IEC 63187 – Tackling complexity in defence systems to ensure safety

James Inge

Defence Equipment & Support

Bristol, UK

Phil Williams

Engineer for Safety Limited

Hastings, UK

Abstract *IEC 63187 is the new functional safety framework being developed by the International Electrotechnical Commission for the defence sector. In this sector, applications are typically complex systems, elements of which may themselves be both technically complex and managerially complex systems in their own right: developed by different suppliers, to different standards, and at different stages in their product lifecycles. Defence systems are also subject to dynamic changes of risk, depending on the context of their deployment. Existing safety standards are not well adapted to this level of complexity. They tend to be aimed at single organisations rather than complex hierarchies, and to focus on the failures of system elements, rather than important emergent properties of the overall system. The new international standard in development, IEC 63187, tackles these problems using modern systems engineering principles. It applies the ISO/IEC 15288 life cycle processes to supplement IEC 61508 and other safety standards, proposing an approach that allows requirements to be tailored to the risk and managed across multiple system layers. This framework is designed to be open, for compatibility with different national approaches to assurance and risk acceptance, and with different traditional standards for realisation of individual system elements. This paper discusses the motivation, principles and approach of IEC 63187 and gives an update of the progress of the drafting of the document through the standardization process.*

1 Introduction

The International Electrotechnical Commission (IEC) is currently drafting a new international standard titled 'Functional Safety – Framework for safety critical E/E/PE systems for defence industry applications'. 'E/E/PE' relates to Electrical, Electronic and Programmable Electronic systems, including software and complex electronic hardware. Such systems are increasingly prevalent in defence applications, even in roles where mechanical systems have traditionally been used. IEC 63187 aims to help suppliers demonstrate that complex defence products, systems and services incorporating E/E/PE are acceptably safe for their customers to operate. This paper explains why a new international standard is necessary in this area, and introduces some of the key innovations in its approach.

1.1 The challenge of defence systems

Systems in the defence sector often have characteristics that are not well catered for by existing functional safety standards:

Managerial complexity: Defence applications are often 'systems of systems' in several of the senses used in the Systems Engineering Body of Knowledge, in that the system elements that make them up are separately defined, acquired and integrated (SEBoK 2021). These elements may be a combination of bespoke new developments, off-the-shelf components, customisations of existing designs, and 'legacy' equipment that is already in service. The different elements are often specified and procured separately from different suppliers at different times, and increasingly may be supplied as services rather than traditionally acquired hardware. Hence they may be at different stages in their product life cycles when brought together to deliver an overarching capability. Existing functional safety standards tend to be limited in scope, and are often intended to be applied within a single organisation, rather than across a complex supply chain.

Technical complexity: Major defence capabilities are often made up of a number of system elements that are complex systems in their own right. Since the 1960s, systems engineering techniques have been developed to manage this complexity, in defence and other industries. However, current functional safety standards do not necessarily apply systems engineering principles and anticipate recursive application through a hierarchy of systems. Safety Integrity Levels (SILs) and similar concepts become difficult to apply in complex systems hierarchies: it becomes hard to decompose SILs and assign them over multiple layers of the hierarchy, especially when the different system elements may be managed separately.

There is also a tendency for standards to focus mainly on guaranteeing safety by controlling the impact of failures of individual system elements. However, in complex systems, emergent properties are a concern, and it is possible for systems to behave unsafely without failures of their individual elements.

Dynamic risk: The hazards and potential losses involved in military systems are dependent on the context of operation, and there is a balance to be made between the safety and the capability of the system. While this is true of most systems, the operating context for military systems can change frequently and rapidly during their operation, resulting in changes to safety objectives and trade-offs. For example, changes to the threat posed by hostile actors may mean that it is necessary to compromise some safety objectives in order to complete the mission. There is often an assumption in functional safety standards that the level of risk will remain largely constant.

