34th Annual INCOSE international symposium

hybrid event

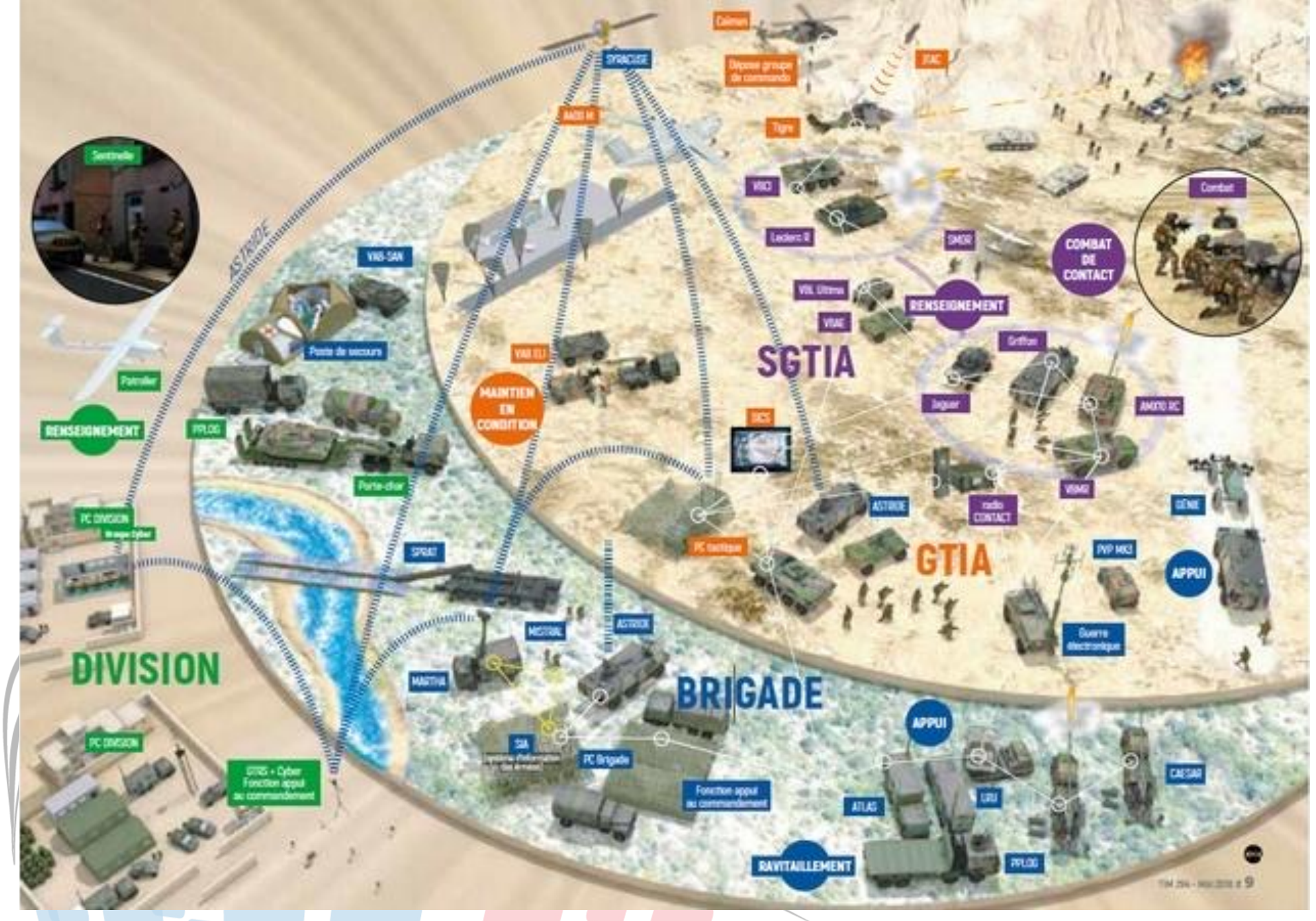
Dublin, Ireland
July 2 - 6, 2024

IEC 63187-1 – Systems engineering – System safety – Complex systems and defence programmes

Katia Potiron (KNDS FR), James Inge (Defence Equipment & Support)

EXTENDING SYSTEMS ENGINEERING FOR SAFETY-CRITICAL DEFENCE APPLICATIONS

IEC 63187-1



Projection d'une unité SCORPION -
© Ministère des Armées
[Le combat aéroterrestre du futur | Ministère des Armées (defense.gouv.fr)]

