Progress on IEC 63187: System Safety for Complex Systems in Defence Programmes

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

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

***Abstract*—Defence programmes deliver capability through systems that are often highly complex, combining system elements with diverse, often cutting-edge technologies, involving multiple stakeholders and complex supply chains, and operating in environments with dynamically changing risk. As well as their inherent hazards, such complex systems have the potential for emergent system interactions to cause unexpected hazards. To address the concern that such complex systems are not sufficiently addressed by current safety assurance standards, the International Electrotechnical Commission is developing a new international standard, IEC 63187. The authors have previously introduced the goals and systems engineering approach of IEC 63187. This position paper gives an update on the progress of the draft standard towards publication and an overview of key areas of development.**

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

I. Introduction

Traditional safety assurance standards typically target specific application or industry domains, and therefore make assumptions about the type of system, operating scenario, development lifecycle, regulatory environment or supply chain typically used in those domains. The systems developed under defence programmes are becoming increasingly complex, often combining elements from different technologies and application domains and a mixture of bespoke and pre-developed system elements. They typically involve relationships between an acquiring organisation and one or more suppliers, rather than in-house development, and are often supported by complicated supply chains and stakeholder arrangements.

IEC 63187 is currently being drafted by the International Electrotechnical Commission (IEC) to address these challenges, using a systems engineering approach to manage the complexity of such systems. The standard focuses on conceptual system design, rather than the realisation of physical or logical system elements. In [1], the authors introduced its motivation, goals, principles and approach. Key concepts in IEC 63187 include:

- extension of ISO/IEC/IEEE 15288 life cycle processes to make them appropriate for safety-critical systems by adding requirements and criteria for their outcomes;
- avoidance of detriment (harm) by setting safety objectives to control hazards, and allocating safety requirements to system elements to ensure or assure that these objectives are met [2, 3];
- setting measures of importance (MoIs) for detriments, hazards, safety objectives and safety requirements, to describe the degree of effort and confidence needed for ensuring or assuring safety in different parts of the system architecture [4];
- reaching agreements between the acquiring organisation and the supplier on what is to be done to ensure safety and what will be provided to assure the system is safe to an acceptable level of confidence; and
- provision for recursive application of the requirements of the standard throughout the system hierarchy, and through the supply chain, to the point where it is practical to realise individual system elements [5].

II. Progress towards Publication

When work started on IEC 63187 in 2018, the draft was branded as a functional safety standard and was expected to be a domain-specific version of IEC 61508 for the defence industry. As described in [1], the draft has evolved to encompass a broader scope and align closer to ISO/IEC/IEEE 15288. It now has the full title '*Systems engineering – System safety – Complex systems in defence programmes*.' An updated draft addressing previous comments on the normative part of the standard, IEC 63187-1, was circulated to IEC national committees in June 2024 alongside the proposal to continue development under the new title [6]. Since then, no major changes have been made to the technical approach of IEC 63187-1. Subsequent work has focused on:

- resolving the comments received on the updated draft;
- improving the explanation of concepts in the annexes;
- improving the structure and clarity of requirements, and ensuring that they align with the 2023 edition of ISO/IEC/IEEE 15288;
- strengthening requirements around the treatment of human factors, enabling and interfacing systems, performance measurement and routes to realisation of system elements; and
- making editorial improvements and improving the consistency of terminology and concepts throughout the document.

This process has now finished and at time of writing, a Committee Draft for Vote (CDV) is awaiting release. The current schedule anticipates resolving CDV comments by the end of 2025, with a Final Draft International Standard in early 2026 and publication of the finished standard in mid-2026.

The focus of work is now to complete the guidance in IEC TR 63187-2. Although this is less mature than IEC 63187-1, it is hoped to be published at a similar time thanks to the shorter review process for Technical Report (TR) documents. IEC TR 63187-2 is expected to include:

- a high-level illustration of how IEC 63187-1 concepts could be applied to a practical example;

- examples of safety views that could be used to represent systems being analysed under the standard;
- guidance on application of human centred design and human factors to complex systems;
- guidance on the transition between IEC 63187-1 and the standards used for realisation of system elements; and
- guidance on development of safety objectives and safety requirements over hierarchies of system elements and suppliers.

To aid adoption of IEC 63187 and help potential users decide whether to employ the standard, production of a 'Part 0' is under discussion, similar to IEC TR 61508-0:2005. This could be a short, non-normative document that would give an overview of the concepts of IEC 63187-1, pitched in-between the very high-level descriptions given in the 'principles' clause and the more detailed explanations in the annexes.

