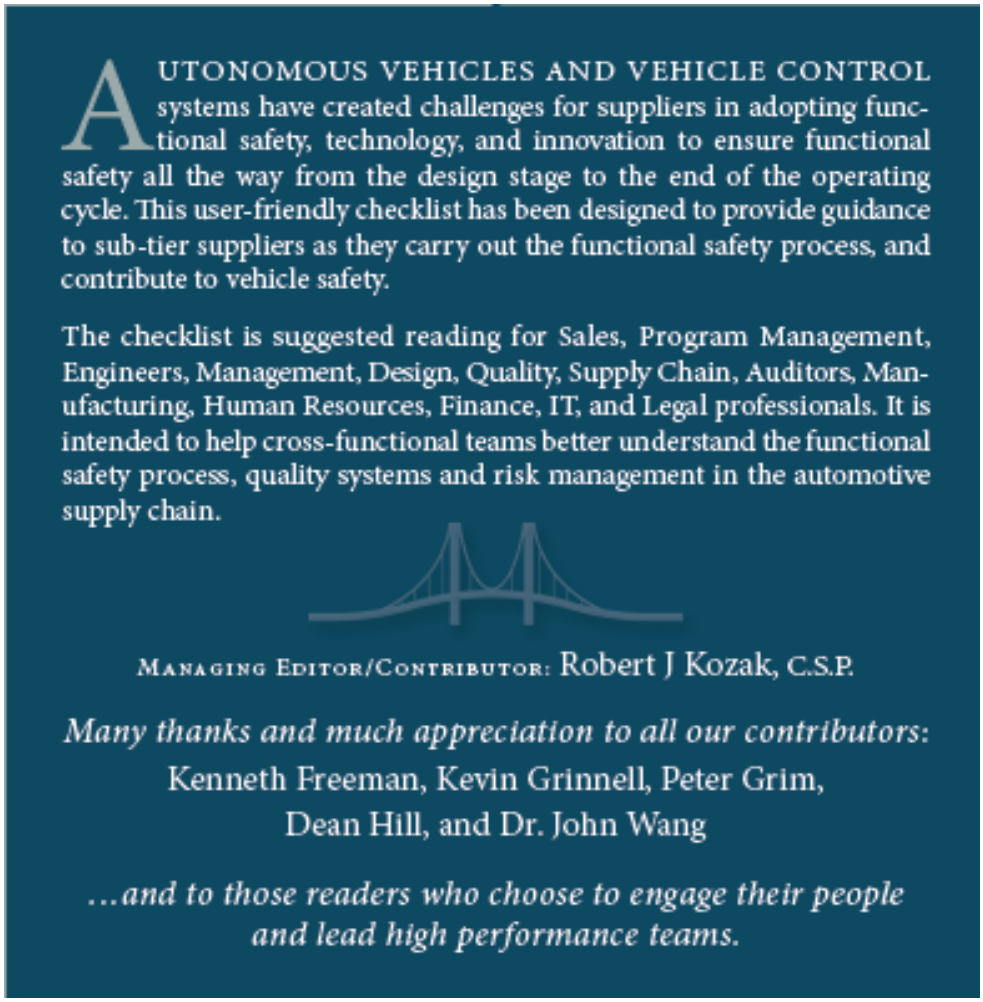
The Michigan Automotive Functional Safety Forum

QUALITY SYSTEM CHECKLIST AND GUIDE FOR CROSS-FUNCTIONAL TEAMS



Special appreciation to Angelo Scangas
CEO-President of [Quality Support Group]

Published 123120 - 2021
2nd Edition 103121 - 2021

Table of Contents

Note-1: Refer to Page 25 for list of Work Products in detail and good reference ISO 26262 Work Product Visualization link

Note-2: This document is free to use as intended and/or modified as necessary for specific personal or organizational use

PURPOSE

The purpose of this checklist is to guide functional safety auditing *under the umbrella* and *fiduciary responsibility* of Automotive Quality Management Systems as performed in accordance with ISO-9001 and IATF-16949.

This document gives guidance to QMS auditors performing QMS audits in projects that involve Functional Safety per ISO 26262 or ISO/PAS 21448. The primary goal of this document is to direct cross-functional teams for a successful QMS audit of projects containing ISO-26262 requirements. This document presence a method for ensuring cross-functional teams have the awareness and background in ISO 26262 and other related standards to conduct *high-level activity* audits as they would for hardware, software engineering, and project management, as examples. Functional Safety is intertwined with quality- oriented activities and work products.

Functional Safety 1) audits, and 2) assessments are defined in the ISO 26262 Standard. When auditing and assessments are defined in ISO/PAS 21448 or ISO 21448, that same rule will apply and definition of auditing shall be per ISO/PAS 21448. UL4600 and its intent in future revisions may address additional requirements with a focus on the Safety Case / Arguments and associated work products.

SCOPE

This guidance document has been created by the Michigan Automotive Functional Safety Forum and its format is applicable for any automotive or other type of road vehicle organizations as a checklist to use for a specific purpose of QMS and FS auditing.

This document is applicable for functional safety projects where faults may occur that cause hazardous events which are ASIL-rated, regardless of whether they are hardware faults or software faults.

The organization shall check for the integrity of customer contractual requirements and/or internal requirements for the FS process deployment, sampling of its safety-related work products, and shall work with their Customer(s) to establish a well-understood set of requirements in developing components and systems for vehicle electrification and autonomous vehicles.

Quality System Audits address essential interaction of *typical* QMS processes such as Sales, Program Management, Engineering, Purchasing, Manufacturing/Maintenance, Management/Leadership, Quality, Internal Audit, Problem Solving, Information Technology (IT), Information Security, Cybersecurity, Finance, and CSRs (Customer Specific Requirements).

Sales Responsibility for Contract-PO / RFQ / Feasibility / Statement of Work / Quote

Verify the responsibilities of Sales relative to Functional Safety Management (FSM)

- ☐ Review [all] customer requirements documentation
- ☐ Ensure quote and funding request comprehends funding for FSM
- ☐ Ensure Customer understands FSM will need to participate in regular technical meetings

Confirm relevant documents for FSM are recorded by Sales

- ☐ Definition of the functions the end-product is required to perform, for each phase of the product usage life-cycle. (i.e. Requirements Matrix)
- ☐ Existing Functional Safety Architecture that the organization's FSM is required to interface with.
- ☐ Definition of the operating environments and the range of dynamic road operating maneuvers and actions required in each phase of the product usage life cycle.
- ☐ Item / Host system technical specification.
- ☐ Item Description per ISO 26262:2018 Part 3.
- ☐ Item Functional Safety Concept per ISO 26262:2018 Part 3.
- ☐ HARA results: Safety goals, all necessary constraints on fault tolerant time interval and associated parameters, ASIL values, scenario descriptions under which ASIL values are determined.
- ☐ Requirements for product design testing and verification, such as DV, PV, required review, demonstrations, qualification, EOL testing, HIL testing, Human Factors testing, special / cyber-security, EMI, and ESD requirements.
- ☐ Timing constraints for product development, key technical items and review/reporting milestones for FSM
- ☐ Protocols for using APQP to manage safety requirements in manufacturing (i.e. as part of Feasibility Analysis).
- ☐ Customer in-plant requirements and constraints (i.e. customer owned end of line tester, software and potential re-flashing)
- ☐ Names and contact for key technical persons on Customer side, such as FSM for project, Thermal Engineer, Reliability Engineer, EMC Engineer, Design Release Engineer depending on the complexity of the product. Supplier-side Functional Safety Manager and/or Product Safety Officer as may be required by CSR)
- ☐ Safety Level(s) (ASILs) has/have been defined/recorded.
- ☐ Required records may include:
  - ☐ Item Definition
  - ☐ Safety Goals (if available at quote phase)
  - ☐ Functional Safety Concept
  - ☐ DIA (Design Interface Agreement)
  - ☐ Safety Plan (Customer / Supplier integration)
  - ☐ HARA Report (The required ASIL(s))
    - ☐ FMEA (Design and System level FMEAs, if available from the customer)
    - ☐ Specifications – Related to functional safety shall be written in accordance with ISO 26262:2018 Part 8 Clause 6.4 Systems requirements definition process or ISO/IEC/IEEE 15288:2015 (or current).
- ☐ Defined Cybersecurity / applicable Standards (example: SAE DIS 21434)
- ☐ RASCI chart is completed, if applicable (customer / supplier responsibilities, part of the DIA)
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

Program Management Responsibility **(may include Functional Safety role)**

Verify the responsibilities of Program Management relative to Functional Safety Management (FSM)

- ☐ Project Manager is appointed at the initiation of product development and is responsible to ensure that a Safety Manager is chosen, and that top management supports required staffing.
  - ☐ Department [records] indicate training completed for staff on ASPICE and ISO-26262 Functional Safety
  - ☐ Part 2, Clause 6 requirements, Prg Mgmt ensures a Product Safety Rep is assigned for each/all projects
  - ☐ Verify Program Mgmt Gate Check-Lists as equivalent to APQP Timing Chart FS-Gantt-Chart tracking FS-activity as manager of the project integrated schedule for key FS-Suppliers
    - ☐ Identified Risk (if any) highlighted / tracked
    - ☐ Mitigation (if risk identified) are planned out and recorded
  - ☐ The organization FS-Outsourced Suppliers are defined and managed on the organization Supplier Log
  - ☐ Outsourced Supplier concerned/risks (if any) are included in Program Mgmt tracker and reporting to mgmt
  - ☐ Program Mgmt tracks Risks / Quality / Timing / Cost as performance record
  - ☐ Lessons Learned tracked / recorded/ used as part of Program Management
  - ☐ Configuration Management and Change Management processes (26262 Part 8; Clauses 7 and 8) have been invoked and enforced
  - ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