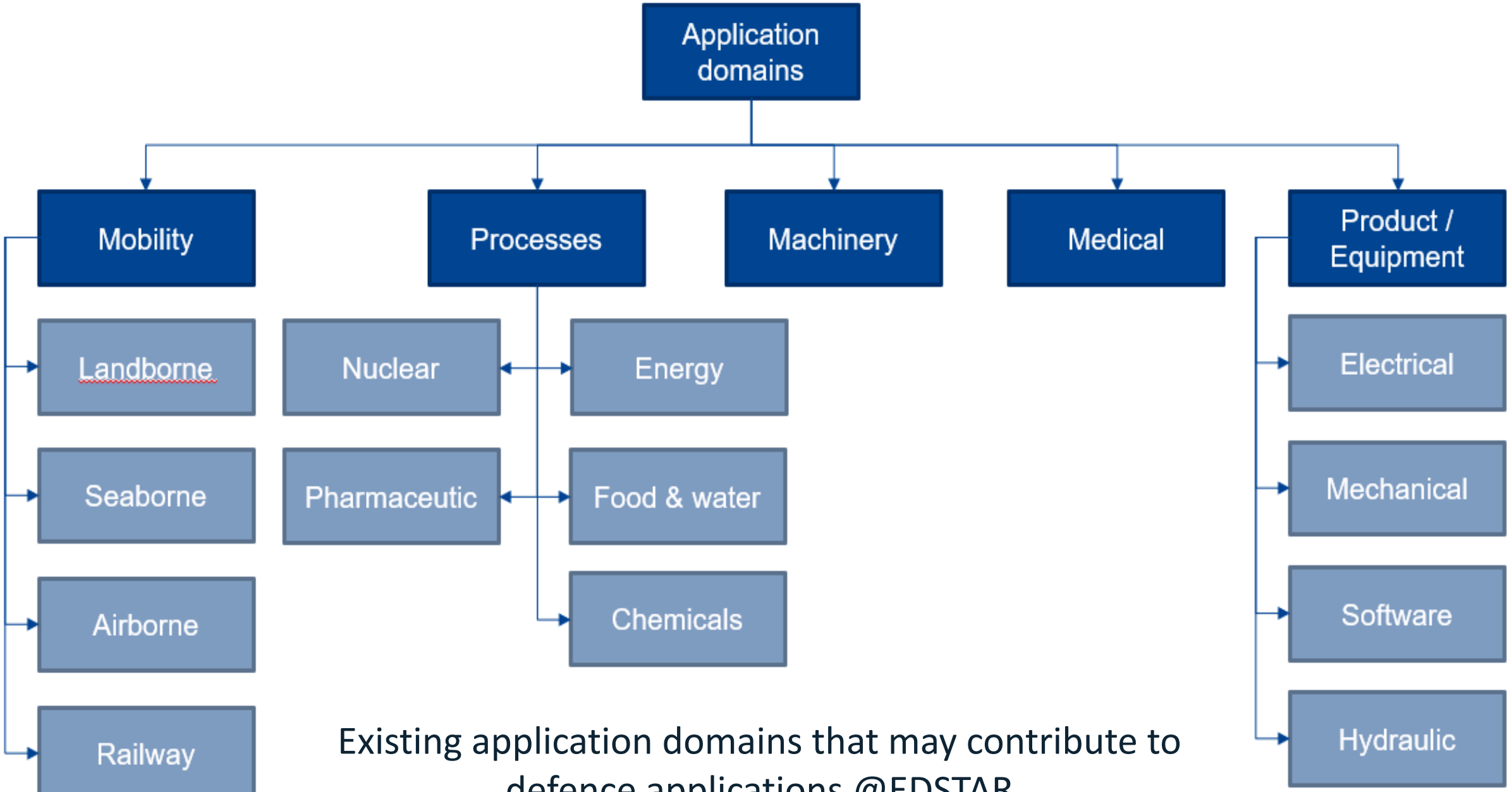
Safety challenges for complex systems

Systems evolve towards:

