SYNOPSYS®

WHITE PAPER

The Role of Confirmation Measures in ISO 26262 Functional Safety Automotive Products

Authors

Shivakumar Chonnad
Principal Engineer, Quality and Functional Safety

Vladimir Litovtchenko
Director, Quality and Functional Safety

Vrezh Sargsyan
Sr. Staff Engineer, Quality and Function Safety

Introduction

Modern automotive systems are built on the foundations of functional safety, long term reliability, and quality. Automotive semiconductor system on chips (SoCs) includes several IP elements which comprise the hardware and software systems that process and control data from the mechatronics (mechanical + electronics) for a specific application. With the increased hardware, software, and mechanical interactions within safety-critical systems, the functional safety development process should address random hardware faults and their failures that occur during the lifetime of the safety related product in a systematic way.

Standards like ISO 26262 provide the framework by specifying objective oriented confirmation measures and the necessary work products related to safety analyses. The minimum goal in a functional safety project can be to achieve the Single Point Fault Metric (SPFM) and Latent Fault Metric (LFM) for random hardware faults. Or it can cover the full spectrum of ISO 26262 standard to demonstrate that the project has systematically followed the standard. Part of the full spectrum systematic activities to meet the standard includes confirmation measures, which in turn includes confirmation reviews, the functional safety audit, and the functional safety assessment.

The confirmation measures are performed to judge whether the key work products provide sufficient and convincing evidence of their contribution to the achievement of functional safety. The completion of confirmation measures can hence clear the release for production step to formalize the decision to release the item, or element, for production, considering the results of the safety lifecycle, including the results of the applicable confirmation measures. Figure 1 illustrates where confirmation measures fit within the systematic functional safety development process.

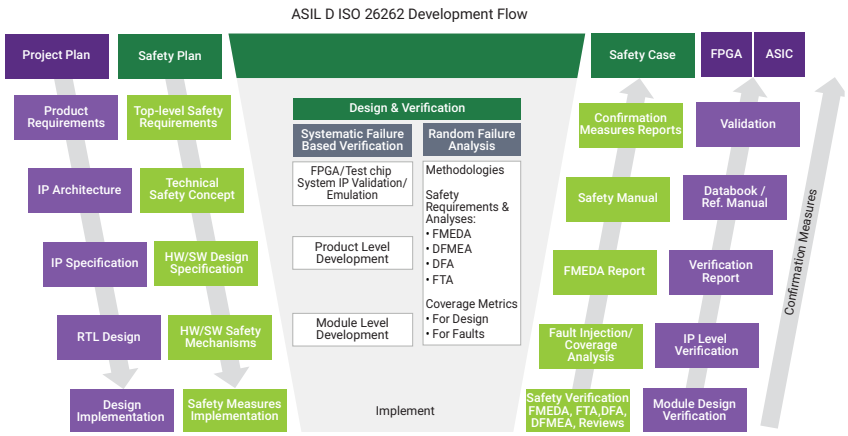


Figure 1: Functional safety development flow with confirmation measures

This white paper explains the various aspects of confirmation measures as defined by ISO 26262 and highlights its role and importance in achieving Automotive Safety Integrity Level (ASIL) compliance goals.

Confirmation Measures: An Overview

As part of the various safety activities that ISO 26262 standard references in a safety lifecycle, the responsibility to undertake the confirmation measures is a key task to be performed throughout the safety lifecycle management as a systematic activity. Confirmation measures include confirmation reviews, a functional safety audit, and a functional safety assessment. Depending on the applicable ASIL, confirmation measures are performed with sufficient independence regarding resources, management, and release authority. Figure 2 illustrates the scope of confirmation measures.

