

Gaining system safety assurance through conformity to IEC 63187-1

James Inge¹[0009-0001-5481-5091], Katia Potiron²[0009-0008-4631-9187] and Phil Williams³

¹ National Armaments – Materiel, Bristol, UK
james.inge@scsc.uk

² KNDS France, 18023 Bourges, France
katia.potiron@knds.fr

³ Engineer for Safety Ltd, East Sussex, UK

Abstract. IEC 63187-1 is a forthcoming international standard that seeks to improve the safety of complex defence systems by embedding system safety within systems engineering practice. Rather than specifying particular technical solutions or system properties, it adopts a goal-based approach, setting requirements and criteria on the outcomes of systems engineering processes. This work examines what it would mean in practice to cite IEC 63187-1 in a contract, and how conformity to the standard could be demonstrated in a way that provides meaningful safety assurance to both acquirer and supplier. It explains how conformity to IEC 63187-1 would differ from traditional product certification, and why IEC 63187-1 cannot be treated as a simple conformance ‘badge’. The authors explore the role of the agreement processes, the treatment of relevant requirements and tailoring, the use of acceptance strategies and safety cases, and the challenges posed by outcome-based conformity assessment. The paper concludes that citing IEC 63187-1 in a contract places significant but constructive obligations on both parties, requiring increased up-front clarity and collaboration in return for improved transparency and confidence in system safety outcomes.

Keywords: complex systems, systems engineering, system safety, conformity assessment, IEC 63187.

1 Introduction

1.1 IEC 63187 – a New Standard for System Safety of Complex Systems

IEC 63187, titled “Systems engineering – System safety – Complex systems in defence programmes,” is a proposed new international standard currently being drafted by the International Electrotechnical Commission (IEC) to improve the safety of complex defence systems. It is being written in two parts: IEC 63187-1 will be a full international standard, covering concepts, terminology and requirements, while supporting guidance will be given in the non-normative Technical Report, IEC TR 63187-2. The development is industry-led and predominantly European, however the working group writing

This version of the contribution has been accepted for publication, after peer review (when applicable) but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections.

The Version of Record is available online at: https://doi.org/10.1007/978-3-032-35506-5_41. Use of this Accepted Version is subject to the publisher’s Accepted Manuscript terms of use:

<https://www.springernature.com/gp/open-research/policies/accepted-manuscript-terms>

the standard also includes academic and governmental representatives, with participation from nations such as Australia, China, Japan and the US.

As described by Ricque et al. [16], the creation of IEC 63187 was motivated by the perceived shortcomings of existing safety assurance standards in addressing the technical complexity of modern systems, and the complexity of the management and supply chain arrangements used to deliver them. Such systems often deliver capability through a combination of newly developed and existing legacy system elements, drawing from multiple technology domains or industry sectors, and are deployed in wide ranging scenarios where the level of risk changes dynamically and cannot meaningfully be quantified at design time. Many of the available safety assurance standards are written around assumptions that are appropriate for their intended application, but make it difficult to apply them to these complex systems. These include assuming that the level of required risk reduction will remain constant, that a particular system of regulatory oversight will be in place, or that there will be particular relationships between system designers and operators. They also tend to use mechanisms (like the Safety Integrity Levels (SILs) in IEC 61508 [3]) that can appear nominally similar between standards but are generally incompatible [6]. A key shortcoming of many of these standards is that they are not designed to integrate with modern systems engineering practice.

IEC 63187 is not intended to replace these other standards, but to bring them together in a framework that allows the power of systems engineering to be used to help manage complexity. It does this by building on the systems engineering life cycle processes described in ISO/IEC/IEEE 15288 [11]. It is intended to be used at the level of systems architecture, to prompt analysis of the interactions between system elements that could lead to unwanted emergent behaviours, and to enable requirements to be set to control them. IEC 63187 can be applied recursively at any level of a systems hierarchy, down to the point at which it is necessary to realise individual system elements. At this point, it assumes that familiar ‘realisation standards’ will be used, such as IEC 61508 [3] for programmable electronics or ISO 26262 [9] for automotive system elements; these would be chosen to be appropriate for the technology domain of the system element [7]. In this way, IEC 63187 bridges the gap between high-level systems architecture and realisation of individual elements.