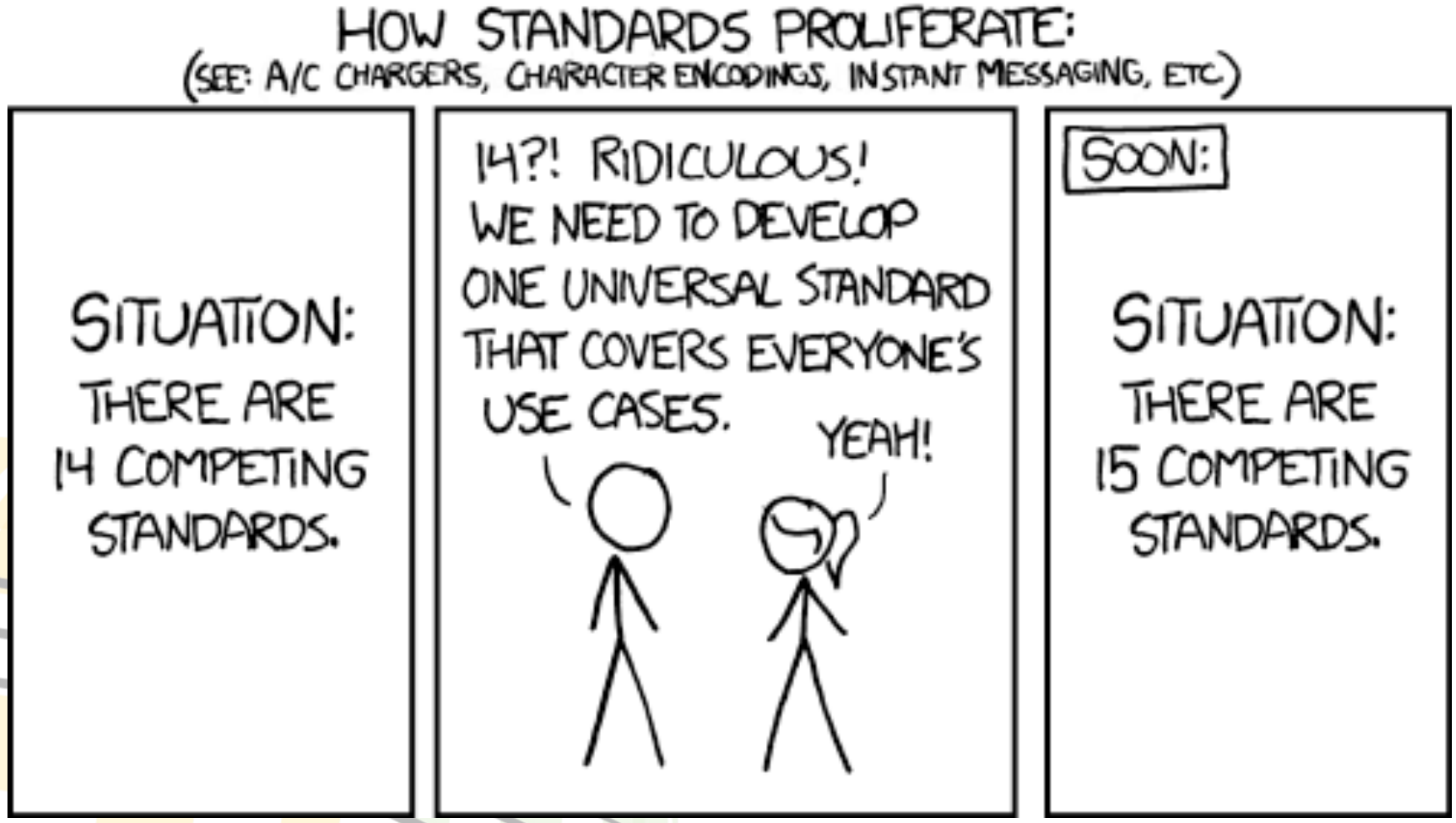
- More complex systems with complex functions and complex architectures,
- Fewer humans to handle safety,
- Dynamically evolving risks,
- More challenging management and supply chain arrangements.

Existing safety standards are not:

- Aligned with Systems Engineering,
- Able to address multi-layered systems recursively,
- Capturing emerging properties at system level (without failure of subsystems),
- Consistent together.



Existing application domains that may contribute to defence applications @EDSTAR



IEC 63187 ID Card

65A/1122/NP

NEW WORK ITEM PROPOSAL (NP)

PROPOSER: Secretariat
DATE OF PROPOSAL: 2024-06-07
DATE OF CIRCULATION: 2024-06-14
CLOSING DATE FOR VOTING: 2024-08-09

IEC SC 65A : SYSTEM ASPECTS
SECRETARIAT: United Kingdom
SECRETARY: Ms Stephanie Lavy
NEED FOR IEC COORDINATION:
PROPOSED HORIZONTAL STANDARD:
Other TC/SCs are requested to indicate their interest, if any, in this NP to the TC/SC secretary

FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☒ SAFETY

TITLE OF PROPOSAL: Systems engineering – System safety – Complex systems and defence applications Part 1 – Concepts, terminology and requirements

☒ STANDARD ☐ TECHNICAL SPECIFICATION ☐ PUBLICLY AVAILABLE SPECIFICATION

PROPOSED PROJECT NUMBER: 63187-1

SCOPE (AS DEFINED IN ISO/IEC DIRECTIVES, PART 2, 14): The project will finalise the development of PR IEC 63187 as an international standard addressing the particular aspects of safety engineering of complex systems focused on defence systems and open to other sectors.

PURPOSE AND JUSTIFICATION INCLUDING THE MARKET RELEVANCE AND WHETHER IT IS PROPOSED TO BE A HORIZONTAL STANDARD. MARKET RELEVANCE SHOULD BE ADDRESSED BY INDICATING THE NEED FOR THE CORRESPONDING STANDARDS WORK AND ITS GLOBAL RELEVANCE (SEE ISO/IEC DIRECTIVES, PART 1 ANNEX C) IF PROPOSED AS A HORIZONTAL STANDARD, IDENTIFY AS POSSIBLE, THE CORRESPONDING APPLICABLE GUIDE(S) AND ASSOCIATED ADVISORY COMMITTEE(S) (SEE GUIDE 108).

