



IEC 63187

Systems engineering — System safety Complex systems in defence programmes

“A speciality engineering view of ISO/IEC/IEEE 15288”

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
- Encourage capture of **emergent properties** at system level (without failure)
- Fully allow interaction with other **engineering domains**

Objectives of IEC 63187

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:

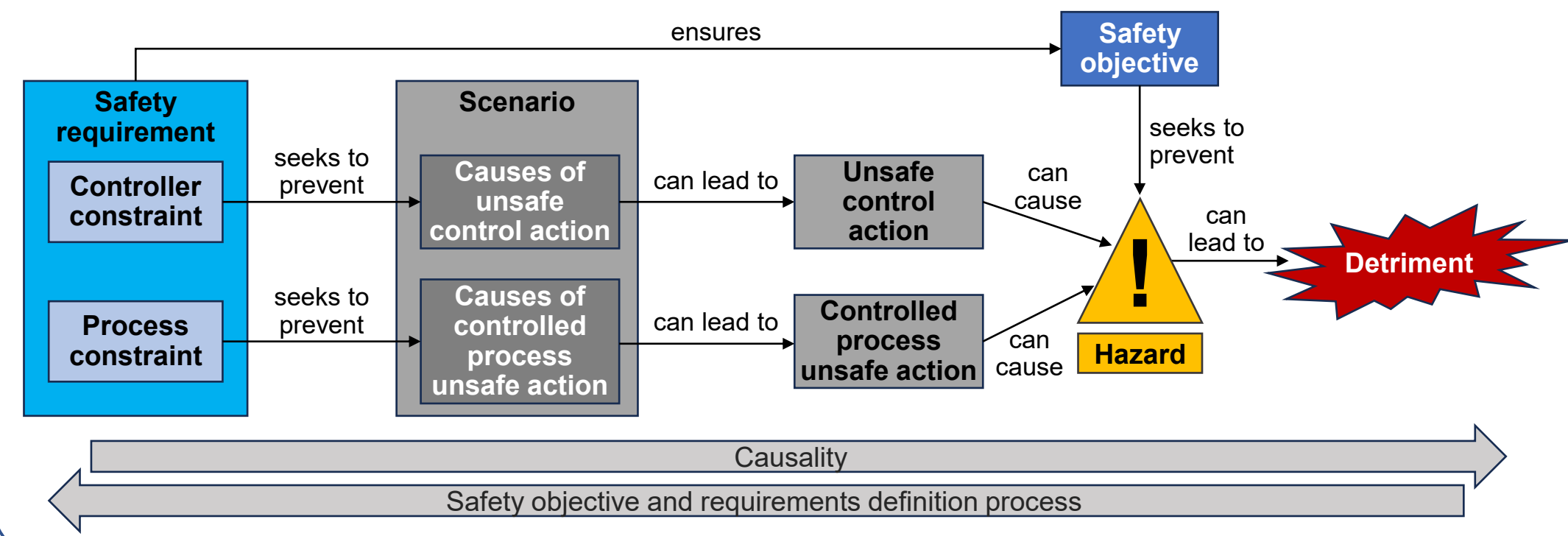
- Propose a way to **embed safety engineering** in systems engineering (ISO/IEC/IEEE 15288).
- Propose an approach enabling **instantiation between system layers** and between supply chain levels **without limitations**.
- Distinguish the system conceptual activities from the realisation of the system 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.

Approach to risk

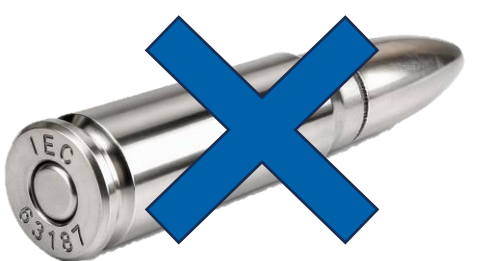
- Defence applications are subject to dynamic risks: likelihood and severity of harm both vary with time over the system life cycle, and also depend on the context of the operational scenario.
- Risk acceptability can only be determined on a case-by-case basis, by the organisation acquiring the system. Acceptability of risks and trade-offs also depends on the scenario.



- Risk is not just a scalar value that varies with time. It is vector of time-varying values that apply in different contexts.
- IEC 63187 does not require a numeric assessment of risk – it would not be practical to calculate.
- Instead, ‘Measures of Importance’ reflect the need to ensure safety or gain assurance in different contexts.
- Measures of Importance capture both the degree or level of importance and the context in which it applies.

Approach to complexity

- In IEC 63187, a ‘complex system’ is defined as one “where the collective behaviour of the system elements entails emergence of properties that can hardly, if at all, be inferred from properties of those system elements”.
- The standard is not a ‘silver bullet’ methodology, but has several features to facilitate safety management for complex systems:
 - Explicit requirements in the standard prompt consideration of emergence in safety analysis and requirements definition.
 - System safety is integrated into systems engineering processes, which are intended to aid management of complexity.
 - The standard can be applied recursively at different levels of a systems hierarchy, so that analysis can take place at an appropriate level of abstraction for study of interactions between system elements.
 - The standard is goal-based and does not specify particular tools or techniques. This allows appropriate tools to be chosen for the project context, using the state of the art as new tools become available.
 - The risk model in IEC 63187 has been chosen to be compatible with control theory, and systems theory, making it easier to apply analysis techniques that address the interactions between system elements and the scenarios that might give rise to hazards and detriments.



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 (Mol) concept allows classifying various artefacts according to associated criteria/parameters and moderation factors to reflect how much they matter to the stakeholder.
- Defining a Mol 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

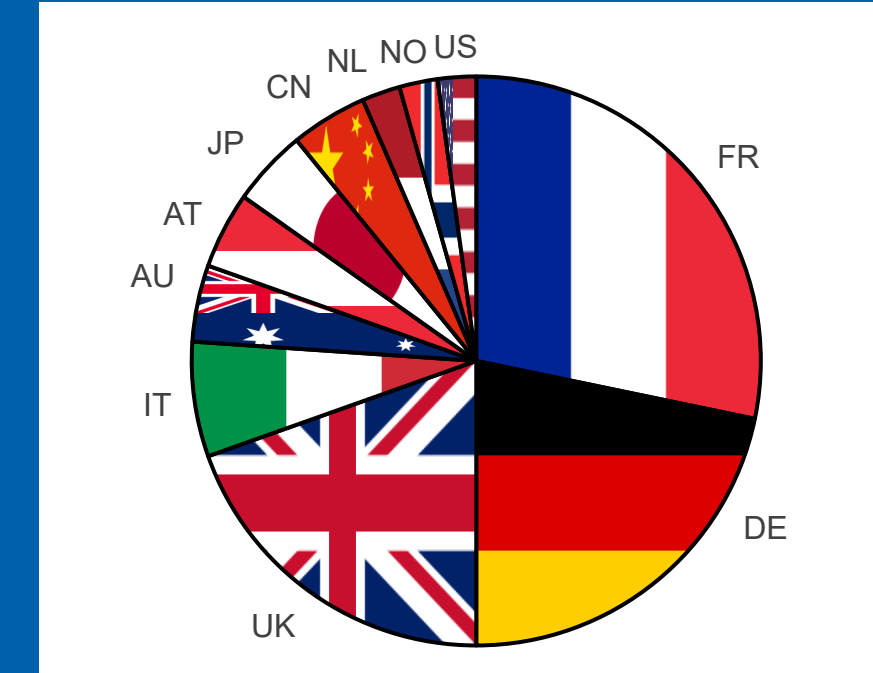
Safety assurance

- 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.