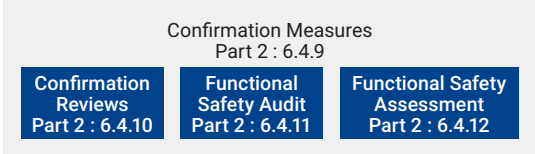


Figure 2: Confirmation measures and its constituents

The applicability of ISO 26262 clauses related to confirmation measures of semiconductors is tailored according to the context in which the semiconductor element is assessed. If the semiconductor device is being developed as a Safety Element out of Context (SEooC), the clauses can be applied at that level. For a semiconductor or IP supplier, the confirmation measures concerning safety at the item level are tailored out, as they are typically out of scope for semiconductor or IP suppliers.

The safety plan defines the activities and procedures for achieving functional safety, which includes scheduling of confirmation reviews, the functional safety audit, and the functional safety assessment. The level of independence of a person that carries out a confirmation measure is specified in the safety plan based on the ASIL. The safety manager is responsible for scheduling the confirmation measures. The details of a confirmation measure are planned by the resource responsible for that confirmation measure.

The confirmation review is one of the key constituents of confirmation measures. A confirmation review of a work product is a confirmation that the work product provides sufficient evidence to demonstrate functional safety. The goal of confirmation reviews is to ensure compliance with the ISO 26262 series of standards. To increase confidence in the achievement of the review objectives, the reviewer checks the correctness, completeness, consistency, adequacy, and contents of the work product against the corresponding requirements of the ISO 26262 series of standards.

Although ISO 26262 specifies several work products, the confirmation reviews are performed for specific work products like the safety plan, Technical Safety Concept (TSC), various safety analyses like Dependent Failure Analysis (DFA) and Failure Modes Effects and Diagnostics Analysis (FMEDA), and Safety Case. The work products for confirmation reviews are tailored within the safety plan. For any modifications of the functional safety activities, the rationale is included in the safety plan and reviewed during the confirmation review of the safety plan. A confirmation review can be done in varied approaches and can consist of an organization specific checklist that is based on the safety plan and lists the activities and work products that are required according to the context in which the semiconductor device is assessed. Based on the result of a confirmation review, the work product reviewed is judged to have achieved compliance to ISO 26262, or the findings of non-achievement are shared for further updates. The resources responsible to perform the confirmation review included in the safety plan are independent as per the ASIL of the project. At the end, a confirmation review report is provided that contains a judgement of the achieved contribution to functional safety by the work product. This is illustrated in Figure 3.

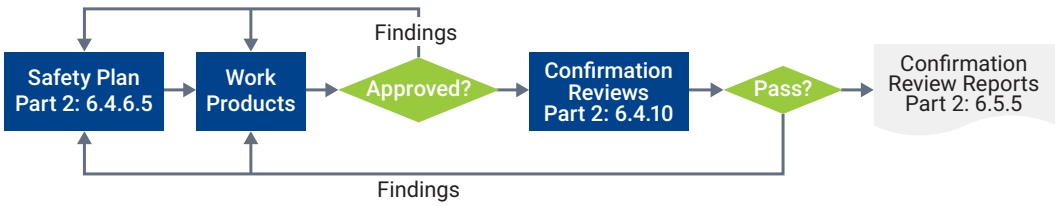


Figure 3: Typical confirmation review activity flow

A functional safety audit assesses the implementation of the processes required for functional safety and is an examination of an implemented process regarding the process objectives. The reference processes required for functional safety are defined in the ISO 26262 standard. The processes pertaining to an item or element are defined through the activities referenced or specified in the safety plan. The confirmation review of the safety case evaluates the argument provided in the safety case to judge whether the argument is sufficiently convincing.

A functional safety assessment (FSA) is required to judge whether the item has achieved functional safety, or whether the element contributes to the item's functional safety level. Though achieving functional safety is only possible at the item level, an FSA of a supplier that develops elements of the item refers only to an assessment with a limited scope and serves as an input for the subsequent FSA activities at the next integration level. The final customer in the item development, the vehicle manufacturer, appoints person(s) to perform an overall FSA to judge an item's achievement of functional safety. This judgement includes a recommendation for acceptance, conditional acceptance, or rejection of the item's functional safety. FSA is done with the appropriate independence to ensure an objective, unbiased viewpoint and to avoid conflict of interest. The use of the term "independence" in this whitepaper relates to organizational independence. For example, depending on the ASIL, the confirmation measure should be performed by a different person than the person(s) responsible for the creation of the considered work product(s), and by a person not reporting to the same direct supervisor or from the same department.

