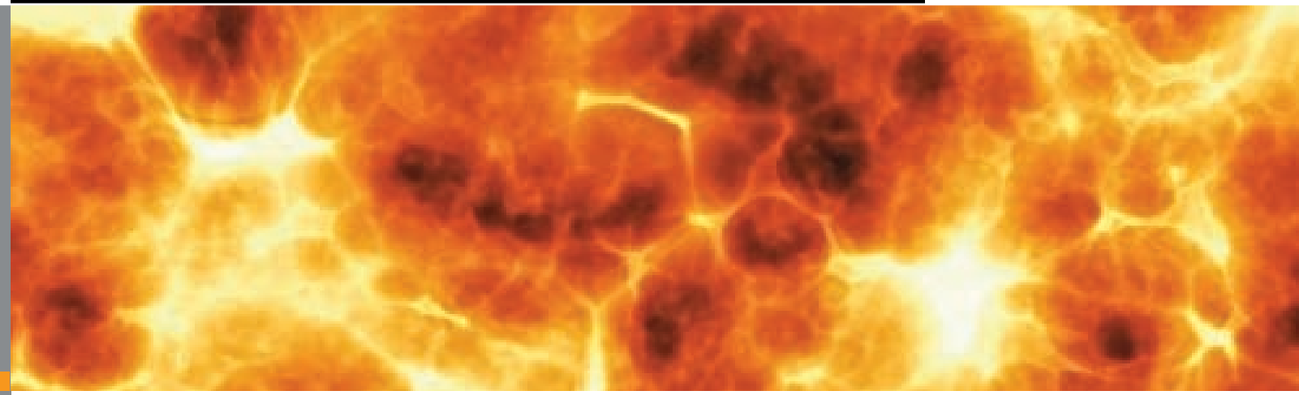
Golden Hill Centre
School Lane
Leyland
Preston
Lancashire
PR25 2TU
Tel: 01772 622200
Fax: 01772 622455
Email: contactus@jfnl.co.uk
Web: www.jfnuclear.co.uk

SAFETY RELATED SYSTEMS



Responsive nuclear engineering and support services

“Safety is the top priority in all industries”

“There is no such thing as zero risk”

- **No physical item has a zero failure rate,**
- **No human being makes zero errors, and**
- **No piece of software can foresee every possibility.**

A Safety Related System manages the risk of failures in machinery and systems which could result in physical injury or damage to the health of people, or impact on property or the environment. James Fisher Nuclear provides a range of engineering design and substantiation services to meet the safety system needs of a broad range of industrial sectors.

JFN engineers use a systematic approach backed up by a comprehensive quality management system to deliver systems to a range of international, national and customer specific standards including:

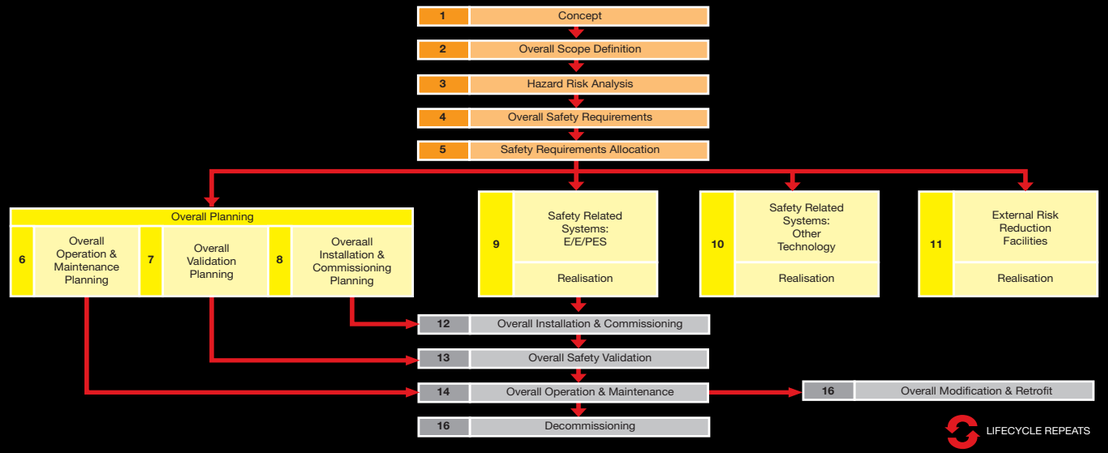
IEC61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety related Systems
IEC61511	Functional safety - Safety instrumented systems for the process industry sector
IEC61513	Nuclear power plants. Instrumentation and control for systems important to safety
IEC62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
BS EN ISO 13849-1	Safety of Machinery, Safety related parts of control systems, Part 1 (General principles for design)
DEF 00-54	Requirements for Safety Related Electronic Hardware in Defence Equipment
DEF 00-55	Requirements for Safety Related Software in Defence Equipment
DEF 00-58	HAZOP Studies on Systems Containing Programmable Electronics
BNF.EG.0090_1	Sellafield Limited - The Engineering of Electrical, Electronic and Programmable Electronic (E/E/PE) Safety Measures

