Putting importance into context: moving from the abstract to the concrete with IEC 63187

James Inge

Defence Equipment & Support

Katia Potiron

KNDS France

Joseph Machrouh

Thales Land and Air Systems

Abstract *When developing a complex system, it can be impractical and prohibitively expensive to apply the ultimate degree of rigour to safety assurance of every part of the design. Some way of measuring the relative importance of different artefacts is needed, to allow effort to be applied proportionately. The forthcoming system safety standard, IEC 63187, defines the concept of a 'measure of importance scheme' (MoI scheme) to achieve this aim. IEC 63187 is being drafted to supplement systems engineering processes with requirements to make them appropriate for complex safety-critical systems such as those found in defence. However, IEC 63187 applies to the abstract domain of systems engineering and does not tell one how to actually realise concrete system elements using technologies like software, programmable electronics, machine learning or traditional mechanical engineering. Understanding how to move from the abstract to the concrete, considering the usage scenarios in the operating environment, will be vital to putting the new standard into practice. This paper reviews what needs to be taken into account when transforming from an abstract MoI to the importance metrics used in existing realisation standards and presents an example of how this might be achieved for a machine learning-based system element, using ED-324/ARP6983 (EUROCAE and SAE 2025) to support IEC 63187.*

1 Introduction

When developing complex engineered systems, there are many cases when it is desirable to use one standard or framework of standards for safety of the overall system, but other standards – often multiple standards – for safety of individual system elements. This can arise for several reasons:

- To allow incorporation of off-the-shelf (OTS) system elements that have already been developed according to a different standard than the higher-level system. E.g. use of standard industrial smart devices in nuclear power generation (IAEA 2023).
- When the system elements are mechanical, hydraulic, electrical, E/E/PE system elements that are addressed by separate safety standards.
- To allow system elements to be developed to a more appropriate standard, for instance where the technology or operational domain of the system element is different to the higher-level system, or its designers are more familiar with a different standard. E.g. use of standards such as IEC 61508 (IEC 2010) or DO-178 (EUROCAE and RTCA 2012) to develop programmable elements in support of classification society type approval of (principally mechanical) maritime systems (Hawthorn 2019).
- When the scope of the higher-level safety standard does not cover necessary aspects of the system element development or does not provide the desired level of detail. This occurs when using the UK Defence Standard Def Stan 00-056, which envisages that other standards will be used as "recognised good practice" to fulfil its requirements (MOD 2023). It will also feature in the use of the forthcoming international standard IEC 63187 (IEC 2025), which focuses on the conceptual design of complex systems rather than the realisation of individual system elements (Inge and Potiron 2024a).

In these cases, it is necessary to answer several questions: Which standard should be applied to the system element development (or in the case of OTS elements, which standards will be regarded as providing acceptable assurance about previous development)? How should the chosen standard be applied to be consistent with the system's needs and with other safety standards that might be used for other system elements? And what further measures might be necessary to ensure an acceptable level of safety, with sufficient assurance that it will be (or has been) achieved?

It is unlikely to be proportionate or cost-effective to apply the most rigorous development and assurance practices to every part of a system, so most safety standards include some way to focus effort on the most important or critical parts of the design. But some standards are more rigorous than others, and the schemes that different standards use to decide where to apply effort are not generally compatible with each other, even when they look superficially similar. This raises a further question: how to coordinate the overall development, so that similar levels of rigour are applied to similarly important parts of the design, when different system elements are developed according to different standards?

This paper examines how these questions might be answered in the context of complex systems using the measure of importance (MoI) scheme concept introduced in IEC 63187. *IEC 63187 – Systems engineering – System safety – Complex systems in defence programmes* is a future international standard currently being drafted to add system safety requirements and criteria to the process outcomes described in ISO/IEC/IEEE 15288 – *System and software engineering – System life cycle processes* (IEC 2023). The motivation, goals and principles of the forthcoming international standard are introduced in more detail by Inge and Potiron (2024a), but the intent is to build on the approach to management of complex systems taken by ISO/IEC/IEEE 15288 and make it appropriate for development of complex safety-critical systems, in particular those found in the defence sector. The approach described in the new standard is anticipated to resolve some of the shortfalls of traditional safety standards when applied to more complex systems and systems-of-systems. IEC 63187 does not deal with the realisation of individual system elements, but its MoI scheme concept provides a bridge to the importance measures used in the safety standards used to realise those elements (referred to as 'realisation standards' in this paper).