This circulation is motivated by the SMB decision to ask for reinstating all project reaching schedule limits. The attached version of the standard corresponds to the previous CD stage amended with answers to a number of national committee comments. The project schedule is to answer the comments raised by this circulation and subsequently propose the CDV stage

TC65 Industrial-process measurement, control and automation / SC65A System aspects / WG18 ~~Functional safety of IACS in defence applications~~ -> System safety in complex systems and defence programmes

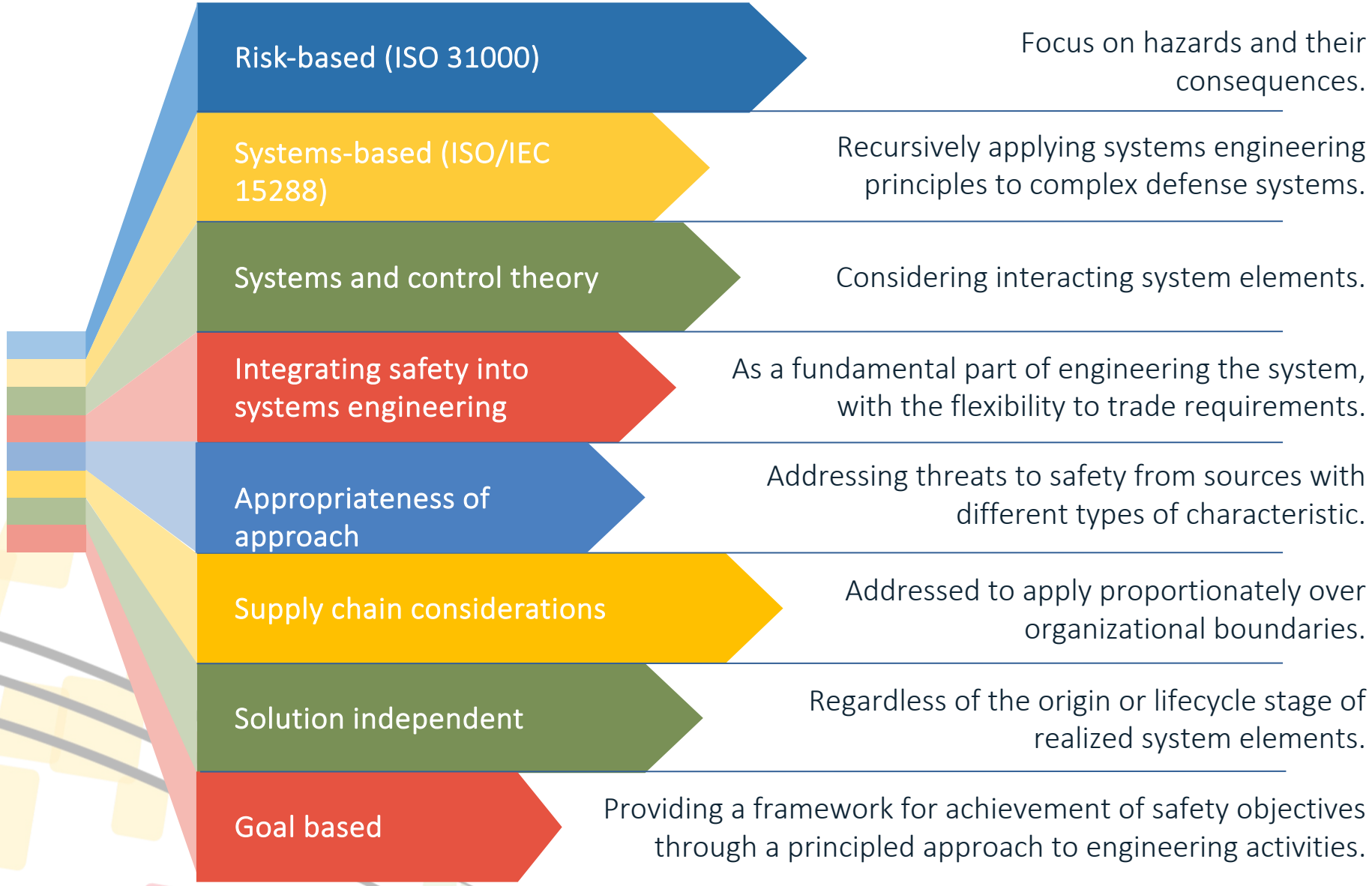
IEC 63187-1: Systems engineering – System safety – Complex systems and defence programmes
Part 1 – Concepts, terminology and requirements

IEC TR 63187-2: Systems engineering – System safety – Complex systems and defence programmes
Part 2 – Guidance on application

10	Participating countries
~40	Working group members
28	Plenary meetings since 2018
178	Comments received for the CD

IEC 63187-1

Based on 8 fundamental principles.



IEC 63187 objectives with regard to systems engineering

- Propose an approach of safety engineering embedded in systems engineering (ISO/IEC/IEEE 15288).
- Propose an approach enabling instantiation between system layers and between tiers without limitations.
- Distinguish the system conceptual activities from the realisation of the system physical and logical elements.
- Propose a seamless interface with existing safety standards for the realisation of system physical and logical elements.

Systems engineering approach to system safety

Why integrate system safety into systems engineering?

- Safety is an emergent property of the overall system, not a feature that can be added on.
- It is needed to ensure that safety is considered appropriately throughout the system life cycle.
- It’s more effective to use systems engineering as a starting point and add safety-specific requirements, than to add systems engineering concepts to the various safety standards used across the defence sector.
- WG 18 then defined IEC 63187-1 as “A specialised instantiation of ISO/IEC 15288 for the safety aspects of the lifecycle of systems”

How to integrate system safety into systems engineering?

