IEC 61508/IEC 61511 Checklist for use during SIS design and implemenation

The objective of this checklist is to provide guidance for those SIS related activities that normally are the scope and responsibility of the system integrators.

No.	Subject/ requirement	Requirement / control question	Deviation, finding or Action Y/N/NA	Result / recommendation / action
Management of functional safety (IEC 61508-1, ch. 6, IEC 61508-2, ch. 7.7, 7.9/ IEC 61511-1, ch.5)				
	Roles and responsibilities	Have an overall responsible been denoted for the SIS design, implementation, and installation? If several responsibilities exist; have means to ensure coordination and exchange from one phase to another been implemented?		
		Have the skills/competence been described for the various activities that are being performed during SIS design, implementation, and installation?		
		Has it been verified that personnel involved in SIS design have the necessary competence?		
	Verification and validation planning and executing	Have an overall verification and validation plan been established that include: • All activities necessary to *verify* that each phase of the design, implementation, and installation complies with what was specified when entering the phase (e.g., that the implemented hardware and software complies with the specified design specification). Verification activities may be unit tests, integration tests, design reviews, documentation reviews and so on. • All activities necessary to *validate* that the selected hardware and software design is (1) suitable in terms of meeting the overall safety requirements and (2) suitable in terms of not introducing negative side effects on the SIS ability to respond to process demands, or on other systems. The validation plan may include various reviews, FSA,		

		FATs and SAT.		
		Have any formal assessments of compliance to the IEC requirements, like e.g., functional safety assessments (FSA), been defined and included in the verification and validation plan?		
		Is there a clear traceability between the tests specified in the factory acceptance test (FAT) and the site acceptance test (SAT) and the detailed functional safety requirements of the SIS?		
		Has any reviews been planned and performed to check for incompatibilities between the SRS, the detailed functional safety requirements of the SIS, the specified SIS tests (particularly the FAT and the SAT), and SIS related documentation?		
		Do the FAT and SAT include "response to failure and unexpected inputs" as well as "correct operation"?		
	Implementing and monitoring	Are procedures and systems in place to ensure that the recommendations from the hazards and risk analysis are taken into consideration during design, implementation, installation, and preparation for operation and maintenance?		
		Have procedures and systems (tools) been established to follow-up any deviations found during verification and validation activities?		
		Are assumptions made regarding environmental and operational conditions taken into account in all phases of the SIS design and development phases?		
	Management of change	Have procedures and systems (tools) been established for handling design and configuration changes of hardware and software, including necessary analysis and allocation of responsibilities.		
	Preparing for operation	Have a system been established for safe transfer of any outstanding deviations and findings from the design phases and to the operation phase?		
		Have an overview of all SIS related documentation been established, showing which phases they are prepared, which phases they are being used, and how they are linked together?		
Conceptual design (IEC 61511-1, ch. 6, IEC 61508-2, ch. 7.2)				
1	**SIF specification**	Does the SRS provide the following information for each SIF? Alternatively, have a detailed safety requirement specification been developed that describes:		

		• Characteristics of demands:
		  ○ The sources of demands (why and how they arise, "scenarios")
		  ○ The types of demands that the SIF shall respond to
		  ○ If human errors may create demands on the SIF
		  ○ Demand rates
		• The specified SIL of the SIF, and if relevant, the anticipated reliability of the SIF (for example in case the maximum PFD is specified to be less than 0.5E-3 for a SIL 3 SIF)
		• The expected response to process demands
		• Safe state in case of SIS failures (spurious operation, safe detected failures and dangerous detected failures)
		• Safe and dangerous failure modes of each SIF component
		• Interface with other systems (other SIFs, the BPCS, or outside
		• Expected operational conditions
		• Maintainability
		• Human interaction necessary to restore, restart or intervene with the SIF?
		• Function test intervals
		• Procedures that are necessary in order to start and restart the SIS
		• Means to set overrides, inhibits and bypasses, and how they should suspended
		• Means to provide operators and maintenance personnel with status information on bypasses, inhibits, and overrides
		• Response to detected failures
		• Mean time to repair, and necessary provisions to make this repair time achievable
		• Protective means against environmental extremes
		• Facilitation of safe access from remote locations (if this is an option)
		• Function testing, including:
		  ○ Test strategy (one test, or several subtests)
		  ○ Test coverage (to what extent the different failure		