2 Previous work

2.1 The IEC 63187 safety artefacts

In the IEC 63187 model of safety, the key safety artefacts are detriments, hazards, safety objectives and safety requirements. A hazard is a state or set of conditions that, when combined with environmental conditions, will lead to a detriment. These detriments are harm to, or a reduction in value of, something of importance to stakeholders. As well as injury or loss of human life, detriments may include any other type of harm that is unacceptable to the stakeholders of the system, such as property damage, environmental pollution, reduction of capability, mission failure, harm to reputation, or loss or leak of sensitive information. Safety objectives are defined for the system-of-interest and are required to address all hazards introduced by that system. Safety objectives are also required to satisfy any safety requirements assigned to the system-of-interest, such as to perform a safety function as part of a higher-level system, addressing hazards arising elsewhere in the system architecture. Safety requirements are then set to meet the system-of-interest safety objectives (Fig 1). Safety requirements may be either functional or non-functional. They are decomposed and assigned to individual system elements as appropriate, flowing in a cascade through the system hierarchy and becoming safety objectives for lower-level system elements. The process of defining hazards, safety objectives and safety requirements is applied recursively until, at some point, one must stop dealing with

an abstract system hierarchy and start designing realisable system elements. At this point it is necessary to transform the safety requirements into design criteria that are relevant to the individual system elements and the realisation standards used to develop them. This is described further by Inge et al. (2023).

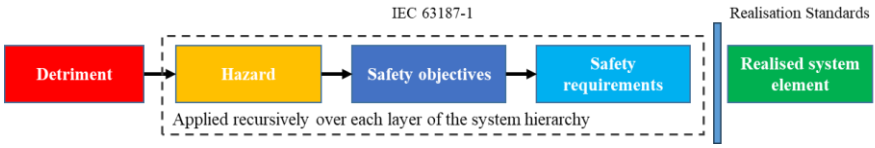

Fig 1. IEC 63187 safety artefacts.

2.2 The need for measures of importance

Most safety standards recommend particular activities or practices in order to develop systems that can be regarded as sufficiently safe, within a particular context and operating domain assumed by the safety standard. These include techniques and measures that reduce the risk of harm (such as engineering safety features into the design) and also techniques and measures that increase confidence in the level of safety that has been, or will be, achieved (like carrying out testing or reviews). Both types of technique and measure (to ensure and assure safety) involve a cost-benefit trade-off and are subject to the law of diminishing returns: as desired levels of safety and the need for confidence in the achieved level increase, the techniques and measures required for further improvement become increasingly expensive. On some projects, it may be cost-effective to apply the same level of rigour to everything, but when building a complex system it is often impractical to apply the most rigorous safety techniques and measures to the whole development. Instead, a pragmatic approach must be taken that guides effort to the most important concerns.

For these reasons, most safety standards define some mechanism for measuring the relative importance of different parts of a development with regard to safety and adjusting their requirements accordingly. These include Safety Integrity Levels (SILs, IEC 61508 – *Functional safety of electrical/electronic/programmable electronic safety-related systems*), Automotive Safety Integrity Levels (ASILs, ISO 26262 – *Road vehicles – Functional safety*) and Design Assurance Levels (DALs, ARP 4754B – *Guidelines for development of civil aircraft and systems*). Previous work (Potiron et al. 2024, Inge and Potiron 2024b) has surveyed some of these mechanisms, finding that although they appear nominally similar, the various standards contain differences in approach and detail that mean that in general they are not directly compatible with each other. They differ in terms of how they are measured, what they are applied to, and what practices should be applied at different levels. The various different mechanisms also tend to have limitations that mean that, while they are useful in the intended context of application of their standard,

they are not necessarily helpful when applied to a complex systems hierarchy in which individual system elements may be complex systems in their own right.