Figure 4 illustrates the flow of activities from the safety plan to the functional safety assessment report (FSAR) encompassing all confirmation measures activities.

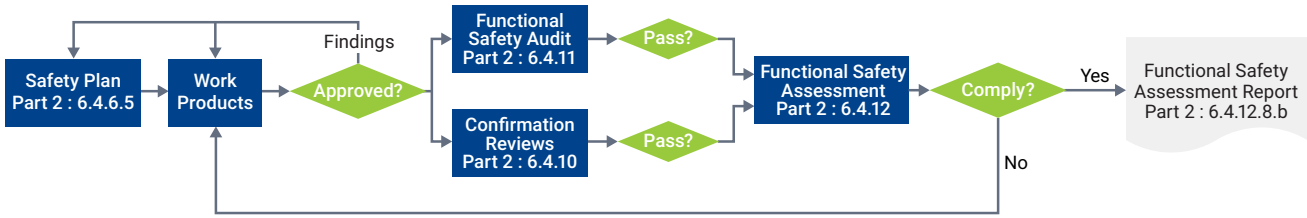


Figure 4: Confirmation measures activities

Functional Safety Audit

The functional safety audit is within the scope of confirmation measures. ISO 26262 defines functional safety audit as examination of an implemented processes with regard to the process objectives. The purpose of functional safety audit is to determine whether an organization's procedures comply with the requirements of ISO 26262 as well as whether the organization is following its own policies and functional safety processes at different phases of product development. ISO 26262 requires functional safety audit to be conducted where the highest ASIL (B, C, or D) is required. It is finalized before the release for production. The person responsible for carrying out audit (the auditor) must have a sufficient level of skills, competence, and qualification, and is given sufficient authority to fulfill their responsibilities. The typical inputs to a functional safety audit comprise of the processes and audit scope and the auditee documentation. The outputs include the audit report and an updated organization specific checklist for that functional safety audit. This is illustrated in Figure 5.



Figure 5: Inputs and outputs of functional safety audit

The functional safety audit aims to identify potential systematic failures in the product development processes, functional safety tasks, and activities. In contrast to functional safety assessment, the functional safety audit is not to judge whether the required level of functional safety has been achieved; it is only to confirm that the required processes are being followed and implemented correctly. The functional safety audit is performed during at least at two stages of product development. The first functional safety audit is conducted at an early stage of a project once product requirements and architecture are defined (typically referred to as readiness audit). A functional safety audit performed in an early phase in a project is beneficial to identify weaknesses in the processes.

The second functional safety audit is done after the design and verification activities are completed in an implementation phase (referred as implementation audit). This is illustrated in Figure 6 where the two audits are typically performed in a project flow. This is a high-level overview, and there may be other intermediate phases that are not shown in the figure.

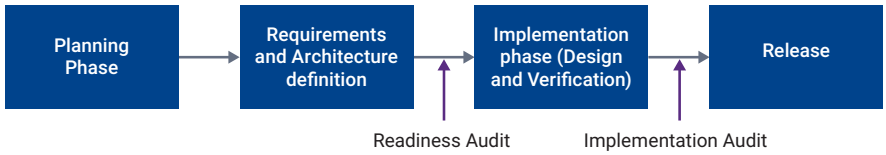


Figure 6: Functional safety audits at different phases of a project

The purpose and the scope of the two functional safety audits are different and are specified and communicated before the audit. The purpose of readiness audit is to check the readiness to execute the project. The audit scope at this stage will examine the project plan, safety plan, and supporting processes such as configuration, change, and documentation management plans. The readiness audit also confirms that the team has reviewed previous lessons learned (if any) and previous audit findings are addressed.