Engineering / Design Responsibility **(may include Functional Safety role)**

Verify the responsibilities of Engineering / Design relative to Functional Safety Management (FSM)

Engineering / Design Inputs include

- ☐ Product Specifications and Special Characteristics
- ☐ Boundary and Interface Requirements
- ☐ Identification, Traceability and Packaging
- ☐ Analysis of Risks and Mitigation
- ☐ Targets for reliability, durability and serviceability
- ☐ Statutory and Regulatory Requirements
- ☐ Embedded Software Requirements
- ☐ Special Requirements for Engineering consideration to Manufacturing (i.e. ESD, EMI, EMF)

☐ Department records indicate training completed for all required staff members on ASPICE and ISO-26262

- ☐ Systems Engineering training - especially for complex systems

☐ For Engineering FS-projects, refer to I.A. above for guidance in determining if:

- ☐ Awarded Business *-or-*
- ☐ Out-of-Context

FSM Deliverables (Outputs) include:

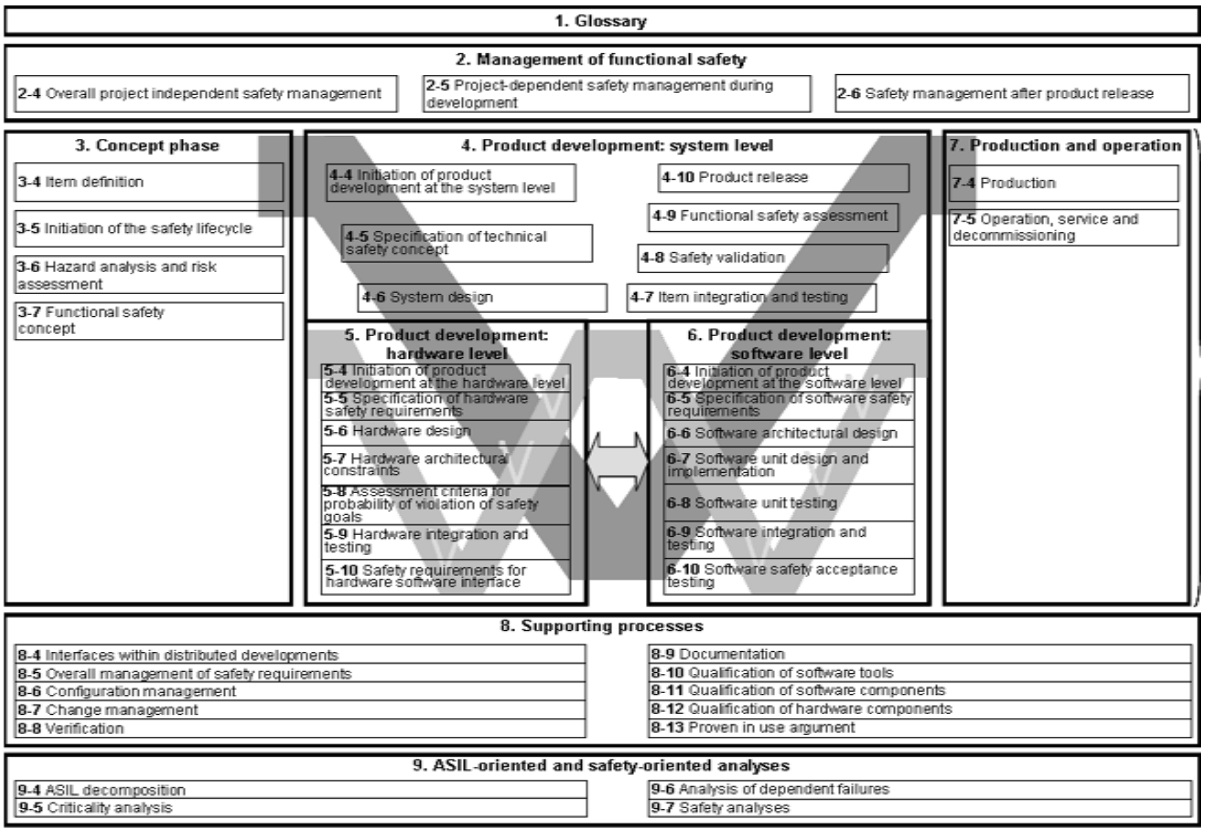
- ☐ Item Definition
- ☐ HARA (ASIL is included in a HARA report)
- ☐ Safety Goals / Functional Safety Requirements / Attributes of the requirements
  - Check for completeness of defined requirements - guidance includes:
  - ✓ For each safety goal, at least one mitigating safety-related function must be created.
  - ✓ For each safe state; at least one mitigating safety-related function is defined
  - ✓ For each assumption; at least one general safety requirement is defined
  - ✓ For each; safe state emergency operation requirement, user information requirements and recovery requirements are defined if, applicable
- ☐ Requirements Analysis & Mgmt
- ☐ Architecture & Functional Modeling
- ☐ Function Behavior Modeling – Validation of HW/SW Mapping
- ☐ D-FMEA, System-FMEA, P-FMEA and Software-FMEA
- ☐ FMEDA with
  - ✓ Safe Failure Fraction (SFF) computation
  - ✓ Calculate Single Point Fault Metric (SPF) and Latent Fault Metric (LFM)
  - ✓ Safety Element Out of Context
  - ✓ Failure Rate over Children (sub-parts of a FS project)
  - ✓ Traceability of safety mechanisms to rqmts & SW/HW implementation
- ☐ DFA (Dependent Failure Analysis)

  The objectives and scope of a dependent failure analysis depend on the sub-phase and the level of abstraction at which the analysis is performed. This information is defined prior to conducting the analysis, for instance in the safety plan.
- ☐ FTA
- ☐ End-to-End Traceability - from requirements and to safety analysis such as FTA/FMEA
- ☐ Work Product/Documentation Generation or release authorization
- ☐ Applicable Cybersecurity Controls
- ☐ Functional Safety Audit / Functional Safety Assessment and all required actions closed out per target

-continue Engineering / Design-

- ☐ Functional Safety Mgmt Commitment and Support / APQP Milestones
- ☐ Safety Case & Arguments for
  - ✓ Evaluating the rationale
  - ✓ Assumptions & Supporting Evidence

  Note: Refer to Appendix-B for FS Case Overview
- ☐ Lessons Learned are tracked, recorded and used as part of Engineering Management
- ☐ Design Risk Analysis (FMEAs)
- ☐ Reliability Study Results
- ☐ Production Special Characteristics
- ☐ Production Design Error-proofing (e.g. DFSS, DFMA, FTA)
- ☐ Product Definition (e.g. 3D-Model, GD&T, Technical Data Package)
- ☐ Product Design Reviews
- ☐ Service part requirements (i.e. diagnostics, serviceability and repair instructions)
- ☐ Packaging and labeling requirements for shipping
- ☐ Life Cycle requirements



Enhanced V-diagram from ISO 26262:2018 Part 1 illustrates overall workflow between ISO phases Functional Safety work interfaces

- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

-end Engineering / Design-

Functional Safety Manager Responsibility

Verify the responsibilities of relative to Functional Safety Management (FSM)

- ☐ Work-load (i.e. list of Functional Safety Projects and/or other non-FS projects)
- ☐ Functional Safety Assessment and recorded properly
- ☐ Functional Safety Audit has been completed and recorded properly
- ☐ Safety Case has been completed and recorded properly
- ☐ Metrics – FS Phase-Gate Review Scorecard
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations
- ☐ Promptly escalates concerns and suggested actions to top management for resolution
- ☐ Confirmation Assessment – refer to additional information in Guidance and Reference Material

  As referred to in ISO-26262 and Part-2, C.23-24 and Annex-C for the following work products:

  - Hazard Analysis & Risk Assessment (HARA)
  - Safety plan
  - Item integration and testing plan
  - Validation plan
  - Safety analysis
  - Software tool criteria
  - Proven in use argument
  - Completeness of the safety case
  - Functional safety audit
  - Functional safety assessment

