

Treating Dynamic Risk and Complexity in IEC 63187

James Inge
National Armaments-
Materiel
Bristol, UK
 0009-0001-5481-5091

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

Joseph Machrouh
Thales Land & Air Systems
94628 Rungis, France
 0009-0002-8470-5130

Odd Ivar Haugen
Det Norske Veritas
Trondheim, Norway
 0000-0002-6513-0362

Abstract—This position paper presents an update on the development of *IEC 63187 – Systems engineering – System safety – Complex systems in defence programmes* and explains several key concepts in its approach. IEC 63187 is a new draft international standard, currently being developed by the International Electrotechnical Commission (IEC). Previous presentations of this work have attracted questions around the treatment of complexity and dynamic risk. The authors explain here how they envisage that these topics will be addressed through application of the standard.

Keywords—dynamic risk, system safety, systems engineering, complex systems, standardization, IEC 63187

I. INTRODUCTION

Drafting of IEC 63187 was prompted by defence industry concern that existing safety assurance standards were not sufficient for the complexity of some military capabilities and did not integrate with the acquisition and development practices used to deliver them. Although aimed at defence programmes, its concepts are generic and may have utility for similar programmes in other application domains. Previous position papers [1], [2] discussed the motivation, goals and general approach of the new standard, but have given rise to questions on its treatment of complexity and dynamic risk.

II. COMPLEXITY

IEC 63187 defines a ‘complex system’ 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”. It explicitly recognises that hazards may emerge from harmful interactions with the environment or between system elements, not just from failure of components or functions. To conform to the standard, emergent properties or behaviour that contribute to hazards must be identified and treated. To facilitate this, IEC 63187 addresses complexity in three main ways:

- Application of a systems engineering methodology. Rather than inventing a new methodology, IEC 63187 defines additional requirements and criteria on the outcomes of the ISO/IEC/IEEE 15288 systems engineering life cycle processes. These are already used to develop complex systems; IEC 63187 ensures that safety is considered thoroughly during the process.
- Recursive instantiation. The new standard is intended to be applied recursively at different levels of a systems hierarchy, with no fixed top or bottom level. This allows choice of an appropriate level of abstraction for analysis of interactions between system elements.
- Goal-based requirements. IEC 63187 does not specify safety analysis techniques. Users can apply the

techniques and guidance that are likely to reveal emergent behaviours in their context. Today this might include System Theoretic Process Analysis [3] or the Safer Complex Systems Framework [4], but other more appropriate or powerful approaches can be used as they become available.

III. DYNAMIC RISK

The evolving complexity of modern systems has exposed critical limitations in traditional risk assessment paradigms, which predominantly treat risk as a static, singular quantity derived from the product of likelihood, L , and severity, S . Dynamic Risk Assessment methodologies have advanced the field by incorporating real-time operational data, key system metrics and environmental variables to continuously update risk estimates [5]. However, they still tend to assume that risk can be distilled into a single, evolving scalar value, as in (1).

$$R(t) = f(L(t), S(t)), \quad R(t) \in \mathbb{R} \quad (1)$$

This reductionist approach fails to address the multi-dimensional and context-dependent nature of risk in systems that simultaneously serve diverse stakeholders, missions, and operational context. Complex systems do not exhibit a monolithic risk profile but rather a plurality of concurrent, context-specific risks that manifest differently for different stakeholders like operators, maintainers, responsible managers, mission planners and the public. Different contexts can also change the acceptability of a given level of absolute risk. For instance, an unmanned air system may present high collateral risk to people in a populated area, moderate operational risk to pilots due to system failures, and low strategic risk to mission success due to redundant fail-safes; these risks coexist simultaneously rather than sequentially.

To resolve this conceptual deficiency, we have to shift paradigm from scalar risk representations to a risk vector model that characterises a system’s risk as a collection of context-dependent values that collectively define its safety posture, (2), over a set of contexts $c1 \dots cn$.

$$R(t) = (R_{c1}(t), R_{c2}(t), \dots, R_{cn}(t)), \quad R(t) \in \mathbb{R}^n \quad (2)$$

The relevant context is not only the external environment, but the system-in-context, including system state and operational modes, mission, humans and the mechanisms by which they interact, roles, responsibilities and authority. The risk vector not only accommodates temporal dynamics (e.g. real-time updates from sensor data) but also spatial and stakeholder-specific variations, enabling a more granular and adaptive safety management framework.

Rather than using a definition based on probability and severity, IEC 63187 uses similar wording to ISO/IEC/IEEE

15288 and ISO 31073: it defines risk as the “effect of uncertainty on stakeholder objectives” [6]. Risk is not used directly to set the level of rigour of the development or safety assurance processes. Instead, Measures of Importance (MoI) are used to direct effort. These are assigned to safety artefacts such as detriments, hazards, safety objectives and safety requirements. The MoI is not just a scalar quantity, but includes contextual information about the scenario of use, the stakeholders involved, or the mode of operation in a complete scheme (MoI scheme) [7].