Customer determination of risk acceptability: in many other industries, the acceptable level of risk is determined to a certain extent by civil regulation; or the organisation supplying the product is able to set their own risk appetite. In defence, often the arbiter of risk acceptability is the organisation acquiring the system, normally a national defence ministry or an agency working on their behalf. Civil safety legislation often explicitly excludes defence systems from its scope, or gives powers to the government to exempt particular applications in the interests of national security. Functions performed by defence systems are sometimes also uniquely military in nature, and not well covered by civil product safety standards. Defence procurement organisations have a dilemma: they are generally held accountable by their government, so need assurance from suppliers that the equipment they procure will be safe to operate. However, they do not wish to overly constrain implementation options, limit operational capability or impose unnecessary costs on their projects.

While all of these characteristics are common in systems found in the defence sector, in practice they could be found in other sectors using complex technology or where the interactions of system elements is complex. IEC 63187 is initially directed at the defence sector; however, there is nothing inherently defence specific in its normative requirements.

1.2 The IEC 63187 approach

When developing a complex system, safety is neither something that can be managed independently, nor the end goal of the system. It is an emergent property of the system as a whole, rather than a separate feature that can be designed in. Similarly, safety is not the outcome of a single technical or managerial process,

but the result of the multi-disciplinary combination of activities that go into designing, manufacturing, deploying and operating the system.

IEC 63187 recognises this, and also recognises that a standardized body of good practice already exists in disciplines like systems engineering, risk and quality management, which may not be specifically aimed at managing safety, but nonetheless supports delivery of safe socio-technical systems. Rather than attempting to duplicate these standards, IEC 63187 builds on them to explain how they can be extended using systems thinking and systems engineering to produce an effective framework for managing the functional safety aspects of a complex system.

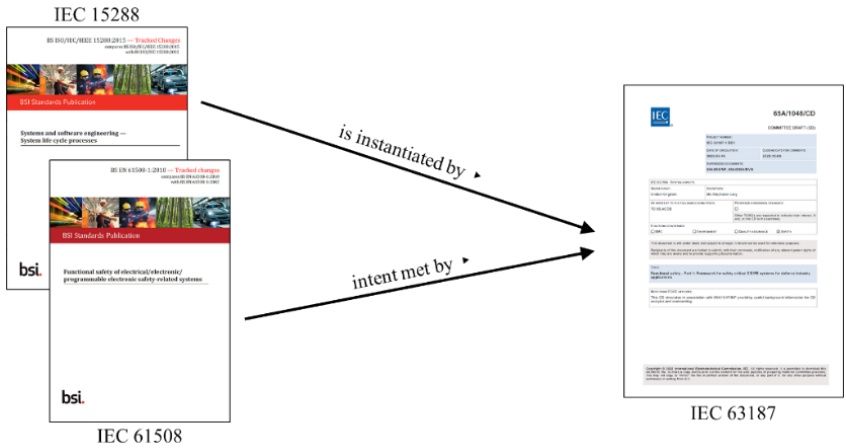

Fig. 1. IEC 63187 pedigree

In particular, IEC 63187 builds on the systems engineering framework of IEC 15288 (IEC 2015). Although IEC 61508 is the 'horizontal standard' or 'Basic Safety Publication' for functional safety of E/E/PE systems[1], the detailed approach described in IEC 61508 is only appropriate for those defence systems that fit the functional concept described in the standard. Instead of building directly on IEC 61508, IEC 63187 aligns more directly to IEC 15288. It takes the concept of systems engineering processes managed within a life cycle framework, and specifies additional requirements on those processes to achieve the intent of IEC 61508 for defence systems. These additional requirements are targeted at ensuring both that the safety objectives for the system will be achieved, and that adequate assurance information will be produced to give the acquiring organisation

[1] Meaning that it gives "fundamental principles, concepts, terminology or technical characteristics, relevant to a number of technical committees and of crucial importance to ensure the coherence of the corpus of standardization documents" (IEC 2022a)

confidence that this is so. Beyond this, IEC 63187 also provides a framework for understanding the interaction between hazards at different layers of the systems hierarchy, and specifying safety requirements on the lower layers.