2.3 The IEC 63187 MoI approach

The current draft of IEC 63187 (IEC 2025) defines a measure of importance (MoI) as a "metric that describes the degree of confidence, together with relevant contextual information, needed when ensuring or assuring safety", noting that it can be expressed on a continuous, quantised or ordinal scale. An MoI scheme is a "set of rules for aggregation, decomposition and inheritance of MoIs and MoI scales". From these definitions, it is apparent that the standard does not define one singular measure of importance scheme or assume a particular scale of measurement. Instead, it allows an MoI scheme to be defined flexibly to meet the needs of the parties acquiring and supplying the system, to allow a recursive application of the MoI scales without limitation up and down the supply chain and systems hierarchy. The aim is to allow selection of appropriate practices to demonstrate that the design is safe, and to allow assurance and engineering effort to be prioritised to the areas where they are most needed, taking stakeholder concerns and priorities into account.

IEC 63187 requires an MoI to be assigned for each detriment, hazard, safety objective and safety requirement, for each usage scenario defined as part of the system operating environment, as shown in Fig 2. The MoI includes both a level on an MoI scale and additional context including the relevant usage scenario. This reflects that the importance of something depends, and even sometimes can only have a meaning, with a specific context.

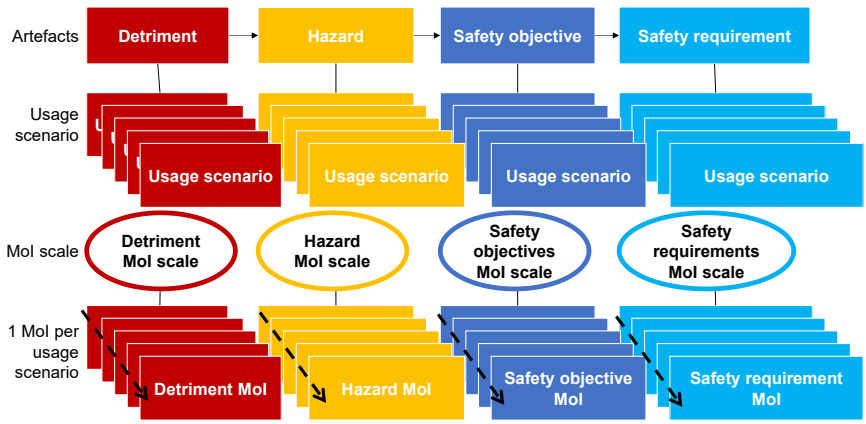

Fig 2. Measures of importance and usage scenarios.

Fig 2 also shows that the MoI for each type of safety artefact may be measured on a different MoI scale, allowing as much or as little granularity in the scheme as is needed. The MoI for a detriment is assigned on the basis of the severity of that

detriment, combined with such conditioning factors as are necessary (see Fig 3 for examples). The MoI for a hazard is set by combining the MoI of the associated detriments according to combination rules in the MoI scheme and applying further conditioning factors. A similar process is followed with safety objectives and safety requirements, as shown in Fig 3. The MoI scheme is agreed between the acquirer and supplier. It defines the conditioning factors that determine whether an MoI should be higher or lower on an MoI scale, and aggregation and disaggregation rules (e.g. for when a safety objective addresses multiple hazards or is satisfied by multiple safety requirements).

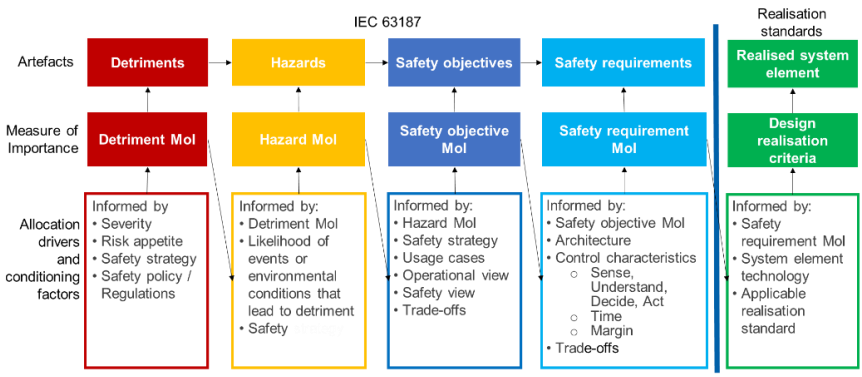

Fig 3. Assignment of measures of importance (Potiron et al. 2024).