Similarly, IEC 63187 is not expected to replace defence safety standards such as the US MIL-STD-882E [2] or the British Defence Standard 00-056 [15]: defence ministries are likely to continue to use their own standards to express their own national requirements, which will vary due to different legal regimes, especially with regard to acceptance of risk. However, IEC 63187 could be used at a higher level – to help set requirements for elements of a complex system that will be procured through separate contracts, or at a lower level – to help a prime contractor demonstrate that a complex system is sufficiently safe.

Although IEC 63187 is being written for the defence sector, its requirements are generic in nature. Its principles are likely to be applicable to development of other complex systems that exhibit similar challenges outside defence programmes.

1.2 The Need to Demonstrate Conformance to IEC 63187-1

A key feature of the standard is that it is built around an explicit relationship between an ‘acquirer’, the organisation that acquires or procures a system; and a ‘supplier’: the organisation that provides the system, or some of its elements. Although the acquirer and supplier could be two parts of the same organisation, such as the capability development directorate and the procurement directorate within a national defence ministry, it is likely that they will be two separate entities, with a commercial relationship governed by a contract. The acquirer and supplier might be a national defence ministry their prime contractor, or a contractor and one of their lower-tier subcontractors. The standard is designed to be applied recursively at any level of the supply chain.

In such a contractual relationship, a responsible acquirer will wish to be assured that the system that they are buying is adequately safe to protect their stakeholders’ interests and that it is appropriate to pay the supplier. Conversely, the supplier will wish to know that they have done enough to achieve acceptable levels of safety, both to justify their claim for payment and to reduce the risk of future costs or reputational damage should the safety performance of the system not be as intended. Unfortunately, it is difficult to measure safety performance directly and test whether the safety effort has been adequate. Demonstrating empirically that rates of harmful events are sufficiently low may require lengthy in-service experience [13]. Demonstrating safety through testing is made more difficult by the fact that defence systems are often expected to operate in a wide range of different scenarios, and that when these systems are complex, they may demonstrate emergent behaviour: unexpected behaviours that cannot be predicted from analysis of the individual system elements, caused by interactions between those elements or between the system-of-interest and other systems or the environment. For these reasons, sufficiently extensive testing in a full range of representative scenarios will typically be impractical. The acquirer and supplier need a different method of judging that enough has been done, a method that can deliver an answer within the time-scales required by their contractual payment plan.

Using a standard like IEC 63187-1 provides a potential solution. Its authors believe that, once published as an international consensus standard, the standard will represent recognised good practice in system safety engineering for complex systems. The premise is that if its requirements are complied with, it will lead to provision of assurance that the system is (or will be) acceptably safe. This would allow the challenge of directly demonstrating the safety of the system to be replaced by the – hopefully more tractable – challenge of demonstrating conformity to the standard: showing that its requirements have been met in the real world.

At time of writing, IEC 63187-1 has reached the Committee Draft for Vote (CDV) stage of approval [4] and a Final Draft International Standard (FDIS) is being prepared. As it approaches readiness for final publication, it is timely to ask what it will mean to include IEC 63187-1 in a contract. What will a supplier have to do to conform, how will they demonstrate that they have done so, and what assurance will conformity give to the acquirer?

This paper adopts an analytical approach based on interpretation of the IEC 63187-1 CDV. The analysis focuses on implications for contractual application and conformity assessment, rather than empirical evaluation.