IEC 63187 does not specify functional safety requirements for the development or realisation of particular system elements. However, it puts in place a framework by which their requirements and safety objectives can be derived. IEC 61508 can still be used under IEC 63187 to realise those system elements for which it is suited. Similarly other standards such ISO 26262[2] or DO-178C[3] could be used, as appropriate to the application domain.

[2] ISO 26262: Road Vehicles – Functional Safety.

[3] DO-178C: Software Considerations in Airborne Systems and Equipment Certification.

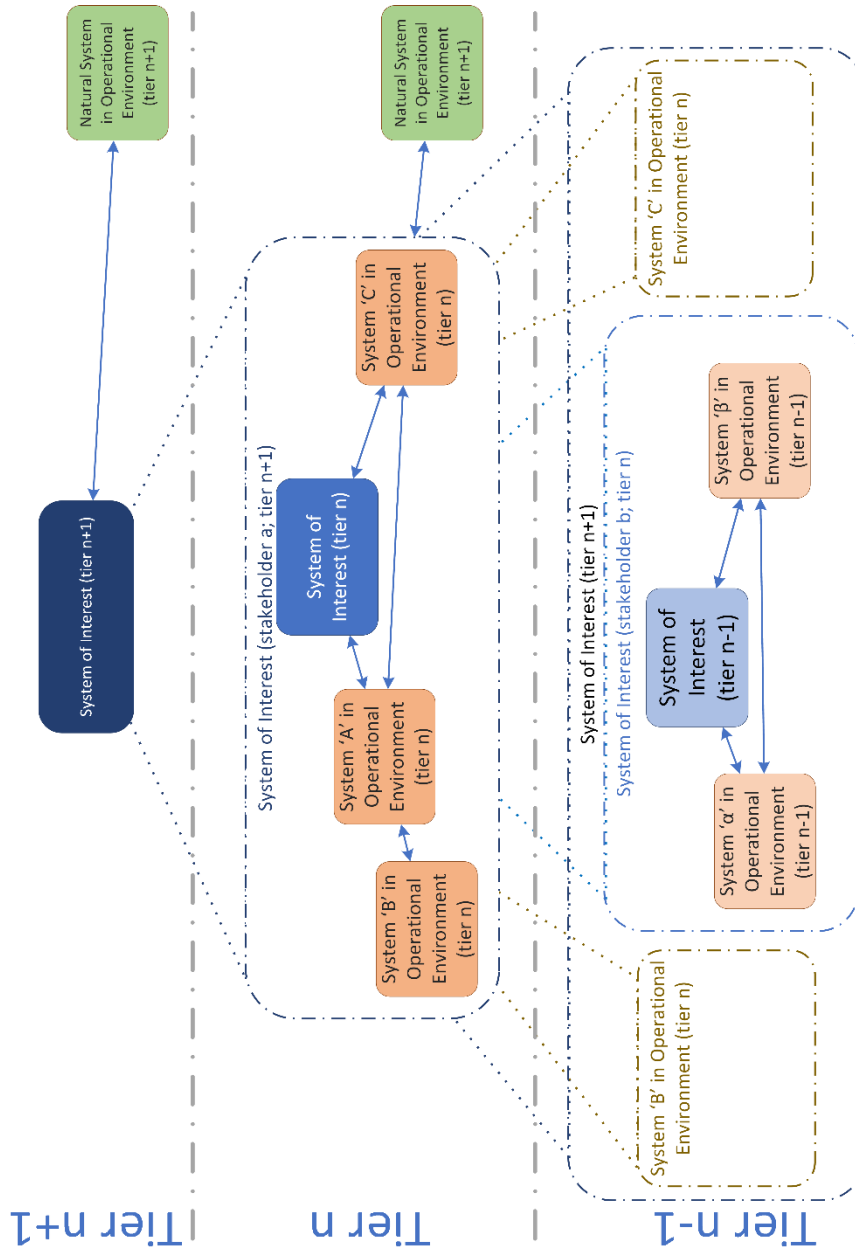

Fig. 2. Hierarchy of System Tiers (IEC 2022)

