ISO13849 and ISO26262 for the same Domain

Michael Kieviet, innotec GmbH

Abstract: The safety application standards ISO13849 and ISO26262 are designed for totally different applications. The ISO13849 focuses to reduce the risks and handle the hazards by coming from machines. The ISO26262 is applicable for active safety automotive systems. Normally the use of both standards in the same application is not very common. But in some special cases the standard can be used in parallel.

Very often designer and manufacture of electronic control elements for mobile machines are confused about the jungle of safety standards. A lot of standards could be applicable in a project. Sometimes it is necessary to use standards with the same focus depending from the mission or the local laws of using the system.
In case of applications like electrical mobile safety system it can appear, that more than one standard is applicable. Always, if a component will be designed for different kinds of vehicles, this situation happens. For instance: An inductive sensor including a CAN interface must be used as gear sensor in road vehicles or as a gear sensor in a mobile machine.

How to decide which standard is applicable.

Limitations of use the ISO26262 are very obvious and easy to decide.

1. The ISO26262 is only for cars with weight less than 3.5t.
2. The ISO 26262 is only for assembly-line produced road vehicle.
3. The ISO26262 is only for electrical and electronic components and systems.

This standard does not include programmable electronic systems, special cars, trucks, motor bicycles, VANs or other specialties. In all these cases the IEC61508 should be used.

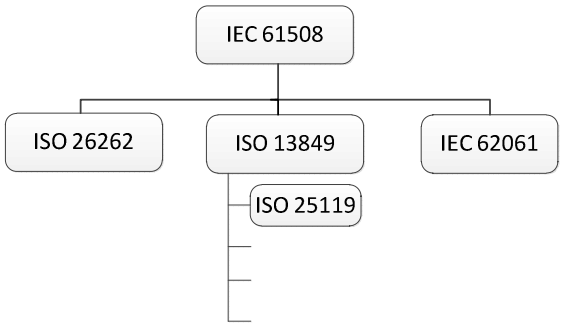

Figure 1: Hierarchy of standards

Under the circumstances that the application runs under the rules of the European Machinery Directive the ISO13849 or the IEC62061 must be used.

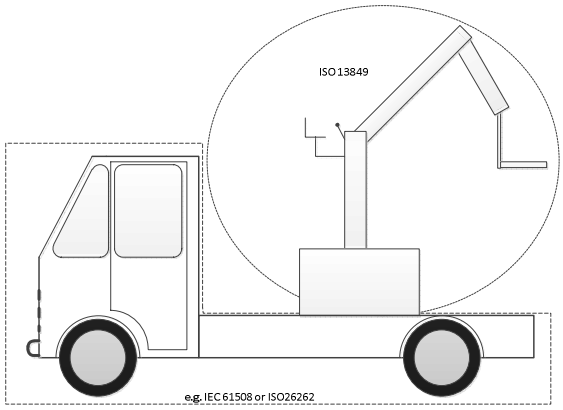

Figure 2: Standard-Domains

Figure 2 shows possible domains with different standards in one application. In such application all machinery parts must be designed according the ISO13849 and/or IEC62061. All car related parts like steering control, ESP, Airbag, etc. have to be designed according IEC61508. But from the practical view the ISO26262 is closer to the application and should also be used there no special truck standard is

available. This will always be the fact with the knowing; that ISO26262 does not focuses to this kind of applications.

Comparison of ISO26262 and ISO13849

If components will be used for passenger vehicles and in machineries, a common understanding about main differences in the standards must exist.

In fact the ISO26262 includes ten parts with nearly 400 pages in sum. In comparison the ISO13849 which has just two parts with around 200 pages and a lot of references to IEC61508 with seven parts and additional 700 pages. This will give just a subjective imagine about the effort. The main difference is the philosophy behind the standards. The safety function in machinery is usually an additional functionality which does not controls the process. That means, if the safety components will be removed, the machinery will still work. This implies additional components and of course additional costs for getting a safe system. The ISO26262 has the intention to provide the functional component as an intrinsic safe device. This should reduce the part costs, but increase the development costs.

Risk analysis

The cradle of both standards is the hazard and risk analyses. The hazard and risk analyses based on the concept, of identifiation the hazards during the lifecycle of a system. The result of the risk analysis is the required safety level (ASIL/PL) for the risk reduction. ASIL means Automotive Safety Integrity Level and starts with “A” for low risks end ends with “D” for the most critical functions. PL means Performance Level and starts also with “a” and ends with “e”. Both standards provide this criteria as a question list for each identified hazard.