Setting MoI levels for each type of safety artefact allows the importance of different concerns in the system architecture and design to have an influence at the systems engineering level, not just on the architecture and design of individual system elements. For instance, the MoI assigned to a safety objective could be used to help determine the acceptable types of architecture for the overarching system, or to influence how particular systems engineering lifecycle processes are to be carried out.

The use of conditioning factors allows the MoI scheme to be constructed to reflect the priorities, concerns and risk appetite of the acquirer – and should be agreed with the supplier when developing system elements under IEC 63187. Conditioning factors can be used to reflect differing societal concerns. For instance, conditioning factors can be used to distinguish between detriments with the same level of severity, but different levels of acceptability to the public, e.g. to reflect that radiological injuries are seen as more concerning than blunt force trauma. Conditioning factors on hazard and objective MoIs can be used to reflect other types of concern, such as increasing the level of importance when less trusted technologies are used, such as artificial intelligence; or when a particular system element has a higher degree of control over hazards, with less scope for intervention if it fails. Potiron et al. (2024) give examples of how such conditioning factors could be applied in practice.

Conditioning factors can also be used to reflect the importance of the likelihood of a hazard arising or leading to a detriment. However, this is not a requirement of IEC 63187. In defence systems, it is often impractical to make a realistic estimate

of likelihood, as the operating environment may change dramatically between usage scenarios, or dynamically during a mission. For this reason, the draft standard uses a definition of risk based on that used in ISO/IEC/IEEE 15288 and ISO 31000 – *Risk Management – Guidelines*, as the "effect of uncertainty on stakeholder objectives". This contrasts with the definitions used in many other safety standards, based on a combination of probability and severity of harm.

Including the context of the usage scenario as part of the MoI allows conditioning factors to be applied more intelligently. For instance, the MoI for a particular detriment might be higher in a training scenario than during combat, because of the social expectation that training should be safe. However, a safety requirement might be less important (lower MoI) during a training scenario because of an expectation that timely and effective emergency services would be available. The usage scenario will determine which conditioning factors are relevant or admissible. At the level of realised system elements, the additional context is also helpful in applying a realisation standard. For instance, when a single system element satisfies several safety requirements, knowing that their associated MoIs are only relevant to certain usage scenarios may mean being able to avoid applying onerous assurance requirements to parts of the system element that are not relevant to those scenarios.

The approach of applying generic, user-defined Measures of Importance is very flexible. This allows it to work at any level in the abstract hierarchy of system requirements and architectures, being applied recursively to systems and their system elements and adapting to the context of their operating environment. So long as there is an overall consistency of MoI schemes, MoI scales, accepted conditioning factors and allocation drivers, different MoI schemes can be used at different tiers of the system hierarchy, to suit acquirers and suppliers at different tiers of the supply chain. At some point though, it is necessary to transition to the level of realisable system elements that can be designed and build into actual mechanical, hardware, software and programmable elements…

3 Moving from the abstract to the concrete

IEC 63187 does not prescribe how the development of system elements should take place or be assured, so it is necessary to adopt other standards that are appropriate for the technologies and operational domains involved. While these are likely to include standards for software, programmable electronics and data, standards for developing systems using more traditional technologies are also likely to be needed, such as for hydraulic or pneumatic machinery.

The acquirer and supplier of a particular system element will need to make an agreement on the MoI scheme that gives the rules for assigning MoIs at the IEC 63187 level, the realisation standard(s) to be used to implement the system element, and the rules for transforming from MoIs to the importance metrics used by the realisation standards. These arrangements could be proposed by either the customer or supplier but will need to reflect the safety strategy for the project and be agreed

by both parties. These three areas of agreement are interlinked: while the choice of realisation standard may be influenced by the MoI assigned to a safety requirement, the MoI scheme can be optimised to work more effectively with particular standards; and the chosen standards and MoI scheme will obviously then have a strong influence on the transformation rules. Some of the factors that might be taken into account when making these decisions are discussed below.