2 How does IEC 63187 tackle complex systems?

2.1 Recursion and iteration through the systems hierarchy

While traditional standards assume a fixed hierarchy, are intended to be applied to a complete system and have different requirements for different system elements such as hardware and software, IEC 63187 explicitly recognises an abstract, flexible, systems hierarchy. As shown in Fig. 2, at each tier of the hierarchy, there is a bounded 'system of interest' operating within a certain environment[4]. The environment is outside the scope of the engineering control for the system of interest. If aspects of the environment do need to be engineered, then a higher tier can be added to the hierarchy with those aspects included in the scope of the higher-tier system of interest. The system elements composing a system of interest can either be considered as atomic units that can be realised directly and do not need further analysis, or they could be considered as systems in their own right, and analysed in a lower tier in the hierarchy. The system of interest forms part of the operating environment for systems in the tier below. This hierarchic approach allows the management of complexity by allowing the detailed design of individual system elements to be abstracted, allowing analysis at a higher level. This approach allows systems to be considered at a high-level tier that are in the operational domain and inclusive of people, aspects of the natural environment and technological systems.

IEC 63187 is intended to be applied recursively throughout the hierarchy until the bottom tier, where more specific requirements can be set for realisation of particular system elements. Depending on the systems breakdown and supply chain involved, individual participants may apply the standard at multiple tiers, or just one. This approach allows systems to be considered at differing levels of abstraction, and of aggregation of disparate physical elements. These facilitate the use of the standard from early concept stage through to in-service operation, and beyond. They also allow for the standard to be applied throughout the supply chain from a user with the need for a capability, through its acquisition agency right through to suppliers of system elements.

[4] In practice there can be many systems of interest at each tier, each of which may have a different 'owner' of that interest.

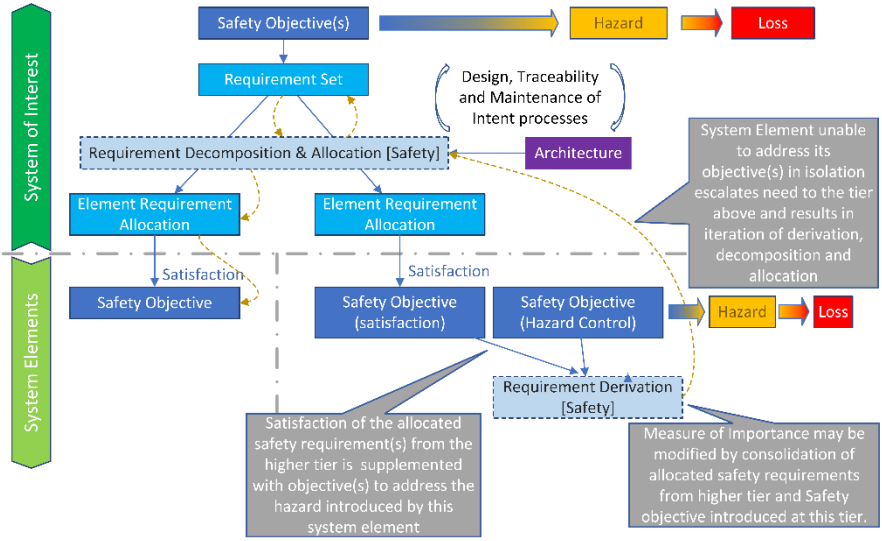

Fig. 3. Derivation of safety objectives and requirements (IEC 2022b).

At each tier of the system, safety objectives for the system element of interest are expected to be set to allow it to satisfy safety requirements set by the tier above, as shown in Fig. 3. In turn, that tier will set safety requirements to be met by the objectives of lower-tier system elements. In this way, requirements are derived for the bottom-tier system elements that can be traced back to achievement of the top-level functional safety objectives for the overall system.