1.3 Challenges in Demonstrating Conformity to IEC 63187-1

IEC 63187-1 takes a different approach to system safety than many other standards. It does not specify particular properties of a system-of-interest that if ensured, will result in an acceptable level of safety. Instead, it takes the view that if the right outcomes are achieved by the processes that are used to engineer the system, then it will give confidence that a safe system is likely to result. As the discipline of systems engineering has been developed to manage the engineering of complex systems, IEC 63187-1 adopts the systems engineering processes from ISO/IEC/IEEE 15288 – System and software engineering – System life cycle processes [11]. It does not add new tasks, activities or outcomes to these processes. Instead, IEC 63187-1 sets requirements and criteria on the existing systems engineering process outcomes in ISO/IEC/IEEE 15288. These are intended to ensure that safety is considered appropriately through the architecting and management of the system design, throughout its life cycle. This relationship between the standard means that conformance to IEC 63187-1 implies a requirement for conformance to ISO/IEC/IEEE 15288, at least to the level of outcomes (see section 2.2).

This approach is goal-based: rather than specifying exactly how each process should be carried out, which activities should be implemented, which techniques should be used or what documents should be produced, IEC 63187-1 requires the acquirer and supplier to reach agreement on what will be done. Instead of giving detailed implementation guidance, IEC 63187-1 sets out how the outcomes required by ISO/IEC/IEEE 15288 should take safety into account and gives criteria to test whether this has been achieved.

For example, one outcome of the ‘design definition process’ described in ISO/IEC/IEEE 15288 is that “interfaces between system design elements comprising the system are defined” [11]. The IEC 63187-1 CDV places a requirement on this outcome that “safety relevant aspects of interfaces between system elements are defined” [4], but does not state exactly how this should be done. Instead it gives criteria to help determine whether the outcome has been achieved: the definition has to include safety constraints on system design element interfaces, emerging hazards, and relevant aspects of interfaces between the system design elements, human system elements and humans external to the system. This makes the requirement testable, without being prescriptive.

The IEC 63187-1 approach is a very flexible: it allows the acquirer and supplier to choose the precise activities that are carried out to be appropriate for their circumstances and for the context of the system itself. Guidance such as the Safer Complex Systems Framework [14] could be used to inform the exact choice of methodology, or more recent guidance could be used as it becomes available. The standard also allows for whatever life cycle model to be used that the organisations find suitable, and for newer, more powerful tools and techniques to be adopted as they become available. This is particularly important to allow IEC 63187 to be deployed in developing areas of

technology such as artificial intelligence, where standards are rapidly evolving. However, this flexibility makes conformity assessment more challenging.

It is tempting for acquirers and suppliers to look for certification of conformity to a standard, issued by a reputable certification scheme as a ‘badge’ that will indicate that a product or supplier is good enough. ISO/IEC 17000 describes a ‘certification scheme’ as a type of conformity assessment scheme, i.e. a set of rules and procedures that identifies specified requirements, describes the entities those requirements will be applied to and provides the methodology for determining whether they conform [10]. Conformity assessment is used to determine whether products, systems, services or people conform to a standard or specification [5].

It is not appropriate to attempt to certify a system against IEC 63187-1 in the same way that products may be certified to conform to standards such as IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems [3]. While IEC 63187-1 does set clear requirements and criteria, they apply to the process by which systems are engineered and do not specify testable properties of the system itself.

It could however be possible to certify the systems engineering processes used by a supplier, in the manner in which the processes forming a quality management system may be certified to conform to standards like ISO 9001 – Quality management systems – Requirements [8], or to certify the organisation’s capability to deploy their processes. This would pose challenges. IEC 63187-1 is intended to be used as a flexible framework for planning safety engineering activity, rather than a rigid set of processes, so it does not provide a fixed set of rules to certify against. ISO/IEC/IEEE 15288, on which it is based, also allows considerable variation in conformance. Nonetheless, although organisations are not typically certified against ISO/IEC/IEEE 15288 [17], the standard does include an informative process reference model to support assessments, and some organisations do advertise an ISO/IEC/IEEE 15288 certification service. A similar approach could be taken for IEC 63187-1.