		modes may be detected)		
		Are the essential and secondary SIF functions described in a separate functional safety requirement specification of the SIS?		
Detail design/Implementation (IEC 61511-1, ch. 11, IEC 61508-1, ch. 7.4)				
	General requirements	Has it been clearly stated if the IEC 61508 or the IEC 61511 requirements are used as basis for the design?		
		Have any deviations from regulations, codes and standard practice been identified, e.g., • Authority regulations • Company internal requirements and guidelines • Standards like API RP14C • OLF070 guideline		
	Hardware design	Have all safe and dangerous failure modes of each SIF component been identified and described?		
		Have potential constraints associated with the SIF components been identified? For example: • Any limitations in how the SIF components may respond to hazardous events? • Potential negative effect from spurious activation, function testing, and real process demands on the components lifetime • Any constraints to how long time the components may resist an accidental or hazardous event		
		Have diagnostic features and their provisions been described? For example; has an analysis been performed that identify which dangerous failure modes that may be detected and what means that must be in place to ensure that the these failure modes continue to be detected during the components lifetime?		
		Have protective means against CCFs been evaluated and taken into account: • Through the design, implementation, and installation *work processes and procedures?* • In the hardware *architecture?*		
		Have protective measures against CCFs between different protection layers been evaluated and implemented, for example between a		

		NAS function and a PAS function?		
		Have superfluous functions, that are functions provided by a component without having been specified, been identified and analyzed with respect to the potential of affecting the SIF performance?		
		For SIFs that are not designed fail-safe: Is the rationale of not selecting a fail-safe design of the SIF documented?		
	Software design	Have consideration been made to whether the IEC 61508 or IEC 61511 requirements apply to the software development? • IEC 61511 may be used if using limited variable language or fixed programming language • Else, the IEC 61508 must be used		
		Have a software specification been developed based on the detailed functional requirement specification of the SIS? Is there a clear traceability between the SIS functional requirements and the software requirements?		
		If the IEC 61508 requirements apply and are used; Have the software development tools been verified (for example by filling out a checklist) against the SIL dependent requirements in requirements of the IEC 61508-3, regarding: • Software requirement specifications • Software architecture design • Support tools and programming language • Software realization (detail design) • Software module testing and integration • Integration of hardware and software • Software safety verification and validation • Software modifications • Functional safety assessment of software		
		If the IEC 61511 requirements apply and are used; • Are the software development tools proven in use for safety applications or certified for use up to the specified SIL level? • Is fixed programming or limited variability language used for software implementation?		

		Have potential constraints of the software implemented functions been identified and analyzed, including the impact of configuration and parameter set-up, timing, software task sequences?		
		Have the consequences of wrong task sequences, overstress, lack of communication, wrong input parameters, or unexpected input combinations been analyzed?		
		Have the causes of dangerous software failures been identified and analyzed?		
		Have means to avoid or detect dangerous software been accounted for in the hardware and software design?		
	Development of reliability model	Has a functional or system model been established showing how all SIS components of interact in order to perform the SIF? Does the model also include interface with other components and systems (e.g., with the process control system, to operator stations, and so on).		
		Has an analysis, like e.g., an FMEA, been performed to identify all components that upon failure may impede the SIS from performing the SIF?		
		Has it been assessed if utility supplies (power, hydraulic, pneumatic) must be included in the reliability model?		
	Development of data dossier	Has the source and assumptions made for the reliability data been clearly stated?		
		If components are based on new design; Has (1) an assessment been performed to evaluate the reliability of the new design compared to historical performance (safe and dangerous failure rates), or (2) a qualification testing been performed to assess and document the reliability of the new design?		
		Has the assumptions behind the diagnostic coverage (DC) been explained?		
		Has the assumptions behind the safe failure rate been explained, for example: • What type of safe failures that have been included in the failure rate estimate? • Whether or not the contribution from non-critical components has been omitted. Non-critical components are components that are not included in the SIF, but which have		

		been included for other purposes, for example to provide status information (e.g., valve position sensors).		
		If the selected reliability data deviate from previous operational experience on similar equipment (e.g., in OREDA); Has the rationale for selecting reliability data that differs from previous operation experience been explained?		
	Determination of architectural constraints	Has the selected CCF fraction (β) been explained, by e.g., using checklists? Does the selected CCF take into account operational as well as design related issues?		
		Is the safe failure fraction (SFF) well documented in terms of e.g.,: • Clearly showing that the SFF is calculated for the component as a whole, and not only for electrical/electronic/ programmable electronic part parts of the component. For example if the SFF comprises the solenoid part as well as the mechanical part of a solenoid valve • Clearly showing the factors that contribute to a low or high SFF. For example by showing if a high SFF is due to a high spurious trip rate or a DC?		
		Have the rationale for classifying SIF components as either type A or B been clearly stated? Alternatively, if using the IEC 61511 approach; Has the rationale for selecting HFT-SIL relationship for sensors, final elements and non-PE logic solvers been explained (there are three options available in the IEC 61511, part 1, chapter 11.4.3 and 11.4.4)?		
	Calculating the probability of SIF failing dangerous	Has it been evaluated if the SIS is operating in the high/continuous or low demand mode?		
		Has the mathematical approach to reliability modeling been explained?		
		Have the main assumptions of the selected mathematical approach clearly stated, for example regarding handling of CCFs and redundant configurations with different types of component?		
		Has it been evaluated how the probability of failure on demand (PFD) target should be placed within the specified SIL?		
		Have sensitivity analysis been performed for the estimated PFD (or		

