0x51F77A59

Offshore Oil Platform Safety System

System Decomposition Report

Generated 2026-09-07 — Derive by AIRGen

derive.airgen.studio • info@airgen.studio

About This Report

This report was generated autonomously by the Derive@AIRGen systems engineering platform. An AI agent decomposed the system into subsystems and components, classified each using the Universal Hex Taxonomy (a 32-bit ontological classification system), generated traced requirements in AIRGen, and built architecture diagrams — all without human intervention.

Every component and subsystem is assigned an 8-character hex code representing its ontological profile across 32 binary traits organised in four layers: Physical (bits 1–8), Functional (9–16), Abstract (17–24), and Social (25–32). These codes enable cross-domain comparison — components from unrelated systems that share a hex code or high Jaccard similarity are ontological twins, meaning they occupy the same structural niche despite belonging to different domains.

Duplicate hex codes are informative, not errors. When two components share the same code, it means UHT classifies them as the same kind of thing — they have identical trait profiles. This reveals architectural patterns: for example, a fire control computer and a sensor fusion engine may share the same hex because both are powered, synthetic, signal-processing, state-transforming, system-essential components. The duplication signals that requirements, interfaces, and verification approaches from one may transfer to the other.

Requirements follow the EARS pattern (Easy Approach to Requirements Syntax) and are traced through a derivation chain: Stakeholder Needs (STK) → System Requirements (SYS) → Subsystem Requirements (SUB) / Interface Requirements (IFC) → Verification Plan (VER). The traceability matrices at the end of this report show every link in that chain.

Referenced Standards

- EN 13565-1
- EN 60079-29-1
- IEC 60268-16
- IEC 61508 — Functional safety of E/E/PE safety-related systems
- IEC 61511 — Functional safety — Safety instrumented systems for process industry
- ISO 7731
- NFPA 15

Contents

Acronyms & Abbreviations

Acronym	Definition
LOPA	Layer of Protection Analysis

Decomposition Tree

Offshore Oil Platform Safety System	51F77A59
├ Blowout Prevention System	DFF73859
├ Emergency Evacuation System	50FD7A59
├ Emergency Shutdown System	51F77A59
├ Fire Protection System	55F73A58
├ Fire and Gas Detection System	55F77A19
├ HVAC Safety System	51F77A59
├ Process Safety System	55F77A59
├ Public Address and General Alarm System	54FD7A18

Specification Tree

Requirement coverage by subsystem. Columns show count of requirements tagged to each subsystem across document types.

Subsystem	SUB	IFC	ARC	VER	Total
Blowout Prevention System	0	0	0	0	0
Emergency Evacuation System	0	0	0	0	0
Emergency Shutdown System	0	0	0	0	0
Fire Protection System	0	0	0	0	0
Fire and Gas Detection System	0	0	0	0	0
HVAC Safety System	0	0	0	0	0
Process Safety System	0	0	0	0	0
Public Address and General Alarm System	0	0	0	0	0

Stakeholder Requirements (STK)

Ref	Requirement	V&V	Tags
STK-REQ-001	The Offshore Oil Platform Safety System SHALL detect and respond to all credible major accident hazards — including hydrocarbon release, fire, toxic gas exposure, and well blowout — in sufficient time to prevent escalation to a platform-level emergency. Rationale: The duty holder has a legal obligation under the Safety Case Regulations to demonstrate that major accident hazard risks are reduced to ALARP. The safety system is the primary engineered barrier between a process upset and a catastrophic event. Without timely detection and response, minor releases escalate to fires, explosions, and potential loss of life.	Test	stakeholder, session-324
STK-REQ-002	The Offshore Oil Platform Safety System SHALL enable the safe evacuation of all personnel from the platform within the time-to-untenable-conditions established by the Safety Case quantified risk assessment. Rationale: Offshore Installation Managers and platform operators need confidence that in any credible emergency scenario, the safety system provides sufficient warning, communication, and evacuation support to get all personnel off the installation before conditions become unsurvivable. This is the overriding stakeholder concern — every other safety function exists to buy time for evacuation.	Demonstration	stakeholder, session-324
STK-REQ-003	The Offshore Oil Platform Safety System SHALL comply with IEC 61511 for safety instrumented systems and IEC 61508 for safety-related hardware and software, achieving the Safety Integrity Levels specified in the Safety Requirements Specification for each safety instrumented function. Rationale: The regulatory authority (HSE in UK, BSEE in US) requires formal demonstration that safety instrumented systems meet recognised functional safety standards. Non-compliance risks enforcement action including prohibition notices that halt production. IEC 61511 is the process-sector implementation of IEC 61508 and is the universally accepted basis for SIS design in oil and gas.	Inspection	stakeholder, session-324
STK-REQ-004	The Offshore Oil Platform Safety System SHALL achieve a spurious trip rate of no more than one per year per safety function on average, to prevent unnecessary production shutdowns while maintaining required safety integrity. Rationale: Platform operators and the duty holder need the safety system to be dependable in both directions: it must trip when needed (safety integrity) and not trip when not needed (availability). Each spurious platform shutdown costs approximately USD 1-5 million in lost production and restart costs. Excessive spurious trips also degrade operator confidence, increasing the risk of alarm overrides. The one-per-year target balances safety and operational economics per industry practice.	Analysis	stakeholder, session-324