III. Areas of development

A. *Measures of Importance*

The MoI concept will be key to understanding how to implement IEC 63187, and frequently generates questions when work on the standard is presented. IEC 63187-1 will require acquirers and suppliers to agree an MoI scheme for a development. The MoI measures which detriments, hazards, safety objectives and safety requirements are most important to the stakeholders for a defined context; the MoI scheme gives the rules for aggregation, decomposition and inheritance of MoI scales and the conditioning factors that raise or lower them according to stakeholder concerns [4]. MoI levels will be initially set using the severity of a detriment for a defined context, then flowed to other safety artefacts. The conditioning factors can reflect societal concerns, stakeholder risk appetite, policies or regulation, or system architecture considerations such as redundancy or the directness of control over a hazard. As well as influencing the assurance rigour and the system architecture and safety requirements at a conceptual level, MoI levels should influence the criteria for realisation of system elements [7]. This could mean transforming the MoI level for a safety requirement to a specific parameter of realisation standard (e.g. a safety integrity level), but might mean setting a variety of parameters to determine how it should be used, how the context of the measure will be understood in the realisation of the system element, or even determining the choice of realisation standard. To avoid over-constraining the solution space and give the opportunity for candidate architectures, design decisions and risk trade-offs, it is necessary to supply more context than a simple scalar MoI level. The MoI scheme should specify the context linked to the MoI scale for each safety artefact, e.g. the conditioning factors and allocation drivers that led to the assigned MoI level, and the usage scenarios in which a measure is valid.

The IEC 63187-1 'general concept and rationale' annex has been strengthened for the CDV to give more explanation of how MoI scales and MoI schemes will be applied. Further guidance is also being developed in IEC TR 63187-2.

B. *Human Factors*

IEC 63187-1 recognises that humans are a vital part of many systems and may often be considered as system elements in their own right, not just operators outside the system boundary. At any life cycle stage, human activities may form part of the system-of-interest or the environment in which it operates and could cause, modify or help control hazards. Throughout IEC 63187-1, requirements and criteria ensure and assure that human roles and responsibilities are considered in the safety strategy and system design, and that human factors (HF) analysis is part of the system engineering process [8]. In IEC TR 63187-2, guidance is being developed to explain the principles of the system safety approach to HF, give guidance on what might typically need to be done to meet the IEC 63187-1 requirements and illustrate how HF analysis can be applied to a practical example.

Broader Application

The scope of IEC 63187 is specifically 'complex systems in defence programmes'. However, the authors believe that there is little in the standard that is specific to the defence domain and that some other domains share the same challenges. The concepts of the standard should be capable of being applied to similarly complex systems in other domains where there is a relationship between a supplier and an acquirer who sets expectations about the level of risk that can be accepted and the confidence required in demonstrating that the system is safe.

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 System safety of complex systems in defence programmes, which is developing IEC 63187. Opinions presented in this paper are those of the authors, rather than the IEC or their employers.

References

[1] J. Inge and K. Potiron "System safety for complex and defence systems," in 43rd International Conference on Computer Safety, Reliability and Security (SafeComp), Position Paper. Firenze, Sep. 2024.

[2] 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 - 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Paris Saclay, France: Institut pour la Maîtrise des Risques, Oct. 2022.

[3] 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.

[4] K. Potiron et al., "IEC 63187-1 : définir les Mesures d'Importance pour les systèmes complexe," in Congrès Lambda Mu 24 - 24e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Bourges: Institut pour la Maîtrise des Risques, Oct. 2024.

[5] K. Potiron and J. Inge, "Extending systems engineering for safety-critical defence applications," in INCOSE International Symposium, vol. 34. Dublin, Ireland: Wiley, Jul. 2024, pp. 199–209. doi: 10.1002/iis2.13141.

[6] IEC Secretariat, "New work item proposal 65A/1122/NP," Geneva: International Electrotechnical Commission, Jun. 2024.

[7] J. Inge and K. Potiron, "A systems viewpoint on the integration of subsystems developed with hetrogenous safety standards," in Computer Safety, Reliability and Security. SAFECOMP 2024 Workshops, A. Ceccarelli, M. Trapp, A. Bondavalli, E. Schoitsch, B. Gallina, and F. Bitsch, Eds., LNCS 14989. Cham: Springer Nature Switzerland, Sep. 2024. doi: 10.1007/978-3-031-68738-9_1.

[8] A.-S. Smouts and K. Potiron, "Intégration du facteur humain dans l'ingénierie système, approche de l'IEC 63187," in Congrès Lambda Mu 24 - 24e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Bourges, Oct. 2024.