New hazards can also be introduced at any system layer. They could result from failure modes of systems elements, deliberate implementation choices, or unintentional interactions between system elements. Such hazards may well not be present in lower-tier system elements, but only emerge through integration. IEC 63187 requires analysis to take place to reveal whether such hazards are present and further safety objectives to be set to control them. In some cases, these hazard control objectives may be discharged by setting safety requirements on lower-tier system elements. In others, this will not be feasible, and it will be necessary to iterate the requirement setting activity for the tier above. This may result in additional safety requirements being placed on other system elements, or even generate a need for a new system element to control the hazard. In this way, IEC 63187 seeks to address emergent hazards.

2.2 Risk Model

IEC 63187 adopts the ISO/IEC/IEEE 15288 view of risk as 'the effect of uncertainty on stakeholder objectives'. It does not use the traditional measure of risk as a function of the likelihood and severity of an outcome as this is not necessarily helpful in the context of safety analysis in an abstract systems hierarchy.[5] The likelihood/severity approach also does not lend itself to dynamic risk scenarios, where the probability and severity can be expected to change more frequently than the analysis can be carried out. Instead, IEC 63187 focuses on uncertainty in the control of hazards, which are defined as system states or sets of conditions that, together with a particular set of environmental conditions, will lead to harm. Hazards are 'owned' and managed at the tier of the systems hierarchy in which they are necessarily introduced, for example by the choice of a particular technology to implement a system element. Where a hazard is identified, safety objectives are set to control the impact of this hazard and prevent it resulting in harm or loss. Requirements are then set and allocated to system elements to ensure that the safety objective is met. This approach lends itself to application of control theory and systems engineering-based techniques such as System-Theoretic Process Analysis (STPA) (Leveson and Thomas 2018).

Aside from being used to judge the tolerability of potential accidents, traditional standards use the likelihood/severity risk metric to define the level of rigour required in designing particular parts of a system, or the level of confidence required that particular requirements have been achieved. As IEC 63187 does not use this risk metric, it has to propose an alternative method to determine where effort should be prioritised to control hazards and provide assurance. To do this, it introduces the concept of a 'measure of importance'.

2.3 Measures of Importance

The IEC 63187 concept of a 'Measure of Importance' (MOI) describes the degree of confidence required when ensuring or assuring safety. It plays a similar role to concepts like Safety Integrity Levels (SILs) or Design Assurance Levels

[5] For example, it is not possible to assess the risk due to failure of a subsystem such as an electronic control unit (ECU) as an isolated system: it is necessary to understand the rest of the system in which the ECU operates, like a vehicle or aircraft, to understand the likelihood that failure of the ECU could propagate to a hazardous state in the top-level system. Further information is needed about the operating environment to understand the likelihood that an accident might result, and the severity of the harm caused. Such an analysis may be feasible in relatively simple systems using techniques such as Failure Modes and Effects Criticality Analysis (FMECA), but it is not feasible in more complex systems, where system elements are being independently developed and information about the higher system tiers is not available.

(DALs) in other standards, in defining the level of rigour to be applied in different systems engineering processes. The MOI concept is however more flexibly defined, to enable it to be recursively applied at different system layers. In fact, although it provides an example in an informative annex, IEC 63187 does not define a specific MOI schema, but requires one to be drawn up as part of the safety acceptance strategy and agreed between the acquirer and supplier. This allows the concept to be tailored to align to national legislation or regulatory requirements, and to reflect particular concerns of the acquirer. For instance, the schema can prioritise harm to humans as more important than financial loss, seek extra rigour for particular types of hazard that cause societal concern (e.g. radiological hazards), or require extra scrutiny for particular technologies.

Measures of importance can be applied to hazards, safety objectives and requirements, potentially with different scales for each. The MOI for a hazard will be based on the severity of the associated loss, conditioned by factors such as the organisation's risk appetite in different operational contexts. While likelihood of the loss would but not be taken into account directly, the degree of contribution of the hazard to the loss could also be a conditioning factor[6]. Hazard MOIs are used to set MOIs for associated safety objectives, which in turn are used to set MOIs for their supporting safety requirements, again with conditioning factors taken into account. These conditioning factors allow the MOI schema to reflect the overall safety strategy for the system, trade-offs between safety, capability and other concerns, and the importance of different system elements to the overall architecture. The allocation of MOIs to safety requirements means that there will be a flow down to lower-level system tiers. However, a translation may be necessary, as these tiers may use different MOI schemas. At the bottom system layer, there will also need to be a translation from the MOI schema to measures specific to the chosen implementation standards, such as SILs or DALs.