3.1 Factors to consider in construction of the MoI scheme

Conditioning factors that reflect stakeholder concerns and priorities. It is expected that the MoI for a safety requirement will be based on the MoI for the associated safety objective(s), which are in turn based on the linked hazards and detriments, as shown in Fig 3. Conditioning factors can be used to increase or decrease the importance of a safety artefact compared to the MoI level that would otherwise be inherited from linked artefacts.

The conditioning factors that are relevant will vary with different usage scenarios and include probabilities of hazardous conditions being present, degree of control over hazards, risk appetite for different kinds of detriment, etc. As an example, if stakeholders are more concerned about harm to bystanders than involved personnel, this could be captured as a conditioning factor. Safety requirements might then attract a higher MoI score if they influenced the risk of harm to bystanders.

Contextual information that will be relevant for the realisation standard. When the realisation standard is known in advance, it is advantageous if the MoI scheme reflects the parameters used to determine the importance metrics used in that standard.

Rules for aggregation and disaggregation of MoIs. How should MoIs be assigned when a safety requirement satisfies more than one safety objective, or more than one safety requirement is necessary to satisfy the same safety objective? Similarly, how should the MoI value be assigned when more than one conditioning factor is relevant? These rules may take architectural considerations such as redundancy into account. They should be constructed to avoid 'saturation' of the scheme, where a high MoI set on a system element's safety objective leads to every low-level safety requirement ending up with an equally high MoI.

Level of granularity required. MoI scales need at least enough granularity to represent the different outcomes required in terms of assurance or confidence-building activity. Further granularity may be helpful in enabling prioritisation between safety requirements, or between safety requirements and other requirements on system elements, so long as this does not make the MoI scheme too complicated for practical use.

3.2 Factors to consider in selecting realisation standards

Level of confidence provided by applying a standard. Different standards are designed to give an appropriate level of confidence about safety in different operational domains. For instance, ISO 26262 is designed for systems (road vehicles) where the maximum detriment from an individual event is relatively low. In contrast, systems in other operational domains, such as railways, commercial aviation or nuclear power generation can differ by orders of magnitude in how many people are potentially at risk and the level of confidence deemed necessary. This influences the rigor of the practices they require.

If the standard(s) proposed to be used for development (or already used, if the system elements are pre-existing) do not provide sufficient assurance to satisfy the stakeholders, the acquirer and supplier will need to agree what supplementary techniques and measures are to be taken to improve confidence. These might include additional assurance activities such as independent analysis or review of the design.

Cost-effectiveness of the practices recommended by the standard. Some standards are intended for operational domains such as consumer goods or road vehicles where high production volumes allow design and safety assessment costs to be spread over many units. Practices that are cost-effective in these domains, e.g. destructive testing, may not be cost-effective for small production run or one-off developments. Conversely, standards for complex, high-criticality one-off systems may assume higher budgets and recommend practices that cannot be justified on smaller developments. The practices required by the standards in different operating domains therefore reflect compromises between the level of confidence they provide and the cost of application.

Appropriateness to the technology used for implementation. Are the practices the standard requires relevant for the design of the system element being realised? Does the scope of the standard cover the whole of the development? If not, multiple standards might need to be used, for example to cover the mechanical and the electronic parts of the design, or to address different sources of detriment, such as cyber. Alternatively, the MoI scheme might need to specify additional requirements or design criteria, such as additional deliverable documentation to support further safety analysis by the acquirer.

Assumptions made by the standard. For instance, DO-178C assumes the existence of a ‘certification authority’ that will approve products. When DO-178C is used outside the context of the regulated aviation industry, agreement is needed as to who will carry out the certification authority role. Whether or not such assumptions can be resolved may have a bearing on whether a given standard can be used, and what degree of assurance can be obtained from it.

Familiarity of developers with the standard. Costs and timescales may be increased if the supplier is asked to use unfamiliar practices. There will need to be a

balance between the perceived safety or confidence benefits of using the standard and the disruption it causes in the development process.

3.3 Factors to consider in transforming between MoI and design criteria

Choice of standard. If more than one realisation standard has been agreed to be potentially appropriate, how will the specific standards to be used be chosen? Different standards could be applied according to the MoIs attached to the system element's safety requirements. Different, or additional, standards could also be invoked when particular conditioning factors have been used, e.g. if a cyber security concern is linked to a hazard.