Reference Confirmation Measure Record

Example: Confirmation Measure Record

CONFIRMATION REVIEW									
Item	Reference Doc No.	Topic Description	N / A	Accepted	Conditional	Rejected	Comments / Remarks	Action(s) Logged in Action Table? Yes	No
1		Is the version number correct?	☐	☐	☐	☐		☐	☐
2		Correct editor/reviewer in code db?	☐	☐	☐	☐		☐	☐
3		Change log / Change description?	☐	☐	☐	☐		☐	☐
4		Status is “review”?	☐	☐	☐	☐		☐	☐
5		Template(s) used?	☐	☐	☐	☐		☐	☐
6		Delivery defined?	☐	☐	☐	☐		☐	☐
7		Correct editor FSM or authorized person and independent examiner?	☐	☐	☐	☐		☐	☐
8		Confirmation review for all ASIL documents described?	☐	☐	☐	☐		☐	☐
9		Are the safety analyzes coordinated with customer? Note: in DIA with the customer	☐	☐	☐	☐		☐	☐
10		SW Tools Evaluation maintained and SW Tools versions current?	☐	☐	☐	☐		☐	☐
11		FSM responsibilities defined?	☐	☐	☐	☐		☐	☐
12		Is the safety lifecycle described? How is a necessary adjustment (tailoring) documented?	☐	☐	☐	☐		☐	☐
13		Are the responsibilities for the activities described? - Integration and Testing - Validation & SW plan - FSM Assessment (ASIL B, C, or D) - FSM Audit (ASIL B, C, or D) - Safety case (ASIL A, B, C or D)	☐	☐	☐	☐		☐	☐
14		Is there a plan to evaluate the functional safety in the project?	☐	☐	☐	☐		☐	☐
15		Are methods and techniques from ISO 26262 described?	☐	☐	☐	☐		☐	☐
16		Safety activities described?	☐	☐	☐	☐		☐	☐
17		Supporting processes for functional safety described?	☐	☐	☐	☐		☐	☐
18		Production interface defined?	☐	☐	☐	☐		☐	☐
19		Customer interface documented?	☐	☐	☐	☐		☐	☐
20		Safety Pln part of the Prj Pln or referenced in the project plan?	☐	☐	☐	☐		☐	☐
21		Are the project-independent safety aspects named; e.g. safety culture, competence & quality mgmt?	☐	☐	☐	☐		☐	☐
22		Is the V&V plan created?	☐	☐	☐	☐		☐	☐
23		Planning for safety activities include responsibilities / identification of the resulting work products?	☐	☐	☐	☐		☐	☐
Overall Rating based on above reported ■ Accepted I ■ Conditional I ■ Rejected:							Comments: >>>		

Purchasing / Supplier Development Responsibility for Advance Sourcing / Supplier Selection

Verify the responsibilities of Purchasing relative to Functional Safety Management (FSM)

- ☐ Functional Safety Requirements are specified in the purchasing specification
- ☐ Suppliers used shall be approved and listed in the approved supplier list
  - ☐ Evidence selected suppliers have an established functional safety culture
- ☐ For functional safety related components:
  - ☐ Data Sheet is available for the component and Safety Manual is available if applicable.
  - ☐ Components should be AEC-Q100, AEC-Q200 or AEC-Q300 qualified to the appropriate level (unless otherwise approved by design and functional safety)
- ☐ Defined Org / FS-Supplier relationship in relationship with Purchasing *and*
  - ☐ Sales / Engineering
    - ☐-No Design Resp ☐-Design Support ☐-Full Design Responsible
  - ☐ *and/or* Mfg-Site / Phase of APQP development
  - ☐ Defined role/responsibility of who / how FS-suppliers are identified
  - ☐ Verification of Approved Supplier List record indicating Supplier SOW

    Note for QMS Auditors: The FSO interfaces with supplier manufacturing for confirmation from plant on compliance with each functional safety requirement. FSM interface monitors any changes to the BOM while in production to ensure that all parts satisfy FS requirements throughout production, until decommissioning of production facility. FSM must have input to scorecards or other process monitoring tools, to report status and be capable of escalating concerns
- ☐ Design provides requirements to purchasing that specify details for functional safety which will include ASIL level
- ☐ The FSM performs ASIL decomposition to establish ASIL level for the supplier
  - ☐ Supplier is informed in the purchasing documentation (e.g. Contract or P.O.)
- ☐ When a contract includes design / development work, the distributive development process applies which would require that a DIA be established between the customer and supplier.
  - ☐ When a design requires safety related off the shelf components, supplier shall provide a safety manual
  - ☐ Rqmts for ISO-26262-Traceability / Configuration Mgmt / Cyber Security
  - ☐ Objective evidence of FS-supplier training/compliance to ASPICE and ISO-26262
  - ☐ FS-supplier's "Critical Work Projects/Confirmation Measures, (ISO-26262, P-2).
- ☐ Evidence procured components meet functional safety measures/requirements in the purchasing documentation
  - ☐ Component Functional Specification
  - ☐ Component Test Requirements
  - ☐ Component Test Results
  - ☐ Safety Manual and Data Sheet
- ☐ Purchasing's Risk Register identifies supply base risks- and mitigation (if applicable)
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

Mfg-OPs / Supplier Mgmt / Warehousing Responsibility

Verify the responsibilities of Mfg-OPs relative to Functional Safety Mgmt (FSM) Parts 7, Clauses 5-6-7

- ☐ Project Management is responsible to ensure that a Safety Manager is appointed at the beginning of each FuSa project and is competent to fulfill this role
  - > Competence as defined in IATF-16949; Clause 7.2 and ISO-26262 Part 2; Clause 5.4.4
- ☐ Site [records] indicate training completed for all required Mfg-Site members on ISO-26262.
  - ☐ Part 2, Clause 6 requirements, Program Mgr initially assigned each/all FSM-projects with a role to ensure a Safety Manager has ongoing project responsibility
- ☐ Where is FS referenced within the Mfg-OPs processes, procedures and Mfg QMS Management Review
  - ↳ Refer to Management of Safety Requirements, Part 8, Clause 6, for Manufacturing OPs
    - ☐ Review of Mfg-Site latest FuSa Self-Assessment Survey, Auditors/Auditees, Score and Action-items
    - ☐ Per Part 8, Clause 5 – <u>Date of last independent Manufacturing Safety Assessment</u>

      Part 2 – Management of Functional Safety
      A. Safety Culture – Policy, Objectives, and Management Review
      B. Competencies & Roles and Responsibilities
      C. 5mpact Analysis
      D. Functional Safety Plan
      E. Confirmation Measures – Audits, Assessments, and Confirmation Reviews
      F. Safety Case
      G. Release to Production

      Part 7 – Production / OPs, Service and Decommissioning
      A. Functional Safety in Production Planning
      B. ASILs in Process Flow, PFMEA, Cntrl Plns and Work Instructions
      C. Safety Culture in the OPs – Policy, Objectives, Management Rvws

      Part 8 – Supporting Processes
      A. Distributed Interface Agreement
      B. Specification and Mmgt of Safety Rqmts
      C. Configuration Management
      D. Change Management
      E. Verification
      F. Documentation Management
      G. Software Tools Qualification

      By Who (title and qualifications)

      Safety Assessment Score = [% ISO 26262 Compliance Rating]

      Actions to date indicate critical thinking skill / problem solving competency
- ☐ Mfg-Ops maintains copy of current ISO-26262 / Record Repository / How Configuration Mgmt is Controlled
- ☐ List of past / current year FuSa projects within the Mfg-Site and Release to Production approvals
  - ☐ If there are not current FuSa projects, review Pre-Production / Proto-NPI FuSa projects
  - ☐ Review FuSa pass-thru requirements to sub-suppliers of Pre-Production and/or Production
- ☐ Mfg-Site / OPs risks are identified, mitigated and measured
  - ☐ Mfg-Site Mgmt Review records with traceability to FuSa Risk reviewed, actions and mitigation
- ☐ Specific tests / test coverage is carried out that relate to FS, and specified on the Control Plan
- ☐ Tests / inspections are performed using calibrated equipment at specified intervals
  - ☐ MSA's are performed and qualified to assure measurement & operator error are under control
- ☐ Red Rabbits / golden standards used to verify test equipment as specified in Control Plan
- ☐ Nonconforming process effective for Test / Inspc'tn failures, documented rework/retest instructions in appropriate language(s)
- ☐ Engineering changes properly deployed ***<u>and validated</u>*** per Part 8, Clause 8
- ☐ Production machines are properly maintained and environmental controls such as ESD in place

- ☐ Re-Flashing process is fully controlled in accordance with ISO 26262 as it relates to
  - ☐ Configuration Mgmt of both product and software test equipment (Part 8, Clause 7) *as interaction...*
  - ☐ ...and Change Control per IATF 16949 and ISO 26262 (Part 8, Clause 8)
  - ☐ Change Validation Assessment and Traceability per ISO 26262
  - ☐ Proper testing / labeling
- ☐ Contingency plan including cybersecurity is in place and monitoring at required frequencies
- ☐ Annual Layouts & Functional Testing performed in accordance with customer requirements
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations
  - ☐ Records of proper set up including first off and last off parts
  - ☐ Traceability of components and materials is recorded
  - ☐ Process capability is maintained for special characteristics
- ☐ Significant process events are recorded, such as, tool change or equipment repair
- ☐ Monitoring / measurement of the Mfg-process is recorded, analyzed and evaluated to ensure valid results
- ☐ Work instructions are available and in appropriate language(s)
- ☐ Layout inspection & functional testing is performed as per control plans
- ☐ Control plan shall include list of alternative controls and kept up current as living documents
- ☐ Restart verification is performed for the defined period of downtime
  - ☐ Confirmation that all features of the error proofing device or process is effectively reinstated
- ☐ Records and process sampled using the automotive process to assure confidence in results and risk-based audit trails, such as. customer complaint / field failure / corrective actions
- ☐ Site shall maintain a list of its FS products to assure that it can effectively audit its own operations and to share this data with external audit organizations such as QMS certification bodies

- supporting processes continued on next page -

Supporting Process

Ethics / Human Resources / Training / Competence

Verify the responsibilities relative to Functional Safety Management (FSM)