- **All standards follow a risk-based approach to determine the requirements of safety functions.**
- **All standards emphasize the importance of the whole risk and the interdependence of its parts, in contributing to the reduction of risk.**
- **All standards use a classification scheme for representing and specifying the ‘Safety Integrity Level’ (SIL) requirements of safety functions.**
  - **Under IEC61508 these are identified as SIL 1, 2, 3 & 4.**
- **All standards provide similar logical step approaches from system concept through to decommissioning.**

The key differences between the standards are terminology. IEC 61511 and IEC 61513 provide more sector-specific guidance than IEC 61508.

Safety targets can be achieved using mechanical or software devices. In general, mechanical devices are relatively simple and hence easier to implement and justify. Software devices are used in more complex systems which are consequently more challenging to implement and justify. JFN has experience in developing safety systems using both mechanical and software devices.

The Safety Lifecycle Process



Safety Requirement/Concept & Scope - IEC61508 Phases 1 & 2

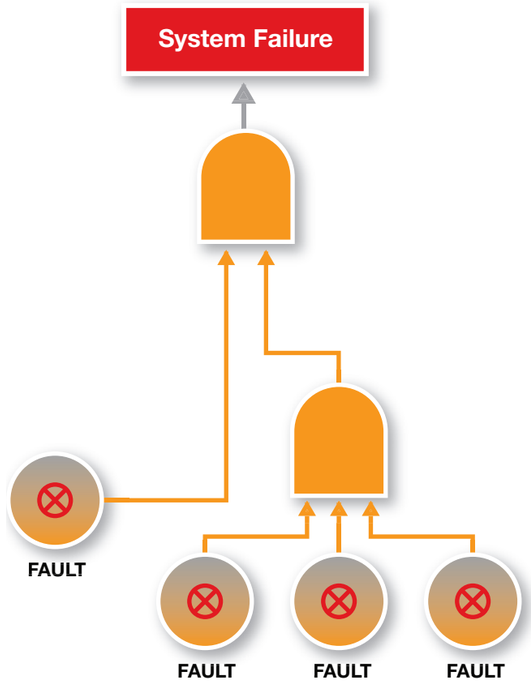
The Safety Lifecycle first critically examines the potential hazards and carries out a high-level analysis of the functional safety requirements. This Hazard Analysis will identify whether functional safety is necessary to ensure adequate protection against a potential/significant hazard and define the risk mitigation strategy.

Risks and Hazard Analysis - IEC61508 Phase 3

The next phase is to carry out a thorough examination of the risks arising from the equipment under control. This process systematically studies the occurrence of hazards causing alarm and the degree of severity of the harm. Hazards are assigned a numerical risk weighting from the product of 'incident frequency' and 'incident severity'.

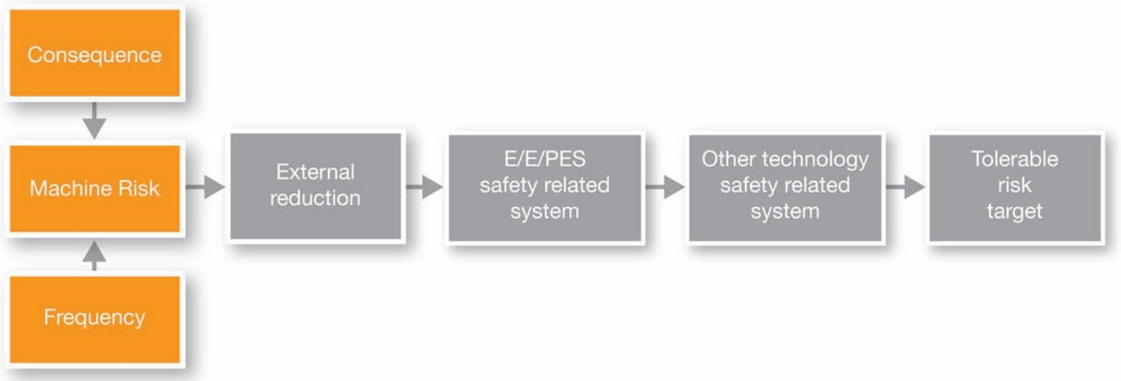
JFN routinely deploys a battery of tools to support the analysis of risks as required by IEC 61508 and IEC 61511 including checklist, model and graph methods as well as HAZOP, FME(C)A, FMEDA, ETA and FTA.

