www.ams.com

Technical Article

ISO26262: ams deploys unique technology to meet every new safety requirement

Roland Einspieler

ISO26262: ams deploys unique technology to meet every new safety requirement

Roland Einspieler

As electronic devices become more complex, they have more functions that can fail. In safety-critical automotive, industrial and medical applications, functional failures can, in the worst case, cause harm or even death to users.

This growing exposure to safety risks in vehicles led, at the start of 2012, to the introduction of the new ISO26262 (Road vehicles – functional safety standard), which applies to all electric and electronic systems in road vehicles up to 3.5t in weight. The standard applies not only to vehicle OEMs but also to component suppliers.

This article shows how ams implements the requirements of ISO26262 in its latest automotive contactless position sensors. It also shows how ams is implementing general safety features in its position sensors to make applications in automotive, industrial and medical applications much safer and fit for the future.

The requirements of ISO26262

Figure 1 shows the safety lifecycle laid down by ISO26262, with its ten defined points. This lifecycle corresponds exactly to the phases of automobile development and production.

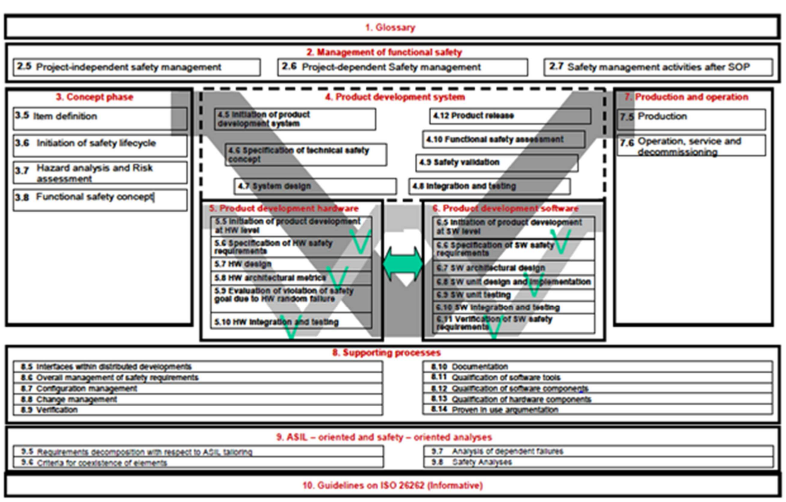

Fig. 1: model of the safety lifecycle laid down in ISO26262

Normally, every new application has an Automotive Safety Integrity Level (ASIL), graded from A to D. This ASIL reflects the safety risk to which the application exposes the road user. In an application with ASIL D (high risk), the safety requirements are much more onerous than for an ASIL A application.

The grading applied to an application is the result of exhaustive hazard analysis and risk assessment, a process which is defined by ISO26262 (see Figure 2).

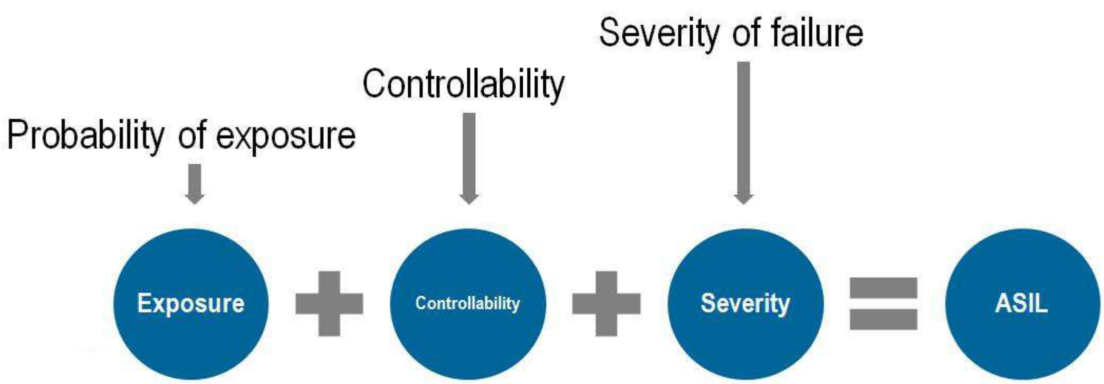

Fig. 2: the factors determining the ASIL grade applied to an automotive application under the provisions of ISO26262 [1]

How safety requirements follow from the ASIL grading

The functional safety requirements are determined by the nature of the application – for instance, a functional safety requirement of a braking system is that it must always respond to pressure from the driver's foot on the brake pedal.

The technical safety requirements are derived from the functional safety requirements. The technical safety requirement describes how to implement the functional safety concept – the nature of this description is defined in parts 4-6 of ISO26262. For instance, in a braking system a technical safety concept will describe the method by which pressure from the driver's foot on the pedal actuates the brakes. From the technical safety concept, hardware and software safety requirements may be defined.

As Figure 3 shows, in general the OEM creates the functional safety concept, and a supplier implements it with the most appropriate design.

Fig. 3: the component supplier is normally responsible for ensuring the technical safety requirements for any given function [2]

It is clear from this short introduction to ISO26262 that a completely new safety process flow has to be created for each application. This means that, for a component that is specific to a single application, the component supplier has to implement only one process flow.

The challenge is much greater when it comes to electronic parts that can be used in multiple applications, such as standard sensors manufactured by ams, since a separate process flow is required for each application in which the sensor may be used.

How standard ams sensors fulfil the requirements of ISO26262

Every new standard sensor from ams is now developed in accordance with the process defined in ISO26262. In addition, the aim of ams is for every part to meet the target ASIL grading for every application in which a customer might use it. This means that ams carries out a different safety analysis for each potential application, using the ASIL grading provided by the customer for the application.

As part of its ISO26262 development flow, ams carries out a Failure Mode, Effects and Diagnostic Analysis (FMEDA) for each application in which a device may be used (see Figure 4). FMEDA is an extension of the previous concept of a failure mode and effects analysis, which establishes a device's critical failure mode.

The results of the FMEDA are affected by the safety requirements set by the customer for each application. In other words, this FMEDA will be done for each position sensor and for each application in which the sensor might be used.

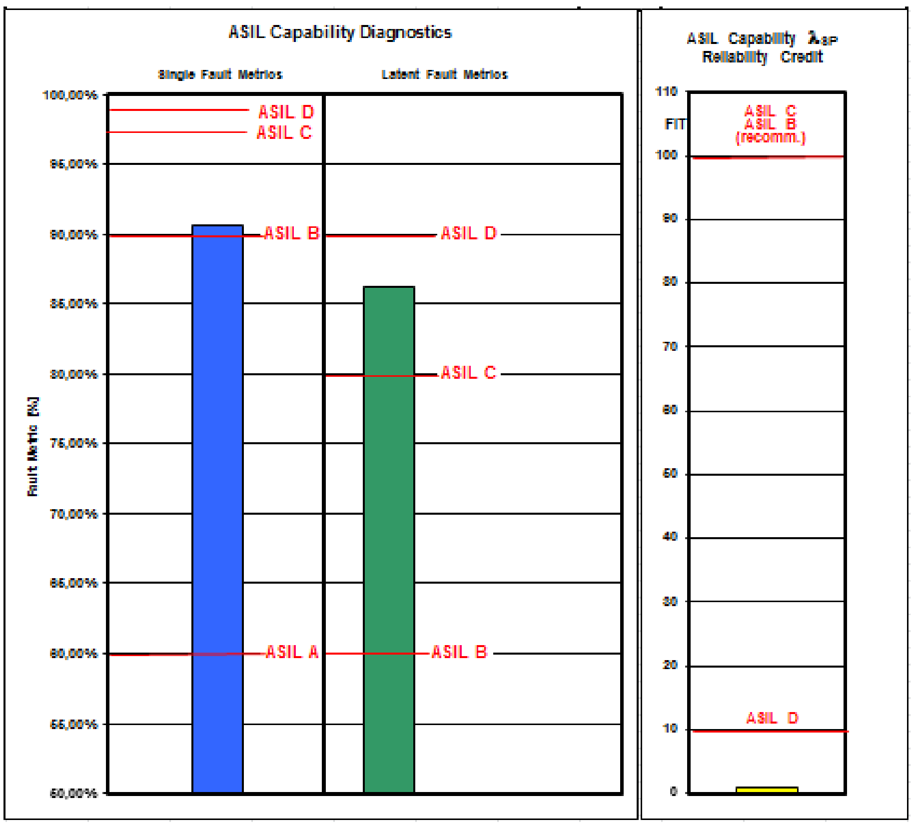

Fig. 4: FMEDA process flow.

Figure 4 shows the outcome of an ams FMEDA. For each application, ams calculates the single fault metric, the latent fault metric and the FIT (Failure In Time) rate.

In addition to the FMEDA, a safety tree is also used as an analysis tool. The safety tree shows all possible errors in a system and the reasons for these errors. An important concept for customers, the safety tree makes it easier to perform safety analyses correctly and to calculate an ASIL grade. Figure 5 shows the concept of the FTA (Failure Tree Analysis).

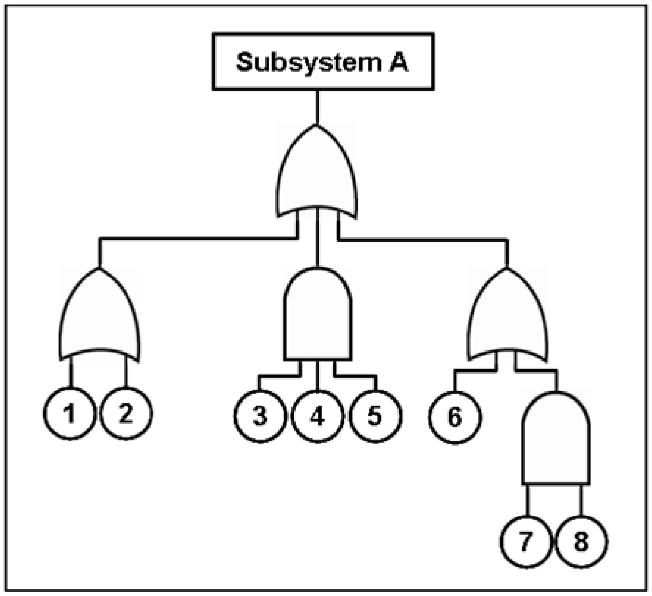

Fig. 5: the concept of the safety tree

The process of analysing the safety performance of an ams sensor does not stop here: ams also supplies to customers a FIT rate calculation for each sensor. The FIT rate measures the average number of occurrences of failure in a device over 109 hours of operation (equivalent to 114,000 years). 1 FIT = 1 error in 109h. This calculation varies with changes in the operating temperature of the device.

Designing hardware devices for safe operation

Some years ago, before the automotive parts industry was required to follow the stringent rules of ISO26262, ams had already started to implement unique techniques for ensuring the safe operation of all its magnetic sensors. These techniques are extremely effective in the safety-critical applications found in automotive, industrial and medical end products.

Depending on the ASIL requirements of the customer, ams has can offer either a single-die device or a redundant (dual-die) package.

The latest generation of Hall-effect position sensors from ams also incorporates new ‘3D’ technology: the sensors can measure displacement in the x, y and z axes. This technology is particularly useful for OEMs that must achieve compliance with ISO26262.

This is because the 3D sensors from ams can reach ASIL B or ASIL C (depending on the application and the safety requirements of the customer) with a single die. An internal safety tree in these 3D devices checks the device for every possible internal error every time it is started up. While competing contactless position sensors must use dual dice, the single-die device from ams offers considerable cost and system-design advantages.

In the most safety-critical applications, such as the pedals, a dual-die solution is mandatory. Two sensors and two power supplies work in parallel, and a microcontroller compares the two outputs. If there is a discrepancy, the microcontroller detects an error.

ams has developed stacked-die technology to meet this requirement, in which the two independent sensors are stacked in a single package .This ensures that both dies occupy the same magnetic field position, and so will generate the same measurement outputs when operating correctly.

Fig. 6: stacked dice in a single package

Most important errors and detection methods

Immunity against magnetic stray fields

If a magnetic position sensor is placed close to an external magnetic field source, this magnetic field is influencing the output of the sensor. Strong magnetic fields can be found, for instance, in brushless DC motors.

The contactless Hall-effect position sensors made by ams are suitable for use even in the presence of these very strong external magnetic fields. Patented ams technology enables its sensors to work correctly in magnetic fields up to 25,000A/m without requiring any external shielding (see Figure 7).

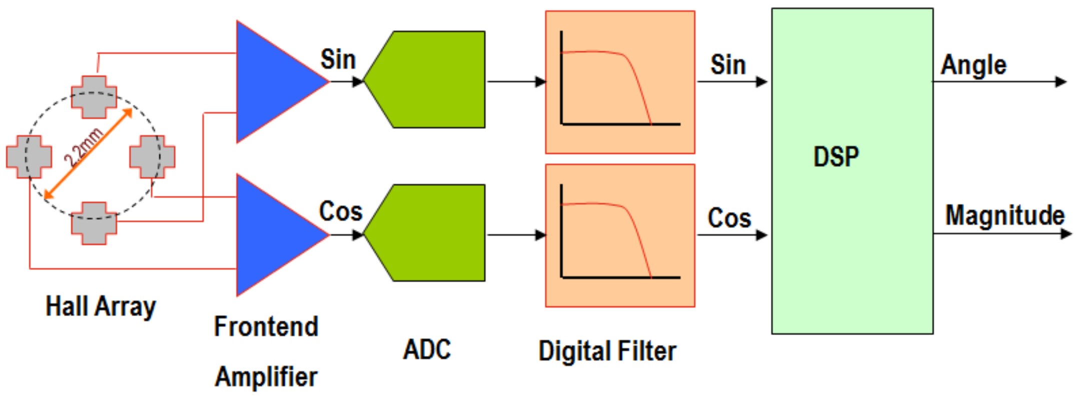

Fig. 7: patented ams technology ensures its contactless position sensors are immune to stray magnetic fields

System error checking

In automotive applications, it is mandatory for an electronic control unit (ECU) to detect every error in a sensor. If there is a broken GND or VDD signal, it is essential that the sensor sends a constant known value to the ECU.

All new position sensors from ams feature automatic detection of broken GND and broken VDD. If the supply or the GND in the application are broken, the sensor automatically enters a Safe mode. In this mode, the ECU can detect an error in the sensor application and trigger the appropriate safety procedure.

This detection feature works in all applications, in single-die and stacked-dice packages, and over a temperature range of -40°C to 150°C. It also operates in the special 4-wire configurations that are possible with dual-die devices, replacing the fully redundant 6-wire configuration required in single-die devices.

Missing magnet detection

Clearly a broken or missing magnet will disable a magnetic position sensor in any application; it is essential from the point of view of safety to detect this kind of error. In ams sensors, this can be detected by reading out the position of the magnet using the device's automatic gain control feature. If the value is too high, the sensor detects an error and enters a Safe mode.

Detection of a non-functioning device

The detection of a faulty sensor is very important, since it could be providing an output signal that shows the wrong position. All ams sensors provide a number of extended signals available in parallel, which can be correlated to check for consistency. These signals can be switched to test buses on the sensor to get information about the sensor's operating status. The information on the sensor's operating status can be read by a microcontroller, enabling the vehicle's control system to know if there is a problem.

Conclusion

Safety has long been one of the most important elements of the ams company philosophy. ams has therefore embraced the requirements of ISO26262, introducing additional production process flows and FMEDA into the development and production of its automotive position sensors.

As a result, ams is able to ensure that every automotive customer can use any position sensor in any application, knowing that it will be able to achieve the ASIL grading, and offer the safety functions, required.

For further information

ams AG
Tel: +43 (0) 3136 500
info@ams.com
www.ams.com