C2000™ MCU SafeTI™ control solutions:

An introduction to ASIL decomposition and SIL synthesis

Jitin George
Product Marketing Engineer
C2000 Microcontrollers
Texas Instruments

Introduction

Functional safety is becoming a more mainstream requirement as automotive and industrial systems continue to increase in complexity. An Automotive Safety Integrity Level (ASIL)-decomposed (or SIL-synthesized) architecture offers a reliable and robust path to achieving the highest levels of diagnostic coverage and gives end-equipment designers increased flexibility when developing safety-critical systems with high ASIL or SIL requirements.

An important safety-critical consideration for systems that target a high ASIL or SIL is that single-point failures should not lead to a complete loss of the safety function. By leveraging a decomposed or synthesized architecture, dual-channel systems can provide true fail-operational or limp-mode capability, in addition to meeting the highest ASIL or SIL targets.

This white paper provides insight into the historical use of a dual-channel approach to achieve functional safety, and explores the concept of ASIL decomposition and SIL synthesis, along with the benefits of using such architectures to achieve the highest levels of diagnostic coverage.

History of the dual-channel approach to functional safety

The history of functional safety in the context of electronic systems is derived from the need to safely operate machines that have the potential to cause injury or property damage. Functional safety standards were first established for applications like machinery or aviation because of the potential impact that could result from a safety-related failure. In such systems, a dual or multichannel approach to functional safety was effective in providing the highest probability of diagnostic coverage to help detect or prevent random hardware failures.

Machinery applications typically use integrated drive-based safety functions to reduce the risk of physical injury that could result from a malfunction in the machine's control. Triggering safe-torque-off (STO) safety functions de-energizes the power stage and subsequently removes the torque from the motor upon the occurrence of a credible fault.

The International Organization for Standardization (ISO) 13849 requires that machinery-related safety functions such as STO comply with a category 3 or category 4 type of topology. These are the most stringent levels of the standard. The requirements for categories 3 and 4 per ISO 13849 mandate the use of a dual-channel architecture to help guarantee the safety of related functions with a high certainty when dangerous faults occur. **Figure 1** shows the resulting functional safety circuit for a dual-channel implementation of the STO function.

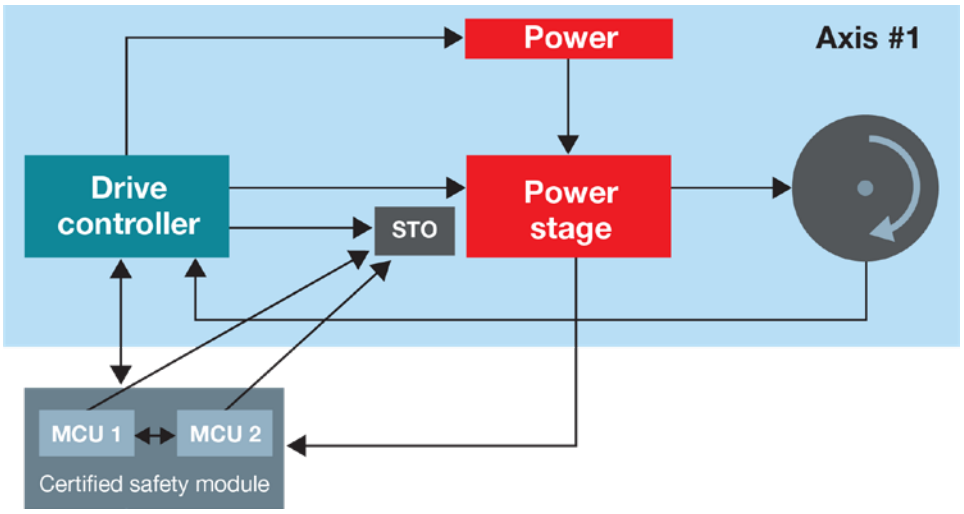

Figure 1. *Dual-channel implementation of an STO function.*

The certified safety module block shown in **Figure 1** monitors the main drive controller and motion system and issues an STO signal upon detection of a defined fault. This STO signal can come from either of the two microcontrollers (MCUs) in the event of failure. These MCUs are in constant communication about machine health and the motion system. At any instant, at least one of the MCUs will have the ability to issue an STO.

This approach is used to implement advanced STO topologies like safe limited speed (SLS), safe limited position (SLP) and safe speed range (SSR) to help bring the motor and motion equipment to a pre-determined safe state when such faults are detected. The independence of the safety module from the main system controller enables higher levels of diagnostic coverage. Consequently, STO topologies must be designed to help avoid common cause failures such as interruption of the power and clock sources.

Dual-channel architectures have been used in industrial functional safety applications that must comply with International Electrotechnical Commission (IEC) 61508 SIL 3 or ISO 13849 PLd and PLe (category 3 or category 4)-rated systems.

In the next sections, I'll explore more specifically the concept of ASIL decomposition and SIL synthesis in the context of automotive and industrial applications, respectively, and the associated constructs that the latest IEC/ISO standards have established.

ASIL decomposition according to ISO 26262

The ISO 26262 standard was originally published in 2011 to help address the functional safety of electrical and electronic systems in series-production road vehicles. This standard uses a risk classification scheme called Automotive Safety Integrity Levels (ASILs) that express the capability of a safety-related function. The four ASILs identified by the standard are ASIL A, ASIL B, ASIL C and ASIL D, with ASIL A dictating the lowest capability and ASIL D being the most stringent.

Electric power steering, airbag deployment and antilock braking systems are some of the traditional examples of ASIL D-rated applications in the automotive space. As automobiles continue to evolve and incorporate complex electrical/electronic/programmable electronic (E/E/PE) dominated systems, the number of applications that

require higher performance levels and the highest levels of diagnostic coverage continue to expand. ASIL D-rated applications have the potential to benefit from an ASIL-decomposed architecture that gives end-equipment designers increased flexibility when developing safety-critical systems with high ASIL requirements.

According to the second edition of ISO 26262-1:2018, the definition of ASIL decomposition is "Apportioning of redundant safety requirements to elements, with sufficient independence, for the same safety goal. The objective being reducing the ASIL of the redundant safety requirements that are allocated to the corresponding elements[1]." ("Elements" as defined in the ISO 26262 standard are system components [hardware or software]; hardware parts or software units.)

For ASIL D-rated systems that demand the highest levels of diagnostic coverage, it becomes very important to ensure that a single system fault does not lead to a complete catastrophic loss of a function. Decomposed architectures help achieve this goal and can be a critical design option when developing such systems.

Table 1 shows the allowable ASIL decomposition combinations according to ISO 26262-9:2018(E). In the right column, the ASIL level in bold and parenthesis is the parent safety integrity level before decomposition.

ASIL before decomposition	ASIL after decomposition
ASIL D	ASIL D(**D**) + ASIL quality management (QM) (**D**) or ASIL C(**D**) + ASIL A(**D**) or ASIL B(**D**) + ASIL B(**D**)
ASIL C	ASIL C(**C**) + ASIL QM(**C**) or ASIL B(**C**) + ASIL A(**C**)
ASIL B	ASIL B(**B**) + ASIL QM(**B**) or ASIL A(**B**) + ASIL A(**B**)
ASIL A	ASIL A(**A**) + ASIL QM(**A**)

Table 1. *ISO 26262 recommended rules that govern ASIL decomposition.*

To provide a simple example that illustrates how to use ASIL decomposition, the next section looks at how a typical electronic steering lock system with an ASIL D functional safety requirement can be decomposed into ASIL B (in support of D) + ASIL B (in support of D)[2].

ASIL decomposition example – electronic steering lock

A steering lock is a bolt driven into the steering column when the steering wheel is completely turned or when the vehicle is locked. The main purpose of a steering lock is to prevent unauthorized operation and serves as an antitheft device.

The functional safety goal of a steering lock is that it shall not engage unintentionally while the vehicle is being driven. The consequences of the steering lock engaging unintentionally could be catastrophic; therefore, this function is rated ASIL D. **Figure 2** shows a preliminary architecture where a body control module (BCM) communicates over the Controller Area Network (CAN) bus with the MCU, which in turn drives an actuator through a bridge driver to drive the bolt into the steering column and lock it.

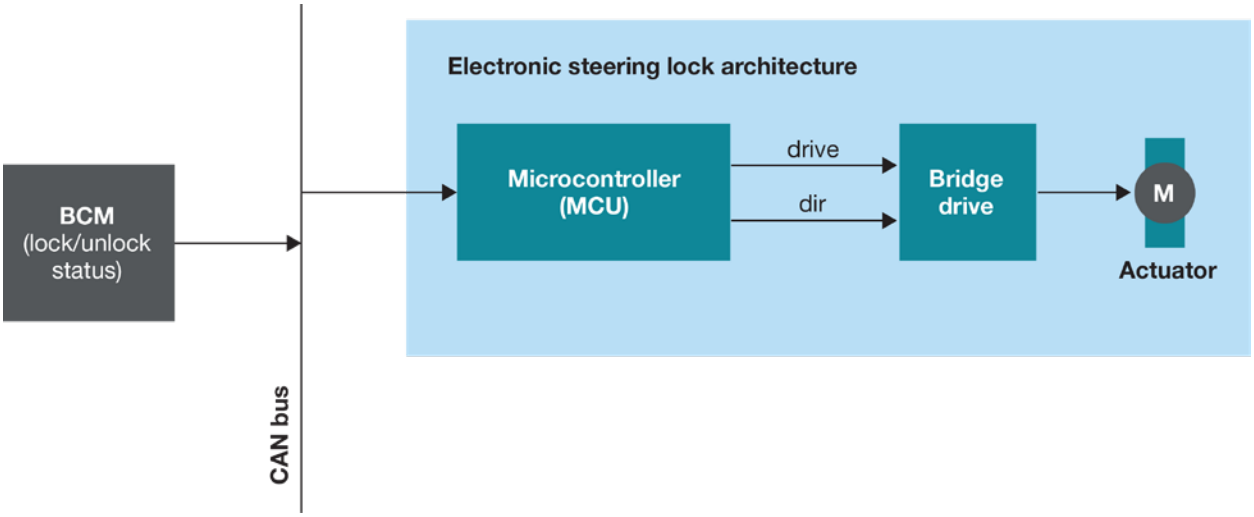

Figure 2. *Preliminary architecture of an electronic steering lock.*

This is a single-channel architecture and requires an MCU to drive an H-bridge to meet the random hardware metrics of ASIL D. Constraints on the design could force the use of an MCU that is not rated to ASIL D. Even if the MCU met the ASIL D metrics, a single MCU that communicates with the BCM could still have a communication failure that leads to engaging the steering lock while the vehicle is in motion. This can be addressed by decomposing this requirement.

To appreciate the correct way to use ASIL decomposition, let's briefly review an incorrectly decomposed implementation.

In the flawed architecture shown in **Figure 3**, the BCM sends a command to either lock or unlock the steering column. There is an additional antilock braking system/electronic skid protection module (ABS/ESP) that communicates the vehicle's speed over CAN. The primary MCU is responsible for driving the actuator operating the bolt into the steering column. The secondary MCU is responsible for enabling the H-bridge only if the vehicle is at rest. However, as you can see from **Figure 3**, the secondary MCU is receiving the vehicle speed information through the primary MCU; there is no independent connection to the vehicle's CAN bus. Consequently, a common cause failure on the primary MCU could result in incorrect vehicle speed information being transmitted to the secondary MCU. This could lead to the probability of violation of the system safety goal (PVSG).

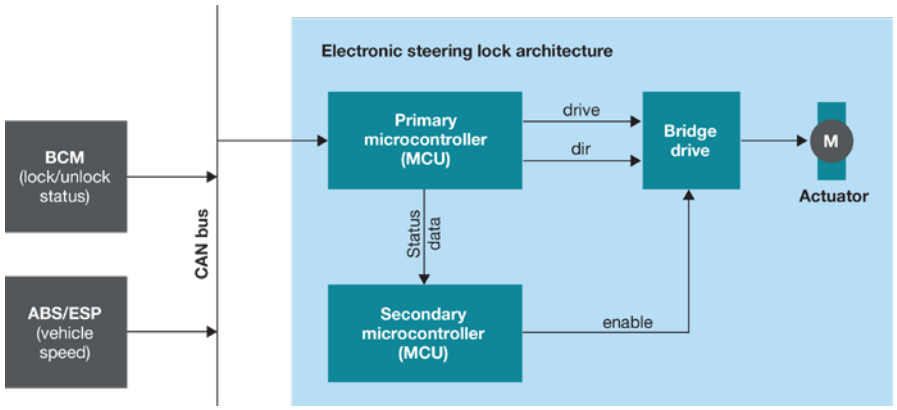

Figure 3. *Flawed attempt at ASIL decomposition for an electronic steering lock.*

Figure 4 illustrates a better method of decomposing the steering lock example. Using two independent CAN buses helps avoid common cause failures. The BCM module uses the body CAN bus to send lock/unlock commands to the primary MCU. The ABS/ESP module uses the chassis CAN bus to communicate with the secondary MCU, which will enable the H-bridge only when the vehicle is stopped.

In addition to being a more robust way to achieve the safety goal, this ASIL-decomposed architecture also enables the use of two ASIL B MCUs (as governed by the ASIL decomposition rules in ISO 26262) to implement an ASIL D function.

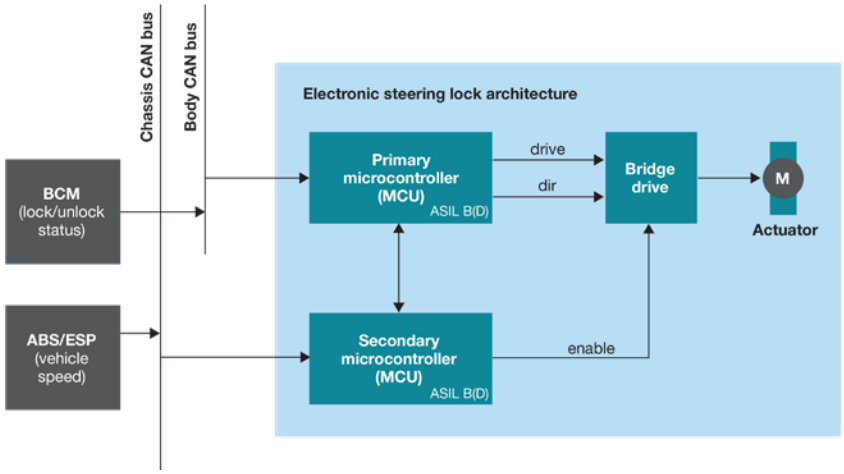

Figure 4. *Correct use of ASIL decomposition for an electronic steering lock.*

Applicability to IEC 61508 – SIL synthesis

IEC 61508 has a similar construct called SIL synthesis[3]. SIL synthesis essentially allows the synthesis (or combining) of two redundant elements with a systematic capability of N to have a systematic capability of N + 1, as long as N is less than or equal to SIL 3. The rules that govern SIL synthesis according to IEC 61508 are:

- SIL 2 + SIL 2 → SIL 3.
- SIL 1 + SIL 1 → SIL 2.

The IEC 61508 standard does not allow recursive (or multilevel) SIL synthesis. For example, SIL synthesis (according to IEC 61508) does not permit either of the following:

- SIL 2 (in support of **SIL 3**) + [SIL 1 (in support of **SIL 2**) + SIL 1 (in support of **SIL 2**)] → SIL 3.
- SIL 2 (in support of **SIL 3**) + SIL 1 (in support of **SIL 3**) → SIL 3.

In contrast, ISO 26262 does allow multilevel decomposition.

IEC 61508 also mandates a two-channel implementation for SIL 4 systems (the hardware fault tolerance has to be >0 for a SIL 4 function). Otherwise, ASIL decomposition and SIL synthesis are equivalent constructs in the ISO 26262 and IEC 61508 standards, respectively.

Benefits of ASIL decomposition or SIL synthesis

An ASIL-decomposed or SIL-synthesized architecture offers a more reliable and robust path to achieve the highest levels of diagnostic coverage through these advantages:

- It's possible to use existing components like an ASIL B or ASIL QM MCU to implement a higher ASIL D system.
- It's possible to deploy a complex or legacy software codebase on an ASIL QM MCU while programming an ASIL D safety MCU to implement lower-complexity (lower development effort) supervisory functions. An example would be an electric vehicle (EV) traction inverter/motor control running on an ASIL QM MCU and a safety supervisor MCU that can de-energize the complex-control MCU in the event of a fault.
- By implementing a decomposed or synthesized architecture as dual channels, there is the added possibility of achieving a true fail-operational limp-mode capability that the system could rely on until the completion of appropriate repairs or system recovery. By contrast, an architecture implemented on a single device would only have the ability to de-energize as a safe-state response in the event of a catastrophic failure such as a loss of power.

An added benefit of an ASIL-decomposed dual-channel architecture is the flexibility to choose MCUs based on inherent strengths so that system integrators do not have to sacrifice their system performance goals. For example, the acceleration performance of an EV traction motor or efficiency of a DC/DC converter does not have to be compromised by the limited pulse-width modulation (PWM) performance of a general-purpose ASIL D MCU.

Instead, the system may be architected to take advantage of an optimized C2000 real-time-control MCU, designed specifically to control complex, high performance control-loop functions in conjunction with a cost optimized ASIL D capable MCU, such as any part from TI's Hercules TMS570 Functional Safety MCU

family that addresses the requirements of the safety supervisor to achieve an ASIL D system. With the industry trending toward even higher performance expectations (such as the use of wide-bandgap field-effect transistors), the need for specialized control solutions is becoming even more pronounced. In similar fashion, the demand for housekeeping functions like cybersecurity or the ability to run an Open Systems and Their Interfaces for Electronics in Motor Vehicles (OSEK)-compliant operating system is also increasing in automotive systems, adding an additional burden on the housekeeping MCU. A dual-channel, ASIL-decomposed architecture enables the selection of MCUs for each of these functions (real-time control and safety/security functions) based on their respective strengths and also helps future-proof designs for further evolution on either vector. This means that as things continue to evolve, system integrators could address control functions or safety/security functions independently, without disrupting what they've already designed for the other.

Conclusion

ASIL decomposition and SIL synthesis are constructs outlined in ISO 26262 and IEC 61508, respectively. Their inclusion in those standards gives end-equipment designers flexibility to meet the highest levels of diagnostic coverage – also defined by those standards. Taking advantage of these principles enables the use of lower ASIL or SIL rated components while still meeting the needs of the highest ASIL or SIL systems.

Additionally, when decomposed elements are implemented as two completely independent channels, the system can be made robust against common cause failures like power and clock and even be designed to support true fail-operational limp-mode functionality.

Finally, ASIL decomposition or SIL synthesis also enables component choices to be made based on inherent strengths so that system integrators do not have to compromise their system performance goals.

Learn more about the technical advantages of the C2000 MCU portfolio for automotive and industrial applications.

References

1. ISO 26262-9:2018(E).
2. D.D. Ward and S.E. Crozier. "The uses and abuses of ASIL decomposition in ISO 26262." [Online]. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6464473. Accessed Dec. 1, 2018.
3. IEC 61508-2:2010.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265