Toward the application of ISO 26262 for real-life embedded mechatronic systems

Jean-Marc Astruc, N Becker

Toward the application of ISO 26262 for real-life embedded mechatronic systems

J-M. Astruc[1], N. Becker[2]

1: Continental Automotive France SAS, 1 avenue Paul Ourliac F-31036 Toulouse,
jean-marc.astruc@continental-corporation.com
2: PSA Peugeot-Citroën, Centre de Belchamp F-25218 Montbéliard,
nicolas.becker@mpsa.com

1. Introduction

The document ISO 26262 entitled 'Road vehicles – Functional Safety' [1] is a standard being issued by the TC22/SC3/WG16 working group of the International Standard Organization. Its scope is the functional safety of electric and electronic (E/E) embedded systems installed in automotive vehicles.

Its future utilisation for real-life systems raises several questions:

- The actual embedded systems are not based exclusively on E/E technology. They also include components from other technologies, such as mechanical, hydraulic, pneumatic, etc. The EMS (Engine Management System) shown in figure 1 gives an example of such a real–life system:

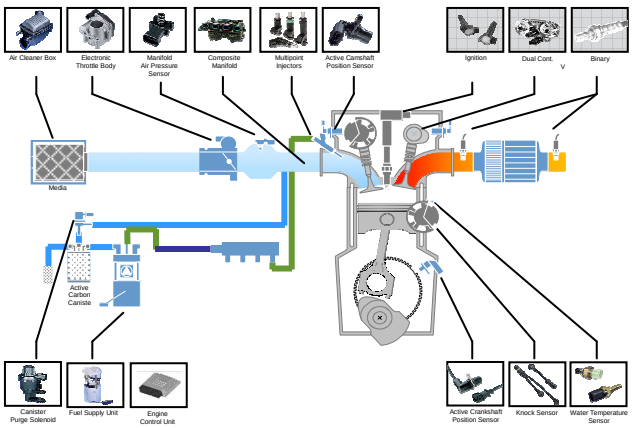


Figure 1 – Multi-Point Injection EMS

  The functional safety of these systems needs to address all these technologies. The appearance of ISO 26262 that addresses E/E systems and components raises the need for ensuring the consistency of the safety studies between the E/E development and the development of other technologies.
- The development of electronic systems and components in the automotive industry is seldom a top-down process based on an academic V cycle model. Development has to cope with existing elements, and in most cases with pre-existing vehicle architecture. Moreover, the elements are often designed using incremental improvement and rely on reuse of existing blocks. The safety lifecycle has to be adapted and flexible in order to address these various situations.

This contribution presents an overview of the different strategies that can be followed to enable compliance of the safety case with ISO 26262 in these real-life situations.

2. Elements of other technologies

The elements of other technologies are explicitly mentioned at several places of the standard.

The part 2 of ISO 26262 describes the requirements on management of functional safety. These include the need for a safety manager, the development of a safety plan, and the definition of confirmation measures (safety review, safety audit, safety assessment). These requirements are intended to be used for the development of the E/E systems and elements. However, they can easily be extended to the elements from other technologies.

Those elements of other technologies appear on the safety lifecycle of ISO 26262 as shown in figure 2:

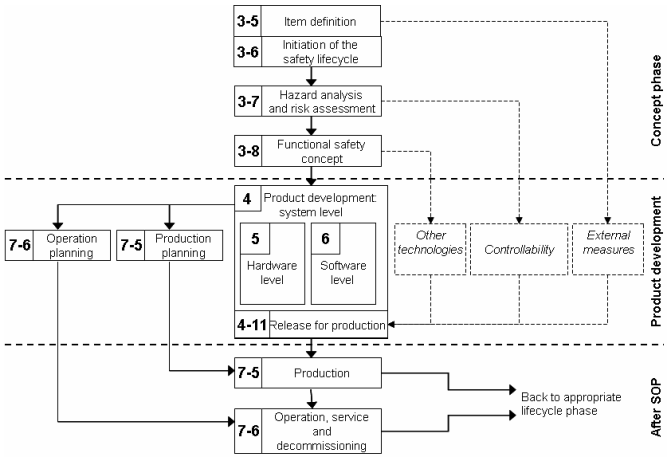


Figure 2 – Safety lifecycle of ISO26262

2.1. System definition

The first step of the safety lifecycle is the definition of the perimeter of the system to be analyzed which may include elements of different technologies such as mechanical parts, hydraulic, energy storage, etc.

