Integration of Human Factors into Complex System Safety

James Inge[1], Katia Potiron[2], Mark Carter[3] and Ian Hartwell[4]

1 Defence Equipment & Support

2 KNDS France

3 BAE Systems

4 RISIKO

Abstract *Safety-critical systems are growing ever more complex and interlinked, especially in industries such as defence. Despite increasing complexity, automation and digitisation, humans remain vital actors in these systems. People need to be considered at the system level, as part of the system architecture and design, not just as potential causes of failures. Concerns about the adequacy of existing safety assurance standards have prompted development of IEC 63187, a draft international standard that is expected to be published during 2026. IEC 63187 delivers a system safety framework tailored for complex systems in defence programmes, building on the systems engineering life cycle approach from ISO/IEC/IEEE 15288. This paper explains how IEC 63187 incorporates human factors throughout the system life cycle, outlines the supporting guidance, and compares its approach with other safety standards. It provides practical insights for engineers, safety managers, and regulators seeking to apply human factors in complex, safety-critical systems.*

1 Introduction

Modern engineered systems are increasingly complex, especially in the defence sector. Defence capability is often delivered through systems of systems, involving a mix of elements using diverse technologies, some newly developed and others already in service, designed to differing standards and provided via a complex ecosystem of suppliers. As an example, the chain 'from sensor to shooter' may involve numerous collaborating system elements, including crewed and uncrewed air platforms, land vehicles, missile systems, communication links and command centres – and the people that operate them (Fig 1). The hardware and software elements may all be geographically separated, separately procured from different supply chains and designed under different standards or regulatory regimes, and the people

may belong to different organisations and nationalities. While in service, their configuration, operating environment and the way that they are operated typically continues to change and evolve. This complexity makes it harder to ensure systems are safe[1] and to demonstrate that their safety objectives are met before deployment and throughout their life cycle.

Fig 1. Defence capability often involves numerous collaborating system elements (Copilot).

The challenges described above are not unique to defence, but in the defence industry they have prompted demand for a new safety standard to address complex systems. Since 2018, the International Electrotechnical Commission (IEC) has been developing IEC 63187, *Systems engineering – System safety – Complex systems in defence programmes* (IEC 2025). This future standard, expected to be published during 2026, supports the integration of safety views into the system engineering processes described in ISO/IEC/IEEE 15288, *System and software engineering – System life cycle processes* (ISO 2023). IEC 63187 attempts to provide a framework tailored for the challenges of the defence industry, using a systems engineering approach to manage the complexity involved. Previous work has described the goals and motivations of the standard (Ricque et al. 2022, Inge and Potiron 2024) and its strategy of adding requirements and criteria to the outcomes of the ISO/IEC/IEEE 15288 systems engineering life cycle processes to make them suitable for safety-critical applications (Potiron and Inge 2024). This paper presents the approach that IEC 63187 is expected to take to human factors (HF)[2].

[1] The term 'safe' is used in this paper as 'the absence of intolerable risk', where 'risk' is used in the sense of ISO 31073 (ISO 2022) as the 'effect of uncertainty on objectives'. Effects are deviations from the expected; they may be positive or negative, and can be introduced by a system operating according to its specification and functionality, as well as by failures or external disturbances.

[2] IEC 63187 adopts the definition of human factors as the "scientific discipline concerned with the understanding of interactions among human and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance", taken from ISO 26800 (ISO 2011).

Humans have always played a central role in the safety of defence systems and are likely to continue to do so for the foreseeable future. It is attractive to automate systems to increase reliability and performance, and to remove people from harm's way, but having a human in the loop is often essential for ethical reasons. Beyond this though, human control can still be vital to make systems resilient: able to continue operating safely in the face of unforeseen circumstances.

As modern systems become more complicated, it becomes harder to maintain a mental model of the system state, or to predict all possible hazardous failure modes. This challenge is compounded in complex systems, which can exhibit unwanted emergent behaviours – hazards that arise from interactions between system elements even when all individual components function as intended. A stark example is the Boeing 737 MAX incidents, where the reaction of the Manoeuvring Characteristics Augmentation System (MCAS) to faulty sensor data led to the loss of two aircraft and 346 deaths. The pilots were not aware of the existence of the MCAS or how it could behave. While its designers had considered the effects of uncommanded MCAS operation, they had not considered the pilots' ability to control the plane when these effects were combined with other likely outcomes of the same causal factors, such as multiple alerts and warning indications from other cockpit systems (NTSB 2019).