Ref	Requirement	V&V	Tags
STK-REQ-005	The Offshore Oil Platform Safety System SHALL support online proof testing and partial-stroke testing of safety instrumented functions without requiring process shutdown or degradation of the protected function below SIL 1. Rationale: Maintenance technicians on offshore platforms operate under severe logistical constraints — helicopter access, limited crew size, compressed maintenance windows during turnarounds. If proof testing requires a process shutdown, it either doesn't get done (degrading safety integrity over time) or requires costly production outages. Online testing capability is essential to maintain target SIL throughout the proof test interval.	Demonstration	stakeholder, session-324

System Requirements (SYS)

Ref	Requirement	V&V	Tags
SYS-REQ-001	The Fire and Gas Detection System SHALL confirm a hydrocarbon gas release at or above 20% LEL within 10 seconds of gas reaching any detector in the affected zone, using 2ooN voting logic to eliminate single-detector false alarms. Rationale: The 10-second detection confirmation window derives from the overall escalation timeline analysis: a typical high-pressure gas release reaches flammable cloud dimensions within 30-60 seconds. Combined with the <1s ESD actuation requirement, a 10s detection window leaves approximately 20-50s margin before ignition probability becomes significant. The 20% LEL threshold is the industry-standard alarm setpoint per EN 60079-29-1, providing early warning before reaching the 60% LEL high-alarm trip threshold.	Test	system, detection, session-324
SYS-REQ-002	The Emergency Shutdown System SHALL actuate all designated final elements for an ESD Level 1 (total platform shutdown) within 1 second of receiving a confirmed hazard input, including closure of all ESD valves, isolation of ignition sources, and initiation of process depressurisation. Rationale: The 1-second actuation budget is allocated from the overall safety system response time target. Logic solver scan time (100ms) plus solenoid valve response (200ms) plus ESD valve stroke time (remaining budget) must fit within 1s. This is achievable with TMR logic solvers and spring-return fail-close actuators. Exceeding 1s delays isolation of the hydrocarbon source, allowing the flammable inventory to grow and increasing the probability and severity of ignition.	Test	system, esd, session-324
SYS-REQ-003	The Emergency Shutdown System SHALL achieve SIL 3 for all ESD Level 1 safety instrumented functions, with a probability of failure on demand (PFDavg) no greater than 1x10^-3 over a 12-month proof test interval. Rationale: SIL 3 allocation for ESD Level 1 functions derives from the LOPA (Layer of Protection Analysis) performed during the Safety Case. An ESD Level 1 failure leaves the platform with no automated means of isolating the entire hydrocarbon inventory during a confirmed major hazard. The 1x10^-3 PFDavg is the upper boundary of SIL 3 per IEC 61511 Table 4, and the 12-month proof test interval reflects the typical offshore maintenance cycle (annual turnaround).	Analysis	system, safety, session-324