		rate of dangerous failures for high/continuous mode), to assess the implications of uncertainty in reliability data (e.g., failure rates, β-factor)?		
	Avoidance and control with systematic failures during software development	Has a software requirement specification been established and based on the detailed functional requirement specification of the SIS?		
		Has a software development and verification plan been established, for example by using the principles of the V-model?		
		Does the software development and verification plan comprise review of software safety requirements with respect to potential ambiguity, review of software requirement implementation, review of ability to capture software failures during implementation and testing, and a list of tests necessary to ensure the software integrity (unit tests, integration tests)?		
		Have procedures been established for analyzing the impact of software corrections and modifications?		
		Have procedures been established for avoidance of introducing software failures during implementation and testing?		
	Avoidance and control with systematic failures during design processes	Have means to avoid, reveal and correct systematic failures during the design, implementation and installation been implemented, for example design reviews, documentation reviews, loop checks and so on?		
		Are the personnel involved in SIS design, development and installation/commissioning familiar with how systematic failures are introduced, how they may be avoided, and how they may be revealed?		
	Preparing for avoidance and control with systematic failures in operation	Have means to avoid and reveal systematic during operation and maintenance related activities been analyzed and accounted for in the hardware and software design? One example is to perform human HAZOP or task analysis to identify assess human error vulnerabilities, and use this knowledge to improve the SIS design.		
		Have means to avoid introducing (CCFs) during operation and maintenance been evaluated and accounted for in the hardware and		

		software design?		
		Have operation and maintenance related activities been analyzed in order to identify necessary bypasses (in field), inhibits, and overrides (in software)?		
		Have means to monitor status on bypasses, inhibits, and overrides been considered and taken into account in the hardware and software design?		
		Have means to avoid improper setting and restoration after bypass, inhibits, and overrides been evaluated and taken into account in the hardware and software design?		
		Have means to avoid human errors that may cause a demand on the SIF been evaluated and taken into account in the current hardware and software design?		
		Have potential vulnerabilities of human interfaces (e.g., operator stations and displays) on the ability to detect and control hazardous events and process demands been considered?		
		Does the current SIS design provide useful alarm descriptions, alarm prioritization, and guidance on the sequence of events during a response to a true or false process demand?		
		Have assumptions like e.g., mean repair times, response to dangerous detected failures, constraints on operational and environmental exposure been captured in relevant operating and maintenance procedures?		
		Have means to avoid unauthorized access to the SIS been evaluated and accounted for in the design?		
		Have means to ensure safe access to information needed as part of integrated operation been considered, and taken into account in the design?		
		Does the hardware and software design facilitate function testing?		
		If condition monitoring is applied for components; Has the contribution from condition monitoring been considered when specifying the scope of function testing and inspections?		
		Have the constraints of the function test compared to a real process demand been specified?		
		Has other means to partially test the function been considered (e.g., partial stroke testing of valves)?		

		In case the function test is split into two or more subtests, e.g., separate testing of input and final elements; • Has the need for bypasses, inhibits, and overrides been evaluated? • Have the possibility for testing interfaces between different SIS applications, for example emergency shutdown system (ESD) and fire and gas detection system (F&G) been considered?		
		Have a list of all documents from design, implementation and installation that must be updated during the operation phase been prepared?		
		Have assumptions and constraints that must be accounted for during operation and maintenance (e.g., constraints on environmental exposure) been clearly stated?		
		Have all the issues related to safety integrity verification of the SIF been addressed in a safety analysis report (SAR)?		
	Preparing for software modifications	Have means to analyze the effect of software modifications, verify the software changes prior to installation been identified, and document the software changes been accounted for in SIS management of modification procedures?		
		Have procedures been established that show how SIS modifications are to be initiated, approved and implemented during the operation phase?		
	Preparing for SIS performance monitoring	Are the performance targets established for the SIS unambiguously lined to the SIL-requirements, for example the PFD??		
		Have the necessary facilities (tools, systems) for data collection been identified?		
		Have procedures been established for data collection, classification, and analysis?		
		Have means to collect data on CCF events been considered?		
		Have procedures been established that describe how the measured SIS performance may be used to update e.g., the function test interval, initiate root cause analysis, improve operation and maintenance procedures?		

Installation and commissioning (IEC 61511-1, vh. 14, IEC 61508-1, ch. 7.13				
		Have measures against introducing systematic failures and CCFs been accounted for in the installation and commissioning procedures		
		Have means been implemented to ensure that any failure introduced during installation and commissioning, e.g., leaving detectors with cap on, are revealed before the SIS is put into operation?		