While an organisational assessment of conformity to IEC 63187-1 could give evidence of the organisation’s capability to use the standard, the fact that IEC 63187-1 calls for the acquirer and supplier to make agreements about their safety strategy means that certifying a supplier in isolation does not give strong assurance about whether a particular implementation of the standard will conform. The outcome-based nature of both IEC 63187-1 and ISO/IEC/IEEE 15288 mean that the methodology needed to demonstrate conformity will need to concentrate on testing that the outcomes are met, rather than that a particular set of activities has been carried out; what this means in practice may vary from system to system and will need to be agreed between the acquirer and supplier as part of the Agreement Processes.

2 What Does “Conformity to IEC 63187-1” Mean?

2.1 Requirements and Criteria

According to Clause 6 of the CDV, conformance to IEC 63187-1 means that “all the relevant requirements will have been satisfied to the required criteria specified and

therefore, for each relevant clause and sub clause, all the normative clause objectives have been met” [4]. What does this mean in practice?

Under the goal-based principle of its design, the normative clauses in IEC 63187-1 set out their objectives and define clear requirements and criteria to allow those objectives to be satisfied. Conforming to the standard means meeting these requirements to at least the level specified in the standard. More specifically, conformity requires not just that relevant objectives are satisfied, but that they are demonstrated to be satisfied: this is the first requirement of Clause 6.

Most of the requirements in IEC 63187-1 are not requirements for the system-of-interest itself. Instead, they are intended to result in the establishment of an effective system safety framework as an integrated part of the broader systems engineering effort. To actually improve safety, it is necessary to put this framework into effect. Hence Clause 6 also contains a requirement that a claim of conformance also entails that the following outcomes shall be achieved:

- Safety hazards of relevance to the system-of-interest are identified.
- Requirements on the system, its operation and throughout its life cycle stages to address the contribution to hazards through causal or control aspects, are generated.
- The decomposition and allocation of requirements, including to enabling systems, maintains their effectiveness in addressing contribution to hazards.
- Emergent properties/behaviour of the system implementation/operation that contribute to hazards are identified and treated.
- The system requirements addressing system contribution to hazards are satisfied.
- The confidence obtained in addressing the above is commensurate to the system’s contribution to risk, and it is assured that this confidence is maintained throughout the life of the system.

The above criteria capture the key purpose of IEC 63187-1: to provide assurance that that hazards associated with a system are identified (including emergent hazards arising from interactions in complex systems), that requirements are set to control the hazards, and that those requirements are satisfied.

2.2 Relevant Requirements and Tailoring

In addition to the flexibility allowed in deciding how to conform to the requirements of IEC 63187-1, there are several other areas of variability, concerning with which requirements it is necessary to conform:

- the selection of which requirements are relevant;
- the choice of whether to implement systems engineering processes at the level of tasks or outcomes; and
- the tailoring of requirements.

The concept of IEC 63187-1 is to enhance the systems engineering processes described in ISO/IEC/IEEE 15288 [11]. However, ISO/IEC/IEEE 15288 recognises that not all its processes will be relevant to every system development. It therefore allows

conformity to be claimed to a declared subset of those processes. This relevant subset may be influenced by factors such as the scope of what the supplier is contracted to provide. If a particular ISO/IEC/IEEE 15288 process is not relevant to the systems engineering effort, then it is likely that the corresponding requirements in IEC 63187-1 will not be relevant either. IEC 63187-1 recognises this and therefore only requires satisfaction of ‘relevant’ clauses. However, it requires that the selection of which requirements are considered relevant is made explicit and justified with regard to safety.

