ISSN 2754-1118 (Online)
ISSN 2753-6599 (Print)

The Development of a Hybrid Nuclear Requirements Hierarchy (HNRH) and its Application to a Non-Specific Fusion Facility

Wendy Owen

Independent Consultant

Abstract

This paper forms a concluding article resulting from a several workpieces carried out during 2021—2022 as part of a research project on fusion hosted by the Nuclear Futures Institute (NFI) at Bangor University. The project considered current approaches to design safety (and associated topics, including security and environmental risk) in a wide range of highly regulated industries, both nuclear and non-nuclear. A comparison mapping between nuclear and non-nuclear sectors was developed, and this led to:

- *The development of a Hybrid Nuclear Requirements Hierarchy (HNRH).*
- *The application of the HNRH to a non-specific fusion application.*

It is these that are the focus of this paper. By the nature of its derivation, the HNRH is applicable to or suitable for adaptation for any "hybrid nuclear" application, i.e. a design or facility where the expected radiological risk contributes only a small part to its overall safety risk profile (this small part also when considering its surroundings and operating environment as a whole, not purely considering its internals, internal hazards, or only the impact of untoward events in its immediate vicinity). This may occur where the "nuclear quota" of the design (or through operation of said design) is evidently minimal, either by design or by a low level of consequence or impact of a radiological hazard in the event of a system failure or other mishap.

1 Introduction

Through 2021, as part of a research project on Design Safety Guidelines (DSGs) for future fusion plant, a literature search was conducted concerning current best practice on design safety (and associated topics) in a wide range of highly regulated sectors, both nuclear (fission-based only) and non-nuclear, the latter including process, renewables, biotech, rail, aviation, automotive, space, defence, water and environmental.

The reasoning behind this project was to acquire a sufficient level of knowledge of representative approaches to design safety that could be applied or adapted to future fusion plant; fusion here (and more widely) being acknowledged from a safety perspective as a "hybrid" of both nuclear and non-nuclear sectors.

The work from 2021 is not included here, although a summary is provided in Section 2.

This paper focuses on work carried out during 2022 on the subsequent development of a Hybrid Nuclear Requirements Hierarchy (HNRH) and its application to a non-specific fusion application. Observations and recommendations are also presented.

© Wendy Owen 2025.

The author has more recently been involved with safety cases for; a low-consequence nuclear decommissioning project (not dissimilar to the discussions herein), a new build full-scale nuclear fission plant, and an accreditation organisation dealing with recent significant regulatory changes and approaches to design safety in the construction sector.

2 Summary Of Earlier Outputs

2.1 Preliminaries

The work from 2021 is not included here, although a summary is provided below as an introduction to the work carried out during 2022. The whole project report amassed to over 150 pages.

Earlier work developed the research methodology, describing the approach taken to the identification, capture, collation, derivation and management of data, based on current practice in requirements engineering.

The characteristics of design safety, etc. in a wide range of (non-nuclear) highly regulated industries including process, renewables, biotech, rail, aviation, automotive, space, defence, water and environmental, were then described. The next focus was on capture of the same or equivalent characteristics of sub-sectors within the nuclear fission-based industry, including power plant, fuel cycle facilities, experimental rigs, medical applications, and decommissioning.

All literature supporting the work was sourced from publicly-accessible industry references, published within the last fifteen years or so; many papers were reviewed, with a small number subsequently selected for noteworthy discussions on design safety, safety cases, security, human factors, and environmental risk.

2.2 Requirements Database

The data associated with the work became extensive and was held in a requirements database, specifically developed during the project. This database formed the primary hub and “cog in the wheel” for the management of the requirements data, and also for the subsequent transposition of the data as described here. The data could be easily filtered and searched, and was stored and structured in such a manner that it could be easily moved or adapted into other applications.

2.3 Cross-Sector Requirements Mapping Table

The requirements captured had strong association with potential hazards and thus provided the basis for determining a hierarchy of safety goals, as seen across today’s highly regulated industries. The requirements captured from both nuclear and non-nuclear sectors were further analysed, developed and transposed into a Cross-Sector Requirements Mapping Table, to enable comparisons of data between the nuclear and non-nuclear sectors.

3 Derivation Of The Hybrid Nuclear Requirements Hierarchy (HNRH)

The HNRH developed during the course of the work is regarded as a significant output from this project.

Figure 1 provides a simple diagrammatic view of the heritage of the (baseline) HNRH and its potential application, to emphasis the relationships. It can form the fundamental reasoning or rationale behind the framework for a Safety Management System (SMS), or a requirements specification (SRS) and associated project deliverables.

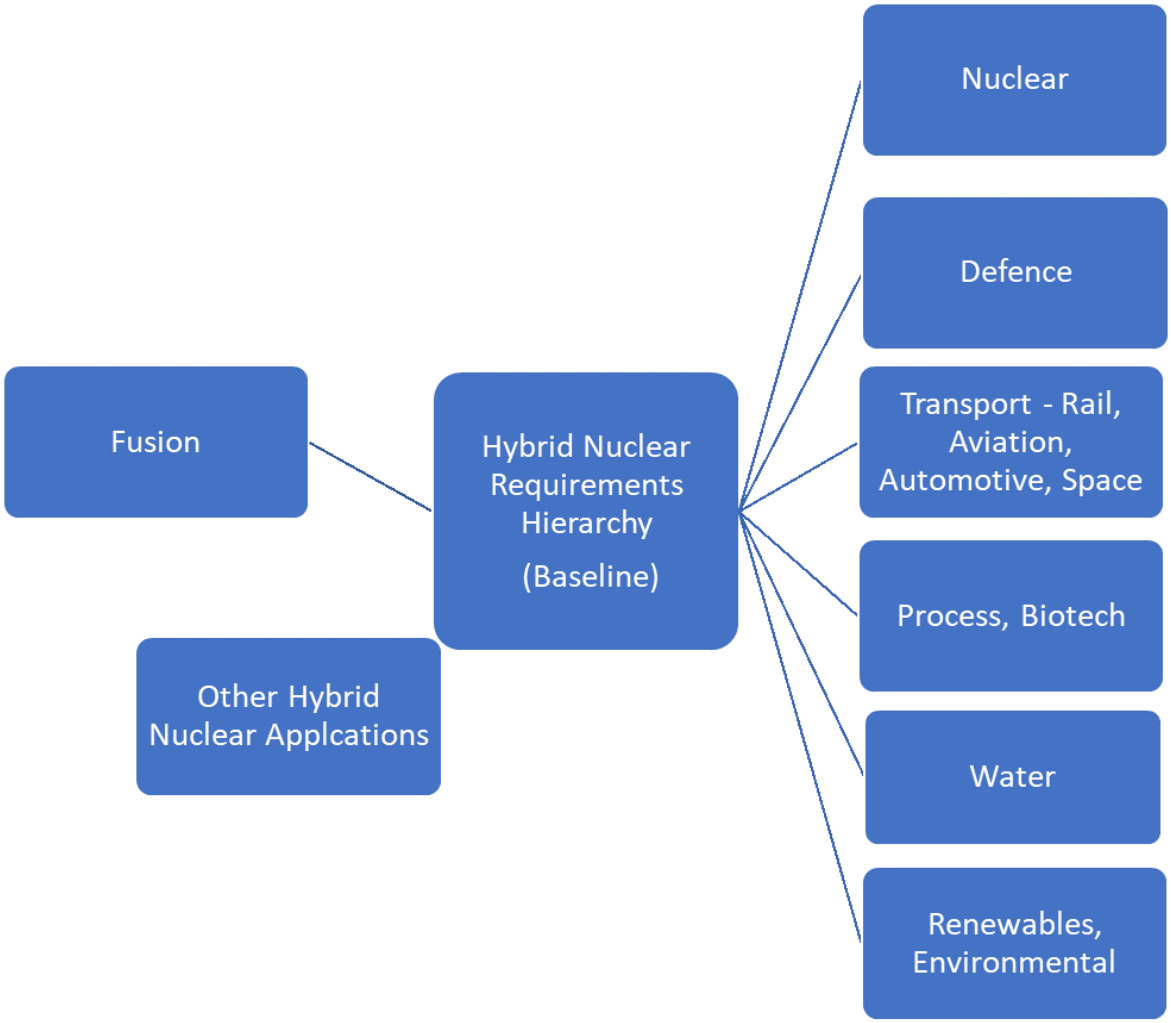


Figure 1 ~ Hybrid Nuclear Requirements Hierarchy: Application, Baseline and Heritage

The Mapping Table (described in Sub-section 2.3 above) provided the "groundwork" to generate the HNRH. Essentially, the data from both nuclear and non-nuclear sectors was transposed into a Requirements Mapping and, subsequently, into a Hierarchy of Safety (and associated) Goals. This is shown in the HNRH (Table 1 in Appendix A), wherein each requirement has a requirement identifier, a requirements hierarchy level, a short precis of the requirement and the commentary provides a fundamental description of the requirement in more detail.

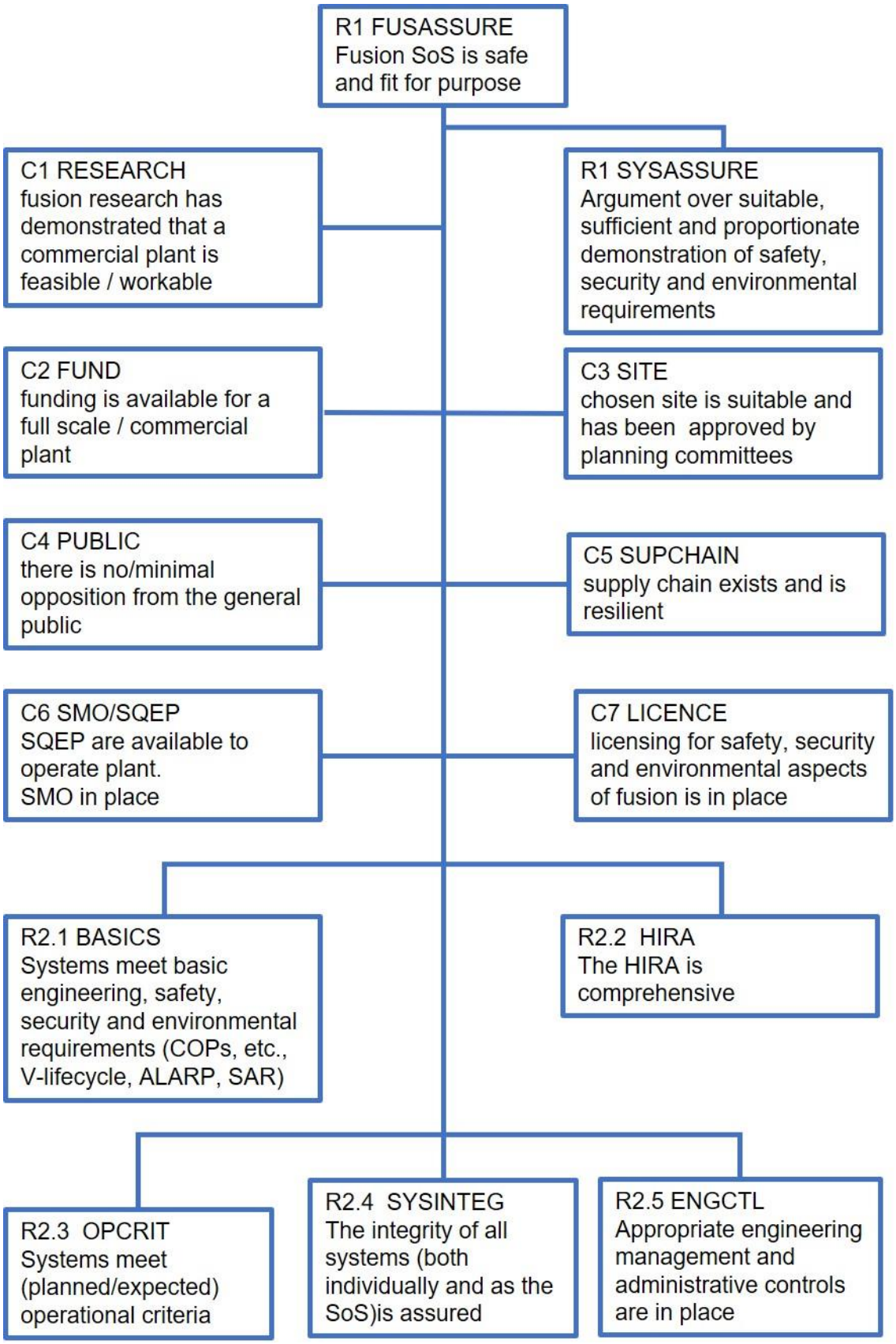


Figure 2 ~ Hybrid Nuclear Requirements Hierarchy: Requirements Schema

By the nature of its derivation, the HNRH is applicable to or suitable for adaptation to any "hybrid nuclear" application, i.e. a design or facility where the expected radiological risk contributes only a small part to its overall safety risk profile (this small part also when considering its surroundings and operating environment as a whole, not purely considering its internals, internal hazards or only the impact of untoward events in its immediate vicinity). This may occur where the "nuclear quota" of the design (or through operation of said design) is evidently minimal, either by design or by a low level of consequence or impact of a radiological hazard in the event of a system failure or other mishap.

The HNRH has also been transposed into a high-level requirements schematic/diagram, which is complementary to, and supports, the hierarchy framework, and should also be used as a reference guide (refer to Figure 2). At present this is indicative and contains only two levels; it could in theory be further developed for Level 3 and 4 requirements and applied to generic or specific hybrid nuclear applications.

A key point in the application — or reasonable use — of the HNRH herein proposed is that there is "active demonstration" of the existence of a hybrid nuclear system, rather than a nuclear or non-nuclear system, i.e. the framework has not been derived in a manner suitable for use on either nuclear systems (those where the predominant risk is associated with a radiological hazard), nor non-nuclear systems (those featuring no or negligible radiological hazard).

An assessing engineer should consider all aspects (or branches) of the HNRH in Table 1, as also shown in the diagrammatic requirements schema, Figure 2. Things to consider when expanding the lower levels include:

R2.1 ESSENTIALS/BASICS

- Best Practice, Standardisation and Approvals
- Adoption of V-Lifecycle
- ALARP/SFAIRP/ALARA
- Systems Assurance Report (SJR, security, environment), Traceability

R2.2 HIRA

- Hazard Management Strategy, Hazard elimination, Limiting/Minimising Risk
- Comprehensive hazard identification
- Hazard Assessment (Internal hazards, Fire and Explosives events, Electrical, External hazards)
- Hazard/Risk classification, prioritisation
- Human factors, Occupational Health & Safety
- Environmental Risk
- Security (physical, cyber)
- Suitable and Sufficient Risk Assessment (proportionate, worst-case scenario)

R2.3 DESIGNING FOR OPERATIONAL CRITERIA

- Specifications, Safety Criteria, Bounding
- Margins of Safety, Control of Margins
- Operating Limits, max. capability

R2.4 THE INTEGRITY OF SYSTEMS

- Layout, Zones

- Integrity of systems, defence in depth
- Integrity of protective measures
- Integrity of passive & active mitigations and procedures
- Protection systems, Barriers, Emergency systems
- Complex systems, systems integration
- Integrity of Performance
- Scale-ups
- Validation & Verification

R2.5 ENGINEERING CONTROL

- Effective Process and Organisational Safety/Risk Management, SQEP
- Engineering Management, Management of Change
- Control of Records

The following section discusses application of the HNRH to a non-specific fusion facility.

4 Application of the HNRH to the Fusion Sector

The concept of a "hybrid nuclear system" readily includes those associated with fusion energy; the HNRH thus forms a framework for application to fusion technology, systems and Fusion Power Plant (FPP).

The application of the HNRH to a non-specific fusion facility is discussed below with the details provided in Table 1. This table, in itself, can subsequently form the baseline or groundwork for a specific fusion project.

Application of the HNRH to a fusion facility will, for example:

- Consider the impact of new/novel technology. Standards must be used both with caution and commensurately (current standards in the nuclear sector are chiefly geared towards fission applications);
- Exclude Beyond Design Basis Accident (BDBA) events that would otherwise be considered as part of a nuclear safety case (but is not typical of other hazardous industries);
- Apply As Low As Reasonably Practicable (ALARP), as well as As Low As Reasonably Achievable (ALARA), principles for the radiological risks, which are expected to be short-lived; and
- Apply a tiered approach (known as "graded" in the nuclear sector). This is necessary to avoid over-regulation.

There are certain hazards associated with nuclear fusion technology, from experimental facilities to full scale plant of the future. However, it should be noted that the fusion reaction itself is not self-sustaining; there is no "chain reaction" such as that found in fission-based reactors.

Depending on the type of configuration, design and operation, at time of writing, the main "internal hazards" are anticipated (Cook et al. 2001) (Fraas 1974) (IAEA 2021) (Regulatory Horizons Council 2021) (Rooney et al. 2021) (ITER n.d.) to include:

- (Kinetic and Thermal) Energy of the plasma, and magnets.
- Very high intensity electromagnetic fields.
- Temperature excursions.
- Extreme high temperatures (from superheated wall blankets, venting/exhausts/divertors, primary coolant circuits, decay heat).
- Extreme low temperatures (from use of cryostats).
- Very high pressures (leading to failure of rupture discs in divertor circuits or other loss of containment scenario).
- Structural embrittlement of wall/blanket material from neutron bombardment (leading to other hazards).
- Chemical and material toxins, liquid and air-borne (similar to other sectors).
- Tritium release — Most current experimental fusion devices use a mix of deuterium and tritium as fuel. The main radiological hazard associated with a fusion reactor is the potential for tritium release into the locality/environment. However, both the potential for this, and the maximum amount of radiological material that could be released, are extremely low. Tritium is a radioactive isotope of hydrogen with a half-life of 12.3 years. By way of comparison, small amounts of tritium are used in radiopharmaceuticals and hence disposed of as a normal part of safely dealing with hospital waste, and tritiated water is also routinely created and discharged under environmental permit conditions during fission reactor operations.
- Radiological risks also include operational occupational exposure from activated structures, effluents (both liquid and gaseous), dust and waste, although these are at significantly lower levels than in nuclear fission plant and have low level classification (similar to that of hospital waste) and are not long-lived.

Additionally of note is that none of the above internal hazards would require a site evacuation were they to occur, unless combined with a fire, explosive, or security event. The credibility and likelihood of such a "double jeopardy event" depends on the design details, and thus would require assessment/review on a case-by-case basis.

The "external hazards" for a fusion facility are similar to those at other energy sector sites, and typically depend on geographical location, demographic features, and other factors beyond the site boundary; cybersecurity being an exception.

The focus of the fusion hazard suite, compared to fission processes, is thus on what may be regarded in the nuclear sector as "lesser accidents" — even if they are deemed major hazards in other sectors. This does not mean that the radiological hazard should be underplayed; it simply means that it should be assessed alongside all other credible hazards, and should be neither given more or less prominence or attention than the "conventional" or other major hazards — until and unless it can be demonstrated to be a high-risk hazard.

Due to the fundamental differences in the type/nature and risk of accidents associated with a fusion plant, compared to a nuclear fission plant, the application of a tiered (graded) approach is necessary to avoid overregulating the fusion process. The high safety and low radiological hazard of a fusion facility should thus also be factored into a clearly defined, but proportionate, regulatory environment.

As mentioned previously, a key point in the application of the HNRH or framework is that there is practical, visible and auditable demonstration of the existence of a hybrid nuclear system, i.e. rather than a nuclear or a non-nuclear system. Without such demonstration, the system will be more appropriately assessed by a "standard nuclear" (or non-nuclear, as appropriate) assessment regime.

Consideration of this HNRH is thus recommended for the fusion sector, and any other hybrid nuclear application where the radiological hazard is of low consequence, or otherwise constitutes a low risk. This includes fusion plant — these being more widely acknowledged from a safety perspective as a "hybrid nuclear" system. However, in the (currently presumed unlikely) event that a given fusion system/plant cannot easily demonstrate that it is a hybrid nuclear system, a conservative approach is required, and assessment and regulation should default to a standard nuclear framework. At the other end of the spectrum, neither should such a system be considered under (occupational) Health and Safety alone, no more than equivalent systems/plant in other safety-critical industrial sectors featuring major hazards.

At time of writing, there is currently much work happening in the fusion sector, and agility in approach is required. The HNRH presented here, with the framework that it provides for systems and safety assurance, although having a structure, essentially provides an agile and adaptable framework.

5 Conclusions

Key conclusions and significant observations from the project are provided below.

The main conclusions are as follows:

- A research method was developed for the capture and analysis of design safety (and associated topics) in a wide range of hazardous industries, resulting in a comprehensive database of requirements for non-nuclear, nuclear and hybrid nuclear applications.
- The derivation of the HNRH demonstrates that for safety (and associated) goals, a mapping exercise between a varied range of different sectors is possible, although complex and requiring significant prior expertise.
- The primary output of the work is the HNRH of Safety (and associated) Goals. This provides a baseline for requirements management of hybrid nuclear applications.
- The HNRH has been applied to a non-specific fusion facility, Table 1.

A key point in the application of the HNRH is that there is practical, visible and auditable demonstration of the existence of a hybrid nuclear facility, i.e. rather than a nuclear or a non-nuclear system. Without such demonstration, the facility — assuming it contains "nuclear quota" — will be more appropriately assessed by a "standard nuclear" assessment regime. However, in the (currently presumed unlikely) event that a given fusion facility cannot easily demonstrate that it is a hybrid nuclear system, a conservative approach is required, and assessment and regulation should default to a standard/established nuclear framework. At the other end of the spectrum, neither should such a facility be considered under (occupational) Health and Safety, no more than the equivalent in other safety-critical industrial sectors featuring major hazards.

It is noted that the fusion operating environment is not as hazardous as a fission equivalent, more equivalent perhaps to a process sector site in terms of a diverse suite of major hazards and its risk profile. There are best practices and techniques in other sectors that would benefit the fusion industry. It is important to adopt best practice within the bounds of safety, security and environmental assurance, with that best practice coming from a sound historic basis, whilst over time adopting newer techniques that enhance the credibility and value of the safety case.

Cross-sector pollination of ideas and approaches is important to this process, such that — in an ideal world — all sectors are adopting a requisite and proportional level of assurance. As systems and technology become more integrated, including energy systems, this "requisite level of assurance" plays a much larger part of the demonstration of safety. This is expected to impact the fusion sector as much as the inclusion of new technologies and applications in other high hazard industries.

In the two years since this project finished, the fledgling fusion power industry has ramped up to the point where it is now becoming a feasible reality, possibly within the next decade or two. This means that a safety case for a full fusion plant is now on the horizon, not beyond it. Consideration of information from test facilities will ultimately contribute to it, but it will need a SMS framework and a hierarchy of safety goals, the same as any other new technology or power plant being brought to market for the first time. At time of writing, there is still much work happening in the fusion sector, and so agility in approach is also required. The development of safety and associated documentation relating to future fusion power plant therefore needs to incorporate flexibility and agility.

The HNRH presented here, with the framework that it provides, although having a structure, essentially provides an agile and adaptable framework; it should be reasonably bulletproof against changes, and in supporting a requisite level of systems assurance. Adoption of this HNRH is thus recommended for the fusion sector.

The HNRH, given its derivation, can also be utilised on other projects where the "nuclear risk quota" is low. This could include, for example, decommissioning projects, medical, and space applications.

Acknowledgments

The author wishes to acknowledge the support of Welsh Government's Sêr Cymru programme for funding; Bangor University for supporting the energy industry; the Nuclear Futures Institute for hosting the project; and Prof L Williams for project supervision.

References

Cook I, Marbach G, Di Pace L, Girard C, and Taylor N. P. (2001). *Safety and Environmental Impact of Fusion*. EFDA Report, April 2001. European Fusion Development Agreement, Culham

Fraas A. P. (1974). *The Environmental Impact of Fusion Power*. Oak Ridge National Laboratory. Paper prepared for presentation at the American Association for the Advancement of Science, 140th meeting, San Francisco, California, 24th February — 1st March, 1974. https://www.osti.gov/servlets/purl/4344747. Accessed 30th April 2025.

IAEA. (2021). *Fusion Energy*. IAEA Bulletin, May 2021. International Atomic Energy Agency, Vienna. https://www.iaea.org/sites/default/files/fusionenergy.pdf. Accessed 30th April 2025.

Regulatory Horizons Council. (2021). *Report on Fusion Energy*. (31st May 2021, with supplement added 6th August 2021). UK Department for Energy Security & Net Zero and UK Department for Business, Energy & Industrial Strategy, London. https://assets.publishing.service.gov.uk/media/610d4211d3bf7f043e0a0904/rhc-report-on-fusion-energy.pdf. Accessed 30th April 2025.

Rooney M, Roulstone A, Locatelli G, and Lindley B. (2021). *Fusion Energy: A Global Effort — A UK Opportunity*. Institution of Mechanical Engineers, London. https://www.imeche.org/docs/default-source/1-oscar/reports-policy-statements-and-documents/imeche-fusion-report-ao.pdf. Accessed 30th April 2025.

ITER. (n.d.). *Safety and the Environment*. ITER Preliminary Safety Report. https://www.iter.org/mach/safety. Accessed 30th April 2025.

Appendix A. Hybrid Nuclear Requirements Hierarchy

Key:

The "baseline" requirements hierarchy associated with a hybrid nuclear application is reflected in green text, with the details of the baseline in black text.

Its example application to a non-specific fusion facility is shown in blue text, supplanted within baseline black text.

Table 1 ~ Hybrid Nuclear Requirements Hierarchy (HNRH) of Safety (and Associated) Goals and its Application to a Non-Specific Fusion Facility

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
BESTPRAC	1	To apply current Best Practice	Many standards, CoPs, and best practice guidelines exist within individual industries, with a proportion being cross-industry (including engineering/technical safety and functional safety standards and guidelines). The nuclear sector, by example, has a significant number of such documents in place. However, as many of these documents are based on established systems or designs, they can sometimes be difficult to apply to new technologies, or to adapt to advanced industries. The fact that some standards are only sporadically updated by volunteers adds to problems in a fast-moving technology landscape, as the documents can quickly become outdated. Any novel project can do its utmost to comply with best practice, but the use of certain current standards or outdated standards in such a situation may not be appropriate. This can impact the approval regimes or processes and — by implication — the time to market, as independent assessors/reviewers and regulators grapple with apparent non-compliances that the development team do not agree with. Any standards and CoPs associated with fusion will either need to be based upon — or adapted from — existing standards where the engineering/technology is well-established, or new ones will need to be developed where there is no equivalent currently available. If this were not the case, engineering would not be able to advance alongside new technologies, which can appear as "step changes" along a timeline; the change in interlocking system technology from relays to SSI to CBI is a good example of this, which affected a range of sectors. In practice, how well a project develops and presents its assurance case can make a notable difference. A good assurance case will be both "bullet-proof" and future-proof (as far as possible) and provide the necessary confidence to external approvers. This includes the *justification* of adopting standards, or argument in the event of the lack of suitable technical standards.
LIFECYCLE	1	To adopt a Whole Lifecycle approach	The concept of a "whole lifecycle approach" is common across sectors. However, the adoption of a "Standard V-lifecycle", and the Systems Engineering discipline in general, is less apparent in some sectors than others. For fusion, the adoption of current best practice systems engineering (including systems thinking, requirements management, V-lifecycle approach, performance monitoring, continual improvement, etc.) is advised to align with best practice and developments in systems engineering in other highly-regulated sectors.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
INSAF	1	To apply the concept of Inherent Safety	Demonstration of inherent safety is required. This includes having a comprehensive strategy for hazard management, a design in depth approach, and demonstration of ALARP, including consideration of elimination of hazards and reducing the risk of (residual) hazards. This is no different for fusion compared to other hazardous sectors. Caution is advised if using the terms Safety by Design (SbD) or Safety in Design (SiD) as, in many sectors, this apparently relates to occupational Health & Safety during construction and build phases, not technical/design/systems safety.
INSAF - HAZMAN	2	To implement a comprehensive strategy for Hazard Management	Having a strategy surrounding hazard management is an integral part of the approach to inherent safety. One particular — and important — goal highlighted for inherent safety is simplification; the simpler the system, the fewer the hazards, and the lower (or more manageable) are the risks. Today's engineers are designing ever more complex systems for use in ever complex operating environments and, with increasing digitalisation, simplification needs to be a "design feature" to help reduce both the safety and security hazard spectrums. There are certain hazards inherent to a fusion plant which — compared to other applications — are not possible to eliminate or even become more "magnified" in a fusion operating environment. It is these that will require particular attention within a hazard management system and strategy. Many sectors adopt the concept of "pillars of safety" for their SMS, typically between three and six pillars. The nuclear sector typically has six or seven pillars[1]. The equivalent for a fusion facility is proposed as follows: • The physical integrity of the facility — including the plasma containment system and other Structures, Systems and Components (SSCs) — must be maintained. • For all medium/high-risk hazards associated with the facility, there must be effective on-site and off-site monitoring systems, alongside emergency preparedness and response measures. • All safety and security (protection) systems must be fully functional at all times. • There must be secure off-site power supply from the grid. • There must be safe and uninterrupted logistical supply chains and transportation to and from the site. • The operating staff must be able to fulfil their safety and security duties and have the capacity to make decisions free of undue pressure; and • There must be reliable communications with the regulator and other third parties.
INSAF - HAZELIM	2	To consider Hazard Elimination	Hazard elimination is "the first port of call" for risk reduction, and also drives inherent safety. A fusion facility will have certain hazards that are specific to fusion or are an amplification or variation of those found in other sectors, and these will require treatment on a case-by-case basis. However, other hazards associated with a fusion plant are not dissimilar to those in other sectors, and thus should be treated in a similar manner, adopting the objective of elimination where possible and practical. Sometimes wholesale hazard elimination and/or risk reduction is not practically possible without great expenditure to a project, at which point design decisions may conflict with operational or stakeholder cost constraints. Application of Cost-Benefit Analysis (CBA) usually resolves such conflicts.

[1] See, for example, https://www.oecd-nea.org/jcms/pl_66360/nea-supports-the-iaea-7-pillars-of-nuclear-security-and-safety. Accessed 1st May 2025.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
INSAF – DID	2	To employ a Defence in Depth approach	Application of Defence in Depth (DiD) ensures a degree or level of safety integrity in any given application, and also drives the choice of Risk Reduction Measures (RRMs) and the adoption of fail-safe systems. The adoption of a DiD approach within fusion, as a core approach to inherent safety, is recommended. Refer also to discussions elsewhere on balanced assessments.
INSAF - ALARP	2	To reduce risks ALARP	The concept of ALARP/SFAIRP (So Far As Reasonably Practicable) is well-known across industries. The nuclear sector has the additional feature of ALARA, specifically covering radiological exposure. Both apply to the fusion sector. (Semi-quantitative) Risk matrices or scales are advocated at early stages of a project to assess and review risk tolerance, and throughout the design phase. These create both a hierarchy for addressing hazards and an understanding of the project's safety risk profile. The more the risks from a suite of hazards "move into the green zone" (or are made non-consequential from a safety perspective), the closer a system or facility is to becoming inherently safe. The identified higher risk hazards are typically assessed in more detail using quantitative risk analysis (QRA) and other numerical modelling, as relevant, but ultimately with a view to shifting them into the green zone, or at least "the amber zone". Tiered approaches are integral to a risk matrix approach; the loss of perception of hazard hierarchy and risk profile by not using a tiered approach is a factor that can lead to both over-conservatism and subsequent over-engineering. A risk matrix approach is thus recommended to support design decisions and ALARP demonstration. The concepts of BSO and BSL are also highlighted, and these should be determined (usually based upon national requirements for safety risk).
INSAF – RISKCONQ	2	To minimise impact from accidents	Inherently safe systems have no (or negligible) risk. Reducing impact (consequence) is a key tactic to reduce risk. This can include actions taken during an emergency scenario. DiD strategies to mitigate the consequences of accidents, primarily via the use of shutdown systems and containment barriers, do not generally include mitigations associated with emergency planning in the risk assessments of accidents. This results in a conservative approach in the consequence analysis of both severe and less severe accidents, and, in some circumstances, such an approach can result in overengineering and an alternative approach considering the "reliability" of all emergency actions (both system and human) should be investigated. DiD strategies in fusion should effectively be no different to those in other sectors.
INSAF – RISKFREQ	2	To minimise likelihood of accidents	As above, inherently safe systems have no (or negligible) risk. Reducing likelihood is another key tactic to reduce risk. Prevention and RRMs are key contributors to lowering the likelihood. The fusion facility design should aim to be inherently safe. Well-structured approaches to inherent safety to mitigate the likelihood of accidents come primarily via the use of passive designs, configurations (redundancy, diversity) and use of high integrity SSCs. Mitigations associated with shutdown systems and containment integrity are usually included in the risk assessments of accidents, and human reliability analysis should also be conducted as a matter of course (see below).
SOE	1	To define the safe operating envelope	The safe operating envelope (SOE) for the fusion facility should be unambiguously and well-defined.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
SOE-SPEC	2	To specify safe operating criteria	Safety Requirements Specifications (SRS) typically include coverage of a range of safety requirements, both quantitative and qualitative, along with targets and other design criteria. Limits and/or bounds also typically feature, which provide a written specification of the safe operating criteria for a given plant/facility or SSC. The appearance of SRSs is variable between projects but is always driven by the need for management of functional safety. For a fusion application, the development of SRSs should provision information and data on the limits and bounds of operation. It is particularly important that the background, origin or justification to such data be included or cross-referenced.
SOE-MARG	2	To specify safety margins and thresholds	The determination of safety margins provides the foundation for operational safety. Coverage is required of the determination of operational boundaries, limits and thresholds, and a description of the work that led to decisions surrounding them and the DBA. Uncertainty analysis should also be considered as part of the determination of the margins, where merited. As above, for fusion applications, it is particularly important that the background, origin or justification to such analysis be included or cross-referenced. Higher degrees of uncertainty — whether in design or operation — are of interest with new technologies (and should also be accounted for within the wider project/engineering risk assessment).
SOE–MARGCTL	2	To provide control of safety margins	Control of safety margins during operation (and maintenance and shutdown scenario) should be well-provisioned, both through the design itself plus a high integrity range of Control and Instrumentation (C&I) and backup systems. This aspect should be no different in a fusion application to one in other hazardous sectors. However, the uncertainty aspect (as discussed above) may impact the choice of such control systems.
SOE–PROTMEAS	2	To provide protective measures of high integrity	The concept of Design Basis Accident (DBA) should equate to a credible "worst case". Events that are not deemed credible by a team of Suitably Qualified and Experienced Personnel (SQEP) and those of negligible risk should be screened out. A Beyond Design Basis Accident (BDBA) approach should be used only by exception, for example when postulating "unknown unknowns"; it should not be used as the basis of designs or decision-making. Nevertheless, the "fragility" of an accident situation/scenario may be considered as part of the assessment of protective measures, which can impact the choice of measures (primarily systems of some type). This approach can be very appropriate for any "sudden", "rapid" or "extreme" excursions that could be reasonably expected in operation of a fusion plant, that could result in a hazard.
SOE-OPLIM	2	To retain control of operational limits	Control of reactions and transitory parameters such as pressure, heat and flow is key to maintaining a SOE on many energy and process plant. The focus is typically on rate of change of a parameter, monitoring that rate of change, and the associated impact of resultant stresses on SSCs. The extent of parameter monitoring, along with the development of comprehensive reliability centred maintenance programmes for the C&I, should be adequately reviewed and sufficient high integrity change monitoring systems and control functions enabled. This aspect is no different for fusion plant than those in other sectors, however, due to the nature of the fusion process, the control aspect also requires particular consideration of both the "fragility" and "uncertainty" (both discussed above).

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
SOE-MAXCAP	2	To optimise maximum capability	Coverage of "worst case" and "max capacity/capability" is expected, but a risk-based approach is also expected; where it is not deemed necessary (or desirable cost-wise) for safety purposes to cater for incredible/uncredible risks within designs, no additional capability should be required. The absolute maximum criteria for parameters affecting an SSC are typically found in technical specifications and manufacturers data sheets; this exercise then becomes more about matching the SSC's capability to SOE requirements and safety margins (based on the DBA). For SSCs in a fusion plant, it is important that the SSCs supplied have the ability to meet operational requirements — based on the DBA and SOE requirements — and in the long term to provide optimum usage and performance.
DETPROT	1	To provide capability in detection and protection	The fusion facility design should provide for adequate detection and protection (in all operational states and during emergencies)
DETPROT-CICOM	2	To provide appropriate and sufficient protection systems (C&I, comms.)	The form, configuration, functionality and purpose of C&I should be determined, to cover operations, maintenance, surveillance and emergencies. The majority are usually for monitoring and/or protection, including activation of emergency systems and staged responses. Communication systems should also be implemented to cover operations, maintenance, surveillance and emergencies. Both types of systems should incorporate features to mitigate dependent failures. Both C&I and comms systems have become increasingly digital in recent years (with wider technology moving towards cloud-based computing and, in future, verging towards AI), which presents challenges to both security and safety assurance. The digital segregation/separation of the plant and site from external influences in the digital domain should be assessed. This situation applies as much to fusion applications as it does in other industrial sectors.
DETPROT-BARR	2	To provide appropriate and sufficient barriers (containment)	Application of the concept of Layers of Protection (primary, secondary, tertiary) is advisable, and the extent and/or number of safety barriers should be commensurate with the DBA, and, by implication, hazards specifically associated with fusion as well as other (more conventional) hazards. Barriers are often discussed in terms of physical barriers, but sometimes other forms (geographical, zonal, functional, operational/human) are also relevant. The extent of barriers, in the context of necessary and sufficient barriers, should be reviewed, e.g. where there are few major hazards, or the risk profile is generally lower, using a risk-based CBA approach they would not be justified/warranted.
DETPROT-EMER	2	To provide appropriate and sufficient emergency systems	The general approach to the development of emergency and shutdown systems and emergency planning should be include arrangements that are commensurate with the risk profile and the safety integrity of the protection systems, although a conservative approach may be considered to align with "worst case" scenarios. Protection may include, for example, emergency shutdown and pressure relief systems. However, unnecessary/extensive inclusion of such systems can result in a higher rate of spurious failures and, by implication, loss of process/operation. There is a balance to be struck. The development of emergency responses and the implementation of emergency planning should be rigorously conducted for new fusion installations. This includes both the processes and the level of engagement with emergency services and the general public in the vicinity of the plant.
RISK	1	To conduct risk assessment	A suitable and sufficient risk assessment should be conducted on the fusion facility.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
RISK-HAZID	2	To conduct comprehensive identification of hazards	A "templated" suite of hazards should be avoided at all stages of design. Such an approach is contrary to the philosophy behind best practice hazard identification processes, which usually involve a free-formed, brainstorming process where study participants are asked to utilise their experience and judgement but are also highly encouraged to avoid preconceptions and think "outside the box". This is particularly relevant when introducing novel and new technologies, and thus including fusion applications. Coverage of a range of operating scenarios is expected — normal, abnormal, emergency, maintenance or shutdowns, both expected and possible. Hazard identification should be carried out for all operational states, and also at all stages of the lifecycle including manufacture, installation/build and end of life decommissioning. The inclusion of "no failure events" in the hazard identification is also highlighted. This is where one branch (or path) of an event sequence does not lead to an accident, although other branches do. This provides confidence (both qualitatively and quantitively) that the complete range of combinations and perturbations has been considered or modelled.
RISK-HAZAN	2	To conduct comprehensive analysis of hazards	Hazard identification includes identification of causes, failure modes, consequences, event sequences, etc. Hazard & Operability Study (HAZOP), Structured What-If Technique (SWIFT), Claim-Argument-Evidence (CAE), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Modes Effects & Criticality Analysis (FMECA), and related techniques, are advocated to varying degrees. However, credibility or "plausibility" is important for the safety argument and/or demonstration. The techniques chosen for assessment of a fusion plant should represent the best/optimal choice for a comprehensive assessment of the design and operations, with safety goals and safety demonstration in mind. To support the choice of techniques and associated analysis/analyses, Goal Structuring Notation (GSN), or a similar approach, is recommended for the development of the safety case.
RISK–SUITSUFF-P	3	To conduct suitable and sufficient assessment of risks to people	A Hazard Identification (HAZID) study usually encompasses workers and (as relevant) the public in a local vicinity and further afield. For certain fusion plant designs or locations, this may also include "downstream" or "delayed" effects with impact on workers, neighbours or the general public. For example, where relevant, radiological impact can be similar to certain environmental hazards, in that the effects may not be immediate, could be "downstream", and/or subject to delays in the apparent consequences. With such hazards, the short, medium and longer term need to be considered.
RISK-SUITSUFF-E	3	To conduct suitable and sufficient assessment of risks to the environment	A HAZID study sometimes encompasses environmental impact, both in a local vicinity and further afield. This may also include "downstream" or "delayed" effects. The basic tenet of an environmental risk assessment (ERA) is the impact of the system/facility on the environment (typically, on flora and fauna, as well as groundwater or other geological concerns), and also the reverse (where relevant). The possible risk to the environment from hazards other than radiological ones should not be overlooked. As with other hazardous sectors, for a fusion application, the process of ERA can be integrated with people safety at the HAZID stage. Similarly, ground, water, and air monitoring systems in the vicinity of a plant are usually required as part of the mitigation strategy.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
RISK-DBA-DETAIL	3	To conduct suitable and sufficient DBA	Individual perceptions of "suitable and sufficient" can vary, as do perception of the requirements of levels of detail and evaluation, and whether the risk evaluation is qualitative, semi-quantitative, or fully quantitative. The idea of what is "suitable and sufficient" can also be subjective amongst independent assessors and regulators. The robustness of safety argumentation can mitigate this variability. Levels of confidence and uncertainties also play a part in determining whether an assessment is suitable and sufficient. A more detailed analysis is sometimes argued to produce more confidence, but this is not always the case; indeed, it can provoke the opposite reaction, particularly if the input data is not high quality. Too much detailed analysis focussing on certain hazards (with no justified prioritisation) can also ignore or mask other issues, or even be a waste of time. Uncertainty analysis is more commonly used within fully quantitative, very-detailed, specific analysis. As with other hazardous sectors and novel systems, for a fusion application, a case-by-case approach is required to the DBA (until the technology is more established/demonstrated).
RISK-DBA-PROPN	3	To conduct a proportionate DBA	"Suitable and sufficient", discussed above, is not the same as "appropriate and proportionate". The former is about the "amount" or "level" of analysis surrounding the situation, whereas the latter is about whether the extent of the analysis that has been conducted is "in proportion to the risk" of the situation. In many hazardous sectors, tiered approaches are common; the (expected) risk profile determines the extent of analysis, and higher risk hazards attract deeper evaluation. Hence, a large number of high-risk hazards would merit many detailed risk analyses, whereas a small number of low-risk hazards would not attract any detailed risk analysis (and could be closed off by an argument using CoPs). There is arguably no merit or benefit in carrying out a detailed assessment of a low-risk hazard, but there is usually significant benefit to carrying out a comprehensive analysis of a high-risk hazard (as defined by a risk matrix) with a view to reducing its risk contribution to a more acceptable level. A balanced, usually tiered, approach is key to a successful proportionate risk analysis and DBA. A balanced, tiered approach is advocated for the fusion facility so that the assessment is in proportion to the hazards and risk profile.
RISK-DBA-WORSCAS	3	To include a worst-case DBA	The understanding of worst-case scenario(s) forms the basis of safety, and the worst-case scenario(s) should therefore be identified and defined. The questions of tolerability and negligible risk, and what are and what are not credible hazards, are fundamental to developing worst-case scenario and bounding of safety margins. For a fusion application, the worst-case credible scenario(s) should be determined for the case of both (people) safety and environment impact. The background to and arguments behind to the scenario(s) should be clearly evident within the supporting documentation. Any changes to the scope of the worst-case scenario(s) should be subject to formal change control (see later), as this is a fundamental element of the analysis that can reasonably be expected to have impact on the design of a plant, its SOE and/or its protection systems.
RISK-CLASS	2	To classify, categorise and prioritise hazards and risks.	Classification can take various forms, such as; bands on a risk matrix, prioritisation of actions, risk/hazard zones within a layout, classification of incidents/accidents. Classification can also occur "within" individual hazards, such as radiological classifications and fire/explosion zones. Classification of hazards/risks supports decisions behind risk reduction measures and, by implication, supporting the minimisation of risk. Risk classification, risk prioritisation, and risk profiling should be integral to design safety assessments. This philosophy or approach should be no different in the fusion sector to other hazardous sectors.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
RISK-RRMs	2	To implement appropriate suite of passive and active mitigations and procedures	RRMs can be passive, active, proactive, procedural and reactive. The overall approach to designing in protective measures may vary between projects, but passive and proactive RRMs are the best/preferred options, and reactive the least preferred. Newer or novel technology sometimes involves being "inventive" in the approach to assessment and implementation of RRMs, given no/little prior history on which to base or source optimal solutions. In such cases, including for fusion applications, the aim should be to develop a hierarchy for RRMs, based on the above approach, in line with current best practice for novel systems.
RISK-TOLER	2	To set risk targets and implement a risk-based approach	The typical approach to ALARP includes a risk-based approach, often complemented by cost benefit analysis (CBA). The overall risk target is typically devolved or spread amongst various systems and hazards (see also comments elsewhere on balanced designs), where the focus is more on general demonstration of SFAIRP. An "across the board" approach is similarly advised in devising or implementing risk targets for fusion applications/systems. Risk targets may be dominated by certain high-risk hazards. Also, for example, where a radiation hazard and associated dose target is apparent, there will be a focus on ALARA rather than ALARP *per se*.
HAZ	1	To assess internal, external and interface hazards	Both internal and external hazards should be reviewed for the fusion facility. Hazard types and/or the suite of hazards are not always predictable, particularly in newer or novel technologies. To "force" an approach based on an existing hazard suite, system or operation can be detrimental, as it can result in hazards being missed. Hazards are usually identified on a case-by-case basis, typically via HAZID/HAZOP/SWIFT and similar techniques, as previously discussed.
HAZ-INTL	2	To assess internal hazards	"Internal" hazards relevant to the fusion application should be identified and assessed. These are hazards internal to the site where the plant is located, where the cause is due to some type of failure, error or other untoward anomaly occurring within the site boundary.
HAZ-EXTL	2	To assess external hazards	"External" hazards relevant to the fusion application should be identified and assessed. These are hazards external to the site where the plant is located, where the cause is beyond the site boundary but impacts assets and/or operations within the site boundary.
HAZ-INTFACE	2	To assess interface and integration hazards	Integration and interface hazards should also be identified and assessed. These may occur within the plant, elsewhere within the site or at the boundary of the site. Non-physical interfaces should also be reviewed, such as communication functions. There can also be integration hazards between adjacent lifecycle phases, and between different operations. This is particularly prevalent in trial and demonstration systems, or where different parts of the system are added over the course of time. This may apply to fusion applications.
HAZ-INTL-FIRE / EXPLO	3	To carry out an assessment of fire and explosion hazards	In a range of hazardous sectors, Fire and Explosives Safety may be covered within the same remit, although where these hazards are particularly prevalent and/or merit detailed analysis it is advisable that they are studied and assessed in their own right. A similar approach is advocated for a fusion facility.
HAZ-INTL-ELEC	3	To carry out an assessment of electrical hazards	The extent of electrical safety risk assessment varies depending on the application. The requirement for EMI/EMC risk assessment increasingly applies with installations of advanced communications, computer technology, and cybersecurity risks. These types of hazards should be no different in a fusion application, however the magnetic aspect requires due attention.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
HAZ-INTL-OTHER	3	To carry out an assessment of other internal hazards	Other internal hazards to be assessed as relevant to the fusion facility on a case-by-case basis. There are particular hazards associated with nuclear fusion technology, from experimental facilities to full scale plant of the future. Depending on the type of configuration/design and operation, at time of writing, the main internal hazards are anticipated to include : • (Kinetic and thermal) Energy of the plasma, and magnets • Very high intensity electromagnetic fields • Temperature excursions • Extreme high temperatures (from superheated wall blankets, venting/exhausts/divertors, primary coolant circuits, decay heat) • Extreme low temperatures (from use of cryostats) • Very high pressures (leading to failure of rupture discs in divertor circuits or other loss of containment scenario) • Structural embrittlement of wall/blanket material from neutron bombardment (leading to other hazards) • Chemical and material toxins, liquid and air-borne (similar to other sectors) • Tritium release — Most current experimental fusion devices use a mix of deuterium and tritium as fuel. The main radiological hazard associated with a fusion reactor is the potential for tritium release into the locality/environment. However, both the potential for this and the maximum amount of radiological material that could be released are extremely low. Tritium is a radioactive isotope of hydrogen with a half-life of 12.3 years. By way of comparison, small amounts of tritium are used in radiopharmaceuticals and hence disposed of as a normal part of safely dealing with hospital waste, and tritiated water is also routinely created and discharged under environmental permit conditions during fission reactor operations. • Radiological risks also include operational occupational exposure from activated structures, effluents (both liquid and gaseous), dust and waste, although these are at significantly lower levels than in nuclear fission plant and have low level classification (similar to that of hospital waste) and are not long lived.
HAZ-EXTL-GEOTECH	3	To carry out an assessment of geotechnical hazards	Detailed evaluation of geotechnical events is expected where there may be, for example, concerns with the structural integrity of pipework or nuclear criticality hazards. The extent of evaluation for a fusion facility will usually depend on the location of the facility, but all credible events for that location should be considered.
HAZ-EXTL-WEATHER	3	To carry out assessment of extreme weather	Assessment of extreme weather conditions should be carried out. This usually depends on the location of the fusion facility, but all potential credible events for that location should be considered. Such an assessment may be combined with a resilience analysis of the site and should include the impacts of climate change.
HAZ-EXTL-OTHER	3	To carry out assessment of other External and Natural Hazards	Other external and natural hazard events should be assessed as relevant to the fusion facility on a case-by-case basis.
HF	1	To ensure consideration of human factors with the design and O&M	Consideration of human factors is necessary within the design and all aspects of O&M. The human interface aspects of the fusion facility should be highlighted within safety (and associated) documentation.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
HF-INTGN	2	To ensure appropriate design of HMIs	An evaluation of the capability for operator intervention during normal, degraded and emergency operations is required. Organisational structures and organisational measures should also be considered and optimised to improve safety at all stages of the project. Human reliability analysis is an integral part of both safety analysis and safety demonstration. In particular, the shift towards increasing digitalisation affecting operator training and interventions should be evaluated on a case-by-case basis. Human factors and the design of appropriate Human Machine Interfaces (HMIs) are of particular interest with new/novel systems, due to the higher levels of uncertainty in future operations; a fusion facility is no exception.
HF-SQEP	2	To ensure staff are SQEP	Other aspects of human factors to be accounted for include training, competency, independency of assessors, and capability and continuity of periodic safety reviews. The shift towards increasing digitalisation can affect the competence of operators both in day-to-day operations and during in an emergency. Other issues may include an aging workforce, affecting both succession planning and "SQEPness". This can be felt more acute depending on the nature of the hazards and if many roles require significant and specific training. Due to the nature of fusion energy, as a novel system, many operational and maintenance roles are expected to require both significant and specific training.
HF–OCCSAF	2	To minimise risk of occupational safety hazards	The treatment of occupational hazards tends to be either be treated via a "tick box" approach or (for more complex operations) associated with an identified suite of lower risk residual hazards. Any occupational radiological hazards should be suitably assessed by SQEP. In the UK, CDM Regulations[2] play a part in the approach to occupational Health & Safety and tend to be focused on construction and build phases. The treatment of occupational health and safety for a fusion application is not expected to be significantly different from that in other hazardous sectors, including nuclear.
ENVHAZ	1	To minimise hazards and risk to the environment	Environmental Risk Assessment (ERA), Environmental Impact Analysis (EIA), etc., are an integral part of technical risk assessments. These can be integrated with safety risk assessments and are often conducted in parallel during the design phase. Categorisation of environmental risks, Best Available Technique — Environmental Assessment (BATEA), environmental optioneering and monitoring should all be in evidence. The conduct of ERA itself is not expected to be significantly different for a fusion facility to other hazardous facilities, but will incorporate data specific to a given installation and hazard suite.
SYS	1	To ensure systems are safe	Adequate demonstration and assurance of safe systems within the fusion facility/site is required.
SYS-SPEC	2	To specify the basis for safety (SRACs)	Safety Requirements Specifications (SRSs), or Safety Functional Specifications (SFSs), are fundamental to design safety of SSCs. They specify (as relevant) the primary, secondary and tertiary requirements of the SSC, including any bounding criteria and/or caveats for operation. Safety-Related Application Conditions (SRACs) specifically support justification of bounding of the operational conditions, and any other conditions that may be particularly pertinent to the safety of the application. The concept of SRACs may prove useful for developments in fusion applications since the bounding conditions are a fundamental part of the operation. The inclusion of functional safety is "standard practice" in safety-critical and safety-related system applications, covering, for example, control, instrumentation and monitoring systems, as well as communication systems. The concepts can also be incorporated into other types of SSCs. The application of functional safety in the fusion domain is not expected to be significantly different to other sectors, although more unusual conditions should be considered as part of the assessment.

[2] The CDM (Construction Design and Management) Regulations aim to ensure the health, safety, and welfare of all individuals involved in construction projects.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
SYS-CLASS	2	To classify and prioritise hazards/risks	Classification of hazards and/or risks has been discussed previously. "Classification" of SSCs, based on their (actual/expected or perceived) importance to safety, should also be implemented. For fusion applications, a risk-based classification scheme of SSCs is advised (in comparison to a consequence-based classification schema).
SYS-INTEG	2	To ensure systems are appropriately integrated	Whole lifecycle systems engineering should be applied to all SSCs. This includes application of best practice in systems thinking systems integration, systems-based approaches, and associated deliverables. Within the systems architecture (schematics/diagrams), interfaces and integration aspects should be clearly evident; this is particularly important if the systems and/or sub-systems go through a range of configurations during the course of different phases of operation, which may be the case for certain fusion designs.
SYS-INTEG-COGEN	3	To demonstrate safe integration of adjacent or cogen (energy) systems	Whole lifecycle systems engineering should be applied to systems integration of any adjacent or cogen energy systems. It is possible that there may be more than one fusion plant on the site, or other forms of energy generation and storage, as well as connections to the grid. The fusion site assessment should include a SIMOPs (simultaneous operations) safety assessment, as relevant, to demonstrate the safe integration of different units on the site.
SYS-RESIL	2	To ensure systems are resilient in operation	Many performance/operability requirements also support safety integrity and risk reduction. The energy sector has performance targets in terms of reliability of energy production and its energy generation, storage, transmission and distribution systems. The objective of "no single point of failure" is typically met by a range of redundant and diverse designs. Both reliability and resilience analyses should be conducted for the fusion application, to ensure optimal plant reliability during operations and resilience during untoward events.
SYS-VV	2	To ensure systems are appropriately verified and validated	V&V is a fundamental part of the systems engineering whole life V-lifecycle approach and requirements management; it should be formalised on projects from a very early stage through the design and build/installation and test phase, to in-service and maintenance, and through to EOL/decommissioning. "Equipment qualification" is not the same as V&V, but it contributes to it. The approach to V&V for a fusion application, in particular for safety, should follow current best practice. See also whole lifecycle engineering.
SITE	1	To utilise an appropriate site	Demonstration of safety in the selection of an appropriate site, site upgrade or modification is required. The nuances of delivery, operation and maintenance of a fusion facility/plant, from manufacturing to disposal, should all be considered during the siting assessment, alongside its hazard risk profile.
SITE-ZONE	2	To ensure site layout is appropriately zoned	Systems and facilities sometimes have many interfaces (both physical and functional), as discussed above in Complexity. There are often many interface hazards, and also sometimes a range of "domino effects", that need to be considered in the event of an accident. For fixed facilities on a site, domino groups and hazardous zones require review; constraints (operational or physical) also usually feature. Security management can aid the risk from certain interface hazards (see below). Zoning of the fusion site, in terms of both layout and function, including any domino groups and hazardous zones, should be conducted as appropriate.
SITE-MINRISK	2	To ensure impact from site accidents is minimised	Siting considerations for a fusion facility also include: nuclear/radiological aspects, emergency planning, and actions tailored to circumstances, hazards, site characteristics (geology, weather, etc.), locality/populations, local services, etc. To ensure that the impact from potential accidents is minimised, the site hazard risk profile should be consulted when determining emergency planning and impact on the local area and population.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
SCALUP	1	To ensure that scaling-up is demonstrably safe	Scale-ups can encompass a wide range of systems, from "the lab", to pilots and demos, up to near-full scale tests. The transition towards full scale demonstration requires proficient engineering management to be integrated within development of the safety case and use cases, as early as possible. A wide range of test and prototype facilities is beneficial, as these can be used for verification purposes prior to full scale use, e.g. for testing/trialling equipment, clarifying predictive modelling, etc. Parameters can be analysed in detail prior to subsequent stages in a project. The lack of certain types of test facilities and prototypes in-house or in-country can hinder development or progress on projects. Scaling up is often used as a basis when bringing a new product/system to market. Where scaling up is being used as the basis of an argument or justification for the safety of a new fusion facility, this requires particular attention to verification and validation. Configuration control is also essential.
SECUR	1	To ensure system/site is secure	Site security of a fusion facility from a physical, cyber and materials accountancy perspective requires demonstration. This is no different to other hazardous/nuclear facilities.
SECUR-PHYS	2	To demonstrate system/site is physically secure	Many regulated and nationally critical sectors are well-adapted to dealing with physical security threats. Approaches to physical security are well-established. Where merited, sites/plant can be "highly guarded", with their own specialised trained police force. The physical security aspects of the fusion facility should be assessed, and mitigations put in place as appropriate.
SECUR-CYBER	2	To demonstrate system/site is cyber secure	Approaches to cyber-security, at time of writing, are still in development. Some sectors are more advanced and/or more affected than others. Isolation of plant/systems from external threats of this nature can ensure that the risk is minimised. Both older and newer technology should be evaluated. The cyber security aspects of the fusion facility should be assessed, and mitigations put in place as appropriate.
SECUR-MATACC	2	To account for hazardous material quantities	The physical removal or theft of hazardous substances is often considered under security, safety and asset management. Specific material accountancy of any radioactive materials is required, as it is (by international law) necessary to account for it on a local, national and international scale. This aspect is no different for fusion facilities to other hazardous sites where low-medium level radioactive waste occurs.
MANAGE	1	To ensure design and O&M processes are appropriately managed	To ensure that engineering management and other project processes are aligned with safety requirements for the fusion facility.
MANAGE-ENG	2	To identify responsible engineers and stakeholders	Identification of internal and external stakeholders, responsibilities and accountabilities, committees, etc., is important at all stages in the project lifecycle. The structure/framework of engineering management and key deliverables should be in evidence. This is no different for a fusion project to other major engineering infrastructure projects, however the approval bodies through the course of the lifecycle should be clarified (see licencing).
MANAGE-CHANGE	2	To ensure that change is safely management and implemented	Management (and traceability/auditability) of change during feasibility and design phase is important, as are any changes post-build. Change management is particularly important for introduction of new technology such as fusion projects. These may undergo many design changes prior to installation, plus there is a possibility of further modifications post-installation. Every change, however minor, should be documented. Changes should also be assessed for safety, security and environmental impact, as well as for functionality.

Reqt. Code	Reqt. Level	Safety Goal	Commentary on Hybrid Nuclear Application and a Non-Specific Fusion Facility
MANAGE-SMS	2	To ensure development of suitable, sufficient and effective SMS	The Safety Management Plan (SMP, or similarly titled document) contains the SMS framework for the development of the project safety case, including the (expected) technical approach and the top-level safety requirements. A SMP is usually very formal, and formalised. However, a lack of flexibility or agility in the approach, especially with new/novel systems, can result in unwarranted costs and/or unnecessary designs, and even (in the worst case) considerations or items being missed/omitted. This also applies to the development of fusion systems. It is therefore important that the SMP for a fusion project retains an agile, yet also fully auditable, approach.
MANAGE-HAZMAN	2	To ensure development of suitable, sufficient and effective management of hazards	The hazard log/register/record (and associated lists of major hazards, SCEs, ECEs, RCIs) forms the "hub" or cornerstone of the safety case. If a hazard log is incomplete, or contains incorrect information, this undermines the rest of the safety case. Once generated, the hazard register (usually with an integral or associated actions register) remains "live" throughout the remainder of the lifecycle of the project, right through to disposal. It also has strong links or mappings to the requirements register. The development of a hazard log should commence from an early stage of the project, ideally at concept stage. This approach should be no different in a fusion project to applications elsewhere.
MANAGE-SAFCASE	2	To provide suitable and sufficient demonstration of safety	Modern safety cases can be increasing complex, with the requirement to cover aspects of, for example, cyber-security and to integrate with ERA. Regular audits should also form part of the SMS throughout the lifecycle. A fusion project can be expected to develop a modern safety case; this means the adoption of GSN, which is now well established in a number of hazardous sectors. At time of writing, MBSA and/or the Assurance 2.0 approach may also be considered. GSN is particularly adept for assuring the development of new and novel systems.
MANAGE-LICEN	2	To provide suitable and sufficient independent review of safety	In general, licensing processes in the UK (alongside land planning) are quite comprehensive. Existing licensing, regulatory and ISA frameworks should be reviewed at the start of a fusion project to determine appropriateness.

This collation page left blank intentionally.