Review of 15288 processes

Which typically did or did not have a link with safety?
Where further processes necessary for safety-critical systems?

Expected gains

IEC 63187-1 is based on applying these processes in a way that is not restrictive on how they are instantiated within organizations and between stakeholders.

Conclusion

Systems engineering processes in ISO/IEC/IEEE 15288 are sufficiently comprehensive and flexible to encapsulate system safety.
Unnecessary to either redefine the existing processes or add new ones.

Expected gains

Systems engineering processes can be applied consistently, following defined methods and using suitable tools.
This allows a generic and flexible approach to cover the variety of situations presented by complex systems.

Life cycle and recursive approach

- IEC 63187-1 does not mandate any specific life cycle; it:
  - Relies on the pillars of systems engineering (multidisciplinary, multi domain of processes, multiple technologies, multiple skills),
  - Inherits the possibility to be applied recursively on each of the levels of decomposition and by each of the stakeholders of the system.
  - Does not make a dichotomy between the system under control on the one hand and the safety functions on the other, as is the case with IEC 61508.
- This makes it possible:
  - To adapt to different types of programmes, different organisations and different development situations,
  - To cover all phases of the life cycle of the complete system.

How to integrate system safety into systems engineering

ISO/IEC/IEEE 15288 defines systems engineering processes by:

Purpose

The purposes of the systems engineering processes have no reason to change as safety is seen by ISO/IEC/IEEE 15288 as a ‘critical quality characteristic’.

Outcomes

- No outcomes need to be added.
- The outcomes were the logical container for the safety specific requirements. They needed to be defined in more detail to ensure that they were suitable for safety.

Activities and tasks

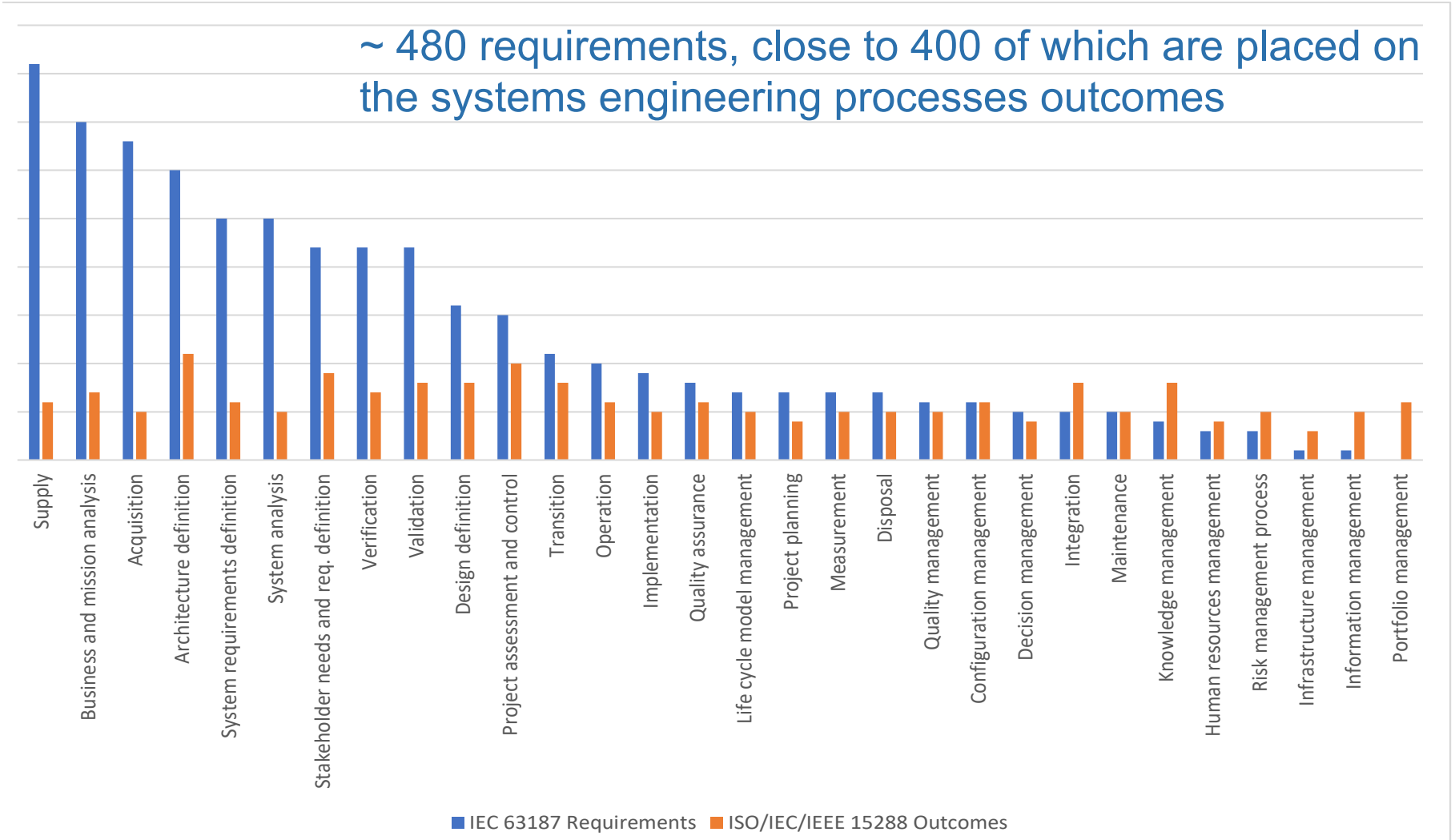
- Activities and tasks were evaluated sufficient to encapsulate safety.
- The activities should not be constrained by adding new safety-related activities, which would have limited the adaptability of the standard.