Automation can reduce the human workload and make it easier to manage complicated systems. It can also improve safety and reliability by removing the potential for human errors in operation. However, automation also makes systems more complex and can make it harder to understand their behaviour. As complexity increases, hazards due to latent design errors and unforeseen interactions tend to become more significant; by definition these are not addressed by the system design.

Fig 2. US Airways Flight 1549 after landing on the Hudson River.

The capacity to adapt to new situations means humans still play a key part in making systems resilient to changing operating environments, unforeseen failures and emergent hazards. Sullenberger's landing of US Airways Flight 1549 on the Hudson River (Fig 2) is an extreme example of human input being necessary to control a hazardous scenario (NTSB 2010). More prosaically, the average human driver can operate a vehicle safely in a far wider range of unforeseen scenarios than can be managed by a state-of-the-art self-driving vehicle (Cummings and Bauchwitz 2024). One of the ironies of automation (Bainbridge 1983) is that it is supposed to reduce work for human operators but leaves them to manage the more challenging

hazards that the designers did not foresee or could not control automatically – while at the same time making the operators less familiar with the way the system works.

In complex systems, the designers cannot hope to identify and control every source of hazards in advance and engineer a system to react the right way. In some cases it will be necessary for humans to step in to diagnose and respond to issues that no automated process anticipated. Given this perspective, the safety engineering effort can no longer be considered comprehensive if it is limited to considering humans solely as potentially faulty controllers external to the system, or as unreliable controls on specific risks. Safety engineering must consider human elements as integral parts of a system and cater for them as such, by promoting human performance and wellbeing, as well as avoiding human error. The design process must make sure that humans have sufficient oversight of the system and sufficient support from it to be able to ensure safe outcomes. Human error is then considered as a symptom of the system design and is not limited to being a cause of failures. This means that human factors must be considered throughout the system engineering process, not just in hazard analysis or the design of physical user interfaces.

2 Previous work

2.1 Literature review

For many years, HF practitioners have realised the tension between the need to remove humans from systems to avoid human errors, and to give humans sufficient control of unexpected events to exploit their adaptability. Various authors (Bainbridge 1983, Reason 1990, Leveson 1995 and Storey 1996) all discuss the need to balance the tasks or functions allocated to humans with those allocated to engineered system elements, to play to their respective strengths. Rasmussen (1987) suggests that human error can be seen as a mismatch between the tasks demanded by a system design and the operator's abilities, performance, or limitations. The system needs to be designed to ensure that humans have the understanding, physical capability and situational awareness to take appropriate actions when called upon. This is not a binary decision of what to automate and what to leave to human control, rather a question of the level of automation, and the level of system-provided support to human decision-making and action. The question is still acutely relevant today, in the age of Artificial Intelligence (AI): AI is further increasing complexity and topics such as the explainability and controllability of AI-enabled systems are areas of current research (Myklebust et al. 2025).

Despite this understanding in the HF field, treatment of human factors in some areas of safety engineering has historically focused on the effects of human errors

and violations, with less emphasis on the positive contribution of humans (ICAO 2021). This can be seen in several current safety standards.

Under IEC 61508[3] (IEC 2010), the 'horizontal publication' that sets the approach to functional safety for international standards, humans may form part of a safety-related system. However, IEC 61508 does not consider HF requirements for system design. Although it requires that design should follow good HF practice, humans are seen mainly as a source of error, or potentially as a means of intervention in the case of malfunction. Wiggins (2024) finds that IEC 61508 takes a mechanistic view of human factors and fails to account for systematic failures caused by physical and emotional factors such as stress, fatigue, or poor motivation – which may be a consequence of the context in which the system is expected to operate.

In the military sphere, both the US MIL-STD-882E, *DoD standard practice for system safety* (DoD 2023) and the UK Defence Standard 00-056, *Safety management requirements for defence systems* (MOD 2023) also consider that systems can include human elements, and recognise that factors that affect their performance need to be taken into account. However, like IEC 61508, they treat people mainly as a source of error.

In MIL-STD-882E, human systems integration (HSI) is recognised as a separate systems engineering discipline, but the main interface with the system safety process is the consideration of human error in the various hazard analysis tasks. In Def Stan 00-056, consideration of human factors is required, but only when human factors might be a contributory cause of a hazard, accident or failure mode; or if they could provide risk mitigation. Def Stan 00-056 does signpost Def Stan 00-251, *Human Factors Integration for Defence Systems* (MOD 2021), for guidance in these contexts, but does not actually integrate with its requirements.