Ethics

- ☐ ISO 26000 Organizational Social Responsibility (if applicable):
  - ☐ 7 Principles – Accountability, Transparency, Ethical Behavior, Respect for Stakeholder Interests, Respect for the Rule of Law, Respect for International Norms of Behavior and Respect for Human Rights.
  - ☐ Check if required by customers or if company has voluntarily adopted this standard
  - ☐ Check for any recent audit results and if corrective actions / management review
- ☐ Corporate Ethics Code – Policy (required under ISO-26262)
  - ☐ Examine how the business processes currently comply
  - ☐ Employees are aware of and involved in Functional Safety policy as part of ethical business decision making (e.g. software development)
  - ☐ Ethics hotline, whistle-blowers protocol and ombudsman

Training / Competence

Verify the responsibilities of relative to Functional Safety Management (FSM)

- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations
- ☐ Records for Engineering, Manufacturing, Human Resources and all other Business Support
  - ☐ Department records indicate training completed for staff on
  - ☐ Awareness of Risk / Functional Safety / Product Safety / Ethics / Escalation
  - ☐ FMEA/Risk Management & Mitigation
  - ☐ ASPICE
  - ☐ ISO/IEC/IEEE 15288
  - ☐ ISO-26262 Functional Safety
    - ☐ ASIL / DIA / HARA
    - ☐ Safety -Assessment, -Audit, -Case
  - ☐ Embedded Software
  - ☐ Cybersecurity
  - ☐ Future other standards
  - ☐ On the Job Training
  - ☐ Related policies for Quality and Functional Safety
  - ☐ Regulatory training and/or awareness

Supporting Process

Management Leadership / Safety Cultural / Risk

Management

Verify the responsibilities of relative to Functional Safety Management (FSM)

- ☐ Management Review is carried out at regular intervals and covers key Functional Safety aspects, as described in ISO 26262:2018 Part 2 Cl. 5, 6, 7
- ☐ Leaders support FS-requirements, -ongoing projects, including resource allocation and budget needs
  - ☐ Robust safety culture is driven top-down and involves cross-functional teams (including legal)
  - ☐ Management engages in Functional Safety Gate Reviews
  - ☐ Executive Management direct engagement with FSM
  - ☐ Unacceptable (Red-Risks) are mitigated and supported by Executive Management Team
  - ☐ FMEA / Risks and actions review to Control Plan
- ☐ Engagement in the escalation of functional safety issues and/or field failures
- ☐ Management has established roles, responsibility and authorities for Functional Safety, e.g.
  - ☐ RASIC Chart / Organizational Chart
  - ☐ Support for individual's authority for Stop Shipment (Judoka) to correct problems
- ☐ Ensure competence of its Mgmt System as defined in IATF-16949; 7.2 and ISO-26262 Part 2; 5.4.4
- ☐ Empowering teams through communications and recognition
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations
- ☐ Verify that top mgmt reviews with process owners Safety Plan deliverables, actions taken and that work products such as safety audits and safety assessments are performed in a timely manner and acted upon

IT Process / Information Security Mgmt Sys & Cybersecurity

Verify the responsibilities of relative to Functional Safety Management (FSM)

- ☐ Infrastructure
  - ☐ maintain the infrastructure necessary for the operation of its processes and to achieve conformity of products and services, which can include buildings / associated utilities, equipment / HW / SW, transportation resources and d) information and communication technology

    Note[-1] Information Technology – S/W-Systems such as Eng CAD-tools, Corrective Action database, and IAIG CS-1
- ☐ IT process, policy and/or procedures are defined and controlled in accordance with ISO-26262 Parts 1-10, the only reference to IT is thru
  - ☐ Bibliography ISO/IEC-15504, there is mention of:
  - ☐ IATF-16949, Section 7.1.3 Infrastructure - the organization ***shall*** determine
  - ☐ Internal Audits of, e.g., ISO-27001, AIAG CS-1, TISAX and follow-up corrective actions
  - ☐ Annual test of Contingency Plan including Cybersecurity (IATF-16949 requirement)
  - ☐ Actions taken to Cybersecurity as it relates product development (ISO 21434)
  - **>** NIST SP 800 definition of cybersecurity; Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
- ☐ IT interacts with the organization's *business processes*, including Functional Safety
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

Supporting Process

Warranty Process

Verify the responsibilities of relative to Functional Safety Management (FSM)

- ☐ Field failures and/or recalls related to FS project, and appropriate actions taken
- ☐ Proactive role of the Warranty process with regard to FS projects and Design Changes
- ☐ Participate and communicate with customers and regulators as required
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

Quality / Problem Solving

Verify the responsibilities of relative to Functional Safety Management (FSM)

- ☐ Focus is safety first and risk based
- ☐ Customer Complaints process and Problem-Solving process
- ☐ Internal Audits, Product Audits, Manufacturing Audits (LPAs) and sampling of FS products and field failure and recalls as applicable
- ☐ Calibration and Testing as related to FSM
  - ☐ Timely reporting of all failures related to calibration and testing for FSM
  - ☐ Failure / Out of Cal analysis performed to determine if customer must be notified
  - ☐ Verification of Test-Software (could be performed with Red-Rabbits)
  - ☐ Measurement System Analysis Studies completed on time per Control Plan
- ☐ [All] staff properly trained in
  - ☐ Product Safety and Functional Safety
  - ☐ Problem Solving, such as AIAG CQI-20
- ☐ APQP / New Product Introduction including Mfg-Site Work Instructions with Special Characteristics
- ☐ PPAP / Sample Submission
- ☐ Functional Safety Gate Review with approved Safety Case prior to PPAP submission
  - ☐ If Safety Case is not completed on time, PPAP submission Warrant indicates omission
- ☐ Annual Layouts that include all functional testing completed to schedule
- ☐ Records retained in accordance with company Records Policy and/or CSR / Regulations

KEY FUNCTIONAL SAFETY ACRONYMS / Links

Refer to ISO-26262:2018 Part-1, Vocabulary

ASIL	Automotive Safety Integrity Level *One of four levels to specify the item's or element's necessary ISO 26262 requirements and safety measures to apply for avoiding an unreasonable risk, with D representing the most stringent and A representing the least stringent level. (26262:2018, pt 1 cl 3.6).*
CAD SC	Cadillac Super Cruise Auto-blog Technology of The Year Winner
DCMS	Documentation Control Management System
DIA	Development Interface Agreement
Element	System, Components, H/W or S/W, H/W-Parts or S/W-units
Faults	Abnormal condition that can cause an element or an item to fail
FCA PSV	FCA Product Safety Video
FMEDA	Failure Modes/Effects/Diagnostic/Analysis
FS	Functional Safety Absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems. (26262:2018 pt1 c. 3.67)
FIT	FIT-Level or rate of a component is the number of safety-related faults expected in one billion hours of operation.
HARA	Hazard Analysis and Risk Assessment *Analysis to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention of mitigation of the associated hazard in order to avoid unreasonable risk (26262:2018 pt1 cl 3.76)*
SEOOC	Safety Element Out of Context *Safety-related element which is not developed in the context of a specific item 26262 or yet awarded business (26262:2018 pt1 cl 3.137). It is also commonly applied to elements which are not specifically commercialized, and hence have no specific customer-driven source of requirements.*
USDOT	National Highway Transportation Safety Admin Monthly Recall Reports National Highway Transportation Safety Admin Monthly Technology & Innovation

KEY FUNCTIONAL SAFETY DEFINITIONS

Refer to ISO-26262:2018 Part-1, Vocabulary

QMS-*Auditing* Quality Management System-*Auditing*

QMS task which ensures that the appropriate requirements have been achieved

Note: *The QMS-Audit is different from an audit as defined in 26262:2018 pt 1 cl 3.5. In this document the 26262 audit is called "Safety FS Audit, called Safety Audit, along with the Safety Assessment. The QMS Audit will look at aspects of the Safety Audit, Safety Assessment and Safety Case for compliance to the intent of ISO-26262 requirements but is not a FS Work Product audit.*

RASIC Chart Defines: Responsibility / Approval / Support / Informed / Consult

Safety Assessment Conducted by a qualified int or ext *independent* body of a FS project

As referred to in ISO-26262 and Part-2, C.12 (and 6.4.12); the goal of the safety assessment is a judgement whether functional safety of the item (or the expected contribution to functional safety of the developed elements) is archived and subsequently provide 1) recommendation for acceptance, 2) conditional acceptance or 3) rejection if functional safety requirement has not been achieved.

Safety Assessment focus includes evaluation of: [c.12.2]-the safety plan and required work products in accordance to ISO-26262 requirements, [c.12.3]-the implementation of the FS safety processes with consideration to FS safety audits that have been performed, [c.12.4]-implemented safety measured as appropriate and effective, [c.12.5]-arguments are provided as to why FS is achieved per 26262-objectives, [c.12.6]-the argument provided in the safety case is sufficiently convincing with consideration the confirmation review of the safety case, [c.12.7]-rationales for the safety anomalies managed to closure in a convincing manner and lastly, [c.12.8]-the follow-up recommendations resulting from previous safety assessments which include any corrective actions performed.

Note: Corrective Action effectiveness of the Safety Assessment FS-project team can be assessed by the QMS Auditor in accordance with IATF-16949 and related clause 10.2, Nonconformity / Corrective Action (Problem Solving).