ISO 26262 does not restrict the scope of the analysis to E/E elements as many system elements such as the sensors and the actuators are inherently a mix of different technologies.

For instance, a fuel injector comprises a hydraulic and mechanical part, linked with the fuel hoses and connected to the combustion chamber or the intake manifold. Additionally, it comprises an E/E actuator that controls the volume and the timing of the fuel injections, which are both critical to the fuel consumption, the pollutants emissions and the engine noise.

A restriction of the scope of the safety analyses to the E/E elements would be artificial and would lead to partial results from the customer safety point of view.

2.2. Hazard analysis and risk assessment (H&R)

The second step of the safety lifecycle is the hazard analysis and risk assessment that is conducted at the vehicle level, taking into account:

- The portion of the mission profile for which a failure in the system may lead to a harm, determining the exposure parameter;
- The ability of the driver or any other road participants to cope with the system failures and avoid this harm, determining the controllability parameter;
- The human consequences if the controllability actions fail, determining the severity parameter.

The ASIL Level is then evaluated by taking into account the three preceding parameters for the different life situations. A safety goal is then formulated with the corresponding ASIL, to specify the system behaviour necessary to ensure the safety. The safety goal represents the top-level safety requirement for the system.

For instance, one safety goal can be "no runaway of the engine".

As seen above, the H&R does not take into account the technologies that will be implemented in the system, but only the potential harm to the driver and the other road users. In this respect, the H&R classification can be derived into requirements allocated to parts of other technologies during the following steps of the safety process.

For instance, if we consider a windshield wiper system, the safety analysis will consider the effects that the loss of the wiper function will have on the drivers visibility, and not the different causes that this loss may have.

2.3. Functional Safety Concept

The third step of the ISO26262 safety lifecycle is to define the Functional Safety Concept, This safety concept is a set of Functional Safety Requirements, derived from the Safety Goal, and allocated to the elements of the system architecture in order to fulfil the safety goal.

The ISO26262 standard requires that the Functional Safety Requirements are allocated to the E/E elements contributing to the safety goal. It also requires those requirements to be allocated to elements from other technologies if they contribute to the safety goal. In this latter case, the standard will not provide guidance on the design methods nor on the safety activities required to ensure its contribution to functional safety.

For instance, a runaway of the engine may be the consequence of an electronic hardware failure or a software bug in the ECU (Engine Control Unit) of the EMS (Engine Management System), or a mechanical failure that makes the Electronic Throttle Body wide open. ISO 26262 provides methods to identify and limit the consequences and/or the occurrence of the former failure modes including E/E-based safety mechanisms. It requires that safety requirements are allocated to the mechanical parts to avert breakdowns, but the nature of these requirements and the means to show compliance is left to each OEM and supplier.

The nature of these requirements will depend on the field of technology.

Examples of such requirements include:

- Reliability requirement;
- Specification of the environment of the part and verification that it can resist to these solicitations: moisture, temperatures, vibrations, number of cycles of stress in use, etc. Such environment specification can be used during testing to show that the reliability of the part is sufficient for the safety concept.
- Identification of safety-related special characteristics, e.g. according to ISO/TS 16949;
- Process requirements.

The consistency of the dependability requirements, for both mechanical and E/E components, is necessary to obtain an efficient safety concept.

A statistical method that can be used for this purpose is known as the stress/strength modelling: for a given reliability target, and for a given failure mode, the model uses two statistical distributions:

- The statistical distribution of the stress factors that the part will meet during its service life, taking into account the variability of driver's usage of the car. This is known as the "stress distribution"
- The statistical distribution of the ability of the different parts that will be produced to cope with the stress factors, taking into account the production variability. This is known as the "strength distribution".

The actual risk of failure of the part can be modelled and compared to the reliability target.

Moreover, the ISO 26262 standard requires that the Functional Safety Concept is verified to fulfil the safety goal. Therefore, it is necessary to take into account all the components that will be necessary to show that the functional safety concept is sufficient to reach the safety goal, whether of mechanical, hydraulic or E/E technology.

