IEC 63187

Systems engineering — System safety
Complex systems in defence programmes

"A speciality engineering view of ISO/IEC/IEEE 15288"

65A/1187/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: IEC 63187-1 ED1	
DATE OF CIRCULATION: 2025-09-05	CLOSING DATE FOR VOTING: 2025-11-28
SUPERSEDES DOCUMENTS: 65A/1122/NP, 65A/1186/RVN	

IEC SC 65A : SYSTEM ASPECTS

SECRETARIAT: United Kingdom	SECRETARY: Ms Stephanie Lavy
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 65,ACOS	HORIZONTAL FUNCTION(S): TC 65/SC 65A Horizontal Basic Safety
ASPECTS CONCERNED: Safety	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE AC/22/2007 OR NEW GUIDANCE DOC).

TITLE:
Systems engineering – System safety – Complex systems in defence programmes Part 1 – Concepts, terminology and requirements

PROPOSED STABILITY DATE: 2030

NOTE FROM TC/SC OFFICERS:

IEC 63187-1 is currently at the Committee Draft for Vote development stage. Publication as an international standard is planned in 2026, subject to international approval.

IEC TR 63187-2 is being drafted as a Technical Report to support implementation of IEC 63187-1.

Motivation for a new standard

The market is evolving towards:
- More **complex** systems with **complex** functions and **complex** architectures
- **New technologies** and new applications of existing technology
- **Fewer humans in the loop** to handle safety
- **Dynamically evolving risks**

Existing safety standards do not:
- Align with **system engineering**
- Address **multi-layered systems** recursively
- Capture **emergent properties** at system level (without failure)
- Fully allow interaction with other **engineering domains**

Objectives

Safety:
- Propose a comprehensive approach for **adapting safety requirements to risk**
- Propose an approach for **risk control** across the layers of a system
- Propose an approach to control situations of **dynamic risk**
- Maintain an open approach towards activities and assurance **outcomes**
- **Account for traditional approaches**, in particular quantitative, for **realised system elements**

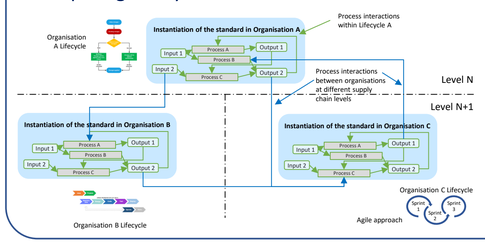
Systems engineering:
- Propose a way to **embed safety engineering** in systems engineering (ISO/IEC/IEEE 15288)
- Propose an approach enabling **instantiation between system layers** and between supply chain levels **without limitations**
- Distinguish the system conceptual activities from the realisation of the system physical and logical elements
- Propose a seamless **interface to existing safety standards** for realising physical and logical system elements

Fundamental principles

- **Risk-based** (ISO 31000): focus on hazards and their consequences rather than quantitative probability; risk is the effect of uncertainty on objectives
- **Systems-based** (ISO/IEC/IEEE 15288): recursively applying systems engineering principles at multiple levels in the systems hierarchy and supply chain
- **Systems theory** and **control theory**: considering interacting system elements that can lead to detrimental effects without component failure
- **Integrating safety into systems engineering** as a fundamental part of engineering the system, with the flexibility to trade requirements
- **Appropriateness of approach:** addressing threats to safety from sources with different types of characteristic
- **Supply chain considerations**: addressed to apply proportionately over organisational boundaries
- **Solution independent**: regardless of the origin or lifecycle stage of realised system elements
- **Goal-based:** providing a framework to identify and achieve safety objectives, rather than a prescriptive set of rules or specifications

Acquisition viewpoint

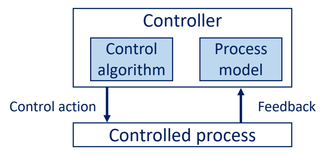
- Defence applications are subject to dynamic risks: detriments (harms), safety objectives and compromises depend on the operational context (CONOPS)
- Risk acceptability can only be determined on a case-by-case basis, by the organisation acquiring the system
- Definition of detriments from the acquirer's own viewpoint (i.e. "what is important")
- Convergence and control of Measures of Importance (MoI) through schemes agreed between parties (i.e. "how important is that?")
- IEC 63187 is applied by organisations across the supply chain, giving a consistent approach
- Each organisation defines its own suitable life cycle on the basis of the generic ISO/IEC/IEEE 12207 life cycles
- Organisations agree on interface arrangements, allowing consistent and traceable engineering



Systems engineering viewpoint

Control theory:
- Detriments from all domains of interest (mission, safety, security, …) can be considered in decision making
- Centred on the Perception–Interpretation–Decision–Action loop.
- Safety viewed as the robustness of control under internal and external perturbations
- Modelling control structures allows scenarios that lead to undesired system states to be identified
- Humans are integrated in the control structures