Table 1: Risk Parameters

ISO 26262	ISO 13849
Exposure (E) E0: never E1: very low	Exposure (F) F1: unlikely and short
E2: low E3: medium E4: high	 F2: often and long
Severity (S) S0: no S1: low to medium S2: havy S3: dead	Severity (S) S1: low reversible S2: irreversible and dead
Controllability (C) C0: no problem C1: easy to control C2: possible to control C3: not possible	Controllability (P) P1: possible P2: not possible

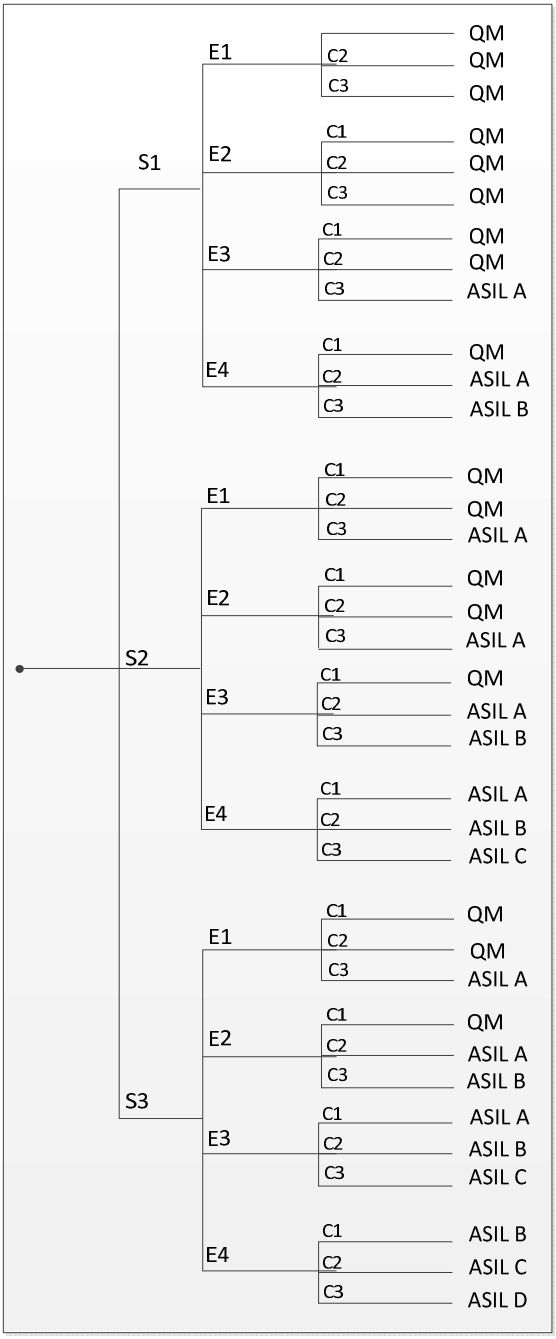

Figure 3: Risk graph for ISO26262

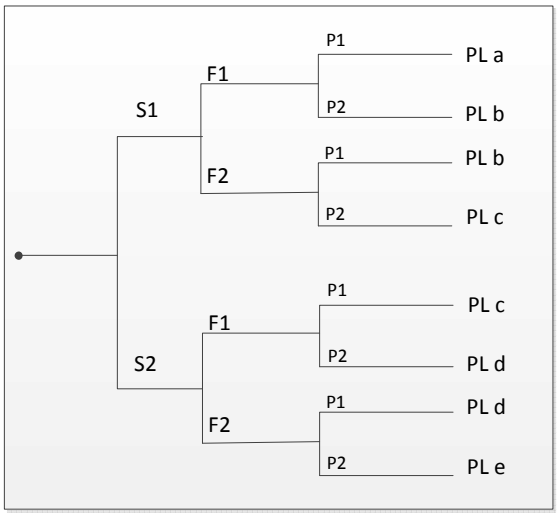

Figure 4: Risk graph of ISO13849

It is important to keep in mind, that there is different qualification of users during the duty phase.
For each individual safety function, the ASIL or PL of the associated element must match the required safety level. The safety levels of the various safety chains forming a safety function have to be greater than or equal to the required safety level of this function.

Reliability parameters

Both standards require a statistical view to the residual dangerous failure rate of a safety function and require a separate Diagnostic Coverage (DC).