Mapping between realisation standard tasks or processes and the IEC 63187 lifecycle and requirements. Some standards include a hazard and risk analysis process that is used to set their importance metric (e.g. IEC 61508), while others (e.g. DO-178C, DO-254) assume that the importance metric has already been set by analysis carried out through application of a different standard at system level. Some standards take both approaches (e.g. ISO 26262 includes a hazard analysis and risk assessment process but also provides for Safety Elements to be developed out of Context (SEooC), using externally provided assumptions about the required level of integrity).

The acquirer and supplier could agree to use the complete realisation standard, transforming the MoI into input parameters to the standard's hazard analysis or requirement setting process. However, an alternative strategy would be to transform the safety requirement MoI directly to the realisation standard importance metric, e.g. by saying that a value like 'medium' or 'high' on a safety requirement MoI scale transformed to a design criteria requiring use of the practices recommended for a given integrity level in a particular realisation standard.

Tailoring of the realisation standard. Does the standard include tailorable or optional requirements, such as recommendations or examples that are expected to be customised by the user of the standard? If so, can the supplier tailor the way the standard is applied as they see fit, or should the MoI scheme require it to be tailored in a particular way to insist on some elements, or flag others as unnecessary? How should this change at different levels on the MoI scale?

Integration of the realisation standard's outputs. The acquirer may require evidence of the application of a realisation standard, to give them confidence that the standard is being applied appropriately, or to feed into other areas of the safety management process. This may not happen automatically if the standard had been de-

signed for application inside a single organisation, rather than in an acquirer/supplier scenario. Different work products or evidence may be appropriate at different MoI levels.

Reverse transformation. If a system element has already been developed according to a particular realisation standard, what level of safety requirement MoI might it support? What evidence would be necessary to demonstrate that?

3.4 Putting it all together

From the considerations discussed above, it becomes apparent that when transforming from an MoI scheme to a realisation standard, a simple mapping between an MoI scale and a metric like an integrity level will not be sufficient. To apply a realisation standard effectively to a system element, more information is needed about the context that the system element will be used in. Some of this context can be captured as part of the MoI scheme using the usage scenarios, and the tailored by using conditioning factors to increase or decrease importance on an MoI scale according to the context of operation. However, when realisation standard importance metrics do not take usage scenarios or equivalent concepts into account, it will often be necessary to provide detail about the context itself, rather than just the quantified MoI value.

To take an example from Potiron et al. (2024), mission type could be a conditioning factor of the detriment MoI. This would allow the MoI to reflect that, as well as different usage scenarios having potential to cause different severities of detriment, the same detriment may be more, or less, tolerable in different usage scenarios, depending on the type of mission being carried out. As the MoI propagates through the system decomposition, to hazards, safety objectives and safety requirements, this could lead to different safety requirements being necessary in different usage scenarios, or the same safety requirement having different MoI values depending on the context of use. Enough of this context needs to be passed to the developer to allow them to understand not just what level of importance is assigned to the requirement, but why, so that the realisation standard can properly be applied.

When constructing the MoI scheme at the level of realisable system elements, the developers will need to consider the realisation standards that will be used, consider what contextual information is necessary to apply them, and decide how it will be provided through the MoI scheme. Depending on the assumptions made by the realisation standard, the context might be encapsulated as part of the level on an MoI scale and transformed directly into one or more parameter of the implementation standard; however, it could also be delivered through deriving specific requirements to address contextual issues, or by providing visibility of the higher-level safety artefacts that the requirements are derived from and the conditioning factors that led to their specific MoI level being assigned for each usage scenario.

Building a workable MoI scheme need not be a daunting prospect. Most of the standards already used for realising safety-critical systems already contain some kind of importance metric, and recommendations for how that metric should be applied. These familiar standards can provide the starting point for identifying the allocation drivers and conditioning factors that need to be built into an MoI scheme. The aim is not to produce a single MoI scheme that can be used with any system and any realisation standard simultaneously. Where it is helpful, different MoI schemes may be used at different levels in the system hierarchy, and for different system elements. The aim is to produce a set of measurement scales and transformation rules that, in the context of a particular system element development, allow stakeholder concerns to be addressed properly by the realisation standards that will be used.

