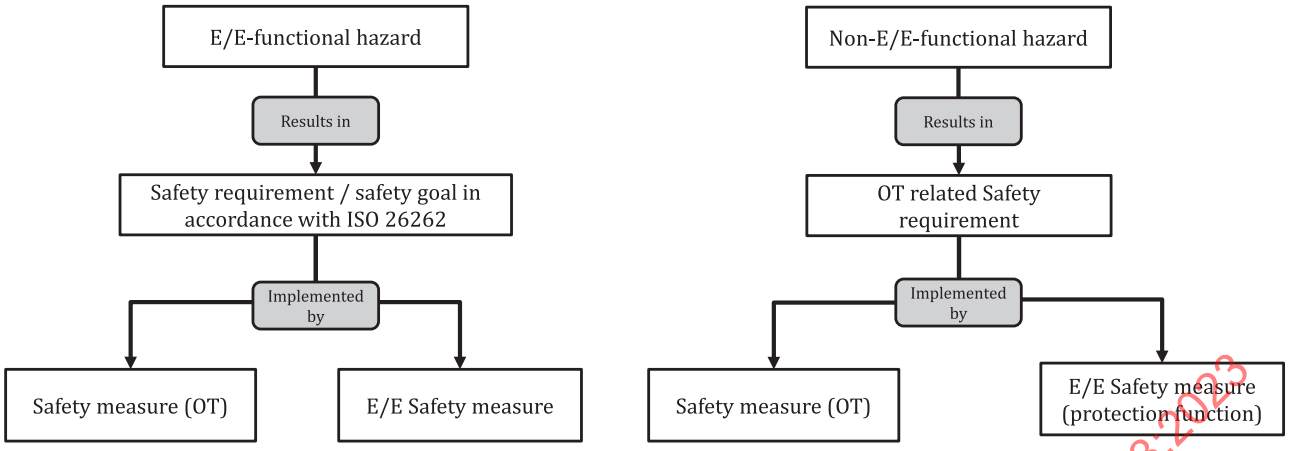


Figure 10 — Visualization of an OT or E/E safety requirement being implemented by a combination of OT and E/E safety measures

This approach is mentioned for the E/E-functional hazard case in ISO 26262-3:2018, 7.4.2.9, NOTE 1 where the possibility of ASIL decomposition-like approach is mentioned.

According to ISO 26262-9:2018, 5.2, the precondition of ASIL decomposition is that the redundant safety requirements are implemented by sufficiently independent architectural elements.

NOTE 1 Dependent failures can exist that render the OT safety measure and the E/E safety measure as not sufficiently independent.

If the architectural elements are not sufficiently independent, then the redundant requirements and the architectural elements inherit the initial ASIL.

NOTE 2 Even in case the independency is not given the additional measures can improve the safety, e.g. impacting the S, E and C parameters or impacting the occurrence probability of the hazard.

NOTE 3 The combined allocation to an E/E safety measure and an OT safety measure can be done on safety goal level as well as on lower level safety requirements.

EXAMPLE 1 Disconnecting an HV circuit with high current load will generate sparks or arcs near the contactors, possibly causing a main contactor stuck closed fault. The protection of against contactor stuck closed is realized by the main contactor SOH monitoring, contactor stuck closed detection of E/E and arc suppression device of OT, see Figure 11.

NOTE 4 Main contactor SOH monitoring and contactor stuck closed detection are considered as sufficiently independent with arc suppression device.