2.4. Technical Safety Concept

The fourth step of the safety lifecycle is the specification of the technical safety concept and the system design.

This phase is restricted to the E/E components of the system. It is intended to ensure and verify the implementation of the functional safety requirements in the system design.

However, some safety mechanisms are dedicated to identify failure modes of mechatronic components; this is typically the case for the diagnostic of sensors or actuators.

In most of the systems, a failure of a sensor or an actuator can lead to incorrect system behaviour and to the violation of the safety goal. In this case the designer has to make a choice: shall the sensor/actuator be designed to be as reliable as required, shall the system be able to detect failures in these components and switch to a safe state, or shall a redundancy be implemented in the system to allow fault tolerance?

As often as not, the designer has to use a combination of these measures, as it is not always possible to ensure the reliability required to leave a single component as a single point of failure for a safety-critical system of ASILC or D. On the other hand some failure modes such as fatigue rupture of the mechanical components are uneasy to diagnose before the loss of the component; it has to be adequately dimensioned.

For instance, in order to avoid failure of the injection fuel system due to overpressure, two strategies may be combined:

- Make the fuel system tolerant to pressure loading;
- Implement a monitoring system including a pressure sensor and pressure limitation strategy for the fuel sub-system.

The ISO 26262 standard also requires a verification of the system design with regard to its ability to maintain the safety goal. This verification shall include both inductive and deductive analyses for the highest safety goal, e.g. FMEA and Fault Tree Analysis. At this stage, the designer shall have a proper rationale that the failure modes of the system are adequately covered, including sensors and actuators.

2.5. Hardware and Software Development

The fifth step of the safety lifecycle is the hardware and software design and verification. These activities are purely related to the E/E components and are well described in the literature on ISO 26262.

Some important requirements of ISO 26262-5 relate to the compliance of the system with hardware failure targets.

As a result of this phase, the supplier shall provide an analysis of the failure modes of its product; it has to be reviewed by the system designer to verify that the actual failure modes of the design are adequately covered and do not introduce additional hazards, for instance due to the technologies or design used.

2.6. Integration and Testing

The next steps are the integration and verification activities based on tests. They take place in three sub-phases:

- The hardware/software integration, dedicated to verify that the software operates correctly on the intended target hardware.
- The system-level verification, dedicated to verify the correct integration of the different components of the system, including sensors, ECUs and actuators.
- The vehicle-level verification, dedicated to test that the safety requirements are adequate and correctly implemented in the vehicle environment.

For each sub-phase, several tests families are performed:

- Verification of the requirements;

- Verification of the coverage and performance of the safety mechanisms;
- Verification of the internal and external interfaces;
- Verification of the robustness.

The verification of the coverage of safety mechanisms often relies upon fault-injection tests, where a particular component will be put into a fault state to verify that the system diagnostics are able to detect this fault and switch the system into a safe state.

When performed at system or vehicle level, these tests will be carried out in particular on sensors and/or actuators. In these cases the failure modes that are injected in the components are not only the E/E failure modes of the sensors or actuators, but also the relevant mechanical failure modes. For instance if the designer has made the choice to have a diagnostic to monitor the fatigue failure in a sensor, the system-level tests shall include a provoked failure in the mechanical part of the sensor to evaluate the ability of the diagnostic to detect and control it.

2.7. Validation

The validation of the system is required at the end of part 4 of the standard. It asks for a complete assessment of the functional safety, based on vehicle tests and analyses taking into account the whole system and all its technologies. If other technologies have been taken into account during the development of the safety architecture, the rationale for their compliance shall be shown in the safety case during this sub-phase.

3. Use-cases for ISO 26262

3.1. Overview

The previous chapter of this contribution was dedicated to the question “How ISO 26262 deals with mechatronic components (i.e. the components of other technologies than E/E technology)?”

The present chapter provides another point of view on the ISO 26262 standard through the question: “How to deal with this standard in the real life of the automotive projects?”

One may think that once this standard will be officially released (by 2011), every E/E system put on the market and embedded in a vehicle will have to fulfil the complete safety lifecycle of this standard shown in figure 1 and will have to comply with each of its requirements.