Safety Audit Conducted by a qualified int or ext *independent* body of a FS project

As referred to in ISO-26262 and Part-2, C.11 (and 6.4.11); the goal of the safety audit is a judgement to the implementation of processes required for functional safety and considering the definitions of the activities of the Safety Plan do, in fact, achieve the process objectives of the 26262-standard.

The Safety Audit is focused on the necessary processes for ASIL rated items. The QM-processes as well must adhere to standards' requirements. Therefore, both ASIL rated items and QM rated items are auditable for objective evidence by the QMS Auditor.

Note: The ASIL rated QM projects would meet the intent of the base IATF-16949 standards and not have requirements found in ISO-26262.

Safety Case Attachment-3 and as defined by ISO 26262

Safety case is an "argument that the safety rqmts for an item are complete and satisfied by evidence compiled from work products of safety activities during development"

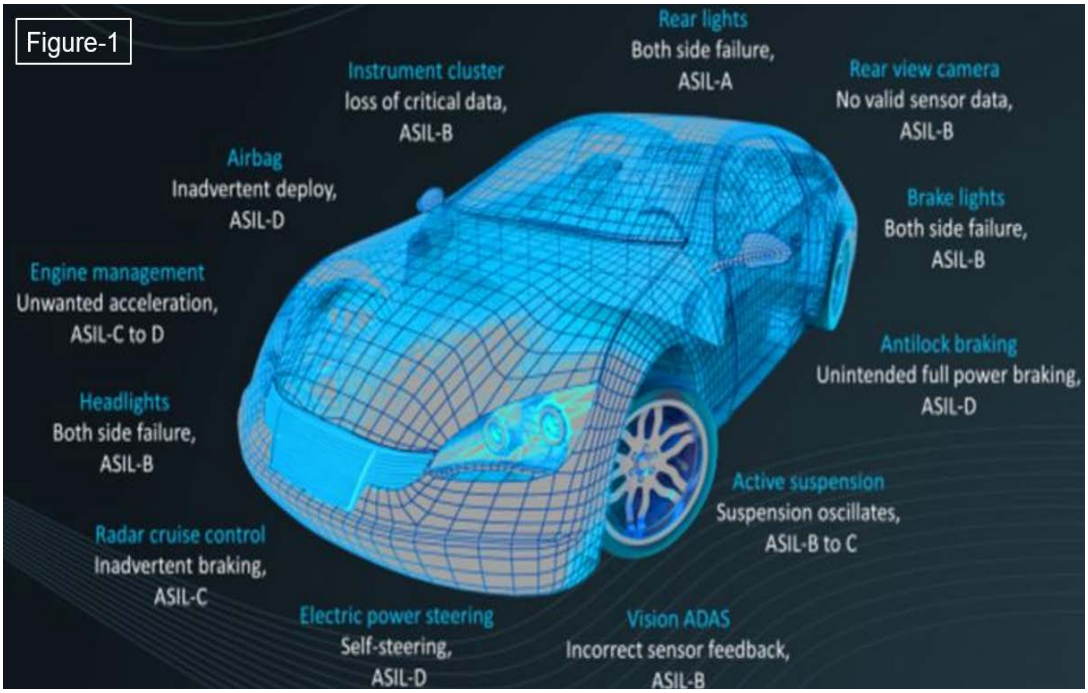
Confirmation Assessment – refer to additional information in Guidance and Reference Material

Referred to in ISO-26262 and Part-2, C.23-24 and Annex-C for the following work products:

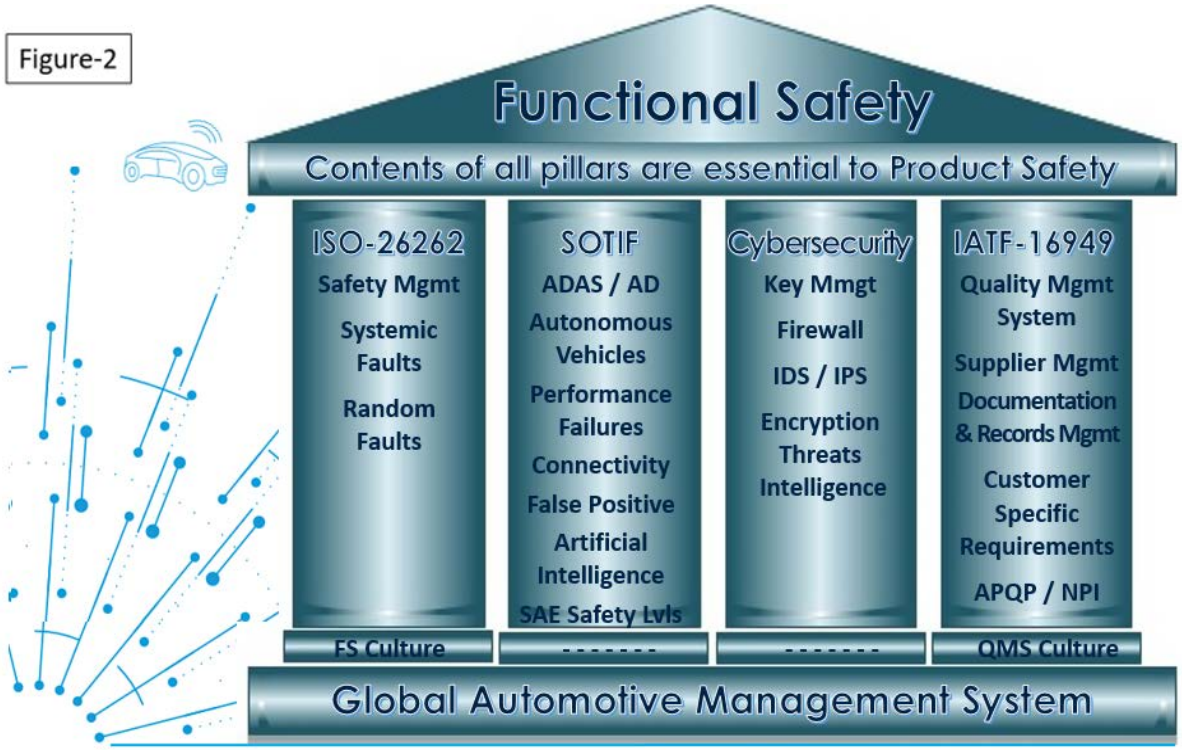
- Hazard Analysis & Risk Assessment (HARA)
- Safety plan
- Item integration and testing plan
- Validation plan
- Safety analysis
- Software tool criteria
- Proven in use argument
- Completeness of the safety case
- Functional safety audit (above
- Functional safety assessment

REFERENCE STANDARDS		Training Consideration
ISO-9001:2015	Base Quality Management System Requirements	Yes
IATF 16949:2016	Automotive Quality Management Systems Requirements	Yes
ISO 26262:2018	Functional Safety Manager Responsible	Yes
QMS Interactive Map	Depiction the organization's interaction of processes	Yes
ISO/PAS 21448	SOTIF - Safety of The Intended Functionality	Yes
AIAG CS1	Cyber Security 3rd Party Information Security	Familiar
NHTSA	Vehicle Cybersecurity	Familiar
ISO 27001	Information Security Standard	Familiar
TISAX	Trusted Information Security Assessment Exchange	Awareness
UL 4600	Safety for the Evaluation of Autonomous Products & System	Awareness
FMVSS	Federal Motor Vehicle Safety Standards [Wikipedia Listing]	Yes
ISO/IEC/IEEE 15288:2015	Key sections	Yes
INCOSE Handbook	Key sections	Yes
ISO 21434	Threat Analysis and Risk Assessment Tool	Familiar
ASPICE	Automotive Software Process Improvement and Capability determination	Familiar

FS Vehicle Functions which may be safety-related. Figure-1 below illustrates many safety-related automotive functions and components in modern automobiles subject to ISO 26262.