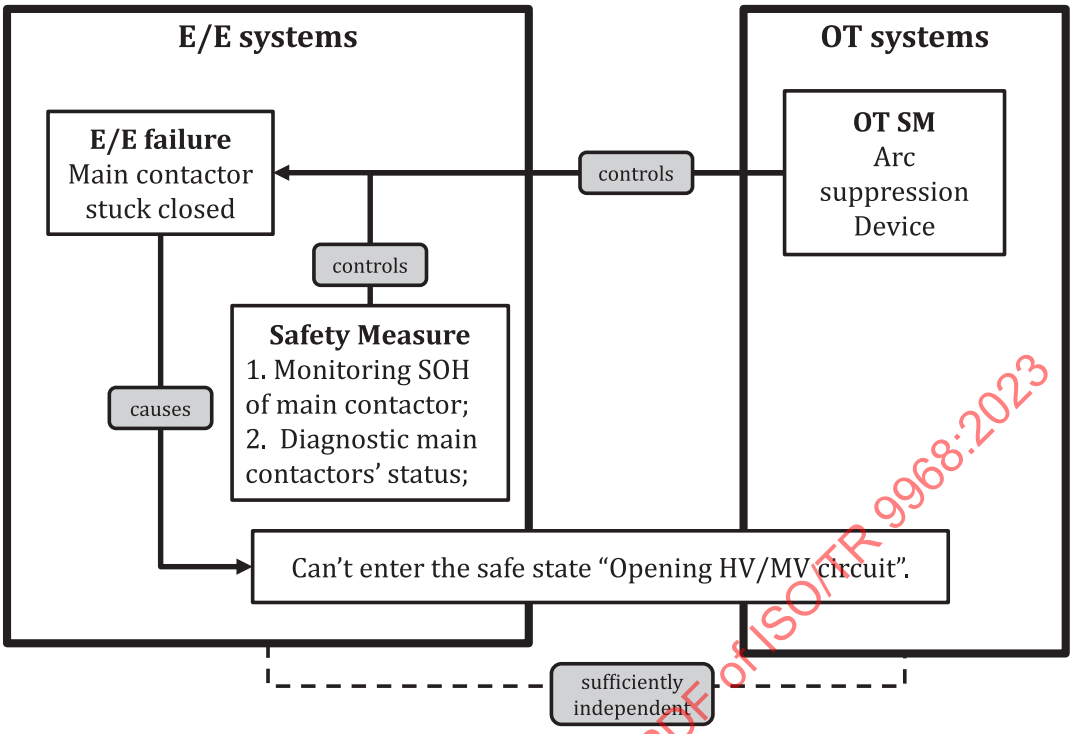


Figure 11 — Visualization of contactor stuck closed failure control

EXAMPLE 2 The protection against high voltage electric shock is realized by isolation paint, IPxxB/D connectors, HVIL isolation cap and E/E safety mechanism to monitor isolation integrity and status of the HVIL, see Figure 12.

NOTE 5 Isolation paint and isolation cap are considered as sufficiently independent with E/E isolation monitoring.

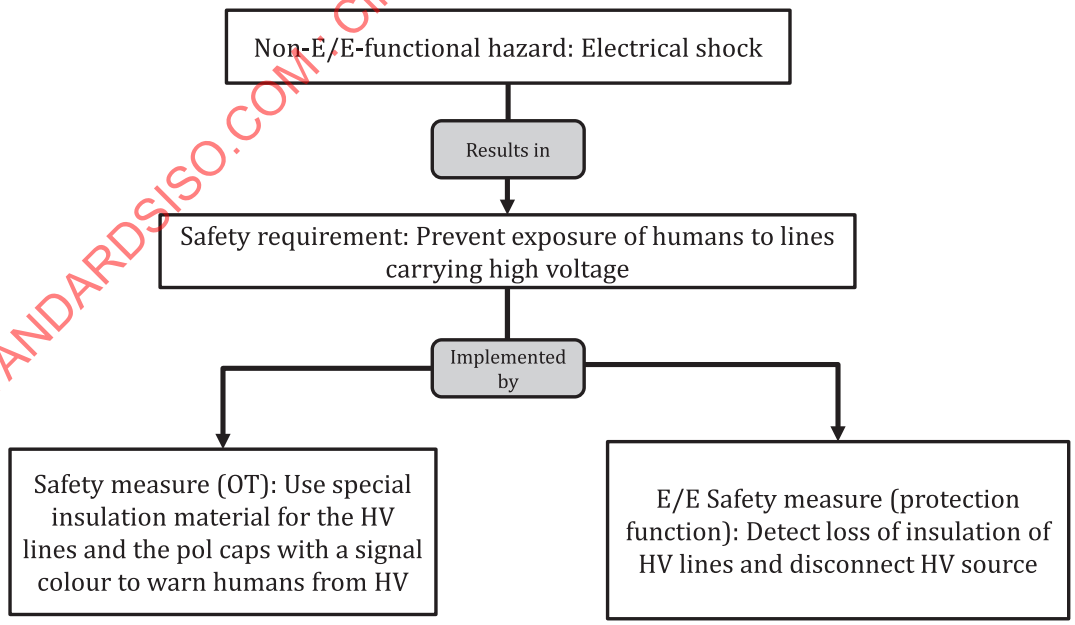


Figure 12 — Example of isolation failure control

EXAMPLE 3 Preventing hazard due to electrolyte leakage by cell edge sealing and E/E SM: electrolyte leakage detection, see Figure 13.

NOTE 6 As the electrolyte leakage perhaps leads to BMS destroyed, thus it is considered not sufficiently independent with the E/E SM isolation monitoring.

