On the safe side with IEC 61508

As the successor to the EN 954-1, ISO 13849-1 is the most important standard for the design of control systems in the field of machine safety. However, is it always the most suitable?

Manufacturers of mobile machines are faced with the task of upholding the legal specifications of the Machinery Directive and the Product Liability Act. For implementation, these refer to the state of the art technology which is described by the harmonized product standards. Therefore, some manufacturers of sensors, actuators, and control units provide their customers with already certified products for use in safety-critical applications. As the successor to the EN 954-1, the ISO 13849-1 is here the most important standard for the design of control systems in the field of machine safety. But is it always the most suitable?

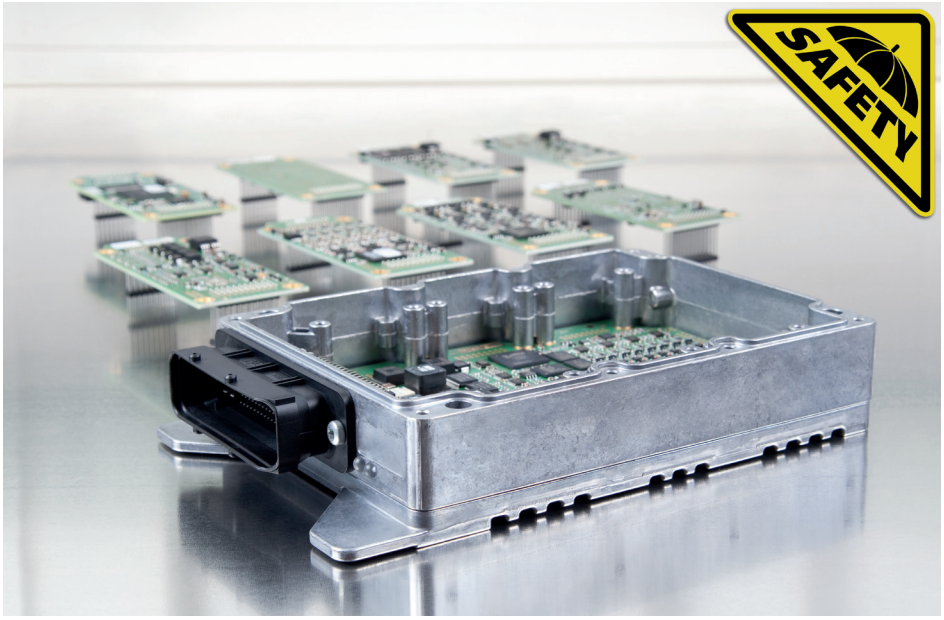

Figure 1: Freely programmable control unit ESX-3XM Safety with extension boards (Photo: STW)

Prior to a manufacturer being able to consider which subcomponents they will use, they must first concern themselves with an analysis of the hazards resulting from their machine. For this purpose, they can use ISO 12100, which defines the general design principles for the risk assessment and risk reduction for the creation of safe machines. The risks determined in this way are evaluated and are reduced to an acceptable extent with the aid of safety classifications. The defined safety functions must then be technically implemented.

Here the question is whether the application of ISO 13849 is always the most sensible method. For manufacturers, the primary fact focused on is that this standard, contrary to its sister standard, IEC 62061, is not only limited to electrical / electronic systems in its application, but is also applicable to mechanical, pneumatic or hydraulic systems. Initially, this appears to be an advantage; nevertheless it cannot be disputed that the electronic control technology dominates in most applications today.

Let us consider the specific disadvantages of the standard ISO 13849. It is applicable to safety-related parts of control units on all types of machinery. In accordance with the EU Machinery Directive 2006/42/EC, this does not include vehicles and methods of transport which are intended for use in public road transport, but rather only machines mounted onto these vehicles (e.g. cranes, loading ramps etc.). ISO 13849 does not contain this limitation, but nevertheless its focus is evidently on stationary machinery, as it's recognizable from several requirements laid down in the standard, and is also reflected in the BGIA Report 2/2008 "Functional safety of machine control units – application of the DIN EN ISO 13849". Safety functions are seen more as additional functions instead of the attempt to safely design the primary functions of the machine. And yet the attachment of light grids to mobile machines, for example, barely makes sense, so what is the alternative?