Example of House of FS

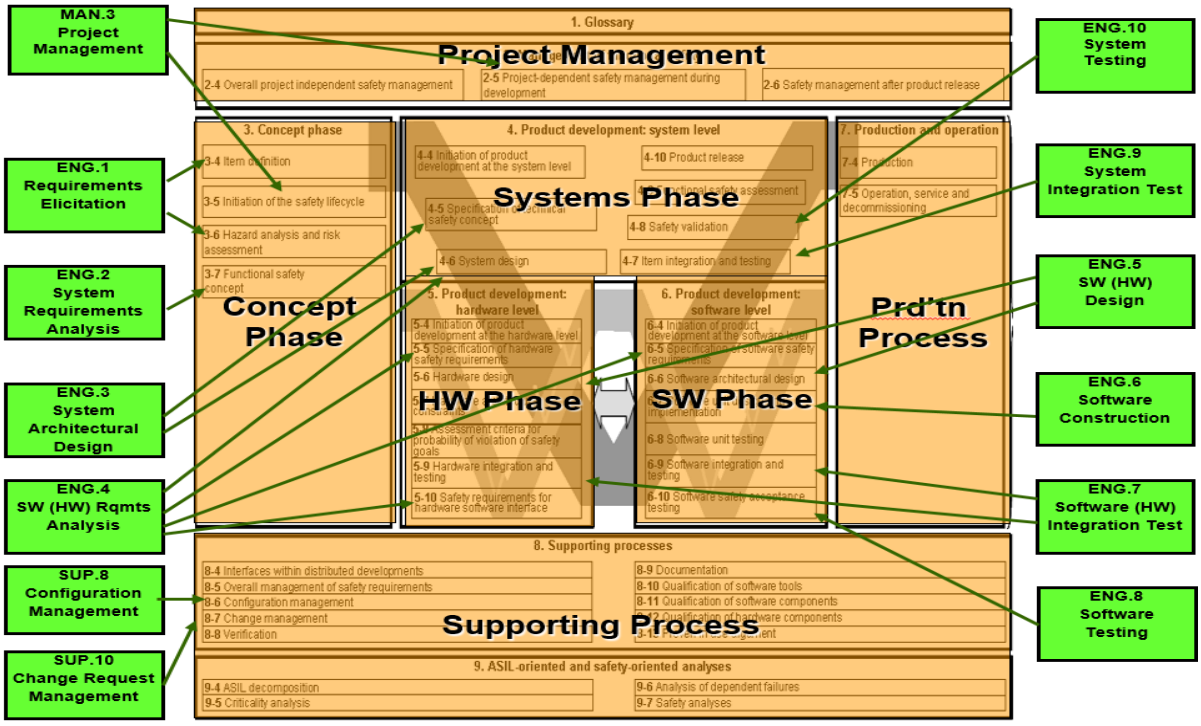


DOCUMENTED PROCESS OUTLINE for performing Quality System Audit

The organization uses the Quality System Checklist as guidance to their FS audit scope

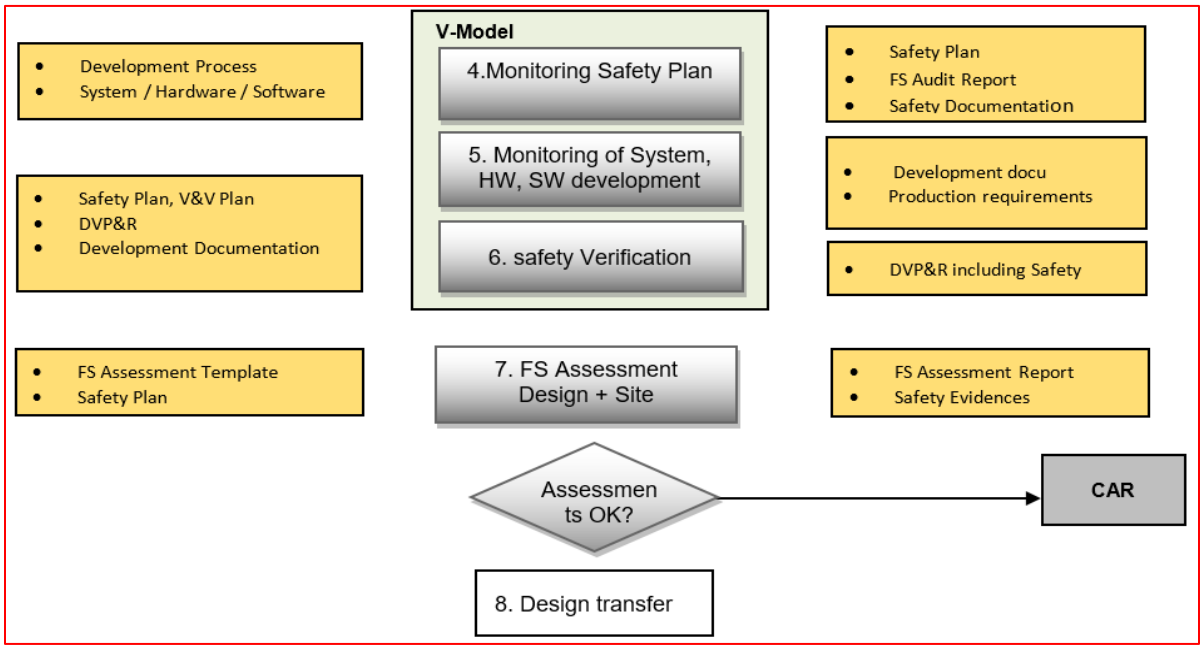
FS V-Diagram Model – ISO 26262 Part-3 high-level representation of Functional Safety Process

Example of FS V-Diagram Model – Aspects of the section for Responsibility



Note: Blocks in yellow are ISO 26262 / green are ASPICE.

Example of FS Process Flow Diagram - suggested the v-model diagram should be used.



RESPONSIBILITIES (IN SUPPORT OF FUNCTIONAL SAFETY)

The organization's QMS Manager ensures the QMS auditors have successfully completed required training as identified in Section 4.0. Ensures an audit focus on R-S-R^2 (Risk-Safety-Regulatory & Records Retention)

Reference ISO-26262:2018; Sections 6.4.8 - Functional Safety Audits and 6.4.9 - Functional Safety Assessment. It is the role of the QMS Audit group to work closely with the organization's FSO, FS Office.

Perform cross-functional review with and/or escalation to the organization's legal counsel as needed to ensure total support of FS-compliance

***Examples of Nonconformities*:**

Requirement: Problem Stmt: Obj Evidence:	QA manual requires design & development planning, and gate reviews with action items addressed in subsequent gate reviews Gate reviews / design process is not always effective Project XYZ-001 OEM Module Gate 3 did not include DV-PV test failures for temp cycle test
Requirement: Problem Stmt: Obj Evidence:	QA manual requires identification of Customer Requirements and Feasibility Review Sales process is not always effective Project ZYI-007 OEM Module Customer's P.O. did not have evidence of review by Sales Director. Customer's P.O. requires ISO 26262, and this was not captured in the feasibility review.

RECORD RETENTION REQUIREMENTS

Audit Records are maintained in the organization Quality System records repository

Legal / Regulatory Compliance review of record retention list and times is part of records requirements

Must be aligned with OEM specific requirements for records retention

DOCUMENT REVIEW AND APPROVAL REQUIREMENTS

Reviewed and approved by the organization Quality System Manager and/or Functional Safety Manager as document owner for IATF-16949 and ISO-26262 alignment/compliance

Guidance / Reference Material

OBLIGATIONS OF THE QUALITY SYSTEM FUNCTIONS SAFETY AUDIT

1.1 Introduction of Obligations outline and QMS FS-Audit expectations

There are several high-level points that should be true of organizations that need to be capable in this functional safety domain.

These points first of all stimulate a discussion on completeness, and second, can lead to a comprehensive but not exhaustive list of "*look-fors"* or QMS auditor protocol of, "show-me" – as in FS objective evidence.

At a similarly high level, what are the key requirements that should be present in an excellent Functional Safety Project, Program, group of related projects requiring Functional Safety to be addressed, or Company.

1.2 Fourteen High-level Points (roughly ordered of their priority)

1. The reference "Functional Safety" generally only applies to ISO 26262. In a more general sense, it may be understood (in an organization-specific way) to comprehend ISO 26262 Automotive Functional Safety, Systems Safety, Safety of the Intended Functionality (SOTIF), UL4600 (Safety considerations for Autonomous Driving), and integration (as appropriate) of safety measures among those.
2. The Company has a documented Functional Safety Process that is qualified (perhaps by an independent such as TUV, DNV, or UL) as an implementation of ISO 26262 and ISO/PAS 21448, which all projects must consider in their planning. The role of planning, which involves Functional Safety responsible leaders, is to establish any compliance requirements that apply to the given project. One of the overarching themes is that considerations of safety cannot be set aside based on commercial concerns.
3. The Company has established a management path for staffing the Functional Safety requirements, providing guidance to departments and Project Management, and enabling an effective and timely escalation channel to upper management to facilitate orderly and efficient resolution of problems and concerns.
4. The Company must commit to competence management with its Functional Safety domain.
5. Data management is critical. Configuration Mgmt, traceability, cataloguing of artifacts and maintaining their status.
6. Leadership visibility – periodic status reports submitted and available to upper management facilitates escalation and scorecards and provides a continuous indication of progress, challenges, and actions.
7. Commitment to people – training, qualifications, certifications, competence management, staff development, drive toward excellence, growing a world-class team; status for safety engineering as a critical and principal corporate process.
8. Regulations and Standards – The National Highway Traffic Safety Administration (NHTSA), a branch of the US Department of Transportation, does not have a regulation which compels the satisfaction of ISO 26262. In the US auto industry, it is a de facto standard imposed by Vehicle Manufacturers internally and upon Tier 1 and 2 supply chain. It serves as a hedge against liability and a demonstration of state-of-the-art practices to do all that can be done in the face of difficult safety requirements, and of doing it correctly. Obligations driven by ISO 26262 and those which may be derived by application of ISO 26262 are due diligence activities aligned to the general duty clause of regulations imposed by US DOT and other Global Regulators. There may be duplication in various regulatory requirements (e.g. Federal Motor Vehicle Safety Standards / Vehicle Regulations > UNECE). may clarify some safety functions that are necessary. Same applies to ISO/PAS 21448 and UL2400.
9. Alignment and integration with IATF 16949 – Many implicit needs of 26262 are actually driven under ISO 9001 / IATF 16949. The quality standard is a prerequisite to ISO 26262, and its activities may be required to be reported by a Functional Safety Assessor. An Assessor generally will not proceed with a Functional Safety Assessment if, for example, there are open action items in the DVP&R.