Ref	Requirement	V&V	Tags
SYS-REQ-004	The Public Address and General Alarm System SHALL deliver an audible alarm exceeding 65 dBA above ambient noise level in all occupied platform areas within 2 seconds of ESD activation, and provide intelligible voice announcements with a Speech Transmission Index of at least 0.5 in all muster areas. Rationale: The 2-second activation time ensures the PA/GA alert reaches personnel before the physical effects of the hazard (gas migration, radiant heat). The 65 dBA above ambient threshold is the minimum per ISO 7731 to ensure alarm audibility in process areas with ambient levels of 85-95 dBA. STI >= 0.5 (the 'fair' intelligibility threshold per IEC 60268-16) is necessary for personnel to understand verbal evacuation instructions above background noise — lower STI means personnel cannot distinguish muster commands from abandon commands.	Test	system, alarm, session-324
SYS-REQ-005	The Emergency Shutdown System SHALL achieve a mean time between spurious trips of at least 8760 hours (one year) for each ESD Level 1 safety function, demonstrated by SIL verification calculation using actual failure rate data. Rationale: Directly derived from the stakeholder one-per-year spurious trip target. The 8760-hour MTBST maps to this target for continuous-demand assessment. Achieving this with SIL 3 integrity requires careful architectural design — TMR voting (2oo3) in the logic solver, redundant sensors with voting, and diagnostic coverage to distinguish dangerous failures from safe failures. Without this target, the system would be over-conservative and economically unviable.	Analysis	system, availability, session-324
SYS-REQ-006	The Fire Protection System SHALL deliver a minimum water application rate of 10.2 L/min/m2 to the design fire area within 30 seconds of deluge valve activation, sustained for a minimum of 4 hours from the firewater storage reservoir without external water supply. Rationale: The 10.2 L/min/m2 rate derives from NFPA 15 / EN 13565-1 for hydrocarbon pool fire suppression on offshore platforms. The 30-second delivery time accounts for deluge valve opening (5s), ring main pressurisation (10s), and system charge time (15s). The 4-hour endurance derives from the worst-case fire scenario duration identified in the Quantitative Risk Assessment, accounting for the time to depressurise and isolate all hydrocarbon inventories plus a safety margin.	Test	system, fire-protection, session-324

Classified Entities

Blowout Prevention System `DFF73859`

Well control safety system for an offshore oil production platform comprising subsea BOP stack (annular preventer, pipe rams, blind/shear rams), surface BOP controls, hydraulic accumulator unit (koome

Emergency Evacuation System `50FD7A59`

Personnel evacuation and escape system for an offshore oil production platform comprising TEMPSC (totally enclosed motor propelled survival craft) with davit launch systems, secondary evacuation means

Emergency Shutdown System `51F77A59`

Safety Instrumented System implementing IEC 61511 SIL 3 safety functions for an offshore oil production platform. Executes hierarchical shutdown sequences (ESD Level 1: total platform shutdown; ESD Le

Fire Protection System `55F73A58`

Active fire suppression system for an offshore oil production platform comprising deluge water spray (process areas, wellhead), foam concentrate injection (helideck, storage tanks), CO2 flooding (encl

Fire and Gas Detection System `55F77A19`

Distributed network of hydrocarbon gas detectors (catalytic bead, infrared point, and open-path), flame detectors (UV/IR multi-spectrum), heat detectors (rate-of-rise and fixed-temperature), and smoke

HVAC Safety System `51F77A59`

Heating, ventilation, and air conditioning isolation and control system for emergency conditions on an offshore oil production platform. On confirmed gas detection or ESD activation, closes HVAC suppl

Offshore Oil Platform Safety System `51F77A59`

Integrated safety instrumented system for an offshore oil and gas production platform (FPSO or fixed jacket). Comprises fire and gas detection, emergency shutdown (ESD), process shutdown (PSD), blowou

Process Safety System `55F77A59`

Safety Instrumented System providing SIL 1/2 safety instrumented functions for process parameter protection on an offshore oil production platform. Monitors process variables (pressure, temperature, l

Public Address and General Alarm System `54FD7A18`

Integrated alarm and communication system for an offshore oil production platform providing audible and visual emergency notifications across all platform areas including open decks, process areas, ac

Traceability Matrix — Derivation

Source	Target	Type	Description
STK-REQ-004	SYS-REQ-005	derives	Spurious trip rate stakeholder need derives the ESD MTBST requirement
STK-REQ-003	SYS-REQ-003	derives	IEC 61511 compliance derives the SIL 3 PFDavg requirement for ESD Level 1
STK-REQ-002	SYS-REQ-004	derives	Safe evacuation need derives the PA/GA alarm and intelligibility requirement
STK-REQ-001	SYS-REQ-006	derives	Hazard response need derives the firewater delivery requirement
STK-REQ-001	SYS-REQ-002	derives	Hazard response need derives the ESD Level 1 actuation time requirement
STK-REQ-001	SYS-REQ-001	derives	Hazard detection stakeholder need derives the F&G detection confirmation time requirement

Orphan Requirements

1 requirement(s) have no trace links (neither derivation nor verification). These should be reviewed for traceability gaps.

Ref	Text (excerpt)	Document
STK-REQ-005	The Offshore Oil Platform Safety System SHALL support online proof testing and partial-stroke testing of safety instrume	stakeholder-requirements