As might be expected, current military human factors standards do take the impact of human factors on safety into account more comprehensively than safety standards, but again, the trend is to focus more on physical interface design and the contributions to hazard analysis. In MIL-STD-46855, *Human Engineering Requirements for Military Systems, Equipment, and Facilities* (DoD 2025), system safety and health hazards are cited alongside human engineering as three of the eight domains of human systems integration, making them key drivers of the system design. As its title suggests, MIL-STD-46855 is focused on human engineering, which it defines as "the application of knowledge about human capabilities and limitations to system or equipment design and development to achieve efficient, effective, and safe system performance at minimum cost and manpower, skill, and training demands". This includes analysis of system functions to determine whether they should be allocated to personnel, hardware, software or a combination; and subsequent influence of human factors in selection of equipment and subsystem design. As well as minimizing human error and avoiding hazards to personnel, it seeks to achieve an appropriate balance between automation and human operation, making sure that the design takes human capabilities and limitations into account while

[3] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.

achieving system performance goals. MIL-STD-46855 does require consideration of human factors early in the system life cycle, informing the high-level design of a system; and requires coordination between all the HSI domains and the broader programme. However, the system safety domain is mainly addressed through compliance with detailed technical design rules in MIL-STD-1472, *Human Engineering* (DoD 2020); MIL-STD-1472 in turn refers back to MIL-STD-882 for system safety.

Def Stan 00-251 takes a similar approach to the DoD standards but is less prescriptive. It recognises that human factors integration (HFI) involves a collaboration with the safety discipline, and lists "system safety and health hazards" and "human factors engineering" (HFE) as separate domains of HFI. The standard proposes candidate process, user and system requirements for human factors, including protection of humans from adverse effects of system use and integration of humans in the design in ways that maximise system safety (MOD 2021). Like MIL-STD-46855A, the system safety aspects are less well-developed than the physical safety aspects in Def Stan 00-251. It focuses predominantly on the human as the user of a system, suggesting requirements to ensure that people can physically use systems while being protected from harm. The system safety requirements revolve around avoiding human errors and allowing the system to recover if they are committed. Although the supporting guidance on the human contribution to system safety (MOD 2018) recognises that humans can contribute positively to safety, "being adaptable and problem solving when things go wrong", the guidance mostly details how the HF effort interacts with the hazard identification and risk management processes. It does encourage human factors planning to take place early in the system life cycle, to help identify system requirements, with allocation of functions between humans and machines as part of the HFE process.

2.2 Discussion – the need for a new approach

In IEC 63187, complex systems are defined as those where the collective behaviour of the system elements entails emergence of properties that can hardly, if at all, be inferred from properties of those system elements (IEC 2025). This means that emergent system-level properties like safety cannot be determined by analysing the system elements independently: *many safe parts do not imply a safe whole*. In the defence sector, military capabilities are often assembled by combining parts such as sensors, weapon systems, vehicle platforms and communication links. These system elements are often separately developed, and in modern systems are increasingly likely to be geographically distributed. When addressing these parts as system elements, it may be convenient to treat the user as a separate entity, outside the boundary of the engineered system, and focus on their interface with the machine. But as systems become more complex, it is increasingly necessary to consider people holistically as part of the wider system and consider more carefully what roles they are expected to play in it.

More than 35 years ago, it was realised that 'human error' was not just caused by the frailties of human cognition, but by a range of performance shaping factors determined by the system, environment and organisation the human was working in (Reason 1990). 'Human performance' is described by the International Civil Aviation Organisation (ICAO) as representing "the human contribution to system performance" (ICAO 2021); this implies that a performant system design needs to take human elements into account.

Despite the body of knowledge available in the human factors and safety engineering literature, HF practitioners have historically found it difficult to integrate HF into broader systems engineering processes (Leveson 2012, ICAO 2021, England 2025). In the defence sector, this is reflected in the scant coverage of HF topics in MIL-STD-882E and Def Stan 00-056 described above. While these military safety standards recognise to a certain extent that the engineered system must provide the conditions to allow people to perform effectively, their human factors requirements tend to be focused on hazard analysis and user interface design – optimising the user interface and system design to minimise human error and hence prevent hazards, or designing the working space to avoid the system harming its operators. They tend to treat human performance more as a potential limitation on system performance, ignoring the positive role that people have in keeping systems safe, and the potential for the human element to make the overall design safer and more resilient in the face of changing or unexpected circumstances. Hollnagel (2014) describes this negative viewpoint as 'Safety I' and argues that complex systems require use of a complementary 'Safety II' viewpoint that looks at why positive, safe outcomes routinely occur. Reflecting this dual approach, Sharples describes the job of ergonomics and human factors as to "minimise the impact of human fallibility and maximise the value of human brilliance" (Salmon et al. 2024).