MOIs are a powerful and flexible concept, but have the potential to be confusing to use in practice. If MOI schemas are not set up appropriately, then application of IEC 63187 may not result in the acquirer gaining the assurance of safety that they desire. This should not be an insurmountable challenge. Acquirers already have to set their expectations for the level of assurance provided by their supply chain, but IEC 63187 makes the requirement more explicit. However, the success of the standard in this respect may well rest on the strength of the guidance available to help implementers to define practical MOI schemas.

[6] 'Conditioning factors' are factors that may influence the allocation of a measure of importance, to allow a higher or lower MOI to be allocated in particular cases. IEC 63187 does not define a particular set of conditioning factors, but allows the organisation using the standard to define them as part of their MOI schema. They might include factors such as the type of people at risk (civilian / military / enemy), the type of operational scenario involved (training vs military operations), or the degree of contribution of a safety objective to the overall safety architecture.

3 Relationship to UK Defence Standards

As an international standard, IEC 63187 needs to be capable of application in any country. This means that it has to remain independent of the requirements of particular legislative or regulatory jurisdictions or acquisition regimes, so will not reference particular national defence standards. It will also not necessarily align directly with the vocabulary in use in different countries, since this varies and common terms like 'hazard' can be interpreted differently, even in countries that share the English language (McDermid 2007). Instead, it will build on the common vocabulary used in other IEC and International Organization for Standardization (ISO) standards. However, development of IEC 63187 has been informed by knowledge of various national defence standards and the thinking behind them.

Notably, the conformance requirements of IEC 63187 have been derived from the same software safety assurance principles originally developed by (Hawkins et al. 2013), which feature as programmable element safety requirement principles in Def Stan 00-055 and Def Stan 00-056. This means that IEC 63187 takes a similar approach to assurance to the aforementioned Def Stans, and to other material based on similar principles, such as the Service Assurance Guidance (SAWG 2022). IEC 63187 also includes the concept of a 'safety case', albeit as a placeholder for all the information generated over the system lifecycle to show satisfaction of the standard. While not calling explicitly for a safety argument, the standard requires various claims to be documented in the safety case, and requires the acquirer and supplier to agree a safety acceptance strategy. This strategy allows the flexibility to specify the need for an explicit safety argument, or other nation-specific assurance requirements. This is intended to allow IEC 63187 to remain compatible with the UK's Def Stan 00-055, the US Mil-Std-882E, and other nation's safety management standards. It can also support the philosophy that only the Duty Holder responsible for operating a system safely is positioned to make claims about the overall safety of the deployed system, taking into account the operational environment and other lines of development, such as training or doctrine. In this context, the information provided through application of IEC 63187 does not provide the overall safety case itself, but supports the overall safety case made by the Duty Holder, when combined with arguments from other areas of their safety management system.

As the UK Ministry of Defence (MOD) has a policy of selecting civilian standards wherever practicable and military standards only where necessary, and prefers international standards to national or military ones (MOD 2022), there is likely to be interest in assessing whether IEC 63187 could replace Def Stan 00-055 and 00-056. While it is hoped that IEC 63187 will provide a convenient means to demonstrate compliance with those standards for complex systems, it is unlikely to replace them. As it only covers functional safety, IEC 63187 does not cover the complete scope of Def Stan 00-056. And for some less complex

systems, it may be more appropriate to continue using implementation standards such as IEC 61508 directly.

For military systems within the scope of IEC 63187, there is still a compelling reason to retain the use of Def Stans: IEC 63187 has various requirements for the acquirer to define the interface between it and the supplier. This includes specifying the acquirer's requirements for a safety strategy and safety acceptance strategy (including the MOI schema), any particular methods or techniques the supplier is required to apply, and the safety artefacts they are to deliver. It also includes reaching agreement with the supplier on issues such as the MOI schema to be applied, or the compliance routes for already-realised system elements. Some of these points are project-specific, but others can be generic to a particular acquirer. For instance, internal regulations in a defence ministry may require particular safety artefacts to be generated. For this reason, the MOD is likely to wish to retain the use of Def Stans in some form, to standardize its approach to meeting these IEC 63187 requirements.

