

System Design and Verification for a Safety Related Integrated Sensor

Vincenzo Sacco, Mathieu Poezart, and Gael F. Close
Melexis Technologies SA

ABSTRACT

This paper presents the engineering aspects of an integrated, monolithic, angular position sensor to be developed as Safety Element out of Context (SEooC) in accordance with ISO-26262[1]. The sensor is a Hall-effect-based angular sensor, used in a wide range of automotive, safety-critical applications such as accelerator pedal position, throttle-valve position, or any other application requiring the accurate measurement of the angular position of a mechanical part. The assumed safety requirements allocated to this sensor have to be developed according to ASIL-C.

The mapping between technical safety requirements and architecture elements, as conveyed by the technical safety concept, will be first presented. Failure mode effect and Diagnostic Analysis (FMEDA)[2], supporting the safety mechanism specification will be discussed next; here a safety mechanism selection guide is also proposed. The paper will finally show how this safety-centric analysis is integrated into a classic mixed-signal integrated Circuit verification methodology.

CITATION: Sacco, V., Poezart, M., and Close, G., "System Design and Verification for a Safety Related Integrated Sensor," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 8(2):2015, doi:10.4271/2015-01-0234.

INTRODUCTION

Over the last decades, the industry has provided a steady improvement in the safety of automobiles. Advances in modern electronics have accelerated the number and features of safety systems. Semiconductor devices, sensors, actuators and computer controlled systems with complex software are integral to these system designs.

This increasing complexity drives the need for a systematic process for safety systems development and engineering to achieve their function. ISO-26262 "Road vehicles - Functional Safety" provides appropriate standardized requirements, processes and an automotive-specific risk-based approach to determine integrity levels, also known as Automotive Safety Integrity Levels or ASILs. ASILs are used to specify applicable requirements of the ISO-26262 standard so as to avoid unreasonable residual risk;

Smart integrated sensors, such as angular position sensors, are used extensively in automotive safety-critical applications. In essence, such smart components are relied upon as the building blocks of an ISO26262 compliant System. The functional and safety requirements allocated to these sensors (digital filtering, infield calibration/re-configurability, temperature drift compensation, self-diagnostics, multiple operating modes) demand a mixed-signal (analog and digital) and software intensive implementation in sub-micron CMOS technologies.

These sensors, being complex safety-relevant elements for which standard hardware part qualifications is not sufficient, needs to be developed in accordance with the assigned ASIL attribute of the target vehicle application.

The ASIL level represents the needed rigor to develop the safety requirements allocated to the sensor (on a scale ranging from ASIL-A to ASIL-D for the most critical applications) and is inherited from the corresponding safety goal at the vehicle level.

SAFETY CONCEPT DEVELOPMENT

The main safety-related activities from which a novel safety concept emerged are reported here.

The first activity in the adopted workflow is the specification of the product safety requirements.

As second activity, a system-level FMEDA[2] of the previous generation of the product was carried through. It represented a gap analysis in this context. The FMEDA allowed understanding the weakest parts from the safety metrics viewpoint.

The third activity ended on a coherent and complete set of safety requirements allocated to the product sub-systems and components. To reach this, the FMEDA and the technical safety concept were elaborated, designed and reviewed.

Specifications of the Product Safety Requirements

In a purely top-down driven development, the safety requirements will be cascaded down from the safety goals at the vehicle level by the OEM and Tier-1. However for out-of-context sensor development, the safety requirements are to be assumed. First, an hypothetical application has to be postulated by sounding the market needs, framing the operational context of the sensor. Once this context is clear, product requirements can be baselined. It is only later that these assumptions on the customer needs are validated by the item integrator at the vehicle level.

The first set of requirements concerns the sensor's function(s) or the "mission(s)": "The device shall provide an angle with an overall error which is within the safety margin of the magnetic angle. Quantitative requirement: Assumed safety margin: $\pm 3\text{deg.}$ "

For components such as sensor with just a single output and a single transfer function, the safety requirements are naturally tightly coupled to the sensor function. Often the safety margin does not need to be as tight as the performance specifications ($\pm 1\text{deg.}$ in this specific example) though. The margin can be exploited to either improve the hardware metrics (fault coverage) or to ease their estimation. Again, in an out-of-context development, the safety margin is an assumption to be validated by the end user. Too large, it will not satisfy the safety concept, too small (e.g. 1:1 with respect to the performance specifications), it might lead to complex safety analysis (because even the second-order correction functions of the sensing chain should then be included in full) [1].

For generic sensors, the product and its functions are often configurable end-of-line. There are then several mission-related safety requirements, calling for a set of related analyses, one for each main configuration. The various configurations can be treated as variants based on the default configuration.

The second and last set of requirements concerns the safe states and indirectly the requirements on the failure reporting mechanisms, that is: the behavior of the sensor output(s) in case of detected failures. This aspect is usually not well documented in legacy and non-safety related products and is a major focus of the system design of a safety-related elements.

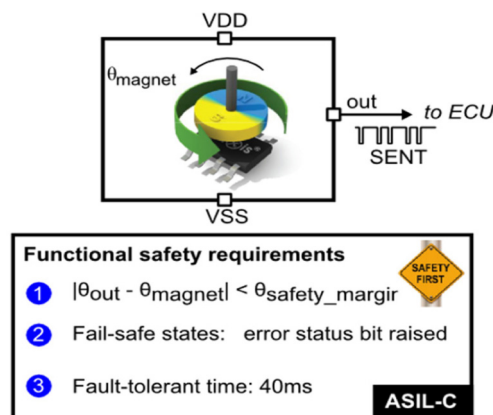


Figure 1. Position Sensor top safety requirements.

Safety Requirement Derivations

The safety goal must be translated in technical safety requirements allocated to the sensor - the responsibility of the OEM and Tier-1. Similarly, the sensor top safety requirements are translated to safety requirements allocated to the sensor's components. This hold for both the mission-related and the diagnostic-related requirements. For instance the magnetic position sensor contains an A/D Converter. The accuracy requirements of the A/D converter shall be derived from the mission-related safety requirements.

FMEDA of the Preliminary and Final Technical Concept

We opted for a refinement of the technical concept of the previous generation (ASIL-QM) product developed before the emergence of the ISO-26262 standard. The FMEDA analysis of this preliminary concept has shown that the residual failures were fairly equally distributed among the sensor's components and that the architectural metrics were more consistent with ASIL-A requirements, especially given the much shorter fault tolerant time interval targeted for the new generation. In line with the assumed ASIL-C requirement for this new development, the challenge was to cover at least 97% of the failures of all the components within a detection time interval of 40ms.

The sensor components are: Hall elements (magnetic transducer), Signal conditioning and acquisition circuits, CPU-based DSP with non-volatile memory and an embodiment of the communication protocol SENT (SAE-J2716), forming altogether a unique signal path. They are supported by a supply system, and an RC-oscillator. Diagnostics are in place too (e.g. A/D converter test points, watchdog, memory BIST).

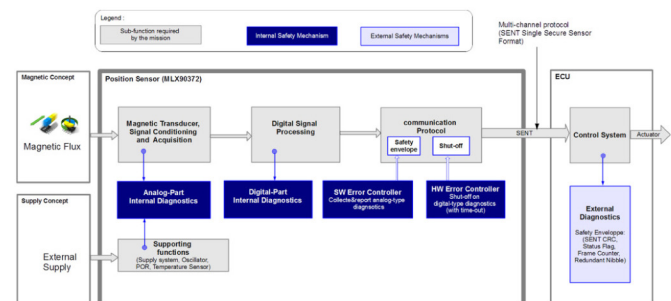


Figure 2. Position Sensor Safety Concept Blockdiagram

The FMEDA highlighted the need for new sub-function-specific diagnostics. A plausibility check based on the symmetry of the hall elements switching circuitry was added. A sequence of test points (test patterns) was added, in the background, to cover the full analog amplification chain. An in-depth FMEDA was executed at the level of the CPU-based DSP and in the context of the sensor, ie. with the sensor's embedded software running on the CPU. The metrics, which were confirmed by fault simulations in the gate-level netlist, are as expected better when the DSP/CPU mission is known compared to generic off-the-shelf micro-controllers, for which the safeness of many sub-blocks is low. Yet parity bits were added to the read-only memory and to the volatile memory. CPU Tests in software were added too to cover the remaining weaknesses mostly in the arithmetic unit. The SW flow control was extended to monitor the micro-processor.