10. Continuous refinement of process – No organization simply begins FS and is immediately at a level such as CMMI-5. Growth to high capacity in ASIL-D systems requires ***process growth and refinement***.
11. Emphasis of Systems Engineering in accordance with ISO 15288 and the INCOSE handbook. SE is its own discipline which requires its own specialized skill set. ASPICE and AGILE are not adequate for complex systems. ISO 26262 is based on a V model which itself is based on historical Systems Engineering such as ISO 15288. The related disciplines of refining, detailing, and otherwise engineering requirements are critical in 26262. Logical errors and omissions will certainly correlate to problems in the Safety requirements. If those problems are not addressed early, resolution will be very expensive. In addition, many standard systems engineering artifacts may be integrated with Functional Safety and SOTIF artifacts, so much can be gained by integration.
12. Analysis of the human role in hazard analysis and safety engineering, including MIT research into comprehensive analysis methods (STAMP/STPA, Systems Theoretic Problem Analysis) shows that the most difficult and hazardous issues are a combination of multiple systems, multiple control levels, and systems that with their controllers and meta-controllers contain unforeseen feedback loops.
13. Safety considerations integrated into project reviews and oversight (full partnership). Product oversight and major decisions must include project functional safety and management of functional safety in the decision-making team and leadership process.
14. Safety must have a key role in product release (a required signature) and in plant decisions through production line and decommissioning. ISO 26262 requires that products may not be released for production until a Safety Assessment is completed. After release for production, changes may be proposed by the production team, such as to address piece-part obsolescence or cost changes. Functional safety must be involved to ensure that new chosen piece parts/ components satisfy all standard and special requirements that the design claimed are required to build a safe product. All instances of the product being manufactured must be as safe as the first ones are. This is the maintenance of Safety Management throughout the product and production life cycle. This aspect is not clearly covered in ISO-26262, however it does mention that Safety is with intertwined with quality- oriented activities and work products.

ISO-26262:2018 Work Products Reference for Functional Safety Case Overview and Auditing

Good reference documentation: icomod.com >>> ISO26262 Work Products Visualized
https://icomod.com/ressources/aux-and-goodies/iso26262-flow-of-workproducts-visualized/

1. Work Products depend on the DIA (Design Interface Agreement) and/ or the type of product, i.e. microchip or complete assembly

FS – Functional Safety Management

2-5.5.1 Org Specific rules/processes for Functional Safety
2-5.5.2 Evidence of Competence
2-5.5.3 Evidence of Quality Management
2-5.5.4 Identified safety anomaly reports if applicable
2-6.5.1 Impact Analysis at Item Level
2.6.5.2 Project Plan Impact Analysis at Element Level, if applicable
2.6.5.3 Safety Plan
Safety Plan – Confirmation Review
2-6.5.4 Safety Case
Safety Case – Confirmation Review
2-6.5.5 Confirmation Measure Reports; [Audits: 1) Prelim \ 2) Final] & [Assessments: 3) Prelim \ 4) Final]
2-6.5.6 Release for Production Report
2-7.5.1 Evidence of Safety Mgmt for Production, Operations, Service and Decommissioning

Concept Phase

3-5-5-1 Item Definition
3-6.5.1 HARA (Hazard Analysis and Risk Assessment)
3-6.5.2 Verification Report of the HARA resulting from 3-6.4.6
3-7.5.1 Functional Safety Concept
3-7.5.2 Verification Report of the Functional Safety Concept resulting from 3-7.4.4

Production Development at the Systems Level

4-6.5.1 Technical Safety Rqmts/Specs
4-6.5.2 Technical Safety Concept
4-6.5.3 System architectural design specification
4-6.5.4 Hardware-Software Interface (HIS) specification
4-6.5.5 Specification of requirements for 2-7.5.1 above resulting from requirements in 4-6-4.8
4-6.5.6 Verification Rpt for system architectural design, HIS-spec, for 2-7.5.1 above and tech safety concept of 4-6.4.9
4-6.5.7 Safety Analysis Report resulting from requirements in 4-6.4.4
4-7.5.1 Integration and test strategy resulting from requirements in 4-7.4.1
4-7.5.2 System Design Specification Integration and test report from rqmts in 4-7.4.2, .3 and .4 (Sys level Test Results)
4-8.5.1 Safety Validation specification including safety validation environment description resulting from rqmts in 4-8.4.1 and .2
4-8.5.2 Safety Validation Report resulting from requirements in 4-8.4.3 and .4

Production Development at the Hardware Level

5-6.4.9 HRS Review Report in accordance with Part 8 Clause 9
5-6.5.1 Hardware Safety Rqmt Specs (HSRs) including test and evaluation criteria for rqmts 5-6.4.1 thru .8
Traceability Matrix including Test Cases to customer requirements (with 5 verified)
5-6.5.2 Hardware/Software Interface Specs (HSIs) refined resulting for requirements 5-6-4-10
5-6.5.3 Hardware Safety Rqmts Verification Rpt resulting for requirements 5-6.4.9 and 5-6.4.11
5-7.5.1 Hardware Design Specifications resulting for requirements 5-7.4.1 and 5-4.4.2
5-7.5.2 Hardware Safety Analysis Report resulting for requirements 5-7.4.3
Part 11 4.6.1.2 – 44-6.2.1.1 Reliability Prediction Analysis
5-7.5.3 Hardware Design Verification Report resulting for requirements 5-7.4.4
Part 4> 4-6.5.5 Spec of rqmts related to production, ops, service and decommission referenced in 5-7.5.5
5-8.5.1 Analysis of effectiveness to cope with random hardware failures (ref 5-8.4.1 thru .4.8)
5-8.5.2 Verification review report of evaluations of effectiveness of architecture (ref 5-8.4.9)
5.9.5.1 Analysis of Safety Goal violations due to random H/W failures (ref 5-9.4.2 or in 5-9.4.3)
5-9.5.2 Specification of dedicated measure for hardware (ref 5-9.4.1.2 and .1.3)
5-9.5.3 Report of evaluation of Safety Goal regarding 5.9.4.3
5-10.5,1 Hardware Intergradation and Testing Report (ref 5-10.4.1 thru .4.6)
5-10.5.2 Hardware Integration and Verification Report (ref 5-10.4.1 thru .4.6)

Production Development at the Software Level

6-5.5.1 Documentation of software development environment resulting for rqmts 6-5.4.1 thru .4.3 and C.4.1 - C.4.11
Software safety rqmts specifications resulting from rqmts 6-6.4.1 thru .4.3 and .4.5
6-6.5.2 Hardware/Software Interface Specifications (HIS) refined form requirements 6-6.4.4
6-5.5.3 Software Verification Report resulting from requirements 6-6.4.6 and .4.7

6.7.5.1 Software Architectural Design Specifications (ref 6-7.4.1 thru .4.13)
6-7.5.2 Safety analysis report resulting from requirement 6-7.4.10
6-7.5.3 Dependent failures analysis report resulting for rqmts 6-7.4.11
6.7.5.4 Software Verification Report resulting from requirements 6-7.4.14
6-8.5.1 Software unit design spec resulting from rqmts 6-8.4.2 thru .4.5
6-8.5.2 Software unit design spec resulting from rqmts 6-8.4.5
6-9.5.1 Software verification spec resulting from rqmts 6-9.4.2 thru .4.5
6-9.5.2 Software verification report refined from 6-9.4.2
6-10.5.1 Software verification spec refined from 6-10.4.2 thru .4.7
6-10.5.2 Embedded software resulting from requirements 10.4.1
6-10.5.3 Software verification report refined from 6-10-4.2
6-11.5.1 Software verification spec refined from 6-11-4.1 thru .4.3
6-11.5.2 Software verification report refined from 6-11-4.1 thru .4.4

Production, Operations, Service and Decommissioning

7-5.5.1 Safety-related content of the product plan (ref 7-5.4.1.1, 7-5.4.1.2, 7-5.4.1.3 and 7-5.4.1.4)
7-5.5.2 Safety-related content of the product plan including test plan (ref 7-5.4.1.5 and 7-5.4.1.6)
7-5.5.3 Control measures report Producibility rqmts spec from reference 7-5.4.1.7
7-5.5.4 Production process capability report resulting from requirements 7-5.4.2.2
7-5.5.5 Safety-related content of the maintenance plan (ref 7-5.4.3.1 thru .3.3)
7-5.5.6 Safety-related content of the service instructions (ref 7-5.4.3.3)
7-5.5.7 Safety-related content of information user availability (ref 7-5.4.3.4)
7-5.5.8 Safety-related content of decommissioning instructions (ref 7-5.4.3.5)
7-5.5.9 Operation, service and decommissioning requirements spec (ref 7-5.4.3.6)
7-5.5.10 Safety-related content of rescue services instructions (ref 7-5.4.3.7)
7-6.5.1 Control measures report (ref 7-6.4.1.1, 7-6.4.1.2, 7-6.4.1.5 and 7-6.4.1.6
7-6.5.2 Production process capability report (ref 7-6.4.1.3 and 7-6.4.1.4
7-7.5.1 Field observation instructions resulting from requirement 7-7.4.1.1