4 A practical example

In the civil aviation domain, a process standard, ARP6983 / ED-324 – *Process standard for development and certification approval of aeronautical products implementing AI*, is being drafted for development and certification of embedded systems such as avionics that are implemented using Machine Learning (ML) elements (EUROCAE and SAE 2025). Gabreau et al. (2022) suggest that ARP6983 will introduce the concept of an 'ML constituent': a system element that is partly implemented using ML techniques, and provide processes for their development, verification and integration into a higher-level system. However, ARP6983 will still assume that system level analysis is undertaken according to ARP 4761A and ARP 4754B, and implementation of the ML constituent is carried out using standards for software and hardware such as DO-178C and DO-254.

Because ML-based system elements are still a relatively new concept in safety-critical systems, it may be beneficial to deploy a standard such as ARP6983 as part of a defence domain IEC 63187 development programme. Once published, the new standard is likely to provide relevant good practice, even outside the regulated aviation context of ARP4761A and ARP4754B. The MoI schemes required by IEC 63187 provide a mechanism to achieve this, allowing contextual information about the usage scenarios for the defence system to be taken into account.

ARP6983 uses two concepts related to usage scenario: Operating Environment (OE) and Operational Design Domain (ODD). OE is defined at the level of the overall system and provides the context in which it is deployed. When decomposing the system into elements that handle different system functionalities, then an ODD must be defined for each system element that is implemented using AI technologies (Fig 4). These ODDs are the refinement of the system's operating environment to produce a set of derived requirements that define the context of the specified function.

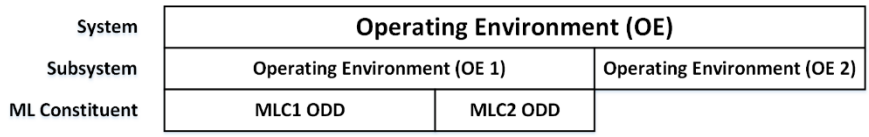

Fig 4. Relation between the Operating Environment (OE) and Operational Design Domain (ODD) for an ARP6983 development.

One potential way of transforming between IEC 63187 and ARP6983 is for IEC 63187 to take the place of ARP 4761A and ARP 4754B, as illustrated in Fig 5. Other transformations are possible but will not be detailed here.

In such a case, analysis of the OE is performed under IEC 63187. This could be done using similar techniques to the ARP standards, but while those standards assume the context of an aircraft platform, the IEC 63187 MoI scheme can be constructed to take into account usage scenarios and conditioning factors that are relevant to the actual OE of the defence system. The MoI scheme can still be set up to produce requirements MoIs on a scale that may be transformed easily to the Design Assurance Levels used in the ARPs, if it is known that DO-178 and/or DO-254 will be used for the low-level implementation of the ML constituent. Application of IEC 63187 also leads to the definition of safety requirements that will be assigned to the ML constituent, including usage scenarios. Those will form the ODD for the ML constituent and its lower-level elements (e.g. training data, validation data sets). Rules can be set in the MoI scheme such that when AI/ML is to be used to fulfil a safety objective, it will lead to compatible safety requirements being set on the relevant system element, such that the correct context is preserved to enable ARP6983 to be used. This may well include factors from the system OE analysis, such as corner cases to be addressed in the training data, that would not necessarily have emerged from analysis according to the aviation standards alone.

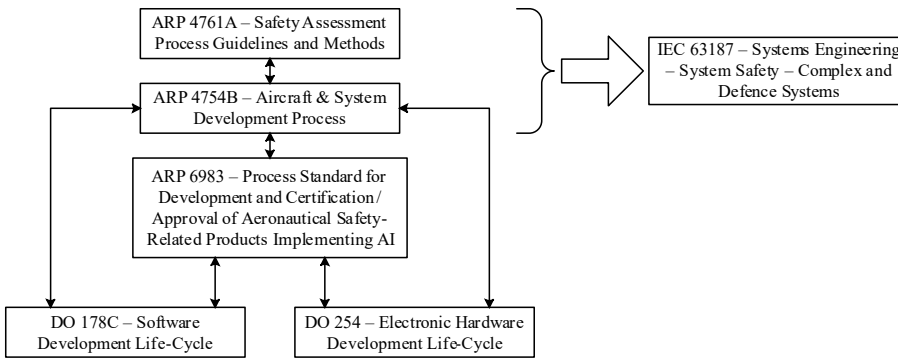

Fig 5. Replacement of system-level ARP standards by IEC 63187.