ISO/IEC/IEEE 15288 allows claims of either ‘full’ or ‘tailored’ conformance to be made. Full conformance may be declared either at the level of the tasks prescribed by the relevant processes, or the outcomes that they are intended to achieve. Opting for conformance to outcomes gives more flexibility to innovate instead of being constrained to standard tasks, while conformance to tasks can give the acquirer more understanding of the supplier’s processes. IEC 63187-1 sets its requirements and criteria at the level of process outcomes, rather than modifying the ISO/IEC/IEEE 15288 activities and task. This means that the choice of conformance to tasks or conformance to outcomes does not directly affect IEC 63187-1 conformity, although the variability in how outcomes are achieved increases the difficulty in certifying against the standard. To ensure that the supplier has adequate understanding of the safety implications of the processes in either case, IEC 63187-1 contains various requirements for the standards, methods and techniques that will be employed to be documented and agreed between the acquirer and supplier.

As an alternative to full conformance, ISO/IEC/IEEE 15288 also allows tailored conformance to be declared, in which case the task requirements, activities or outcomes for the relevant processes may be modified, deleted or not fully achieved. This may affect which IEC 63187-1 requirements are relevant or imply the need for corresponding tailoring. IEC 63187-1 allows such tailoring to take place, but the scope of the tailoring must be justified and agreed by the acquirer and supplier. Tailoring can diminish the value of a conformity claim, because it can make it harder to understand what will actually be done, and to justify that it is appropriate good practice.

2.3 Demonstrating Conformity

IEC 63187-1 does not stipulate how the acquirer and supplier should demonstrate that its objectives and requirements have been satisfied. Instead, the standard requires a safety acceptance strategy and a set of necessary safety-relevant deliverables to be agreed between the acquirer and supplier, as part of the systems engineering Agreement processes. However, the requirement for satisfaction to be demonstrated explicitly implies a need for a safety case approach as part of the safety acceptance strategy.

The standard defines a ‘safety case’ as “all information from the system-of-interest life cycle which is pertinent to the demonstration of the satisfaction of the requirements of this document,” but does not define how this information should be structured or presented. It would be possible to deliver the safety case as an unstructured set of documents, or a simple compliance matrix listing the requirements against references to the evidence of their satisfaction. However, this may not be especially easy for the acquirer to interpret and gain useful assurance information from.

The IEC 63187-1 definition is also compatible with the interpretation of a safety case as a specialisation of an assurance case: an “auditable artefact that provides a convincing and sound argument for a claim on the basis of tangible evidence under a given context” [12], or less formally, a structured argument, supported by evidence, that the system is safe. Such a safety case could build on the advice given in the SCSC Assurance Case Guidance [1], by presenting a series of claims of conformity to the relevant requirements, supported by reasoned arguments that provide a link from each claim to the relevant evidence, the assumptions and context under which the claims are valid, and the justification that the reasoning is sound.

Development of a complex system is likely to generate a significant quantity of information that will contribute to the safety case. IEC 63187-1 also sets requirements for document control, configuration management and traceability that will apply to how this information is managed. The standard does not require use of any particular tooling to manage the safety case, but meeting these requirements is likely to be considerably easier with effective tool support. This implies that tools that can automatically maintain consistency between safety artefacts and the system architecture, or highlight impacted areas for review when changes occur, may be very valuable as an enabler to demonstration of conformity. Model-Based Systems Engineering (MBSE) or Model-Based Safety Analysis (MBSA) tools are likely to assist in this respect.

3 Implications for Contracting

From the discussion above, it should be apparent that using IEC 63187-1 in a contract will not be as simple as quoting the title of the standard as a requirement and waiting for the contractor to deliver. IEC 63187-1 places many requirements and criteria on the outcomes of the ISO/IEC/IEEE 15288 Agreement processes (the Acquisition process and the Supply process). These requirements for agreement are typically paired, with a requirement on the acquirer in the Acquisition Process and a corresponding requirement on the supplier in the Supply process. This gives the acquirer an explicit, active role to play in the implementation of the standard and means that conformity cannot be achieved by the supplier in isolation.