The CESM metamodel [8] can provide a concise way to structure this context, by representing system behaviour in terms of Composition, Environment, Structure and Mechanisms. From this perspective, dynamic risk is not merely a risk value updated over time, but a changing operational risk picture resulting from changes in the system-in-context. A risk vector may therefore describe the plurality of operational risks, while CESM can help explain why and where the vector changes.

For example, the operational risk picture may change because a component is degraded (Composition), because weather or adversarial behaviour changes (Environment), because authority or responsibility between agents is altered (Structure), or because an operational procedure or control logic changes (Mechanisms). CESM can act as an organising frame for asking: what has changed, where in the system-in-context has it changed, how may it affect the risk vector, and why is this change relevant to assurance or operational decision-making?

IV. PUBLICATION UPDATE

IEC 63187-1 has reached a mature draft status. A Committee Draft for Vote (CDV) was published to IEC National Committees (NCs) in September 2025 [6] and approved in November 2025 [9]. Although the votes were unanimously positive, 394 NC comments were received on the draft, with further editorial comments made by the IEC Secretariat as part of the review process. Work since 2025 has focused on addressing these comments, improving the draft, and preparing a Final Draft International Standard (FDIS).

As amendments have only been made in response to comments on the CDV, the structure and concept of the standard have not changed. Many comments related to general technical and editorial issues, improving the clarity and readability of the standard and ensuring compliance with IEC drafting rules. General themes in the comments included:

- Ensuring that requirements and general concepts are explained well, to avoid ambiguity or areas of potential misunderstanding.
- Improving the clause on requirements for ‘enabling systems’: these are systems such as hardware or software tools and test harnesses that support the system-of-interest for some of its life cycle, but are not part of its operational environment.
- Life cycle stages and activities: explaining how requirements for ensuring and assuring safety apply throughout the life of the system-of-interest.
- Definitions: making sure that these are clear, consistent with other standards, and used consistently within IEC 63187-1 itself.

The FDIS was submitted to the IEC Secretariat in August and is likely to be circulated for voting in October 2026. This could allow final publication in late 2026 or early 2027.

The guidance forming IEC TR 63187-2 has also developed further. This is likely to contain illustrative applications of IEC 63187-1 concepts and sections on safety views, human factors, conformance to IEC 63187-1 and links with other standards. At time of writing, a Committee Draft (CD) is in preparation for release to the IEC.

V. FURTHER WORK

It is intended to refine and update IEC 63187-1 based on practical experience once IEC 63187-1 has been published and deployed. IEC TR 63187-2 is also likely to be developed to contain more extensive practical guidance and to capture emerging thought on topics such as those discussed here.

Development of a ‘Part 0’ introductory document, similar to IEC TR 61508-0:2005, has also been tentatively proposed. It would help explain key concepts from IEC 63187 and allow organisations to evaluate whether the standard might be appropriate for their application. However, work on a draft of this document is unlikely to start before issue of Parts 1 and 2.

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, September 2024.
- [2] J. Inge and K. Potiron, “Progress on IEC 63187: system safety for complex systems in defence programmes,” in 44th International Conference on Computer Safety, Reliability and Security (SafeComp), Position Paper. Stockholm, September 2025.
- [3] N. Leveson and J.P. Thomas, STPA Handbook, Boston, MA: Massachusetts Institute of Technology, March 2018.
- [4] J.A. McDermid, S. Burton, P. Garnett, and R. Weaver, Safer complex systems – An initial framework. London: Royal Academy of Engineering, July 2021.
- [5] A. Raveendran, V.R. Renjith, and G. Madhu, “A comprehensive review on dynamic risk analysis methodologies,” J. Loss Prev. Process Ind., vol. 76, p. 104734, May 2022. doi: 10.1016/j.jlp.2022.104734.
- [6] IEC, “IEC 63187-1: Systems engineering – System safety – Complex systems in defence programmes Part 1 – Concepts, terminology and requirements,” Committee Draft for Vote 65A/1187/CDV, Geneva: International Electrotechnical Commission, September 2025.
- [7] J. Inge, K. Potiron, and J. Machrouh, “Putting importance into context: moving from the abstract to the concrete with IEC 63187,” in AI and Safety Critical Systems - Proceedings of the 34th Safety Critical Systems Symposium, M. Parsons, Ed., York: SCSC, February 2026, pp. 229–243. doi: 10.65391/r3348.
- [8] O.I. Haugen, “A systems approach to modelling emergent behaviour in maritime control systems using the composition, environment, structure, and mechanisms (CESM) metamodel,” in 15th International Conference on Performance, Safety and Robustness in Complex Systems and Applications, Nice: Think Mind, June 2025, pp. 1–8.
- [9] IEC Secretariat, “SC 65A Dashboard / Project: IEC 63187-1 ED1”. https://www.iec.ch/dyn/www/?p=103:38:302024289333186:::FSP_ORG_ID.FSP_APEX_PAGE.FSP_PROJECT_ID:1369.23,126413 (last accessed 1 July 2026).