System Safety for Complex and Defence Systems

James Inge
Defence Equipment & Support
Bristol, UK
0009-0001-5481-5091

Katia Potiron
KNDS France
18023 Bourges, France
0009-0008-4631-9187

***Abstract*—Defence capability often requires systems that are complex in technical and managerial terms, and have the potential to cause harm through both inherent hazards and unforeseen interactions of system elements. Moreover, in those cases the risks are often dynamic. Such systems are not well catered for by current safety assurance standards. To address this, the International Electrotechnical Commission (IEC) is developing a new international standard, IEC 63187, that takes a systems engineering approach to safety for complex systems. This position paper summarizes the goals of IEC 63187, its approach, development progress and remaining challenges.**

Keywords—system safety, systems engineering, defence, standardization, IEC 63187

I. Introduction

Modern defence systems are increasingly complex, with complex functions, architectures and supply chains. The level of automation is increasing, and these complex systems are used in diverse environments where risk changes dynamically. Existing safety standards tend not to cater well for these systems: they do not align to the systems engineering approach used to manage complexity, cannot easily be applied to multi-layered systems and supply chains, and do not deal well with safety issues that emerge from interactions between system elements, rather than arising from failures of single system elements [1, 2].

Motivated by these problems, the International Electrotechnical Commission (IEC) is currently drafting a new international standard, IEC 63187, that takes a systems engineering approach to safety. It is being written by Working Group (WG) 18 'System safety in complex systems and defence programmes' of the SC65A 'Systems Aspects' subcommittee of IEC Technical Committee TC65, 'Industrial-process measurement, control and automation.' WG18 has had participants from 10 nations and draws together national experts from industry, government and academia not solely working in the defence sector.

IEC 63187 'Systems engineering – System safety – Complex systems and defence programmes' is being drafted in two parts. Part 1 'Concepts, terminology and requirements,' IEC 63187-1, will be a full International Standard setting normative requirements. Part 2 'Guidance on application,' IEC TR 63187-2, will be a Technical Report offering guidance on applying Part 1. As an international standard, it will not be mandatory for organisations to adopt IEC 63187, but it is being drafted to be suitable for inclusion in contracts between government acquisition agencies and their suppliers, or between suppliers at different tiers of the supply chain.

II. Goals

The goal of IEC 63187 is to provide a comprehensive approach to adapting safety requirements to the level of risk posed by complex systems operated in dynamically changing environments. The standard aims to do this in a way that is agnostic to particular development or assurance activities, and will take account of:

- system elements realised according to traditional processes;
- a heterogenous mix of subassemblies (legacy systems, "off-the-shelf", or bespoke designs); and
- elements of different maturity levels, some at the concept stage, others already in service.

In taking a systems engineering approach to these goals, IEC 63187 aims to be applicable without limitation at different layers of the systems hierarchy and different tiers of the supply chain. It focuses on the conceptual design of a system-of-interest, rather than the realisation of physical or logical system elements, but aims to provide a seamless interface with existing safety standards for development of those elements.

III. Approach

The approach taken by IEC 63187 is built around 8 fundamental principles [1]:

a) Risk: following ISO 31000, focusing on hazards and their consequences, rather than quantitative probability.

b) Systems-based approach: following ISO/IEC/IEEE 15288 with recursive application of multiple processes, technologies and competences at multiple levels in the systems hierarchy and supply chain.

c) Systems and control theory: to manage detrimental interactions between system elements.

d) Safety as an integrated systems engineering discipline: fundamental to meeting overall system requirements, rather than a separate endeavour.

e) Appropriateness of approach: to address different types of threats to safety.

f) Supply chain considerations: for proportionate use in contracts between different tiers of suppliers.

g) Solution-independent: regardless of the life cycle stage or development origin of system elements.

h) Goal-based: providing a framework to identify and achieve safety objectives, rather than a prescriptive set of rules or specifications.

IEC 63187 adopts the systems engineering processes of ISO/IEC/IEEE 15288 with their purposes, activities and tasks. Instead of mandating new processes, IEC 63187 sets additional requirements and criteria on the outcomes of applying the existing processes to safety-relevant systems. Like ISO/IEC/IEEE 15288, IEC 63187 expects a life cycle model to be used, but does not require a particular model, so it can be used equally by organisations implementing agile, spiral or more traditional waterfall development approaches. It has been drafted to be applied recursively throughout the supply chain, rather than just by a government acquisition organisation or internally to a developer. Many of its

requirements relate to agreements that need to be made between suppliers and customers, to define expectations about how work will be done to ensure that systems are safe, and what will be delivered to provide assurance that this is the case [3].

IEC 63187 requires safety objectives to be set at each level of the systems hierarchy, to control hazards that could lead to a detriment (harm to people, or other types of loss). Safety objectives can be met either through architectural decisions or by setting safety requirements, which are decomposed and allocated to system elements. Meeting these requirements becomes an objective for lower-level systems in the hierarchy. Safety analysis at each level examines the effect of implementation decisions and interactions between system elements, which may reveal a need for further safety objectives and requirements, either at the same level, or in higher- or lower-level systems [2].