During the Acquisition process, the acquirer will need to prepare a request for supply (also known as an invitation to tender or negotiate), that sets out what they are requesting. In the parallel Supply process, the supplier prepares a response to this request, and the two parties must reach an agreement on what will actually be done. This agreement is similar in purpose to the Development Interface Agreement (DIA) described in Clause 5 of ISO 26262 Part 8 [9]. Indeed, when ISO 26262 is used for the realisation of a system element in a wider IEC 63187 system, then the agreements required by IEC 63187 are likely to be combined with the DIA.

The agreement is required to cover topics such as:

- the safety strategy that will be implemented by the supplier, including potential selection or tailoring of systems engineering processes;
- the recursion strategy for applying the standard at lower levels of the supply chain;

- the safety acceptance strategy that the acquirer will use to determine whether the system safety effort is acceptable;
- safety requirements for the system elements that will be supplied;
- the Measures of Importance (MoI) scheme that will be applied to safety artefacts;
- standards, methods and techniques to be applied in analysis and development of the system, and acceptable routes to realisation;
- relevant quality evaluation criteria; and
- safety planning and allocation of responsibilities.

The request/response/agreement sequence established by the Acquisition and Supply processes gives flexibility for the acquirer to impose constraints where necessary, but also for the supplier to innovate or suggest where requirements are not practical. In principle, the acquirer could allow the supplier complete freedom to make proposals on the topics above. However, this would greatly increase the risk that the either the system-of-interest itself or the assurance provided about the system would not meet expectations. The request for supply allows the acquirer to include requirements or prohibitions aligned to factors such as integration with their internal processes and tooling, local regulatory or legal constraints (important on international projects), or the risk appetite of their organisation.

A particularly important area for the acquirer to influence is the MoI scheme. This is used to assign a measure of importance to safety artefacts such as detriments, hazards, safety requirements and safety objectives, as described in [6, 7]. The MoI allows trade-offs to be made, guides the application of engineering effort, and indicates where greater levels of assurance are needed. While it is important for the MoI scheme to interface effectively with supplier processes, it is essential that it properly reflects factors that are of concern to the acquirer and their stakeholders.

For the acquirer to comply with the requirements placed on them by IEC 63187-1 is likely to mean that more up-front work is required by contracting authorities when using the standard to acquire a complex defence system. This effort is required both to prepare the request for supply, and to check that the supplier's proposal is acceptable. The expected pay-off for this extra effort is a better understanding of the context and safety requirements for the system and reduced ambiguity about what will be done and what safety assurance will be provided. This is beneficial to both parties, increasing the likelihood that an acceptably safe system will be delivered on time, on budget and with sufficient safety assurance to give confidence that it is actually safe enough.

4 Threats to Validity

The analysis presented in this paper is based on the Committee Draft for Vote of IEC 63187-1, rather than the published standard. This means that its requirements and mechanisms for conformity may change prior to official publication. The interpretation presented here reflects the authors' understanding from involvement in development of the standard and may not reflect all stakeholder perspectives. Additionally, the standard is not yet available for empirical use, and further challenges to demonstrating conformance may become apparent on practical application.

5 Conclusions

This paper has explored how it may be possible to demonstrate conformance to IEC 63187-1, based on analysis of the Committee Draft for Vote of the new standard, and of ISO/IEC/IEEE 15288, to which it is closely linked.

IEC 63187-1 provides a flexible framework for embedding system safety into systems engineering processes, based around a set of agreements between an acquirer and supplier. Its flexibility comes from its goal-based approach, setting requirements on outcomes rather than specific development or analysis methods, system architectures or properties of a deployed system. The systems engineering lifecycle processes on which it is based can also be tailored, in the manner allowed by ISO/IEC/IEEE 15288. This flexibility allows the implementation of the standard to be optimised to be proportionate to the project in question and to meet stakeholder requirements. However, it means that conformance to the IEC 63187-1 is contextual to a particular agreement between a specific acquirer and supplier. It may not be feasible to certify generic conformance to the standard, either at a product or an organisational level.

