ISO26262

Introduction:

"Road vehicles"- Functional Safety- It is an international standard for functional safety of electrical

or electronic systems that are installed in road vehicles, defined by ISO in 2011.

This includes driver assistance, propulsion, and vehicle dynamics control systems.

History:

The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems.

ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic

and electrical safety-related systems.The first edition (ISO 26262:2011), published on 11 November 2011, was limited to electrical

and/or electronic systems installed in "series production passenger cars" with a maximum gross weight of 3500 kg. The second edition (ISO 26262:2018),published

in December 2018, extended the scope from passenger cars to all road vehicles except mopeds.

Aim:

ISO 26262 is a risk-based safety standard, where the risk of hazardous operational situations is qualitatively assessed and safety measures are defined

to avoid or control systematic failures and to detect or control random hardware failures, or mitigate their effects.

Goals:

1.Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning)

and supports tailoring the necessary activities during these lifecycle phases.

2.Covers functional safety aspects of the entire development process (including such activities as requirements specification,

design, implementation, integration, verification, validation, and configuration).

3.Provides an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs).

4.Uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk.

Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved.

Importance:

Specific steps are required in each phase. This ensures safety from the earliest concept to the point when the vehicle is retired.

By complying with this standard, you’ll avoid or control systematic failures. And you’ll detect or control random hardware failures.

(Or, you’ll mitigate the effects of failure.)

The functional safety standard covers all of the functional safety aspects of the entire development process:

Requirements specification

Design

Implementation

Integration

Verification

Validation

Configuration

The 10 parts of ISO26262:

Part1: Vocabulary - terms, abbreviations or definitions for app in all parts of the standard.

for eg: item:Specific sys(combination of systems).starting point for product-specific

safety development under this standard.

Element:A sys, or hardware or software unit in a sys that can be distinctly identified or manipulated.

Fault: Abnormal condition that can cause an element to fail.

Error: self explainatory

Fault Tolerance: Ability to deliver a specified func in the presence of one or more specified faults.

Malfunc behaviour:

Hazard:

Part2: Management of Functional safety.

Hazardous Event

Safety Goals

ASIL

Safety Requirements

part3: Concept phase

part4: Product development at system level.

part5: product development at hardware level.

part6: Product development at software level.

part7: Product and operation

part8: Supporting processes.

part9: ASIL-oriented and safety-oriented analysis

part10: Guidlines on safety standard.

Reference: <https://www.perforce.com/blog/qac/what-is-iso-26262>

https://esc.uk.net/services/automotive-machinery-safety/iso-26262/

https://en.wikipedia.org/wiki/ISO\_26262

video for reference: https://en.wikipedia.org/wiki/ISO\_26262---- ISO26262- Functional Safety at a Glance

ASIL

AUTOMOTIVE SAFETY INTEGRITY LEVELS

What is ASIL?

ASIL is a key component of ISO 26262 and it is used to measure the risk of a specific system component.

The more complex the system, the greater risk of systematic failure and random hardware failures.

There are 4 ASILs named from A to D.

ASIL A is the minimum level of risk and ASIL D is the maximum as you go from A to D, the compliance requirements get stricter.

When determining Automotive Safety Integrity Levels, there’s also a fifth option — QM (quality management).

This is used to note that there isn’t a safety requirement for that component. (But it’s typically still a good idea to comply in order to improve product quality.)

How to Determine ASIL?

ASIL is determined by three factors — severity, exposure, and controllability.

Severity

Severity measures how serious the damages are of a system failure. Damages include both people and property.

There are four classes of severity:

S0: No injuries.

S1: Light to moderate injuries.

S2: Severe to life-threatening (survival probable) injuries.

S3: Life-threatening (survival uncertain) to fatal injuries.

Exposure

Exposure is the likelihood of the conditions under which a particular failure would result in a safety hazard.

The probability of each condition is ranked on a five-point scale:

E0: Incredibly unlikely.

E1: Very low probability (injury could happen only in rare operating conditions).

E2: Low probability.

E3: Medium probability.

E4: High probability (injury could happen under most operating conditions).

Controllability

Controllability is a measure of the probability that harm can be avoided when a hazardous condition occurs. This condition might be due to actions by the driver or by external measures.

The controllability of a hazardous situation is ranked on a four-point scale:

C0: Controllable in general.

C1: Simply controllable.

C2: Normally controllable (most drivers could act to prevent injury).

C3: Difficult to control or uncontrollable.

<https://www.perforce.com/blog/qac/what-is-iso-26262>

https://www.techdesignforums.com/practice/technique/functional-safety-automotive-software-virtual-prototype/