IEC 63187-1 therefore adopts the purpose, outcomes, and activities and tasks from the ISO/IEC/IEEE 15288 processes, and annotates outcomes where necessary with additional requirements and criteria for safety.

Example

- The Acquisition process in ISO/IEC/IEEE 15288 (clause 6.1.1) requires that “a request for supply is prepared” as one of its outcomes.
- To ensure that this request for supply is adequate from safety point of view, IEC 63187-1 sets 12 supporting requirements including:
  - Aspects of the scope of supply that need to be defined,
  - Information that the supplier should be requested to supply, and
  - Information that the acquirer must provide to the supplier, such as particular standards to be used or other constraints on the design.

IEC 63187-1 requirements



2nd edition of IEC 61508 has 1336 requirements

Requirements being on outcomes, producing and updating a document throughout the system life cycle may allow compliance with more than one IEC 63187-1 requirement

IEC 63187-1 requirements

IEC 63187-1 defines requirements on various more specific topics:

Safety Objects

25 Req
-
(Safety objectives, safety requirements and safety design criteria)

Traceability

10 Req
+
some criteria

Safety Relevant Documentation

10 Req
+
some criteria

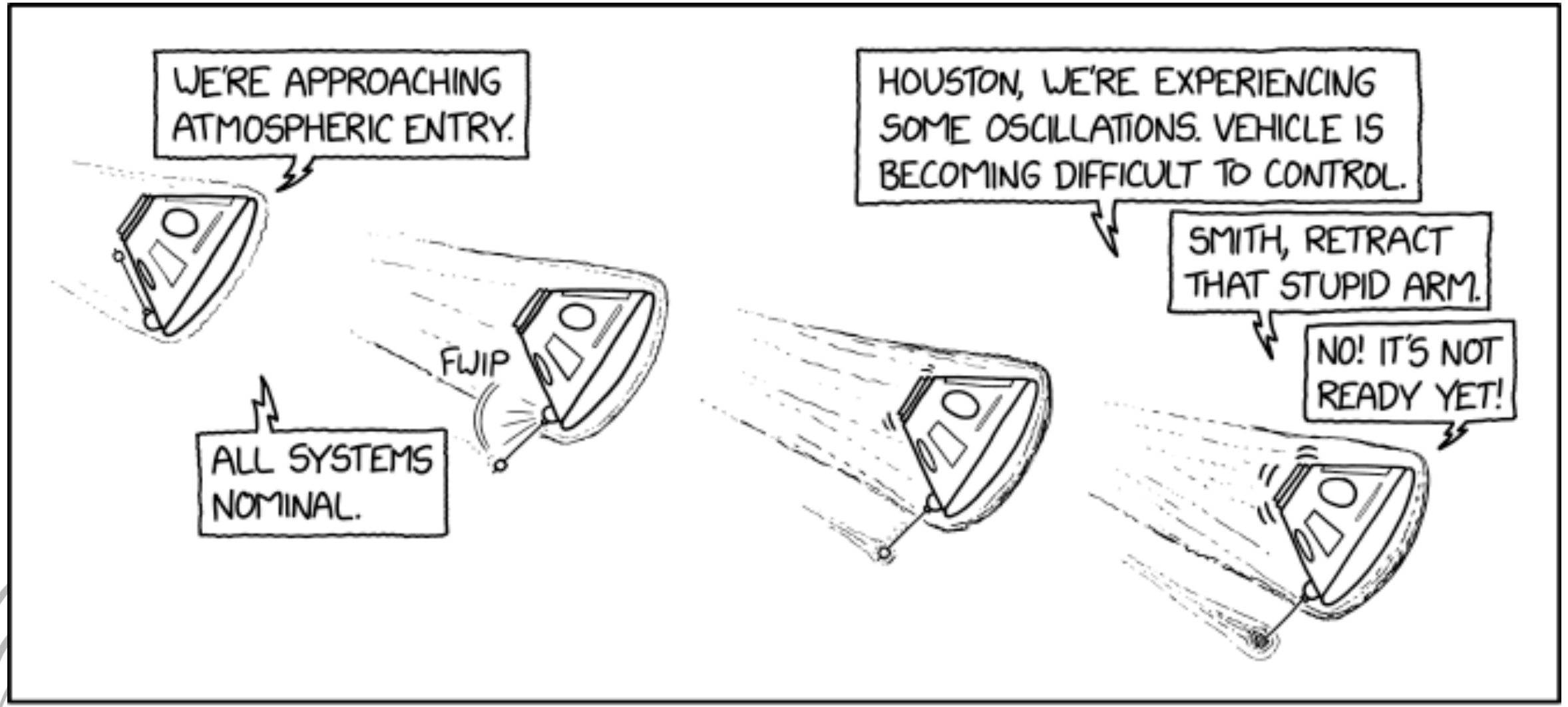
Enabling Systems

30 Req
-
to address productions facilities and organisations up to software compilers or design tools

Realised system elements

30 Req
-
4 routes

Expected gains



Expected gains

A more complete coverage of the system life cycle

- Includes requirements for supporting processes that are often not completely addressed, such as:
  - Human resources,
  - Life cycle model management,
  - Quality management and
  - Infrastructure management.
- Gives attention to safety on a wider range of activities than some other safety assurance standards.
- A focus for the requirements is the agreement processes (acquisition and supply); these are often forgotten by safety standards, but are key to practical realisation of a programme.

Provision for multi-tier supply chains

- IEC 63187-1 takes into account the contribution of suppliers throughout the supply chain to the safety of the system.
- The standard is constructed in such a way that the different suppliers ensure their part and their responsibility with regard to safety.
- For the supplier of a given system, the management of responsibilities at the interface level is addressed both upwards and downwards.

Expected gains

Flexible application to different life cycles

- Safety standards are often not well adapted for application in an agile environment because they are aimed at a V life cycle in a single organisation.
- Application of IEC 63187 is compatible between organisations because the same process outcomes are expected from each supplier, regardless of the life cycle.
- This allows appropriate adaptations to an agile environment, or to other styles of project delivery, with different life cycles for different organisational tiers or suppliers of different system elements

Management of complexity

- Based on ISO/IEC/IEEE 15288, IEC 63187-1 makes full use of systems engineering strategies to manage complexity, in particular:
  - Abstraction of detail,
  - Recursive application of techniques at different levels of abstraction, and
  - Division of the development process into defined life cycle phases.
- This recursive application is possible because the standard does not impose a specific architecture, number of decomposition levels, or set of deliverables.
- Safety is integrated into the systems engineering effort and taken into account right from the concept stage.

Expected gains

Compatibility with existing processes

- Deployment and integration of IEC 63187-1 with existing organisational processes should be straightforward because ISO/IEC/IEEE 15288 is already widely known and understood.
- IEC 63187-1 is not prescriptive in how activities must be carried out to achieve its requirements.
- It is expected that organisations using the standard would build on their existing safety engineering processes, extending them where necessary.

Solution independence

- Because it does not place requirements on how system elements are realised, IEC 63187-1 is applicable:
  - To a heterogenous mix of subassemblies (legacy systems, purchased “off-the-shelf”, or bespoke designs),
  - That vary in terms of the standards that they have been built to and the remaining opportunity to change their design or gain assurance,
  - With elements of heterogeneous maturity, some at the concept stage, others already in service.
- The standard provides different routes to demonstrating that realised system elements meet their safety objectives, depending on the degree of visibility of their design, and the extent to which there is scope to control that design.

Expected gains

Compatibility with other standards

- IEC 63187-1 is not the only standard to consider ISO/IEC/IEEE 15288 as a backbone.
  - ISO/IEC/IEEE 12207 now uses the same set of process purposes and outcomes, with different activities suitable for software engineering.
  - ISO/IEC/IEEE 24641 considers methods and tools for model-based systems and software engineering (even if the use of ISO/IEC/IEEE 15288 is not the same).
  - In the defence sector, ISO/IEC/IEEE 15288 has been adopted by the NATO Life Cycle Management Group (LCMG) as the basis for development of the Life Cycle Management.
- Aligning safety activities to the ISO/IEC/IEEE 15288 process framework is likely to improve interoperability with other standards and compatibility with the NATO life cycle approach.

Key differences between IEC 63187-1 and other safety standards

Particular aspects of IEC 63187-1

- Focus on system safety and systems engineering and not functional safety.
  - Process approach described above,
  - Recognises the very important role played by architecture in safety, and
  - Integrate safety into the system architecture.
- This system architecture focus is needed to address safety issues that result from interactions and undesirable emergent behaviours.

- Adheres to systems theory and control theory, requiring control of hazardous states or situations through a flow of safety objectives and requirements up and down the system hierarchy.
- The focus is to control interaction between system elements and the undesirable emergent properties that may result.

