Automotive Safety Integrity Level

This article is a discussion of ASIL as a means of classifying hazards, particularly to provide a context for comparison with other methods of classifying hazards, risk, quality, or reliability. For a more thorough description of ASIL, methods of its assessment, and its roles within ISO 26262 processes, see ISO 26262 (Automotive Safety Integrity Level).

Automotive Safety Integrity Level (ASIL) is a risk classification scheme defined by the ISO 26262 - Functional Safety for Road Vehicles standard. This is an adaptation of the Safety Integrity Level used in IEC 61508 for the automotive industry. This classification helps defining the safety requirements necessary to be in line with the ISO 26262 standard. The ASIL is established by performing a risk analysis of a potential hazard by looking at the Severity, Exposure and Controllability of the vehicle operating scenario. The safety goal for that hazard in turn carries the ASIL requirements.

There are four ASILs identified by the standard: ASIL A, ASIL B, ASIL C, ASIL D. ASIL D dictates the highest integrity requirements on the product and ASIL A the lowest.[1] Hazards that are identified as QM do not dictate any safety requirements.

1 Hazard Analysis and Risk Assessment

Because of the reference to SIL and because the ASIL incorporate 4 levels of hazard with a 5th non-hazardous level, it is common in descriptions of ASIL to compare its levels to the SIL levels and DO-178C Design Assurance Levels, respectively.

The determination of ASIL is the result of *hazard analysis and risk assessment*.[2] In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system, as adjusted for relative likelihoods of the hazard manifesting those effects. That is, each hazard is assessed in terms of severity of possible injuries within the context how much of the time a vehicle is exposed to the possibility of the hazard happening as well as the relative likelihood that a typical driver can act to prevent the injury.[3]

In short, ASIL refers both to risk and to risk-dependent requirements (standard minimal risk treatment for a given risk). Whereas risk may be generally expressed as

$$\text{Risk} = (\text{accident the of case in loss expected}) \times (\text{occurring accident the of}$$

or

$$\text{Risk} = \text{Severity} \times (\text{Exposure} \times \text{Likelihood})$$
[4][5]

ASIL may be similarly expressed as

$$\text{ASIL} = \text{Severity} \times (\text{Exposure} \times \text{Controllability})$$ [6][7][8]

illustrating the role of Exposure and Controllability in establishing relative probability, which is combined with Severity to form an expression of risk.

2 Levels

The ASIL range from ASIL D, representing the highest degree of automotive hazard and highest degree of rigor applied in the assurance the resultant safety requirements, to QM, representing application with no automotive hazards and, therefore, no safety requirements to manage under the ISO 26262 safety processes. The intervening levels are simply a range of intermediate degrees of hazard and degrees of assurance required.

2.1 ASIL D

ASIL D, an abbreviation of *Automotive Safety Integrity Level D*, refers to the highest classification of initial hazard (injury risk) defined within ISO 26262 and to that standard's most stringent level of safety measures to apply for avoiding an unreasonable residual risk.[2] In particular, ASIL D represents likely potential for severely life-threatening or fatal injury in the event of a malfunction and requires the highest level of assurance that the dependent safety goals are sufficient and have been achieved.[2]

ASIL D is noteworthy, not only because of the elevated risk it represents and the exceptional rigor required in development, but because automotive electrical, electronic, and software suppliers make claims that their products have been certified or otherwise accredited to ASIL D,[9][10][11] ease development to ASIL D,[12] or are otherwise suitable to or supportive of development of

items to ASIL D.[13][14][15] Any product able to comply with ASIL D requirements would also comply with any lower level.

2.2 QM

Referring to "Quality Management", the level QM only means that there are no hazards associated with the given application, so management of safety requirements is not relevant. This is not to say that no controls are required in the development of the product. Even if there are no hazards, there may still be business risk and other risks to manage, and there may be other applicable customer and regulatory requirements for Quality Management.

3 Comparison with Other Hazard Level Standards

Given ASIL is a relatively recent development, discussions of ASIL often compare its levels to levels defined in other well established safety or quality management systems. In particular, the ASIL are compared to the SIL risk reduction levels defined in IEC 61508 and the Design Assurance Levels used in the context of DO-178C and DO-254. While there are some similarities, it is important to also understand the differences.

3.1 IEC 61508 (SIL)

ISO 26262 is an extension of IEC 61508.[2] IEC 61508 defines a widely referenced Safety Integrity Level (SIL) classification. Because of the pedigree and the commonality of the names, it is not uncommon in discussions of ISO 26262 to compare, if not equate to some degree, the new ASIL classifications with the established SIL classifications. While the two standards have similar processes for hazard assessment, ASIL and SIL are computed a different points. Where ASIL is a risk measurement, SIL is a probability or reliability measurement. In the context of IEC 61508, higher risk applications require greater reliability and lower probabilities of failure.

$$\text{failure of probability} < \frac{\text{Risk Tolerable}}{\text{Risk}}$$

That is, for a given Tolerable Risk, greater Risk requires more risk reduction, i.e., smaller value for probability of failure. For the reliability improvements for a continuous hazard, SIL 1 is associated with a failure rate limit of 10^{-5} per hour while SIL 4 is associated with a failure rate limit of 10^{-9}. In short, SIL represents reliability requirements, not risk, even if those reliability requirements derive from risk assessment.