IEC 63187 considers all the system life cycle processes from a safety viewpoint:
- Implementing a "Safety View" (as an aspect of speciality engineering, as per ISO/IEC/IEEE 24748-1:2024 annex D4)
- Supplementing ISO/IEC/IEEE 15288 process outcomes with specialised requirements, criteria and informative notes, to clarify what is needed from the safety viewpoint



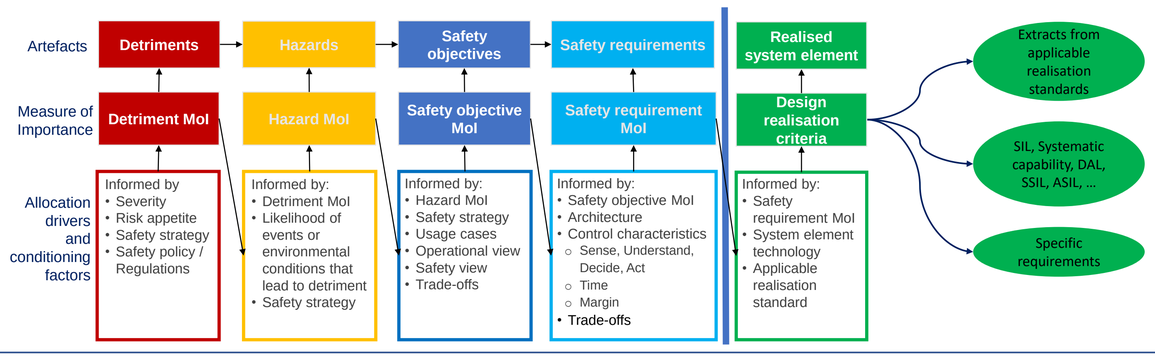
Implementation viewpoint

- The actual production of system elements is not in the scope of IEC 63187. The standard is limited to their specification and acceptance, not the detail of their realisation
- The requirements of IEC 63187-1 do not interfere with the prescriptive standards for the production of system elements (e.g. for E/E/PE: DO178C, IEC 61508-3, IEC 61508-2)
- Inputs to realisation work will be defined based on the detriments, hazards, safety objectives and safety requirements; and the design constraints will integrate the elements necessary for the realisation

	Visibility of design and configuration	No visibility of design and configuration
Controllability of the design	Route to realisation 1_R	Route to realisation 3_R
No controllability of the design	Route to realisation 2_R	Route to realisation 4_R

Safety engineering viewpoint

- No split imposed between the system under control and the safety functions, as is the case with IEC 61508
- The IEC 63187 approach remains compatible with the fundamental principles of IEC 61508 and MIL-STD-882E
- The Measure of Importance (MoI) concept allows classifying various artefacts according to associated criteria/parameters and moderation factors to reflect how much they matter to the stakeholder
- Defining a MoI makes it possible to avoid the saturation of integrity levels that can occur when allocating requirements mechanically



Takeaway points

Systems engineering
- No mandated safety deliverables; safety outcomes are embedded in the systems engineering outcomes, open life cycle adaptable by each stakeholder organisation

Hazards, risks and detriments
- Principles of control theory
- Based on a unique concept to express objectives from all specialities and allow arbitration when necessary

Safety objectives and safety requirements
- Dissociation of constraints on the system of interest (objectives) from the solutions satisfying them (safety requirements) and allows identification of emerging aspects

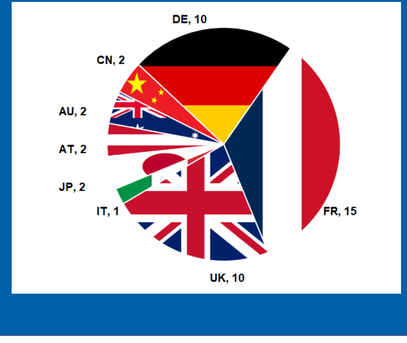
Measures of Importance
- No predefined index (no equivalent to SIL, DAL, ASIL, etc.)
- Definition of normative requirements to allow stakeholders to define ad hoc Measures of Importance in a consistent global framework

Safety performance
- Accounts for the fact that the system safety performance, if expressed only quantitatively as the sum of the realised system element failures, cannot represent the overall system safety

Safety assurance
- Accounts for the fundamental difference between the necessary means to deliver system safety and the necessary means to guarantee their effectiveness

IEC 63187 development ecosystem

50+ Participants from 11 contributing nations



IEC 63187 is being developed by Working Group 18 of the IEC's TC65/SC65A technical subcommittee: Industrial-process measurement, control and automation – Systems Aspects. Members of the international working group are experts nominated by the national standards organisation of each country that takes part.

For more information, contact james.inge@scsc.uk