Particular aspects of IEC 63187-1

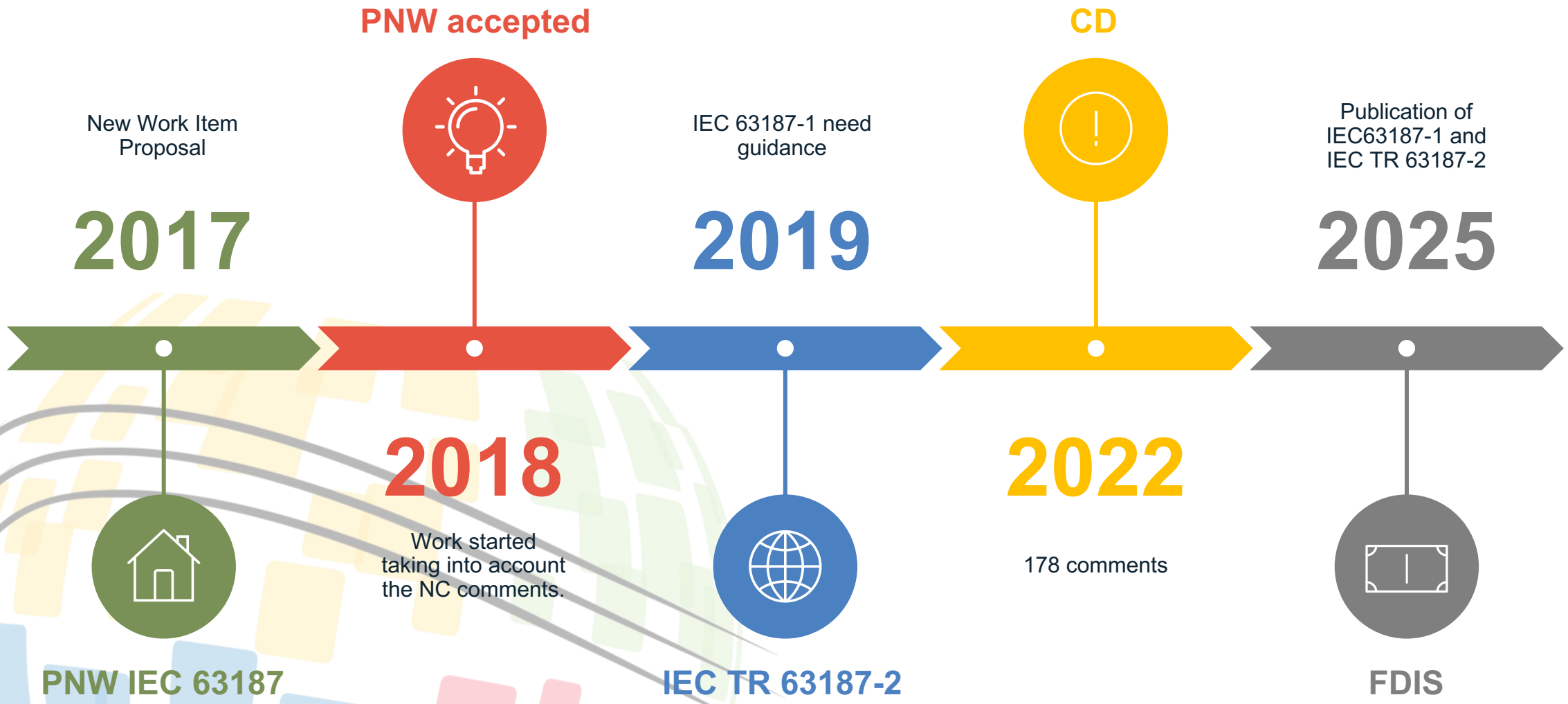
- To allow engineering effort to be focused where necessary, IEC 63187-1 requires Measures of Importance (MoIs) to be established.
- IEC 63187-1 differs in the flexibility of its MoIs:
  - Does not require a particular MoI scheme,
  - Allows a user of the standard to set up a scheme that is appropriate for their context,
  - Starts as part of the acquirer/supplier agreement processes.
- Enables an organisation to define what is important for:
  - The system,
  - Its mission and usage scenarios,
  - Operational conditions,
- Allows to be able to make the necessary trade-offs to find the best mission/safety compromises.

- Many safety standards place requirements on how individual system elements are realised.
- IEC 63187-1 deals with the higher levels of systems engineering, and allows system elements to be realised according to whichever implementation standard is most appropriate, to meet the requirements derived using IEC 63187-1 for a realised element using design criteria.
- The selected MoI for those requirements can be used to inform the choice of standard and the necessary level of rigour to be applied to bound uncertainty and provide confidence to the acquirer.

Conclusion

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 all specialties objectives and allow arbitration whenever necessary.
Safety objectives and safety requirements	• Dissociation of constraints on the system of interest (objectives) from the solutions to satisfy them (requirements) and to identify emerging aspects.
Measures of Importance	• No predefined index (no equivalent to SIL, DAL, ASIL, etc.) • Definition of normative requirements to allow stakeholders defining ad hoc Measures of Importance within a global consistent framework.
Safety performance	• Account 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	• Account for the fundamental difference between the necessary means to achieve safety objectives and the necessary means to guarantee their effectiveness.

Time frame


New Work Item Proposal
2017
PNW IEC 63187
PNW accepted
2018
Work started taking into account the NC comments.
IEC 63187-1 need guidance
2019
IEC TR 63187-2
CD
2022
178 comments
Publication of IEC63187-1 and IEC TR 63187-2
2025
FDIS

Follow us on LinkedIn IEC 63187

Questions

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS