

Application Information

Functional Safety Challenges to the Automotive Supply Chain

By Lisa Clark, Functional Safety Manager, Allegro MicroSystems
and Scott Milne, Product Line Director – Linear and Angle Sensor ICs, Allegro MicroSystems

The electronic content in automobiles has increased steadily over the past few decades and shows no signs of slowing as many high-tech firms and OEMs race towards the development of fully autonomous vehicles. While the range of autonomy varies, from no control to full control, the vast majority of currently available vehicles contain systems with some degree of autonomy, such as electronic stability control (ESC) or lane centering. These electronic systems, which are intended to assist the driver, make an increasing number of decisions for the driver and often entirely remove the driver from the decision making process. These systems have generally increased driver and passenger safety, but can cause harm if they malfunction or have a design weakness. As a result, they pose new development challenges to the entire automotive supply chain.

In 2011, the International Standards Organization (ISO) published a functional safety standard called ISO 26262, outlining industry best practices for safety-related automotive system development. While the adoption of the standard is voluntary, most OEMs worldwide are requiring compliance from their suppliers. Suppliers that delay the adoption of this standard for themselves are likely to experience erosion in their future business opportunities.

The ISO 26262 standard contains requirements for both the development process and for the design of safety-related electronic systems in road vehicles. These requirements are based on a hazard and risk assessment of the system itself. The scope of the standard is limited to malfunctioning electrical or electronic systems. As a result, compliant systems must be able to identify their malfunctions and mitigate their effects such that passenger safety is preserved. For this reason, safety architectures now rely heavily on diagnostics and redundancy to detect malfunctioning system components and to transition the system to a safe state. In general, this requirement reaches IC component suppliers by requiring more content integrated into existing solutions and the capability of running diagnostics and communicating their status.

Take for example a system using a sensor IC as a simple switch. The system must be able to diagnose if the sensor output is in the correct state, because it is a safety-related function. Depending on the requirements and risk of the system, this can be accomplished in many ways. For example,

complex diagnostic circuits and communication protocols could be added to the sensor IC itself. Alternatively, a redundant sensor could be added at the system level—with no enhanced functionality or ability to communicate diagnostics in each single IC. A comparison of the redundant sensor outputs acts as a type of diagnostic protocol since, under safe operating conditions, the outputs of the two sensors should always match within a predefined error window. Both of these vastly different approaches meet system requirements, but have very different implications on both cost and availability of the right hardware (sensor component) to do the job. Component suppliers to the automotive market are now trying to understand and keep pace with the evolving requirements and trade-offs of these safety-related systems, and offer solutions that are easy for their customers to integrate.

Since the introduction of the ISO 26262 standard, the concept of what is considered “safe” has also evolved. In earlier architectures the loss of a system, for example a power steering system, was considered by many as a safe but nuisance occurrence. Categorizing system unavailability as “safe” had direct implications on the system architecture. The architecture would be required to identify any malfunctions that were considered unsafe and mitigate them, but those malfunctions that led to the loss of the power steering system did not require mitigation. This resulted in the need for only certain malfunctions to be identified and not others, thereby limiting the additional functionality required for safety, including on-chip diagnostics in IC components.

The perception of what is considered safe has since shifted as the industry realizes that the sudden loss of power steering can lead to an accident for smaller adults, inexperienced drivers, or the elderly. Automakers are now demanding when safety-related systems fail that they continue to operate to some degree. This “fail operational” or “fault tolerant” requirement has a direct impact on the architecture necessary to support it. The systems must include various levels of redundancy depending on whether the post-failure performance can be degraded from the nominal performance. “Fault tolerant” systems represent the next-generation of safety-related systems, and this topic will be addressed in the 2nd edition of the ISO 26262 standard.

The most direct result of fail operational systems is the use

of redundant system functions in an architecture that allows transition to a backup system if a malfunction occurs in the primary system. In response, IC component suppliers are beginning to offer double and triple die within a single package to support the need for redundancy without occupying more physical space. Offering multichip solutions is one example of how some IC suppliers are developing new technologies to meet specific needs of safety-related systems.

While there are custom developments between system providers and component suppliers, many system integrators use commercial off-the-shelf (COTS) components which have been developed out of a specific system context. The more understanding that the component suppliers have of these evolving system requirements, the better they are able to support them by defining a flexible product line which has the right features, is easy to integrate, and adds value to the system as a whole. It can be challenging to find the right level of flexibility to add to a product. Too much flexibility means that there may be features that are not used, but have a cost; not enough flexibility means that needed functionality must be incorporated by additional components that also have a cost. In general, functional safety has removed the defined boundary between a component and system; all system components must work together in order to meet the overall system requirements. Knowing how best to allocate needed functionality among system components can be considered something of an art, and suppliers are doing their best to understand and adapt. The trend of increased functionality within a reduced footprint is leading some IC suppliers to integrate two completely different functions into a single component, thereby offering a more comprehensive solution to their customers.

Looking forward, the scope of the 2nd edition of the ISO 26262 standard will be extended to include trucks, buses, and motorcycles, and the suppliers to those markets will also be drawn into the domain of functional safety. As the industry approaches the realization of autonomous vehicles, the suppliers of safety-related systems must develop systems that are at least as capable of driving as a human. These systems will rely on myriad sensing elements that interpret the surroundings. Development of these systems must not only focus on malfunctioning electronics—these systems must also be designed with enough acuity to respond safely in all driving situations. A new committee has been established within the ISO organization to address this topic (Safety of the Intended Function, or SOTIF) specifically and will have implications on the accuracy required from systems and their components.

Allegro MicroSystems, as the market leader in Hall-effect sensor ICs, has responded to these evolving challenges by becoming involved with the ISO 26262 technical committee, and by staying close to changes which will be introduced in the second edition. Allegro understands that safety has increased the criticality of clear communication and is working closely with customers to

understand and adapt to their changing needs. Allegro's partnerships with strategic customers facilitate information sharing regarding the future safety needs of various automotive systems. It is through this collaboration that the right types of components are developed to keep up with the changing requirements of safety-related systems.

Angle sensor ICs are one of several Allegro MicroSystems product portfolios that are designed for safety-critical applications. In addition to the advanced diagnostics designed into these devices, there are several additional features that make these parts stand out in the marketplace.

Allegro angle sensor ICs use a technology called Circular Vertical Hall (CVH), which provides a single channel output that responds to the phase of the detected magnetic signal, and is immune to variations in the magnitude of that magnetic signal. This offers several advantages:

1. Variations in the distance between the magnet and the IC (as a result of mechanical variation) have minimal impact on angle accuracy. Second generation ICs like the Allegro's A1335 also include an on-chip magnetic field scaling function, further reducing the impact of any change in magnetic field strength.
2. Large magnetic fields (up to 1500 G) can be used, minimizing the impact of small stray magnetic fields that may be present due to nearby motors, solenoids, or high current traces.
3. CVH technology enables low latency (as little as 10 μ s) and high refresh rates (as fast as 2 μ s), that are ideal for high-speed motor position detection.

The CVH ring is integrated with on-chip EEPROM and back-end digital signal processing that calculates and outputs the angle in a digital word, thereby minimizing system requirements on the ECU (i.e. doesn't require high accuracy ADC resources) and increasing noise immunity by processing all sensitive analog signals on-chip rather than being transmitted on the PCB or wire harness.

Second generation ICs like the A1335 also support multiple digital output protocols to meet the needs of various system designers. For applications like motor control that require very high data rates, these devices support a high-speed Serial Peripheral Interface (SPI) protocol with up to 10 MHz clock rates. For lower speed applications, these devices also support single wire PWM and SENT interfaces to help minimize wire harness cost and weight.

Allegro offers angle sensor ICs designed for both end-of-shaft and side-shaft magnetic configurations. The ability to support side-shaft magnetic configurations can greatly simplify the mechanical design of a system, as the end of the shaft is not always readily accessible. Side-shaft applications are challenging for most angle sensors due to the large mismatch in the magnitude of the tangential versus radial magnetic field.

Allegro's A1335 includes both on-chip harmonic linearization and segmented linearization to calibrate out the error due to this mismatch, enabling high accuracy (less than 1°) depending on the number of harmonics or segments used in the linearization scheme.

In addition to providing advanced diagnostics like Logic Built-In Self-Test (L-BIST), Allegro's angle sensor ICs are typically offered in both single and dual die configurations. The redundancy provided in the dual die configurations helps designers meet stringent functional safety requirements without sacrificing system availability due to potentially mismatched angle measurements from sensors using different technologies. These devices

are packaged in low-profile (1 mm thick) surface-mount TSSOP packages for ease of assembly and increased reliability.

The requirements for automotive safety-related systems will continue to evolve and expand. Suppliers for these systems must be actively aware of new trends and must have a corporate infrastructure which allows them to fluidly adapt their product lines accordingly. Proactively investing in new technologies or product innovation to better serve the automotive safety market will be a strategic activity with wide-ranging effects on market share for suppliers at all levels. Put on your seatbelt, suppliers—it's going to be a wild ride.

Revision History

Number	Date	Description
–	November 17, 2016	Initial release
1	September 12, 2018	Minor editorial updates
2	September 17, 2019	Minor editorial updates

Originally published in Electronic Engineering & Product World in China, October 2016. Reprinted with permission.

Copyright 2019, Allegro MicroSystems.

The information contained in this document does not constitute any representation, warranty, assurance, guaranty, or inducement by Allegro to the customer with respect to the subject matter of this document. The information being provided does not guarantee that a process based on this information will be reliable, or that Allegro has explored all of the possible failure modes. It is the customer's responsibility to do sufficient qualification testing of the final product to ensure that it is reliable and meets all design requirements.

For the latest version of this document, visit our website:

www.allegromicro.com