electronic design
The Authority on Emerging Technologies for Design Solutions

Understanding ISO 26262 ASILs

Electronic Design

Chris Hobbs Patrick Lee
Chris Hobbs and Patrick Lee, QNX Software Systems

Tue, 2013-07-09 14:15

If the questions posted on the LinkedIn ISO 26262 Functional Safety Group are any indication, many people need to understand ISO 26262 Road vehicles – Functional safety, as well as the Automotive Safety Integrity Levels (ASILs) that the standard defines. However, it also appears that only a few specialists seem to understand how ASILs are determined and their implications for the design, building, and validation of safety-related electronic systems in automobiles.

ASILs Aren't SILs

ISO 26262 is an extension of IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC 61508 defines Safety Integrity Levels (SILs). ISO 26262 defines ASILs. It might seem that ASILs are like SILs and that anyone familiar with building a safety case for a system requiring certification to an IEC 61508 SIL should be able to transfer those methods to an ISO 26262 project.

Related Articles

- 10 Standards Organizations That Affect You (Whether You Know It Or Not)
- Automotive Safety Design Gears Up For 65-nm ARM Cortex MCU
- Automotive Communications Demand A Robust Infrastructure

Experience building an IEC 61508 safety case and gathering evidence for it will certainly be invaluable to anyone building the safety case for an ISO 26262 system. But unlike IEC 61508, ISO 26262 is "not a reliability standard."[1] It doesn't set precise numbers for acceptable probabilities of failure. ASILs are not determined in the same manner as IEC 61508 SILs.

When defining SILs, IEC 61508 considers the target failure measures for systems acting in low demand, high demand, or continuous mode. For example, a software component certified to continuous mode SIL 3 is required to have a probability of dangerous failure below 1 in 10 million per hour of operation. IEC 61508 SILs can thus be considered one-dimensional, in the sense that they involve only the probability of failure in the stated operating mode.

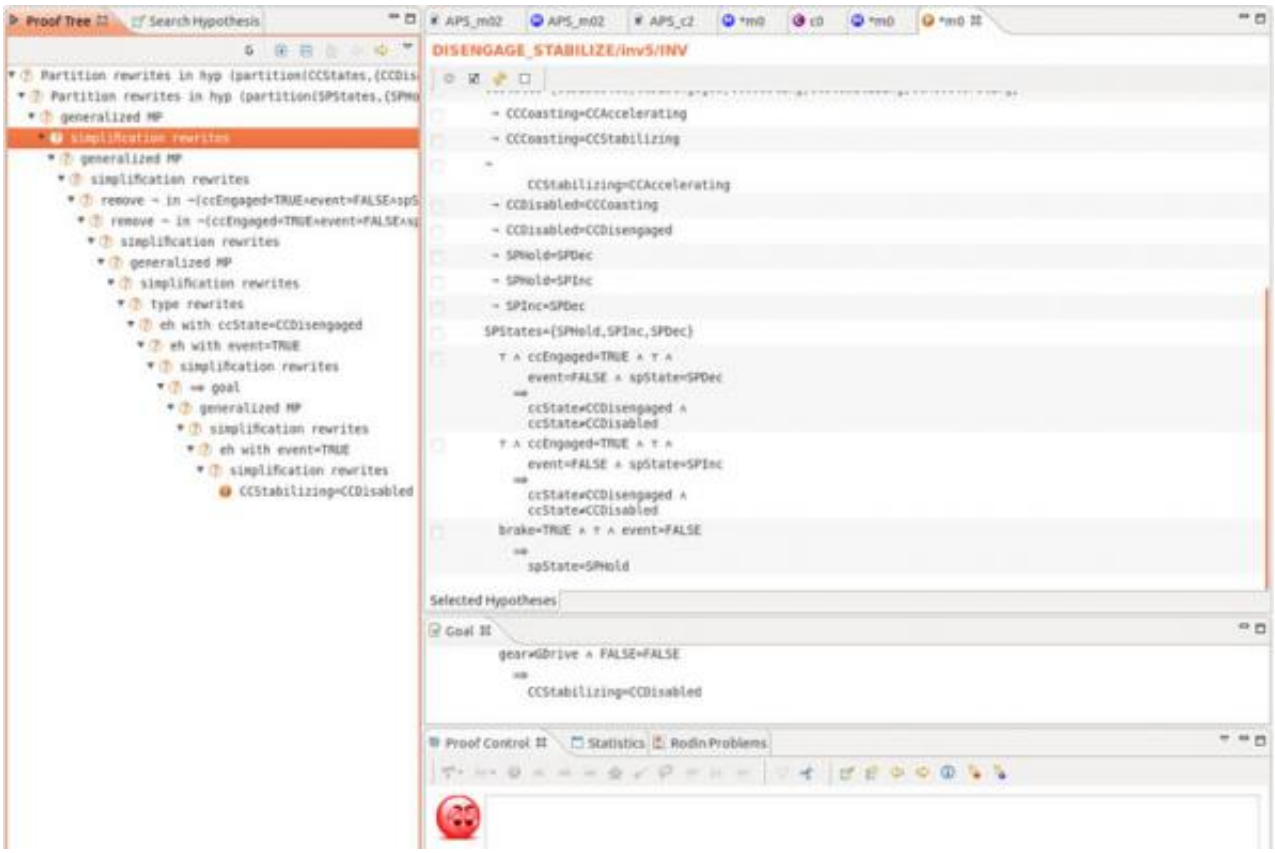
ASIL's, though, are three dimensional, involving three variables: severity, probability of exposure, and controllability. ISO 26262-3, section 7 "Hazard analysis and risk assessment" provides tables that break these three variables down into classes. Probability of exposure has five classes: "Incredible" to "High probability" (E0-E4). Severity has four classes: "No injuries" to "Life-threatening injuries (survival uncertain), fatal injuries" (S0-S3). Controllability, which means controllability by the driver, not by the vehicle electronic systems, has four classes: "Controllable in general" to "Difficult to control or uncontrollable."

A fourth table in this section of the standard shows how these variables must be combined to determine the required ASIL

for an electronic system, subsystem, or component in the vehicle. For example, a component that must be relied upon in a situation that has a medium probability of occurring (E3) and is considered normally controllable (C2) but can result in life-threatening injuries (S3) requires an ASIL of B.

This method for determining ASILs is quite different from the strict dependability (improbability of failure) targets prescribed by IEC 61508. Though ISO 26262 provides details and examples in Annex B of Part 3, determining an ASIL involves many factors that, even with the information in Annex B, require us to make many assumptions.

For instance, the severity classes presented in this annex use the Association for the Advancement of Automotive Medicine's Abbreviated Injury Scale (AIS), but the standard states "other categorizations such as Maximum AIS (MAIS) and Injury Severity Score (ISS) can be used."[2] Similarly, Annex B defines C2 controllability as "90% or more of all drivers or other traffic participants are usually able to avoid harm,"[3] and an E3 probability of exposure is defined as "1% to 10% of average operating time" *(Fig. 1)*.[4]



These definitions are informative, not prescriptive, and leave a great deal of discretion to whoever is building each component system and ultimately to the automaker and suppliers. For example, the phrase defining C2 controllability doesn't state 90% of which drivers, and it includes the word "usually."

We must decide what statistical sample we will use to determine whether 90% of drivers can usually avoid harm and decide whether "usually" means more than 50% of occurrences, more than 90% of occurrences, or something else altogether. Probability of exposure similarly depends on context and interpretation. The probability of exposure to black ice on a bridge is not the same in Florida as in Manitoba.

Further, the standard states that for the controllability and exposure classes, the difference in probability from one "class to the next is an order of magnitude."[5] It doesn't explicitly specify whether this order of magnitude is binary (x2) or decimal (x10). From the examples in Annex B, we can, however, deduce that it is decimal. For example, E1 is "< 1% of average operating time" and E2 is "1% to 10% of average operating time."[6]

ISO 26262: A Goal-Based Standard

Given the number of assumptions we have to make to determine an ASIL, it is not surprising that the Society for Automotive Safety Engineers (SAE) is drafting J2980 – Considerations for ISO26262 ASIL Hazard Classification to provide more explicit guidance for classifying the three dimensions of an ASIL. These guidelines should reduce the breath of possibilities when we make assumptions about severity, probability of exposure, and controllability, but they will not eliminate the need for such assumptions when we determine ASILs.

But if we step back and look at ISO 26262 as a whole, we note that the standard is about preventing harm:

Safety goals are top-level safety requirements … They lead to the functional safety requirements needed to avoid an unreasonable risk for each hazardous event. Safety goals are not expressed in terms of technological solutions, but in terms of functional objectives.[7]

Harm can come from such a large number of factors that, in practice, they cannot all be named and described—or even counted. Thus, building an ISO 26262 system so it does not cause unacceptable harm depends on a wide range of techniques. ASILs are only one part of the strategy, used to help us decide the required dependability of a component based on the risks and severity of the consequences associated with a failure.

IEC 61508 is a prescriptive standard for systems in high-value, low-volume implementations such as nuclear power plants and oil-drilling platforms. In contrast, ISO 26262 is a goal-based standard for relatively low-value but high-volume implementations. It is like other goal-based standards, which have been developed for specific contexts (medical device, train, automobile, etc.), rather than prescriptive standards, which are for a type of system (i.e., IEC 61508 for electronics), and its approach to expressing safety requirements is like that of other goal-based standards.

For example, in a manner analogous to ISO 26262, the IEC 62304 standard for medical devices identifies three classes of medical devices—A (no possible injury or damage to health), B (possibility of non-serious injury or harm), and C (possibility of serious injury or harm, or death)—and focuses on such things as the design, development and validation processes, and tools and techniques used to build the safety case. Both standards also discuss the use of systems or subsystems not developed for the safety-related system in which they will be used.

ASILs are more complex than the IEC 62304 medical device classes. But like these classes, they do not set dependability requirements. ASILs provide guidance to help us establish dependability requirements, based on the probability and acceptability of harm. In many cases we will need to set the numerical values for dependability ourselves, based on the information in ISO 26262 and methods such as ALARP (as low as reasonably practical), GAMAB (globalement au moins aussi bon: "globally at least as good"), or MEM (minimum endogenous mortality).[8]

In this light, the most productive way to respond to questions such as "What will be the ASIL of the driverless car?" may be to develop the standard further to include possibilities such as controllability being exercised by a non-human driver. As the standard reads now, the absence of a human driver means that controllability will always be close to zero, because ISO 26262 defines it as the "ability to avoid a specified harm or damage through the timely reactions of the persons involved,

possibly with support from external measures."[9]

Therefore, we will have to classify every safety-related component as an ASIL D. For the present, this will also be the answer for a more conventional car with human driver if we ask the same sort of question: for example, "What is the ASIL of assisted cruise control?" Until we understand all three dimensions of the ASIL, we cannot know the answer.

We must, therefore, begin by determining our systems' dependability requirements based on all three ASIL dimensions: the probability of exposure to harm should the system fail, the controllability of the situation upon exposure, and the severity of the resulting harm should the situation not be controlled.

Once we have understood these dimensions, assigning the ASIL is a simple matter of looking it up in the standard, Part 3, Table 4. We can then build our ISO 26262 safety case to demonstrate that our component meets our dependability claims, using all the relevant methods and evidence available to us: processes and quality management, formal design, code analysis, testing, proven-in-use data for component parts, and so on.

Finally, when we build the Safety Case, we must demonstrate not just that our system meets the dependability claims we make about it, but also that this dependability is acceptable for our selected ASIL and that our selected ASIL is appropriate for the system we have built.

References

1. William Taylor III et al., "System Safety and ISO 26262 Compliance for Automotive Lithium Ion Batteries," 2012 IEEE Symposium on Product Compliance Engineering, Portland, 5-7 Nov. 2012, www.psessymposium.org/sites/psessymposium.org/files/1569633449.pdf.

2. ISO 26262-3:2011, B.2.1.

3. Table B.4.

4. Table B.2.

5. 7.4.3.4 and 7.4.3.7.

6. Table B.2.

7. 7.4.4.3.

8. Chris Hobbs and Patrick Lee, "Define And State Your Safety Requirements Before Design And Test," *Electronic Design*, 9 Jan. 2012, electronicdesign.com/embedded/define-and-state-your-safety-requirements-design-and-test.

9. ISO 26262-1:2011, 1.19; Strictly, the absence of a driver does not reduce controllability zero because the standard allows passengers and persons outside the vehicle to be included in the determination of controllability.

10. Alma Juarez Dominguez, the University of Waterloo, "Detection of Feature Interactions in Automotive Active Safety Features," https://cs.uwaterloo.ca/~aljuarez/Docs/Thesis_Juarez_Alma.pdf.

Chris Hobbs *is an operating-system kernel developer at QNX Software Systems, specializing in "sufficiently available" software (software created with the minimum development effort to meet the availability and reliability needs of the customer) and in producing safe software (in conformance with IEC61508 SIL3). He is also a specialist in WBEM/CIM device, network, and service management and the author of* A Practical Approach to WBEM/CIM Management *(2004). His blog,* Software Musings, *focuses "primarily on software and analytical philosophy." He earned a BSc, honours, in pure mathematics and mathematical philosophy at the University of London's Queen Mary and Westfield College.*

Patrick Lee *is a member of the QNX Software Systems certification team, where he applies analysis techniques such as fault trees, Bayesian belief networks, formal model checking, and theorem proving to validate and improve the software design in QNX products for safety-critical markets. Before joining QNX, he worked in the development of avionics systems and software tooling for real-time embedded software developers at ECSI and at General Dynamics Canada. He has also worked as an embedded software developer at Nortel, Catena Networks, and Imagination Technologies. He holds a BSc, honours, in electrical and electronic engineering from Bath University and a post-graduate certificate in education from the University of Gloucestershire.*

Source URL: http://electronicdesign.com/embedded/understanding-iso-26262-asils