HAZOP -	Hazard and Operability study
FMEDA -	Failure Mode Effect and Diagnostic Analysis
ETA -	Event Tree Analysis
FTA -	Fault Tree Analysis



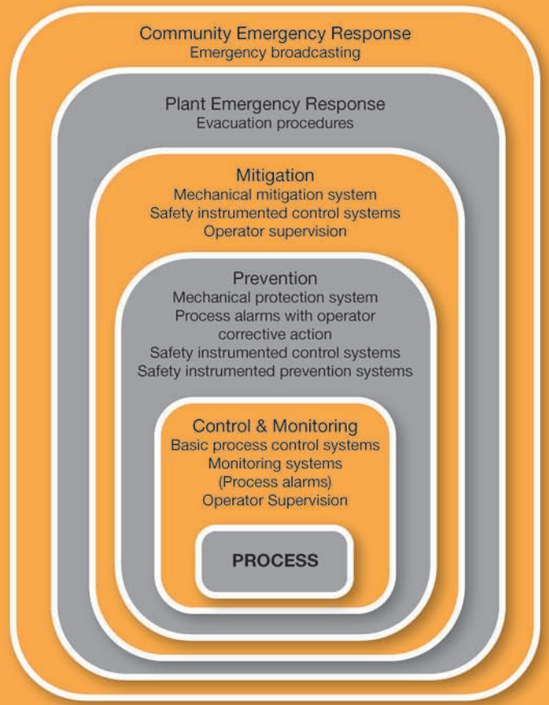
Determination of Overall Safety Requirement - IEC61508 Phases 4 & 5

The next phase is a quantitative evaluation of the failure probabilities which characterise the overall safety performance and a careful consideration of how the safety performance target can be achieved. A specific risk may be reduced by one or more layers of protection to achieve the tolerable risk target. Careful consideration is given to measures such as mechanical protection devices, barriers, access restrictions and control system trips before an electrical/electronic/programmable electronic system (E/E/PES) or another safety related system is used.



Heading here?

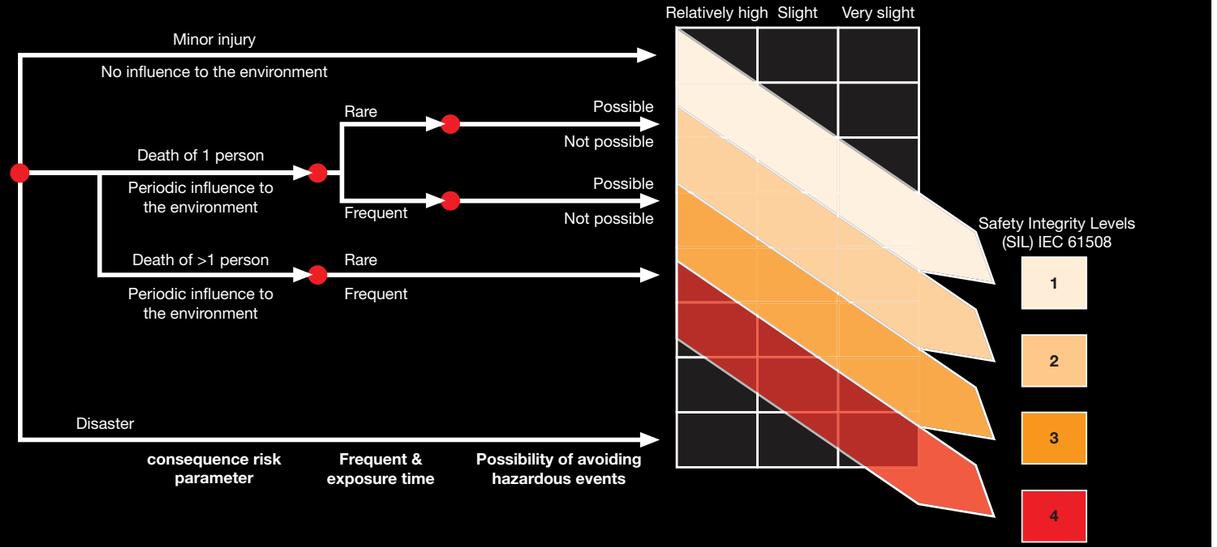
The probability of failure to perform of the system is then evaluated using tools including qualitative and calibrated risk graphs, layers of protection analysis (LOPA) and quantitative risk analysis (QRA)