The functional safety implementation audit happens after design implementation and verification is completed and checks the conformance of the functional safety project execution. The implementation audit confirms that reviews were conducted at different phases and work products required in safety plan were developed, reviewed, and approved at required development phases. The functional safety implementation audit confirms that previous audit findings were addressed, and lessons learned were applied. The functional safety implementation audit looks for evidence for mentioned activities in the form of work products, review report, records, etc. The audit considers:

- Evaluation of the implemented processes
- Availability of work products in the safety plan that the organization-specific rules and processes
- The appropriateness and effectiveness of the performed or implemented safety measures
- The arguments, if provided, as to why the process related objectives of the ISO 26262 series of standards are achieved

Based on organizational etiquette, the functional safety audit findings can be classified as being Non-Conformities (NCONs) to ISO 26262 or to companies' processes, or Opportunities for Improvement (OFI). NCONs would affect the capability to achieve the intended results. The functional safety audit is considered complete only when all NCONs, if detected, are closed. OFIs are potential deficiencies of processes or implementation of those that wouldn't affect the capability to achieve the intended results. For each stage audit, an audit report is created to capture all findings. The functional safety audit is complete before the start of functional safety assessment activity.

Functional Safety Assessment

A functional safety assessment is carried out to judge the achieved functional safety of the item, or the contribution to the achievement of functional safety by the developed elements. This is applicable for ASIL C and D. An FSA may be based on a judgement of whether the technical goals for product functional safety objectives are achieved. The judgement considers the corresponding requirements of these standards, the state-of-the-art regarding technical solutions, and the applicable engineering domain knowledge at the time of the development. Undertaking the FSA needs to consider the planning of confirmation reviews and functional safety audit. Assessments also consider previous FSAs and the follow up of the resulting corrective actions, if applicable, or the results of the FSA activities regarding the elements or work products developed by suppliers, corresponding with the Development Interface Agreements (DIA).

An FSA is planned, at the latest, at the beginning of the product development at the system level. The FSA should be progressively performed during the product development and is finalized before the release for production. One or more persons are appointed to carry out an FSA. The scope of FSA includes the safety plan and the work products with their confirmation reviews, and the evaluation of the implemented processes can be based on the results of the functional safety audit. The appointed functional safety assessors provide an FSAR that contains a judgement of the achievement of functional safety objectives. The functional safety assessor has the authority to perform the FSA according to their discretion, including the breadth and depth of analysis of the safety activities and their results. In large projects involving distributed development, an FSA can be performed by the manufacturer and the suppliers in the supply chain each addressing their own areas of responsibility.

An FSAR is a result of a confirmation measure includes the name and revision number of the work products or process documents analyzed. The report may include a recommendation for conditional acceptance subject to the resolution of identified conditions. In the case of a recommendation for conditional acceptance, the FSAR includes the corrective actions needed. If the recommendation in an FSAR is a rejection of the achieved functional safety, then adequate corrective actions should be performed, and the FSA is repeated. If the item changes subsequent to the completion of confirmation measures, then the pertinent confirmation measures will be repeated or supplemented.

Putting it All Together

Results from conducted confirmation measures include evidence and arguments related to the IP development process and avoidance of systematic and random hardware faults. These reports shall be systematically traceable in a project. For semiconductor IP, typical confirmation measure output include the confirmation review reports, functional safety assessment and audit reports. These reports will help in making a judgement on achievement of functional safety of the product. The supplier's work products for compliance become part of the semiconductor developer's safety argument. At the item level, the vehicle manufacturer evaluates the functional safety of the integrated item. A part of their evaluation can include the work products or information provided by one or more suppliers, including reports of the FSA.

Conclusion and Synopsys Automotive IP

As part of the functional development process for systematic automotive compliance projects, Synopsys systematic automotive IP products follow the confirmation measures per ISO 26262. Acquiring the functional safety assessment report as part of the deliverables of such a systematic automotive compliance project from an SEooC developer will help accelerate the integrator’s safety argument at the next tier.

SYNOPSYS®

©2023 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at http://www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners.
01/06/23.CS966562916-automotive-iso26262-confirmation-measures.

Pub: Jan. 2023