Supporting Processes

8-5.5.1 Supplier Selection Report (ref 8-5.4.2.1 and 8-5.4.2.2)
8-5.5.2 DIA – Development Interface Agreement (ref 8-5.4.3, 8-5.4.5.1 and 8-5.4.5.2)
8-5.5.3 Supplier's Safety Plan (ref 8-5.4.3 and 8-5.4.4)
8-5.5.4 Supplier's Assessment Report (ref 8-5.4.5.3 and 8-5.5.4)
8-5.5.5 Supplier Agreement (ref 8-5.6.1 thru 8-5.6.4)
8-7.5.1 Configuration Management Plan (ref 8-7.4.1 thru .4.5)
8-8.5.1 Change Management Plan (ref 8-8.4.1)
8-8.5.2 Change Requests (ref 8-2.4.2)
8-8.5.3 Impact Analysis and Change Request Plan (ref 8-8.4.3 and .4.4)
8-8.5.4 Change Report (ref 8-8.4.5)
8-9.5.1 Verification Plan (Update – ref 9-4.1.1 and .4.2)
8-9.5.2 Verification Specification (Update – ref 9-4.2.1 thru .2.4)
8.9.5.3 Verification Report (Update – ref 9-4.3.1 thru .3.4)
8-10.5.1 Document Management Plan (ref 8-10.4.1 and .4.2)
8-10.5.2 Documentation Guideline Requirements (ref 8-10.4.3 thru .4.6)
8-11.5.1 Software Tool Criteria Evaluation Report (ref 8-11.4.1 and .4.5)
8-11.5.2 Software Tool Qualification Report (ref 8-11.4.6 thru .4.9)
8-12.5.1 Software Component Documentation (ref 8-12.4.2.1)
8-12.5.2 Software Component Qualification Report (ref 8-12.4.2.2 thru .2.5)
8-12.5.3 Software Component Qualification Verification Report (ref 8-12.4.3)
8-13.5.1 Hardware element evaluation plan (ref 8-13.4.3.2)
8-13.5.2 Hardware element test plan (ref 8-13.4.3.5.1)
8-13.5.3 Hardware element evaluation report (ref 8-13.4.1.1, .3.6 and 4.6 if applicable)
8-14.5.1 Definition of a candidate for proven-in-use Augment Qualification Plan (ref 8-14.4.3)
8-14.5.2 Proven-in-use Analysis Report (ref 8-14.4.4 thru .4.5)
8-15.5.1 Base Vehicle Manufacture or Supplier Guideline (ref 8-15.4.2 and .4.3)
8-16.5.1 Safety rational resulting from requirements 8-16.4.2 thru .4.4)

Automotive Safety Integrity Level (ASIL)

9-5.5.1 Update of architectural information (ref 9-5.4)
9-5.5.2 Update of ASIL as attribute of safety requirements and elements (ref 9-5.4)
9.6.5.1 Update of ASIL as attribute of sub-elements of elements (ref 9-6.4)
9-7.5.1 Analysis of dependent failures (ref 9-7.4)
9-7.5.2 Dependent Failure Analysis Verification Report (ref 9-7.4.9)
9-8.5.1 Safety Analysis (ref 9-8.4)
9-8.5.2 Safety analysis verification report (ref 9-8.4.8)

Example Role & Qualifications of Functional Safety /Product Safety Officer

Expertise needed:

- Appropriate skills in safety technology
- Appropriate skills in technologies (e.g. mechanics, electronics, software, & etc.)
- Knowledge of the legal & normative requirements

Skills/Experience must be appropriate to the possible measure of damage, the extent of the automotive safety integrity level (ASIL), & the complexity of the design. Skills/Experience performing the following:

- Development of Safety Case
- Development of DIA (Dvlpmt Interface Agreement)
- Fault Tree Analysis
- FMEA
- Development of HARA
- ASIL Determination
- ASIL Decomposition
- Application of Safety Mechanisms
- Reliability Analysis
- Development of Test Cases
- Testing for Reliability
- Structural Metric Analysis

The Safety Case for the product will contain the items above, and will also include the following:

- Safety Plan
- Supplier project plan
- Supplier's safety plan
- Supply agreement
- Functional Safety assessment plan
- Configuration & Change management plans
- Document management plan
- Safety Goals
- Functional Safety Concept
- Requirements (Functional, Technical, HW/SW, HIS)
- Design Specifications (H/W & S/W)
- Hardware Metrics (Random H/W failures)
- Confirmation Measure Reports
- Item integration & testing plan
- Validation plan
- Verification Report, Software Verification Plan
- Design & Code Guidelines for Modeling & Programming Languages
- S/W tool qualification report application guidelines
- Release for Production report
- Production Plan, Prod. Plan, Maintenance Plan (Safety content)

Group/Corporate Functional Safety Manage Role:

- Part 2-5: Overall Safety Management
- Part 2-6: Safety Management during Concept Phase and Product Development
- Part 2-7: Safety Management after the Item's Release for Production

The Overall Safety Management provides the framework for safety related E/E-development projects (Ref: ISO-26262-Part 2, Clause 5)

1. Safety culture
2. Competence management
3. Quality management during the safety lifecycle
1. FS Evaluation, particularity proper "life" of the safety-oriented development process in the safety project
2. Creating Reports (agenda/participants/results of assessment/coordination report w/ people interviewed
3. Coverage of the results to the safety team
4. Planning of activities the FS (safety plan) & coordinates whole plan w/ the safety team (Project leaders, Team Leaders)

***SAFETY CULTURE:** PART 2, CLAUSE 5.4.2

2. Company-specific policies and processes
3. Resource management (i.e. sufficient resources for functional safety)
4. Continuous improvement process
5. Escalation process for functional safety
6. Authority of safety managers, responsible parties

***COMPETENCE MANAGEMENT:** PART 2, CLAUSE 5.4.3

Competence is to be assured in accordance with the corresponding responsibility:

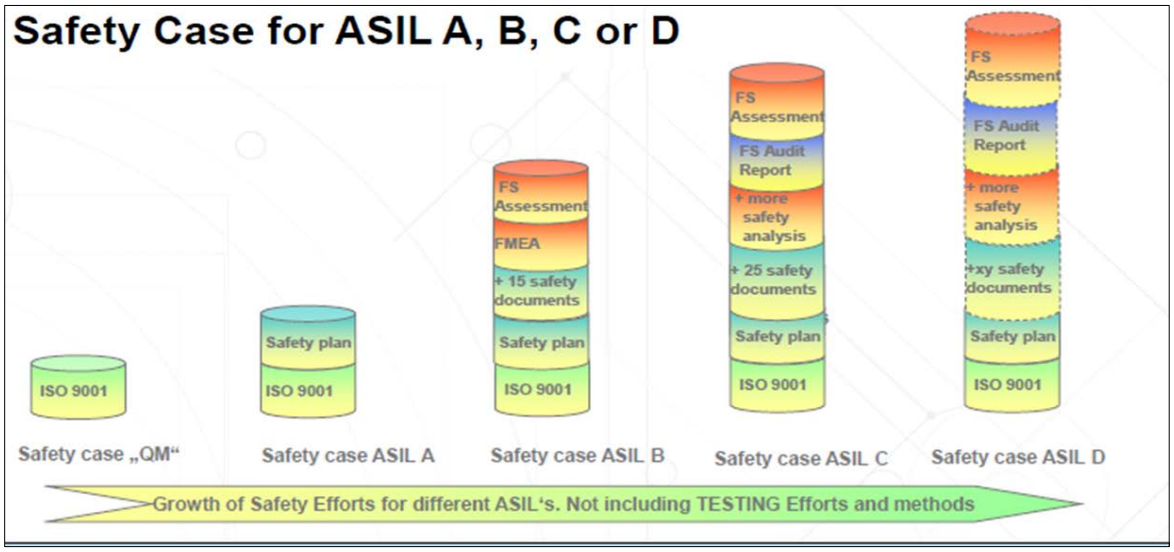
1. Team personal Training, education
4. Documentation of qualifications (e.g. data base)
5. Selection of team members involved in functional safety activities

***Quality management during the safety Life-Cycle:**

Functional Safety Management requires an established Quality Management

Functional Safety	**ASIL A-B-C-D**	⇨	**Mgmt of Functional Safety** Coordinates the requirements to be met by/for FS
Foundation Base	**QM**	⇨	**QMS (ISO-9001/IATF-16949)** Coordinates the requirements for quality

Example Functional Safety Case Overview



- end –

Notes Page

Published by:

The Michigan
Automotive
Functional Safety
Forum

January,
2021

AUTONOMOUS VEHICLES AND VEHICLE CONTROL systems have created challenges for suppliers in adopting functional safety, technology, and innovation to ensure functional safety all the way from the design stage to the end of the operating cycle. This user-friendly checklist has been designed to provide guidance to sub-tier suppliers as they carry out the functional safety process, and contribute to vehicle safety.

The checklist is suggested reading for Sales, Program Management, Engineers, Management, Design, Quality, Supply Chain, Auditors, Manufacturing, Human Resources, Finance, IT, and Legal professionals. It is intended to help cross-functional teams better understand the functional safety process, quality systems and risk management in the automotive supply chain.

MANAGING EDITOR/CONTRIBUTOR: Robert J Kozak, C.S.P.

Many thanks and much appreciation to all our contributors:
Kenneth Freeman, Kevin Grinnell, Peter Grim,
Dean Hill, and Dr. John Wang

...and to those readers who choose to engage their people and lead high performance teams.