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.

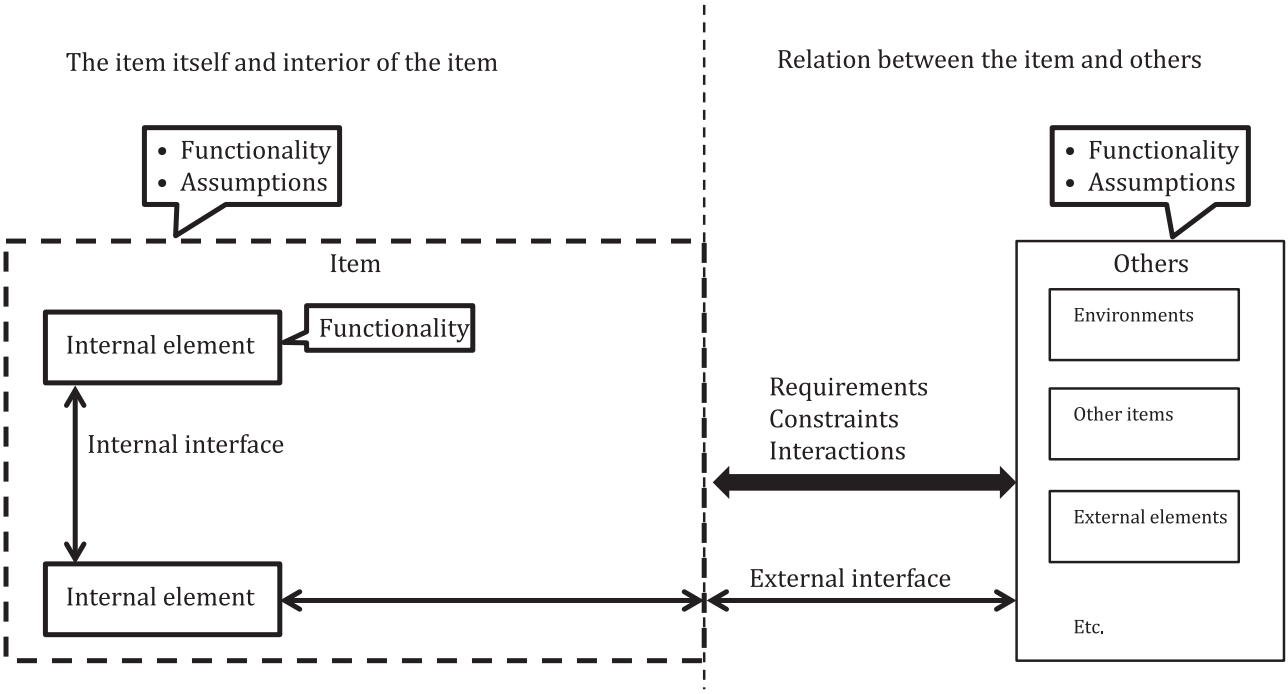

Figure 1 — Visualization of the task of the item definition

5.3 OT is part of the item

5.3.1 General

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

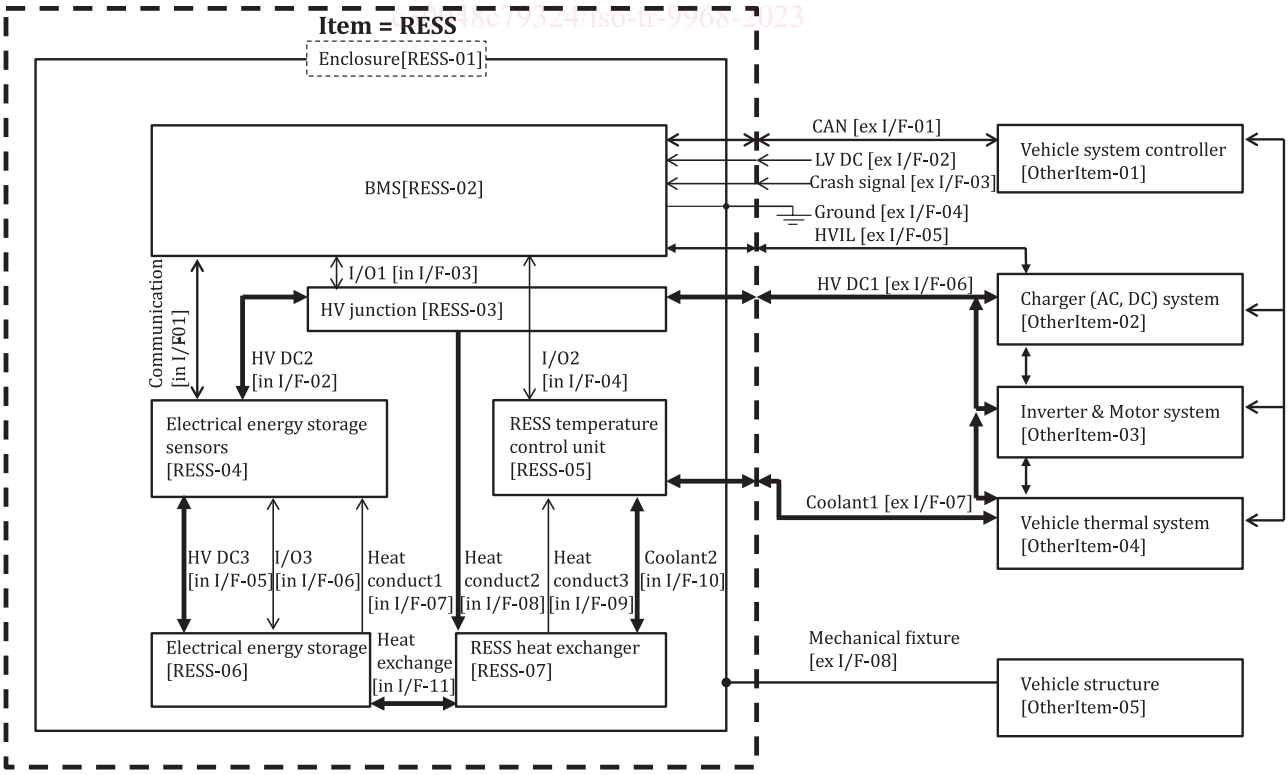

Figure 2 — OT is part of the item – Example

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;