5 Conclusions

The forthcoming complex systems safety standard, IEC 63187, uses an abstract concept of measures of importance (MoIs) as its mechanism for ensuring that engineering and assurance effort will be deployed where it is most important to ensure safety. A key challenge in the practical application of the standard will be for its users to construct workable MoI schemes. These need to enable an efficient transition from abstract, systems engineering level requirements to concrete requirements and design criteria that can be used to realise actual system elements and integrate with the standards used for realisation.

As MoI schemes must be agreed between acquirers and suppliers of systems, they need to embody a principal of proportionality: they must ensure that sufficient confidence in the safety of the system is produced to satisfy the acquirer, while being efficient and cost-effective for the supplier to work to. This paper has presented the philosophy the authors expected to be built into IEC 63187, and explored the considerations that users of the standard may need to take into account when putting it into practice, and given an example to demonstrate that the MoI approach is likely to be both feasible and useful in the development of complex systems.

Acknowledgments 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.

Disclaimers The authors are members of the SC65A Working Group 18 and their respective national standards committees. Opinions presented in this paper are those of the authors, rather than the IEC or their employers. Discussion of IEC 63187 and ED-324/ARP6983 are based on committee drafts, which may change prior to publication.

References

EUROCAE, RTCA (2012) ED-12C/DO-178C – Software considerations in airborne systems and equipment certification. European Organisation for Civil Aviation Equipment and Radio Technical Commission for Aeronautics.

EUROCAE, SAE (2025) EUROCAE ED-324 and SAE Aerospace Recommended Practice ARP6983 – Process standard for development and certification approval of aeronautical products implementing AI. European Organisation for Civil Aviation Equipment and Society of Automotive Engineers. Draft for EUROCAE open consultation.

Gabreau C, Gauffriau A, Grancey FD et al (2022) Toward the certification of safety-related systems using ML techniques: the ACAS-Xu experience. In: 11th European Congress on Embedded Real Time Software and Systems (ERTS 2022).

Hawthorn CR (2019) A systematic approach to certification of complex control systems. In: Proceedings of Marine Electrical and Control Systems Safety Conference (MECSS). IMarEST. doi:10.24868/issn.2515-8198.2019.008.

IAEA (2023) Safe use of smart devices in systems important to safety in nuclear power plants. International Atomic Energy Agency.

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

IEC (2023) ISO/IEC/IEEE 15288 – System and software engineering – System life cycle processes. International Electrotechnical Commission.

IEC (2025) IEC 63187-1 ED1 Committee Draft for Vote (CDV) – Systems engineering – System safety – Complex systems in defence programmes Part 1 – Concepts, terminology and requirements. International Electrotechnical Commission.

Inge J, Potiron K, Williams P et al (2023) IEC 63187: engineering safety into complex defense systems. In: Safety in an agile environment: the International Systems Safety Conference 2023. International System Safety Society.

Inge J, Potiron K (2024a) System safety for complex and defence systems. In: 43rd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2024), Position paper. https://www.safecomp2024.unifi.it/upload/sub/other/position%20papers/SAFECOMP2024_paper_101.pdf. Accessed 8 May 2025.

Inge J, Potiron K (2024b) A systems viewpoint on the integration of subsystems developed with heterogeneous safety standards. In: Ceccarelli A, Trapp M, Bondavalli A et al (eds) Computer Safety, Reliability and Security. SAFECOMP 2024 Workshops. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-68738-9_1

MOD (2023) Def Stan 00-056 – Safety management requirements for defence systems – Part 1: Requirements. Ministry of Defence.

Potiron K, Sghairi M, Rodrigues P et al (2024) 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. Institut pour la Maîtrise des Risques.