This statement is not completely true: to date, the innovation in the automotive industry is mainly driven by the E/E systems. Nevertheless, few of them are completely developed from scratch. One of the reasons for this is that the quality objective, the cost and delay objectives are more easily met by (re-) using well-trusted parts and components than by designing brand new products.

It basically means that each design decision made in the automotive projects needs to take into account those cost/delay/quality objectives while satisfying the constraints of the functional safety, especially regarding the demonstration of compliance to ISO 26262.

This chapter introduces different use-cases for the development of systems in accordance with ISO26262 based on the reuse of existing sub-systems and elements.

3.2. Reuse of systems

Here, the reuse of a system means the use of a pre-existing system developed under the ISO 26262 for a new application[1]. Such reuse of systems addresses a wide range of different cases that may be summarized as follows:

- The system upgrade – It consists of the reuse of an existing system with the application of modification(s). In most of the cases, the modifications are motivated by the introduction of new features. The introduction of the “stop & start” function illustrates a significant upgrade regarding the existing EMS. Actually, it impacts the system behaviour, as well as the hardware architecture and the software design.
- The system carry over – it corresponds to the reuse of an existing system without any modifications or only with minor modifications. The installation of an existing power train or combustion engine, including its EMS, into a new target vehicle gives an example of a carry over for an EMS. Of course, in this example, the EMS will have to be adapted to some of the basic parameters of the targeted vehicle, e.g. gross mass, tire size, and torque consuming equipments. This adaptation is usually done through the adjustment of a sub-set of calibration data, without changing the design and the implementation of the system itself.

In any case of reuse of a system, a comparison analysis is required at vehicle level between the previous use of the system and the future one, in order to identify the intended modifications applied to the system itself, to its environment, and/or to its

[1] Proven in use systems that may not be developed under ISO 26262 are presented in 2.5.

conditions of use; and to assess the impact of these modifications on the functional safety of the system: Are the safety goals the same? Are there new potential hazards? Etc.

The safety lifecycle of ISO 26262 is tailored according to the results of this analysis, in term of safety activities that have to be (re)conducted and work products that have to be reworked. The goal is that any modification applied to an existing system for reuse purpose will comply with the ISO 26262 standard.

Depending on cases, the tailored lifecycle may encompass all or part of the activities of most of the phases of the full safety lifecycle of ISO 26262, starting with a new hazard analysis and risk assessment down to the phases of validation and production of the new system. It may also be simply restricted to a change of some calibration data with the corresponding verification and validation.

3.3. New systems

New systems are E/E systems developed from scratch that do not rely on pre-existing systems in most of the cases. It mainly corresponds to the introduction of a completely new application. It may also consist of pre-existing systems that are impacted with such significant modifications that they are to be considered as new systems. Examples of new systems in the field of power train applications include embedded battery loaders, range extenders and engine management systems for new electrical and hybrid vehicles. These systems are substantially different from the existing ones used for diesel and gasoline combustion engines.

Basically, the new systems have to follow the entire safety lifecycle of the ISO 26262 standard from the definition of the system down to their validation and production, and then the operation in the field until their decommissioning. All the expected work products resulting from those phases that are described in ISO 26262 are to be produced and compiled in a dedicated safety case.

Additionally, though the new systems are in principle developed from scratch, the use of well-trusted design principles is recommended in order to reduce the likelihood of unknown failures related to new designs. This encompasses standardized interfaces for inter-system communication, safety-architectures, dedicated safety mechanisms for the detection and control of failures. The standardised E-Gas monitoring concept for engine management systems of gasoline and diesel engine worked out by the German VDA working group 'E-Gas-Arbeitskreis' is an example of well-trusted safety-architecture that may be used for application other than EMS for combustion engine, provided it fits for the purpose of the new application in terms of diagnosis feasibility, environment constraints, time constraints, robustness, etc.:

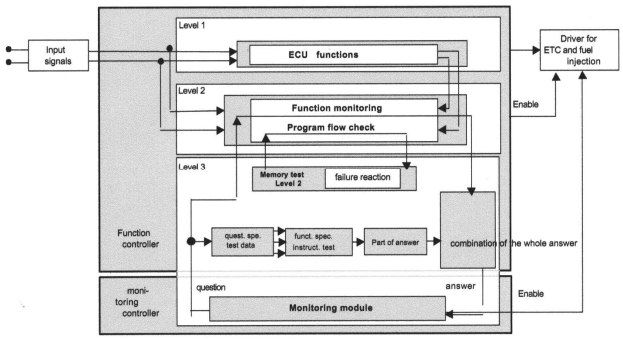


Figure 2 – E-Gas monitoring concept

3.4. Safety-related elements out-of-context (SEooCs)

From a car manufacturer's perspective, the use-cases at system level described above may be sufficient to deal in general with the development of safety-related E/E systems. From a supplier standpoint, it is necessary to develop additional use-cases, especially for the safety-related elements[2] so called SEooCs that are developed from scratch according to ISO 26262 as generic products for automotive applications, i.e. outside of the context of development of a particular system.

The concept of SEooC can be applied at any level of a system except at the entire system level itself, i.e. at a sub-system level, hardware or software level, for safety-related elements of any complexity. Typical examples of SEooC include:

- A hardware ECU (Engine Control Unit) developed for a certain type of EMS applications (low-end, medium or high-end vehicles) with the corresponding basic software that includes hardware build-in tests;
- An ASIC (Application Specific Integrated Circuit) that implements ECU monitoring functions and ensures the cut-off of essential actuators in case of severe failure;
- A module that provides the ECU with the engine synchronization. Engine synchronisation is intended to determine the position of the pistons relative to the combustion cycle for any number of cylinders, cam and cranck target wheel profiles and position, and types of sensors.

The entry point in the safety lifecycle of the ISO 26262 for the development of such a SEooC corresponds usually to the specification of its

[2] For the purpose of this paper, an element designates a part of a system including components, hardware, software, hardware parts and software units

requirements at the adequate level: system, hardware or software, depending on the cases.

Since, in general, the intended use of a SEooC can be anticipated but its actual future usages cannot be fully described, some assumptions need to be stated explicitly, especially regarding the technical safety concept for which the SEooC is intended to be used and its ASIL capability. Here, the ASIL capability of a SEooC designates the set of ASIL dependent requirements of ISO 26262 that the SEooC fulfils in order to cope with the systematic failures (and the random hardware failures when applicable).

The point of exit of the development of a SEooC in the safety life cycle corresponds to the achievement of the verification of this SEooC and of the work products of ISO26262 that are created during this generic phase

The use of a SEooC in a particular application consists in verifying that the assumptions made for the SEooC fit with the purpose of this application before its integration as every other element in the software, hardware or system architecture in accordance with ISO 26262 requirements.

3.5. Qualification of safety-related elements

Another use-case of interest for the suppliers and car manufacturers is the usage of safety-related elements that have not been developed according to the ISO 26262 standard, but that are intended to be integrated in the context of new systems developed under ISO 26262.

This use-case relies on the qualification of such elements. It is basically limited to medium and low complexity elements such as sensors and actuators, hardware modules or software components.

Examples of safety-related elements candidate for qualification may include:

- Injectors developed prior to the release of ISO 26262;
- General purpose DC supply module for ECU and sensors;
- COTS (Commercial Off The Shelf) Math library;
- In-house software controller for ETB (Electronic Throttle Body).

As a minimum, the qualification of such elements necessitates that their specification is available. The qualification is mainly based on requirement-based tests of these elements, i.e. the testing of their functional behaviour and performances, in order to show their suitability for their (re)use as part of the system being developed under the ISO 26262.

Additionally, the qualification of the software-based elements has to address the behaviour of the software components in case of failures or anomalous operating conditions.

In the same way, the qualification of hardware-based elements has to address characteristics such as the failure modes of the elements, the distribution of the failure rate per failure mode, the diagnostic capabilities.

3.6. Proven in use systems and elements

Basically, the scope of ISO 26262 excludes existing systems already in the field that have been developed prior to the release of this standard.

However, new applications may be derived from those systems and will have to comply with ISO 26262 in the case of safety implication. It is likely that all the work products required by ISO 26262 will not be available from the previous development. Consequently, a significant rework will be necessary to produce retrospectively these work products in order to fulfil this standard.

In such a case, a proven in use argument may be used as an alternative to this rework in order to show compliance with ISO 26262, provided relevant field data on existing systems is available.