Table 2: Failure rates

ISO 26262	λ_d	ISO 13849	λ_d
		PL a	$<10^{-4}$
		PL b	$<10^{-5}$
		PL c	$<3*10^{-6}$
ASIL A	$<10^{-6}$/h	PL d	$<10^{-6}$
ASIL B	$<10^{-7}$/h	PL e	$<10^{-7}$
ASIL C	$<10^{-7}$/h		
ASIL D	$<10^{-8}$/h		

As an addendum of required target failure rates the ISO13849 uses Categories (Cat 1-4). In relation to the sum of assumed possible faults it will result in specific HW-Architecture.

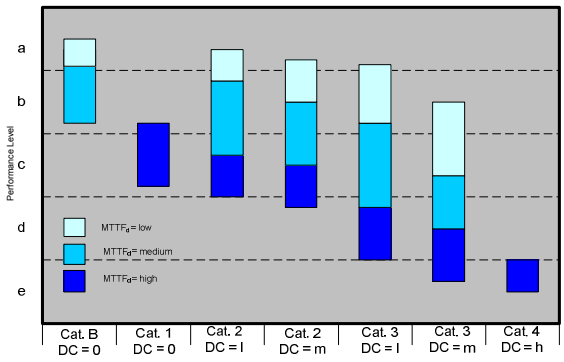

Figure 5: Safety code of ISO13849

This will be handled the ISO26262 by in a different way. The standard does not recommended specified HW-Architectures; it intends to regulate this by additional ranges of Fault-Metrics. On the one side there is the Latent Fault Metric (LFM) and on the other side with the Single Point Fault Metric (SPFM).

Table 3: SPFM and LFM

ASIL	SPFM	LFM
ASIL A	-	-
ASIL B	≥ 90%	≥ 60%
ASIL C	≥ 97%	≥ 80%
ASIL D	≥ 99%	≥ 90%

The matrices can be calculated after an analysis of each element, for instance by a FMEA (Failure Mode and Effect Analysis).

$$LFM = \frac{\lambda_{MPF\ Percieved} + \lambda_{MPF\ Detected} + \lambda_{Safe}}{\lambda_{MPF} + \lambda_{Safe}}$$

$$SPFM = \frac{\lambda_{MPF} + \lambda_{Safe}}{\lambda_{total}}$$

MPF: Multiple Point Fault

Avoiding Systematic Faults

Additionally both standards have requirements to avoid systematic faults. The methods to avoid systematic errors are based on a structured development model. The favorite model in functional safety design is usually the V-Model. The ISO13849 referenced the V-Model mainly

in the software design. The ISO26262 addressed the V-Model for the complete lifecycle including the production. Otherwise, the automotive standard does not address programmable systems like PLC-equivalent-parts.

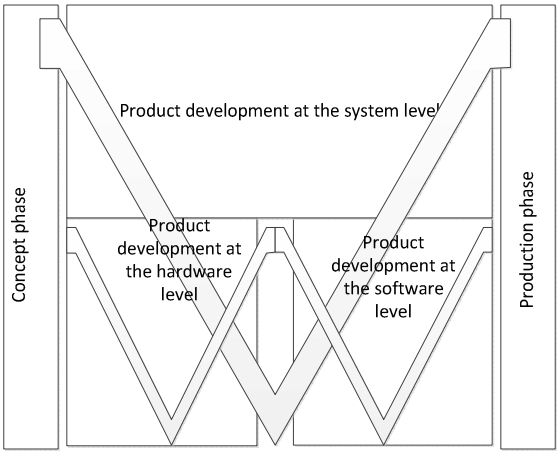

Figure 6: Development Model ISO26262

Verification and validation are the quality assurance measures required to avoid errors during the design and implementation of systems which execute safety functions. It is an absolute “Must” to verify and validate the safety functions in both standards.

Conclusion

To answer the question which standards is easier to handle cannot be done directly. The ISO13849 can be easily applied on the system level, especially if the electro-mechanical components are included. If it is required to design safety elements, the ISO13849 will be referenced to the IEC61508 and in this case the effort in comparison with ISO26262 is similar.

Michael Kieviet
innotec GmbH
Heinrich-Wildung-Weg 3
Phone +49 5422 7540
michael.kieviet@innotecsafety.com
www.innotecsafety.com

References

[1] ISO13849, Safety of Maschinery – Safety related parts of control systems
[2] ISO 262622, Road vehicles – Functional safety –
[3] Wratil, Kieviet, Sicherheitstechnik für Komponenten und Systeme
[4] Wratil, Kieviet, Röhrs, Sicherheit für Maschinen und Anlagen
[5] Löw, Pabst, Petry, Funktionale Sicherheit in der Praxis