Just as there is a need to integrate safety engineering more fully into systems engineering (Ricque et al. 2022), there is also a need to do the same for human factors engineering. The interface between these disciplines needs to be two-way: as well as a 'pull' from system the systems engineering and system safety processes for the input provided by HF, HF analyses need to consider the system holistically and address individual system elements in the context of their role in and interaction with other system elements. This is what IEC 63187 tries to achieve.

3 The IEC 63187 approach

3.1 The IEC 63187 approach to safety

IEC 63187 takes a systems engineering approach to managing safety in complex systems. The standard is written around 8 key principles:

1. **Risk-based** (ISO 31000): a focus on hazards and their consequences rather than quantitative probability; risk is the effect of uncertainty on objectives.
2. **Systems-based** (ISO/IEC/IEEE 15288): recursively applying systems engineering principles at multiple levels in the systems hierarchy and supply chain.
3. **Systems theory** and **control theory**: considering interacting system elements that can lead to detrimental effects without component failure.
4. **Integrating safety into systems engineering** as a fundamental part of engineering the system, with the flexibility to trade requirements.
5. **Appropriateness of approach:** addressing threats to safety from sources with different types of characteristics.
6. **Supply chain considerations**: addressed to apply proportionately over organisational boundaries.
7. **Solution independent**: regardless of the origin or life cycle stage of realised system elements.
8. **Goal-based:** providing a framework to identify and achieve safety objectives, rather than a prescriptive set of rules or specifications.

Principle 2 involves the application of the ISO/IEC/IEEE 15288 life cycle processes for systems engineering (ISO 2023). Like ISO/IEC/IEEE 15288, IEC 63187 does not specify how these processes should be carried out or the form of life cycle to be used, but it prescribes requirements and sets criteria on the outcomes of the processes, to make them suitable for application to safety critical systems.

ISO/IEC/IEEE 15288 deals with systems created by humans and accepts that such systems may also include human components alongside other types of system element, such as hardware, software, data, processes, procedures, facilities, materials, and naturally occurring entities. However, while the standard mentions human factors in its notes and signposts other standards for guidance, it does not set any firm requirement for the topic to be addressed. IEC 63187 adopts the same definitions of 'system' and 'system element' as ISO/IEC/IEEE 15288, but its requirements are much clearer about how human factors should be addressed through the life cycle of the system.

A key part of the IEC 63187 approach is the structure of safety artefacts used to control hazards, following Principle 3. 'Hazards' are identified as states or conditions that could lead to a 'detriment' (some kind of harm or loss), and 'safety objectives' are defined for those hazards to be controlled. 'Safety requirements' are set to meet the safety objectives; these safety requirements may be decomposed through the system architecture and allocated to individual system elements, where they lead to new safety objectives. The distinction between safety objectives and safety requirements allows a separation between intended outcomes and constraints. It lets the system architect allow innovation in how the safety objectives will be achieved, while still setting necessary constraints on design choices. Fig 3 shows that each safety artefact is assigned a Measure of Importance (MoI), a metric that describes the degree of confidence, together with relevant contextual information, needed when ensuring or assuring safety (see Inge et al 2026).

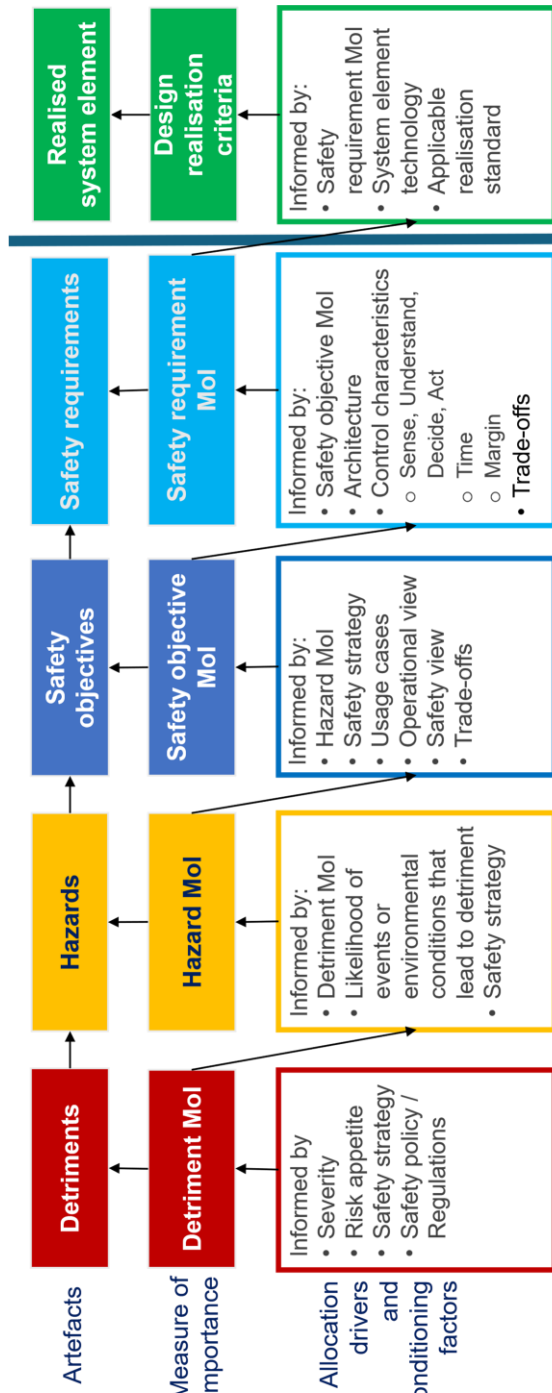

Fig 3. Safety artefacts and Measures of Importance in IEC 63187.

The approach described above addresses complexity in several ways. It prompts analysis at a high level of abstraction, where interactions between system elements can be examined and it is more likely that emergent hazards will be identified. It also aligns well with hazard identification and analysis techniques based on systems theory, such as System-Theoretic Process Analysis (Leveson and Thomas 2018). A top-down safety approach of setting safety objectives and requirements is more efficient for complex systems because it is easier to demonstrate that these requirements have been met, rather than to try to address every possible failure individually; this is impractical in complex systems. Bottom-up analyses are also likely to miss hazards that emerge from interactions between system elements, if those elements are analysed in isolation. The MoI concept helps designers account for relevant context from the higher-level system in the design or selection of system elements.

IEC 63187 will have two parts. The first, IEC 63187-1 (IEC 2025), will set out concepts, terminology and requirements and be a full international standard. The second, IEC TR 63187-2 (IEC 2025b), will provide guidance on compliance with IEC 63187-1, but will have the status of a Technical Report and not contain any formal requirements or recommendations.

IEC 63187 is intended to be applied recursively at different levels of the systems hierarchy and by different suppliers throughout the supply chain, prompting analysis of the interactions between system elements. This is repeated down to the level at which it is practical to realise individual system elements, at which point, safety requirements are transformed to design criteria. IEC 63187-1 itself will not specify how to realise individual system elements; it assumes appropriate standards will be chosen according to the technologies involved.

IEC 63187-1 is also intended to be applied iteratively. Analysis of lower-level system elements during design may prompt the need for new safety objectives or higher-level safety requirements, in order to control hazards that emerge from implementation decisions. Configuration changes, modifications or unforeseen hazards revealed by in-service experience may also prompt review. However, having clearly identified, traceable safety objectives and safety requirements should make it easier to understand the implications for the overall system.

Following Principles 5 and 8, IEC 63187-1 is not prescriptive about the type of analysis techniques to be used to identify detriments and hazards, the architecture of objectives and requirements used to manage them, the MoI scheme used to decide the importance of each safety artefact, or the implementation of the life cycle processes to be used. These can vary between different system elements or suppliers – so long as agreement is reached between the acquirer and supplier at each level. Many of the requirements in IEC 63187-1 are for agreements to be made on what exactly will be done. This flexibility means that appropriate analysis techniques can be chosen according to the type of system and the hazards and technologies involved – these techniques can include relevant human factors analyses.

3.2 Human factors requirements in IEC 63187-1

Requirements affecting human factors appear throughout the current draft of IEC 63187-1 (IEC 2025).[4] Acquirers and suppliers must explicitly agree the roles people are expected to play as part of the safety strategy for the system. This means identifying interactions between different human actors in the system, and with other system elements; and considering the part people play in the perception, interpretation, decision and action loops that control the system. The roles, responsibilities, human interfaces and assumptions about human behaviour are required to be documented, and the impact of human capabilities and limitations must be taken into consideration in the analysis of architecture and solution options, and to inform safety requirements and critical performance measures. The human factors methods and techniques used to develop the system and measure performance are also expected to be documented as part of the development.

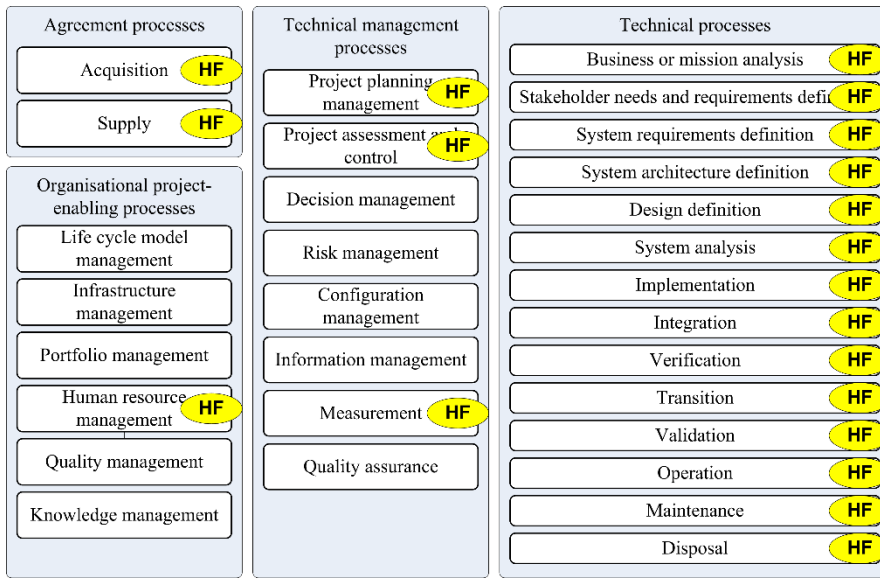

Fig 4. Allocation of IEC 63187-1 human factors requirements across ISO/IEC/IEEE 15288 life cycle processes.

Rather than just mentioning human factors as an input to hazard analysis, IEC 63187 embeds these human factors requirements throughout the entire system life cycle. Fig 4 shows how these requirements are distributed across the ISO/IEC/IEEE 15288 life cycle processes. In the early life cycle stages, the emphasis is on reaching a clear agreement between the supplier and acquirer as to the extent to which the human will be considered in future analyses of the system. The defined human roles and

[4] Note that these requirements may change during the approval and publication process.

responsibilities are then incorporated into the requirements for the subsequent system engineering processes as the safety strategy and system architecture are developed and refined.

While some requirements are explicitly focused on human factors, much of the HF content takes the form of criteria set on other requirements. For instance, the requirement for system analysis results to include safety aspects includes criteria for those results to include documentation of the analysis of human roles and responsibilities, human capabilities and limitations, and assumptions about human behaviours.

The focus of all these requirements is to prompt more consideration of the role people play in the overall system: how they interact with other system elements, and how the tasks they perform contribute to safe outcomes.

3.3 Applying the requirements

The human factors requirements in IEC 63187-1 are goal-based: they set out what outcomes are required but do not introduce a new HF methodology or require specific HF techniques and measures to be used to comply with the standard. Instead, guidance in IEC 63187-2 is expected to explain the intent behind the requirements, helping users of the standard select techniques and measures from the toolbox provided by existing HF literature. This allows the HF methodology used to achieve compliance to be tailored to the context of the programme.

As IEC 63187 is a systems engineering standard, its treatment of HF focuses on interactions between system elements, both human and engineered. This means that it deals more with the roles and responsibilities of humans within the system of interest, and their place in the perception, interpretation, decision and action loops than traditional aspects of HF such as design of human-machine interfaces or workplace environments. These aspects are still important but may be better addressed during the detailed design and realisation of individual system elements, rather than the broader architectural design developed under IEC 63187.

At time of writing, the HF guidance in IEC 63187-2 is still being drafted but is likely to take the approach that human system elements are critical assets in complex systems, requiring adaptability and resilience to manage variations in faults and operational scenarios. Perturbations (events that disrupt normal operations) are inevitable. They may arise from unexpected behaviour of the system itself, changes in its configuration or concept of operations, or changes in its operating environment. These perturbations demand human capability to diagnose, respond, and restore system stability within acceptable risk levels. Application of HF methods should identify aspects of the system design that enable effective human adaptation and optimise tasks supporting this process, such as by helping operators maintain accurate mental models of the system state. While human error is likely during operations, it must be anticipated without diminishing the value of human involve-

ment; instead, roles should leverage human strengths while acknowledging limitations. Human Factors (HF) approaches should examine system-level properties and interactions rather than isolated components, considering contextual influences such as environment, training, and stress. Responses to perturbations are dynamic and cannot rely solely on rigid procedures; flexibility and resilience must be supported alongside compliance with operational boundaries. Overall, HF analysis should integrate adaptability, context-awareness, and systematic support for human performance to enhance system robustness.

The outcome of applying HF in the context of IEC 63187 is for HF and system safety to be *co-engineered*. This means that both safety objectives and human factors considerations should be reflected in the architecture of the system-of-interest. As well as the engineered elements, this will include team, task and training design for the human system elements, and decisions around how functions are allocated between human and engineered elements to achieve appropriate levels of automation or human-machine teaming. Building HF considerations into the Measure of Importance scheme developed under IEC 63187-1 will mean that the MoI of safety requirements and objectives can reflect HF concerns. It also provides a mechanism to flow contextual information about safety concerns into the design of individual system elements, to inform human factors analysis at that level.

4 Conclusions

This paper has presented the approach that IEC 63187 is expected to take to integrating human factors into the system safety effort for complex defence systems. While the role of people as users or stakeholders in these systems is still important, IEC 63187 takes the view that humans can also be fully-fledged system elements in their own right and need to be considered as such during safety analysis.

The increasing complexity of safety-critical systems, particularly in defence, requires a new way of addressing human factors and system safety through the systems engineering process. IEC 63187 responds to this challenge by embedding HF considerations throughout the systems engineering life cycle, moving beyond the traditional 'Safety I' view of humans as sources of error to recognising them as integral system elements, whose functions contribute positively to the safety performance of the system. In doing so, it introduces a 'Safety II' approach, while still recognising the importance of the 'Safety I' This approach recognises that complex systems need resilience, and this often depends on human adaptability and decision-making, especially when unforeseen hazards or emergent behaviours occur.

The key contribution of IEC 63187 to human factors is to establish explicit requirements for HF analysis and definition of human roles, responsibilities, and interactions within the system architecture, unlike existing defence sector safety standards, which typically confine HF to hazard analysis or interface design. By requiring acquirers and suppliers to agree on these aspects, the standard ensures that HF is a core part of the safety strategy for the complex system, not an afterthought.

IEC 63187 is goal-based, specifying outcomes rather than prescribing methods, allowing flexibility in selecting proportionate HF techniques suited to the system context while allowing use of established HF principles and guidance. This flexibility means that the IEC 63187 framework will remain relevant as HF practice evolves, for instance to tackle emerging challenges such as human-machine teaming, AI explainability, and adaptive automation. IEC 63187 will also encourage adoption of a holistic perspective, considering humans as active contributors to system performance rather than external agents of risk.

Ultimately, IEC 63187 represents an important step toward bridging the gap between systems engineering, safety, and human factors. By embedding HF into the architecture of complex systems, it promotes designs that not only minimise human error but also harness human strengths to manage uncertainty and maintain safe operation under dynamic conditions. This shift from reactive to proactive treatment of HF is vital for achieving robust, resilient systems in an increasingly complex and interconnected defence environment.

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. The authors would especially like to thank Bertrand Ricque, who passed away in August 2023 and without whom IEC 63187, which brings together representatives from numerous defence industries and authorities, would not have been possible.

Image credits: Fig 1 was generated by Microsoft Copilot. Fig 2 by Flikr user Greg L, via Wikimedia Commons, used under Creative Commons CC-BY-2.0 license.

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.

References

Bainbridge, L (1983) Ironies of automation, Automatica 19(6):775–779. Elsevier. doi: 10.1016/0005-1098(83)90046-8.

Cummings ML and Bauchwitz B (2024) Identifying research gaps through self-driving car data analysis, In: IEEE Transactions on Intelligent Vehicles. doi: 10.1109/TIV.2024.3506936

DoD (2020) Human engineering, MIL-STD-1472H. Department of Defense

DoD (2023) System safety, MIL-STD-882E w/CHANGE 1. Department of Defense

DoD (2025) Human engineering requirements for military systems, equipment, and facilities, MIL-STD-46855 w/NOTE 3. Department of Defense

England R (2025) Human factors for systems engineers, Z12 Guide. Institute for Systems Engineering. https://ifse.org.uk/Documents/zGuides/Z12_Guide_DIGITAL_V2.1%20(IfSE).pdf. Accessed 18 Jul 2025

Hollnagel E (2014) Safety-I and Safety-II: the past and future of safety management. CRC Press. doi: 10.1201/9781315607511

ICAO (2021) Manual on human performance (HP) for regulators, Doc 10151, International Civil Aviation Organization. https://elibrary.icao.int/product/250419

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

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

IEC (2025b) IEC TR 63187-2 ED1 – Systems engineering – System safety – Complex systems in defence programmes Part 2 – Guidance. International Electrotechnical Commission (unpublished)

Inge J and Potiron K (2024) System safety for complex and defence systems. In: 43rd International Conference on Computer Safety, Reliability and Security (SafeComp), Position paper

Inge J, Potiron K and Machrouh J (2026) Putting importance into context: moving from the abstract to the concrete with IEC 63187. In: Proceedings of the thirty fourth Safety-Critical Systems Symposium (in press)

ISO (2011) ISO 26800 Ergonomics – General approach, principles and concepts. International Organization for Standardization

ISO (2022) ISO 31073: Risk management – Vocabulary. International Organization for Standardization

ISO (2023) ISO/IEC/IEEE 15288 – System and software engineering – System life cycle processes. International Organisation for Standardization

Leveson NG (1995) Safeware: system safety and computers. Addison-Wesley Professional

Leveson NG (2012) Engineering a safer world: Systems thinking applied to safety. MIT Press doi: 10.7551/mitpress/8179.001.0001

Leveson NG and Thomas JP (2018). STPA handbook. Massachusetts Institute of Technology

MOD (2018) Technical Guide TG7.3 – Human contribution to system safety. Ministry of Defence

MOD (2021) Def Stan 00-251 – Human factors integration for defence systems. Issue 2. Ministry of Defence

MOD (2023) Def Stan 00-056 – Safety management requirements for defence systems – Part 1: Requirements. Issue 8. Ministry of Defence

Myklebust T, Stålhane T and Vatn DMK (2025) Artificial Intelligence (AI). In: The AI Act and the Agile Safety Plan. SpringerBriefs in Computer Science. Springer. doi: 10.1007/978-3-031-80504-2_6

NTSB (2010) Loss of thrust in both engines after encountering a flock of birds and subsequent ditching on the Hudson River, US Airways Flight 1549, Airbus A320-214, N106US, Weehawken, New Jersey, January 15, 2009. Aircraft Accident Report NTSB/AAR-10/03. National Transportation Safety Board. https://www.ntsb.gov/investigations/Pages/DCA09MA026.aspx

NTSB (2019) Assumptions used in the safety assessment process and the effects of multiple alerts and indications on pilot performance. Safety Recommendation Report ASR1901. National Transportation Safety Board. https://www.ntsb.gov/investigations/Pages/DCA19RA017-DCA19RA101.aspx

Potiron K and Inge J (2024) Extending systems engineering for safety-critical defence systems. In: 34th Annual INCOSE International Symposium. pp 199-209. Wiley

Rasmussen J (1987) Approaches to the control of the effects of human error on chemical plant safety. In: International Symposium on Preventing Major Chemical Accidents. American Inst. of Chemical Engineers

Reason JT (1990) Human error. Cambridge University Press

Ricque B, Joguet B, Brindejonc V et al. (2022) IEC 63187 : Intégrer la sûreté de fonctionnement au sein de l'ingénierie système. In: 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement. Institut pour la Maîtrise des Risques. https://hal.science/hal-03878071

Salmon PM, Burns C, Broadbent S et al.(2024) The Chartered Institute of Ergonomics and Human Factors at 75: perspectives on contemporary challenges and future directions for Ergonomics and Human Factors. Ergonomics, 68(6), 759–775. doi: 10.1080/00140139.2024.2378355

Storey N (1996) Safety critical computer systems. Pearson Education

Wiggins J (2024) Human factors in functional safety assessment, Safety-Critical Systems eJournal, 3(1)