In commercial publications, ASIL D is typically shown meeting or exceeding SIL 3 but is not compared with SIL 4; while ASIL A is compared with SIL 1.[16]

3.2 SAE ARP4761 and SAE ARP4754 (DAL)

While it its more common to compare the ISO 26262 Levels D though QM to the Design Assurance Levels (DAL) A through E and ascribe those levels to DO-178C; these DAL are actually defined and applied through the definitions of SAE ARP4761 and SAE ARP4754. Especially in terms of the management of hazards through a Safety Life Cycle, the scope of ISO 26262 is more comparable to the combined scope of SAE ARP4761 and SAE ARP4754. Functional Hazard Assessment (FHA) is defined in ARP4761 and the DAL are defined in ARP4754. DO-178C and DO-254 define the design assurance objects that must be accomplished for given DAL.

Unlike SIL, it is the case that both ASIL and DAL are statements measuring degree of hazard. DAL E is the ARP4754 equivalent of ASIL QM—in both classifications hazards are negligible and safety management is not required. At the other end, DAL A and ASIL D represent the highest levels of risk addressed by the respective standards. While ASIL D encompasses at most the hazards of a loaded passenger van, DAL A includes the hazards of large aircraft loaded with fuel and passengers. Publications may illustrate ASIL D as equivalent to DAL B, to DAL A, or somewhere in between.

4 Associated standards

- ISO 26262
- SAE J2980

5 See also

- ARP4761
- ARP4754
- DO-178C
- DO-254
- IEC 61508

6 References

[1] http://www.ni.com/white-paper/13647/en/#toc2 National Instruments White Paper on ISO 26262 functional safety standard

[2] *ISO 26262-3:2011(en) Road vehicles — Functional safety — Part 3: Concept phase*. International Standardization Organization.

[3] Hobbs, Chris; Lee, Patrick (July 9, 2013). *Understanding ISO 26262 ASILs*. *Electronic Design*. Embedded Technologies (Penton Electronics Group).

[4] Kinney, G. F.; Wiruth, A. D. (June 1976). *Practical Risk Analysis for Safety Management*. China Lake, California: Naval Weapons Center. The risk score for some potentially hazardous situation is given numerically as the product of three factors: ...

[5] Chris Van der Cruyssen, *Risk Assessment Guidelines (sheet 4, Kinney method)* (PDF), economie, Belgian Federal Government

[6] Steve Hartley, Ireri Ibarra, Gunwant Dhadyalla (2011), *Functional Safety & Diagnostics of Hybrid Vehicles ("Severity x Exposure x Controllability = ASIL")* (PDF), pp. sheet 8

[7] *Smart & Compact Battery Cell Management System for Fully Electrical Vehicles (Sheet 9)* (PDF), STMicroelectronics

[8] *Hercules™ Safety Microcontrollers - 1 Day Safety MCU Workshop (sheet 25)*, Texas Instruments, Texas Instruments, 2013

[9] "News Release: Freescale Qorivva Microcontroller is First Automotive MCU to Receive ISO 26262 Functional Safety Standard Certification". Freescale Semiconductor. September 6, 2012. Retrieved January 23, 2015.

[10] "Certified tools for functional safety ("Certified for software development up ... ASIL D …")". IAR Systems. Retrieved August 6, 2013.

[11] "Press Release: Vector is the first supplier to deliver an ASIL-D certified AUTOSAR operating system" (PDF). Vector. 2013-02-18. Retrieved August 6, 2013.

[12] "SafeTI™ Design Packages for Functional Safety Applications". Texas Instruments. Retrieved August 6, 2013.

[13] "Renesas Electronics Introduces 4th-Generation V850 Microcontrollers Series (… developed for applications with the highest functional safety requirements (ASIL D/SIL3))". Renesas Electronics. November 4, 2010. Retrieved August 6, 2013.

[14] "Microcontrollers foster ISO 26262 ASIL D-compliant system design.". THOMASNET. September 6, 2012. Retrieved August 6, 2013.

[15] *ARM® CortexTM-R4 Safety Microcontrollers (sheet 3)* (PDF), Vision Series Embedded, Arrow Electronics

[16] Frech, Marcus; Josef Mieslinger (2012). "Functional Safety Seminar & 1-Day HerculesTM Workshop". *Arrow Roadshow*. Arrow Roadshow: 63.

7 Text and image sources, contributors, and licenses

7.1 Text

- **Automotive Safety Integrity Level** *Source:* https://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level?oldid=686102271 *Contributors:* Trappist the monk, IveGoneAway, BattyBot, ChrisGualtieri, Stamptrader, Rk.prashan, WikiOriginal-9, Rapunzel1977 and Anonymous: 3

7.2 Images

7.3 Content license