Under IEC 63187, detriments, hazards, safety objectives and safety requirements have a 'Measure of Importance' (MoI) assigned to them, which expresses how much the customer cares about a given aspect of the system. They are analogous to concepts such as Safety Integrity Levels or Design Assurance Levels in other standards, but are not rigidly defined in IEC 63187. An MoI scheme is agreed between users of the standard, to create an appropriate framework for the context of the system-of-interest [2, 4, 5]. Usage scenarios, allocation drivers and conditioning factors are key concepts of the MoI scheme that offer flexibility and take dynamic risks into account. This allows safety requirements and design criteria to be derived from detriments, hazards and safety objectives in a way justified by the safety strategy.

IV. Development Progress

Development of IEC 63187 started in 2018 under the working title '*Functional safety – Framework for safety critical E/E/PE systems for defence industry applications*.' At that time, the intent had been to produce a domain-specific version of IEC 61508 for the defence industry. As drafting progressed, WG18 realised that a new domain-specific version of IEC 61508 would not ease the issues seen in the market, or be easier for industry to implement. Basing the standard on IEC 61508 would also not favour the systems engineering-based solutions preferred by WG18 to address the issues presented above.

As the old title no longer reflects the approach taken by the standard, it is now proposed to name IEC 63187 '*Systems engineering – System safety – Complex systems and defence programmes*.' This reflects that the standard is based more on ISO/IEC/IEEE 15288 than IEC 61508, and that its scope is not limited to either functional safety or defence systems.

The draft of IEC 63187-1 is now reasonably mature. A formal Committee Draft (CD) was circulated to IEC National Committees (NCs) for comment in September 2022. 178 NC comments were received. These have largely been addressed, and a second CD version was circulated in June 2024, alongside the proposal to continue developing the standard under its new title. At time of writing, the response period had not yet closed, but WG18 plans to resolve comments in time to allow release of a Committee Draft for Vote (CDV) in January 2025. Maintaining this schedule could allow a Final Draft International Standard in October 2025 and publication of the finished standard in early 2026.

It is intended to publish IEC TR 63187-2 at the same time as IEC 63187-1. While the Part 2 draft is currently less mature, as a Technical Report it will be subject to a less onerous review process, meaning it remains feasible to complete both parts of the standard in the same timeframe.

V. Remaining Challenges

Current work is focused on developing the examples in IEC TR 63187-2, so that they provide sufficient guidance to help understand the possibilities offered by the standard and implement it without becoming seen as the only means of compliance.

A particular area of attention is the use of MoIs. As IEC 63187-1 will not prescribe a specific MoI scheme, it is important that users of the standard are able to understand how to agree an appropriate MoI scheme for their application. Demonstration that workable MoI schemes can be constructed will be very important for adoption of IEC 63187 [4, 5].

Other aspects of this work are to provide examples of how the human aspects of systems should be considered alongside the engineered elements [6], how IEC 63187-1 will interact with existing realisation standards through design criteria [4] and the transition of MoIs to importance measures in realisation standards.

Acknowledgment

The authors acknowledge the work of the IEC TC 65 Industrial-process measurement, control and automation / SC 65A Systems Aspects committee / Working Group 18 Functional Safety of IACS in defence applications, which is making IEC 63187 possible.

References

[1] B. Ricque, B. Joguet, V. Brindejonc, N. Semeneri, and K. Potiron, "IEC 63187 : intégrer la sûreté de fonctionnement au sein de l'ingénierie système," in Congrès Lambda Mu 23 "Innovations et maîtrise des risques pour un avenir durable" - 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Paris Saclay, France: Institut pour la Maîtrise des Risques, Oct. 2022.

[2] J. Inge, K. Potiron, P. Williams, and B. Ricque, "IEC 63187: engineering safety into complex defense systems," in Safety in an Agile Environment: the International Systems Safety Conference 2023, Portland OR, USA: International System Safety Society, Aug. 2023.

[3] K. Potiron and J. Inge, "Extending systems engineering for safety-critical defence applications," in 34th Annual INCOSE International Symposium 2-6 July 2024, Dublin, Ireland: INCOSE, in press.

[4] J. Inge and K. Potiron, "A systems viewpoint on the integration of subsystems developed with hetrogenous safety standards", in 19th International Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS2024), in press.

[5] K. Potiron et al., "IEC 63187-1 : définir les Mesures d'Importance pour les systèmes complexe," in Congrès Lambda Mu 24 "Les métiers du risque : clés de la réindustrialisation et de la transition écologique" - 24e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Bourges: Institut pour la Maîtrise des Risques, in press.

[6] A.-S. Smouts and K. Potiron, "Intégration du facteur humain dans l'ingénierie système, approche de l'IEC 63187," in Congrès Lambda Mu 24 "Les métiers du risque : clés de la réindustrialisation et de la transition écologique" - 24e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Bourges, in press.