IEC 61511 - Concept layers of protection (LOPA)

Heading here?

The more critical role played by the safety related system, the more reliable and resistant to faults it must be. The probability of a safety related system performing the required safety function under all stated conditions within a stated period of time is known as the safety integrity of the system and is expressed in levels. Combining all of the analyses, a safety integrity level (SIL) is allocated to the E/E/PES safety related system.



Heading here?

The allocation of a SIL level is a key milestone in a design process based on IEC 61508, as the SIL level defines the design considerations and gives quantitative targets for the system performance and reliability. The safety lifecycle process now has a series of parallel planning and realisation activities before the setting-to-work activities.

SIL level	Typical system architecture
SIL 1	Standard components, single channel or twin non - diverse channels.
SIL 1	Standard components, 1 out of 2 or 2 out of 3, possible need for diversity. Common cause failure allowance needed.
SIL 1	Multiple channel with diversity on sensing and actuation. Common cause failures a major consideration.
SIL 1	Specialist design.

Planning - IEC 61508 Phases 6 to 8

Planning is an essential step to ensure that the installation, commissioning and operating activities support the delivery of the safety functionality of the system. As well as encompassing the usual system delivery considerations, there is the specific requirement to validate the safety functionality and to ensure that the operational and maintenance regime supports the delivery of the functional safety to the appropriate SIL level. JFN has extensive experience of preparing installation, commissioning and testing plans as well as operations and maintenance instructions for safety systems.

Realisation - IEC 61508 Phases 9 to 11

Designing and building the safety system is normally the largest and most time-consuming task, but because of the work which has preceded it, is relatively straightforward. The prior analyses have defined the system architecture and the reliability requirements and given guidance on suitable building blocks for the system whilst the safety requirements will necessitate a simple design. The structured design process used by JFN ensures that safety systems are designed by SQEP staff and delivered with the essential reviews and independent checks. System manufacture is carefully controlled with all suppliers selected for their ability to deliver to the required quality standards. Components and sub-systems are tested and certified as conforming to specification before being built into the system. Once complete, the system is thoroughly tested before installation and commissioning.

Installation, Commissioning, Validation and routine operations - IEC 61508 Phases 12 to 14

Delivering the plans for setting the system from the installation and commissioning phase through system verification into live operation is supported by JFN engineers to ensure that the safety functionality of the system is demonstrably achieved.

Modifications and retrofits - IEC 61508 Phase 15

The requirement for modifications or retrofits can arise from a variety of sources and could be as a result of obsolescence, a change in the operation or a periodic review of the system. Any change to the system requires careful consideration to ensure that the safety functionality of the system is maintained.

The first task is to identify if there has been any change to the functional safety requirements and the impact of any change on the existing safety justification. This assessment will define whether the existing safety analyses and justifications are acceptable or will need to be reworked in part or completely.

The second task is to consider changes to engineering practice since the system was designed. Legacy equipment may require extensive validation and verification in order to demonstrate that functionality is maintained to current standards.

The final task is to take the output of the first two tasks, and plan and execute a programme which steers any proposed change through the entire safety lifecycle.

Care needs to be taken to ensure that the full package of documentation including the safety analyses, design, commissioning, testing, operation and maintenance are updated to reflect the changes made.

Decommissioning - IEC 61508 Phase 16

When there is no longer a requirement for the system, it is decommissioned.

Safety Case Substantiation

JFN has experience of carrying out engineering assessments as part of a Long-Term Periodic Reviews (LTPR). These assessments of legacy installed equipment and plant have been in line with phase 15 of the IEC 61508 safety lifecycle and have led to the design and delivery of appropriate modifications, upgrades and in some cases, system replacement.