IEC 63187 could also be applied at tiers higher than that at which MOD procures systems, as part of understanding and managing the emergent interactions between systems it procures, or as part of studying the end user's needs and selecting suitable new procurement items to fit alongside existing systems to deliver the required capability.

4 Development progress

IEC 63187 is being developed under IEC Technical Committee TC65 (Industrial-process measurement, control and automation), by Subcommittee SC65A – Systems Aspects, the same part of the IEC that maintains IEC 61508. The Working Group drafting IEC 63187 (IEC SC65A WG18) has been meeting since 2018 and currently includes representatives from ten nations. It is drafting the standard in two parts. IEC 63187-1 will contain the normative parts of the international standard, along with informative material including an annex on the concepts and rationale of the standard. Further guidance will be provided in IEC TR 63187-2.

At the time of writing, IEC 63187-1 has been circulated as a Committee Draft (CD) for comments by IEC Members, i.e. national standards committees. The draft will be updated during 2023 based on the comments received, and is planned to be circulated as a CD for an approval vote (CDV) in early 2024. Assuming that the CDV is approved but further technical comments are made, it is likely to be issued as a Final Draft International Standard (FDIS) in late 2024 and eventually published in 2025.

Drafting has started on the supporting guidance in IEC TR 63187-2. This part of the standard will have the status of a Technical Report rather than a full International Standard, meaning that it is entirely informative, rather than setting any

normative requirements. Technical Reports have a more flexible approval route, meaning that there is scope to shape the Part 2 guidance to address comments raised against Part 1 of the standard, and still publish both parts at the same time.

Disclaimer Views expressed in this paper are those of the authors and not necessarily those of the Ministry of Defence or the International Electrotechnical Commission.

References

Hawkins RD, Habli I, Kelly TP (2013) The principles of software safety assurance. In Proceedings of the 31st International System Safety Conference. International System Safety Society. Available: https://www-users.cs.york.ac.uk/rhawkins/papers/HawkinsISSC13.pdf. Accessed 3 September 2022

IEC (2010) IEC 61508 series – Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission

IEC (2015) ISO/IEC/IEEE 15288:2015 – System and Software Engineering – System life cycle processes. International Electrotechnical Commission

IEC (2022) Committee Draft 65A/1048/CD. Functional safety – Part 1: Framework for safety critical E/E/PE systems for defence industry applications. International Electrotechnical Commission

IEC (2022a) Horizontal Standards. International Electrotechnical Commission. https://www.iec.ch/news-resources/horizontal-standards. Accessed 2 October 2022

IEC (2022b) IEC 63187-1 Functional safety – Framework for safety critical E/E/PE systems for defence industry applications – General presentation for CD circulation. TC65/SC65A/WG18. International Electrotechnical Commission

Leveson NG, Thomas JP (2018) STPA Handbook. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. Accessed 17 September 2022

McDermid JA (2007) Comparison of MilStd 882E and Interim Defence Standard 00-56 Issue 3. In Gonzalez AM (Ed.), Proceedings of the 25th International System Safety Conference

MOD (2022) JSP 920 – MOD Standardization Management Policy – Part 1: Directive, Ministry of Defence. https://www.dstan.mod.uk/policy/JSP920_Part1.pdf. Accessed 3 September 2022

SAWG (2022) SCSC-156B – Service Assurance Guidance version 3.0. Safety Critical Systems Club Service Assurance Working Group. https://scsc.uk/r156B:1

SEBoK contributors (2021), System of Systems (SoS) (glossary), SEBoK. https://www.sebokwiki.org/w/index.php?title=System_of_Systems_(SoS)_(glossary)&oldid=65565. Accessed 2 October 2022.