Although organisational certification may provide confidence in the ability of an acquirer or supplier to implement IEC 63187-1, it is likely to be necessary to demonstrate conformity to the standard on a case by case and contextual basis for a given system-of-interest. This will involve identifying the relevant processes and activities, assuring that the necessary inputs have been provided to allow the IEC 63187-1 framework to be implemented, and evaluating whether the required outcomes have been achieved. Part of the standard's requirements are concerned with achieving agreement up front on exactly how this will be done.

Acknowledgments. The authors acknowledge the work of all members of 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, who are developing IEC 63187.

Disclosure of Interests. The authors are members of the SC65A Working Group 18 and their respective national standards committees.

References

1. Assurance Case Working Group: Assurance Case Guidance Version 1. Safety Critical Systems Club, York (2021), <https://scsc.uk/r1245>, last accessed 2026/05/01
2. DOD: MIL-STD-882E – Standard Practice for System Safety. Department of Defense (2023).
3. IEC: IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva (2010)

4. IEC: IEC 63187-1 Committee Draft for Vote (CDV) – Systems engineering – System safety – Complex systems in defence programmes Part 1 – Concepts, terminology and requirements. International Electrotechnical Commission, Geneva (2025)
5. IEC: What is conformity assessment? <https://www.iec.ch/conformity-assessment/what-conformity-assessment>, last accessed 2026/05/01
6. Inge, J., Potiron, K.: A systems viewpoint on the integration of subsystems developed with heterogeneous safety standards. In: Ceccarelli, A., Trapp, M., Bondavalli, A., Schoitsch, E., Gallina, B., and Bitsch, F. (eds.) *Computer Safety, Reliability and Security. SAFECOMP 2024 Workshops*. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-68738-9_1
7. Inge, J., Potiron, K., Machrouh, J.: Putting importance into context: moving from the abstract to the concrete with IEC 63187. In: Parsons, M. (ed.) *AI and Safety Critical Systems – Proceedings of the 34th Safety Critical Systems Symposium*. pp. 229–243. Safety-Critical Systems Club C.I.C., York (2026), <https://doi.org/10.65391/r3348>
8. ISO: ISO 9001 – Quality management systems – Requirements. International Organisation for Standardization, Geneva (2015)
9. ISO: ISO 26262-8 – Road vehicles – Functional safety. International Organisation for Standardization, Geneva (2018)
10. ISO: ISO/IEC 17000 – Conformity assessment – Vocabulary and general principles. International Organisation for Standardization, Geneva (2020)
11. ISO: ISO/IEC/IEEE 15288 – System and software engineering – System life cycle processes. International Organization for Standardization (2023)
12. ISO: ISO/IEC/IEEE 15026-1 – Systems and software engineering – Systems and software assurance – Part 1: Vocabulary and concepts. International Organisation for Standardization, Geneva (2025)
13. Littlewood, B., Strigini, L.: Validation of ultrahigh dependability for software-based systems. *Communications of the ACM*. 36, 69–80 (1993). <https://doi.org/10.1145/163359.163373>
14. McDermid, J.A., Burton, S., Garnett, P., Weaver, R.: *Safer Complex Systems – An initial framework*. Royal Academy of Engineering (2021).
15. MOD: Def Stan 00-056 – Safety management requirements for defence systems – Part 1: Requirements. Ministry of Defence, Glasgow (2023).
16. Ricque, B., Joguet, B., Brindejone, V., Semeneri, N., and Potiron, K. : IEC 63187 : intégrer la sûreté de fonctionnement au sein de l'ingénierie système. In: *Innovations et maîtrise des risques pour un avenir durable – 23^e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Institut pour la Maîtrise des Risques, Paris Saclay, France (2022)
17. SEBoK contributors: Application of systems engineering standards. (2025), https://sebokwiki.org/w/index.php?title=Application_of_Systems_Engineering_Standards, last accessed 2026/05/01