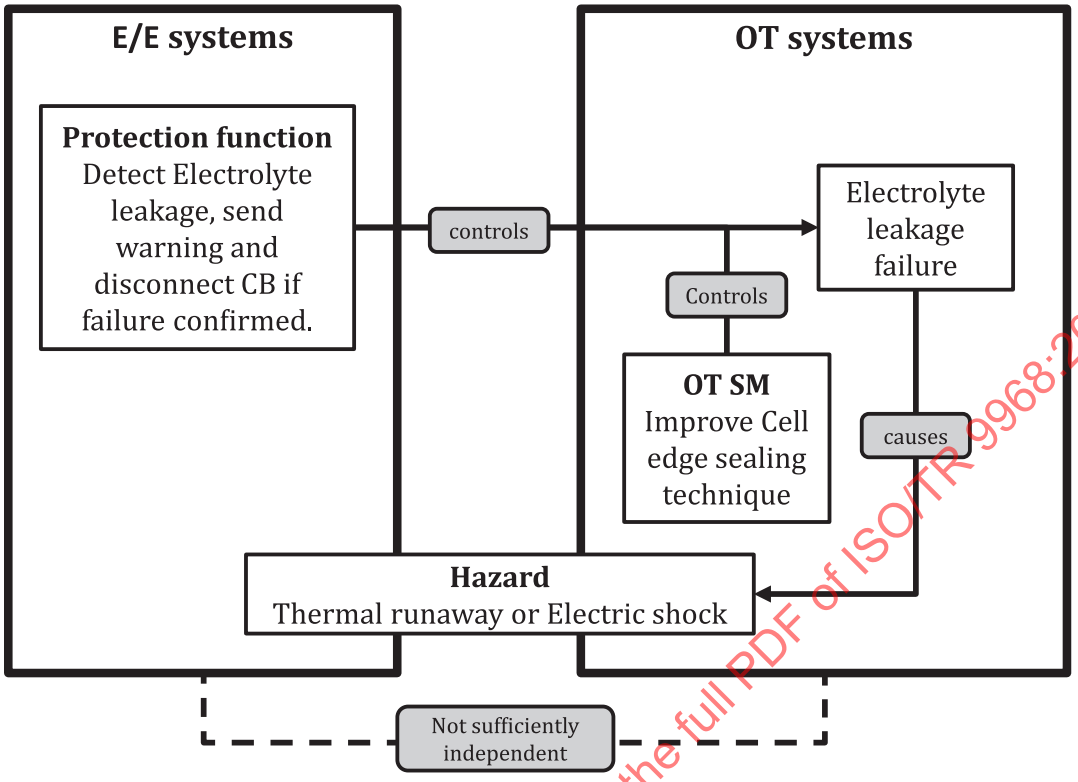


Figure 13 — Example of electrolyte leakage protection

If there are safety measures which eliminate the dependent factors, it can be considered as an appropriate ASIL decomposition.

EXAMPLE 4 Safety measures can be mounting the BMS on the top of the battery, or putting the BMS in an enclosure which meets IP67 intrusion protection level.

7 Verification and validation for RESS

7.1 OT related hazard and hazardous conditions

If corresponding standards are available, the verification and the validation of the identified hazardous conditions and hazards related to the OT is executed according to these standards and expert judgement.

EXAMPLE 1 GB 38031, EUCAR xx, SAND2017-6925, UN 38.3, IEC 60479.

EXAMPLE 2 The toxicity of released gas can be judged according to AEGLs level 2.

If no appropriate standard is available, consider verification of the correctness of the identified hazardous conditions and hazards related to the OT by expert judgement.

NOTE 1 The hazardous conditions can change over lifetime of the OT. This aspect is also taken into consideration for the V&V activities.

EXAMPLE 3 Use aged battery or aged RESS to verify the hazardous conditions for MOL and EOL.

NOTE 2 The V&V activities can include, but are not limited to, test, simulations, analyses and reviews.

If S, E and C parameters are assigned to the OT-related hazards they can be verified and validated according to the ISO 26262 series.

7.2 Case 1: Malfunctioning behaviour of the E/E systems can cause hazards related to the OT

The V&V is executed according to the ISO 26262 series.

7.3 Case 2: Failure of OT causes E/E failures

The V&V is executed according to the ISO 26262 series.

7.4 Case 3: Non-E/E-functional hazards and related hazardous conditions are addressed by E/E protection functions

The V&V of the protection function has following aspects:

a) V&V of the OT-related hazardous conditions and hazards;

b) V&V of the expected necessity of demand of the protection function;

NOTE The expected necessity of demand of the protection function is the expected frequency the corresponding hazardous condition or hazard occurs over lifetime, requiring an intervention of the protection function

c) V&V of the E/E aspect of the protection function; and

d) V&V of the risk mitigation effectiveness of the protection function.

Aspect a) is executed as described in 7.1.

Aspect b), if not already part of aspect a), is executed analogue to 7.1: If there are appropriate standards available, the V&V is executed according to these and expert judgement. If they are not available, V&V is executed according to expert judgement.

Aspect c) is addressed by the ISO 26262 series, but is dependent on the ASIL.

Aspect d) is not addressed in the ISO 26262:2018 series. If no appropriate standard is available, the V&V activities are executed according to expert judgement.

EXAMPLE 1 As to HVIL failure verification, the acceptance criteria is that the HVIL failure related signal is reported when this failure is injected in order to confirm high voltage isolation integrity.

EXAMPLE 2 As to warning in case of a thermal event within RESS, refer to GB38031:2020, Appendix C for the verification test procedure how to inject thermal event. The acceptance criterion is that warning signal is correctly sent out at least 5 min prior to the thermal propagation.

7.5 Case 4: Safety measures of OT addressing functional safety requirements and safety goals.

The V&V is executed according to the ISO 26262 series, in particular to ISO 26262-4:2018, Clause 8.

7.6 Case 5: Combined OT and E/E safety measures implementing a safety requirement

Since case 5 is a combination of case 3 and case 4, the V&V is executed as described in 7.4 and 7.5. If independence between the two safety measures is required, the dependent failure analysis according to ISO 26262-9:2018, Clause 7 can be used to provide the necessary evidence.