More generally, a proven in use argument is an alternate means of compliance to the ISO 26262 requirements that can be applied to any future system or element whose definition and intended conditions of use are identical or have a very high degree of commonality with a product that is already released and in operation. Proven in use argument relies on:

- The relevance of field data during the service period of the candidate to a proven in use argument;
- A disciplined configuration management and change control of the product during and after its service period;

The service period of a candidate results from the addition of the observation period of all the specimens that are in the field and identical to the candidate.

A limit is given by ISO 26262 for the observable incident rate during the service period[3], as shown in table 1. The observable incident rate is the rate of the failures that are reported to the manufacturer and caused by the candidate with the potential to lead to the violation of a safety goal:

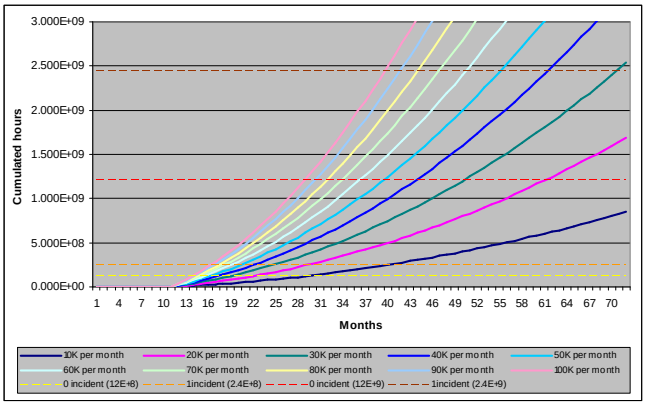
ASIL	Limits for observable incident rate
D	$< 10^{-9}$/h

[3] With a single side lower confidence of 70%, using a Chi-square distribution

C	< 10^{-8}/h
B	< 10^{-8}/h
A	< 10^{-7}/h

Table 1: limits for incident rate

The following chart indicates the number of months necessary for a candidate in the field before being definitively declared proven in use. It depends on the target taken as reference (10^{-9}/h or 10^{-8}/h) and on the number of observed incidents (no or one incident). It depends also on the monthly production, i.e. the number of specimen spread in the field. Here, each specimen is assumed to operate 396 hours per year.



For example, it will take 16 months for a candidate introduced in the field with a production of 40 000 parts per month to be proven in use with regard to a safety goal ranked ASILC in case no incident is observed. It will take 21 months in case one incident is observed.

For a safety ranked ASILD, it will take respectively 44 months without any incident and 61 month with one incident.

In the case where the service period of the candidate meets this target, the corresponding sub-phases of the safety lifecycle for developing the candidate can be substituted by the proven in use argument.

The credit of a proven in use argument may be anticipated to some extend provided the following targets shown in table 2 are achieved with no observed incident:

ASIL	Limits for observable incident rate
D	< 3*10^{-9}/h
C	< 3*10^{-8}/h
B	< 3*10^{-8}/h
A	< 3*10^{-7}/h

Table 2: limits for incident rate (anticipated)

4. Demonstration of compliance

The previous chapters of this contribution give some hints on how the upcoming ISO 26262 can be used in the context of real-life projects, dealing with elements of other technologies and with pre-existing elements.

For the future projects developed under ISO 26262, one of the challenges will be to define and maintain an overall strategy for showing compliance to this standard. This strategy should be developed at the very beginning of the project in a safety plan that takes into account those constraints and combines in the most efficient way the different use-cases presented in this contribution (e.g. credit from the use of other technologies, carried over or upgraded systems, use of SEooCs, qualified elements, or proven in use products).

Another challenge for the companies applying ISO26262 will be to provide the projects with those different use-cases and organize the corresponding work products in a way that they can be easily compiled by any project in a safety case.

5. References

[1] ISO/TC22/SC3/WG16, "*ISO/DIS26262 Road vehicles — Functional safety*" – June 2009

- Part 1: Vocabulary
- Part 2: Management of functional safety
- Part 3: Concept phase
- Part 4: Product development: system level
- Part 5: Product development: hardware level
- Part 6: Product development: software level
- Part 7: Production and operation
- Part 8: Supporting processes
- Part 9: ASIL-oriented and safety-oriented analyses
- Part 10: Guideline