In the case of self-propelled machines, we differentiate between agricultural machines (e.g. tractors), forestry machines (e.g. harvesters), municipal machines (e.g. snow ploughs, cleaning machines), construction machines (e.g. excavators, wheel loaders), lifting and conveying machines (e.g. mobile cranes, concrete pumps), and special machines (e.g. snow cats). With ISO 25119, a product standard for safety-related parts of control systems already exists for agricultural and forestry machines and municipal vehicles. It combines the safety architecture known from ISO 13849 in the form of categories with the well-tried safety lifecycle of the Generic Safety Standard IEC 61508, and likewise displays analogies to the automotive safety standard ISO 26262.

Table 1: Division of the standards

Standard	Type*	Focus	Scope
ISO 12100	A	general design principles for risk assessment and risk reduction	safety of machinery
ISO 13849	B	safety-related parts of control systems (SRP/CS)	safety of machinery
IEC 61508	A	electrical, electronic and programmable electronic safety-related systems (E/E/PES)	functional safety
IEC 62061	B	safety-related E/E/PE control systems (SRECS)	safety of machinery
ISO 25119	C	safety-related parts of control systems (SRP/CS)	machinery for agriculture and forestry
ISO 26262	C	safety-related electrical and/or electronic (E/E) systems	road vehicles up to 3.5 tonnes
IEC 61800 -5-2	C	E/E/PE elements of safety-related electrical power drive systems with adjustable speed	power drive systems (PDS)

* Type of standard: A = basic standard, B = sector standard, C = product standard

The other applications can be subdivided into those with and without road approval. One prerequisite for road approval is the type approval, e.g. according to Regulation (EC) No. 661/2009 "concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor." Here, too, as in the Product Liability Act, "state of the art science and technology" is referred to – and therefore to the harmonized standards. For motor vehicles up to 3,5 t, we have ISO 26262, which has already been at least used as a basis by several commercial vehicle manufacturers, for example for risk analyses. In the field of mobile machines, designs are developed optionally according to ISO 13849, IEC 62061 or IEC 61508, whereby the latter in particular is recommended for drives. The reason for this is the assumption that the path is easier from there to ISO 26262, and, as generally known, in its next version this is also to be applied to Heavy Commercial Vehicles.

However, this is not the only argument for the use of IEC 61508 in the field of machine safety. According to DIN ISO/TR 23849:2014-12, the following applies: "Every complex sub-system which has been designed according to IEC 61508 with the relevant SIL can be integrated as a safety-related part in a combination of SRP/CS, which has been designed according to ISO 13849-1 or as a sub-system in a SRECS, which was designed according to IEC 62061". This statement also applies in the same way for the amalgamation of the standards in IEC ISO 17305. Even although the completion of the new standard is still in progress, we are this initially armed with IEC 61508-compliant products for its introduction.

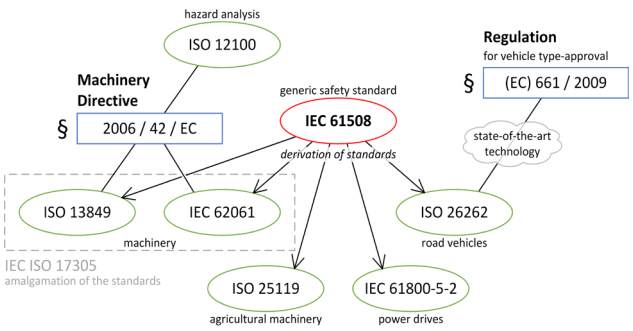

Figure 2: Relation of the standards (Photo: STW)

One valid option

A further point is that we currently do not yet have a product standard for the power electrification of mobile machines which can be extensively applied. IEC 61800-5-2, for example, excludes the application of electrical power drive systems with adjustable speeds in rail drives and electrical vehicle drives. In such cases, only the application of IEC 61508 or a derived sector standards, such as IEC 62061, remains a valid option.

Finally, we should consider the fact that safety-related communication protocols are also increasingly being used in mobile machines. Accordingly, ISO 13849-1 refers to IEC 61508-2, which in turn provides a choice of two data communication architectures. With the White-Channel, the entire transmission path must be developed compliant to the standard, whereby with the Black-Channel, only the end points are considered safety-relevant and the transmission is protected via a special protocol. In both cases, for non-rail applications, IEC 61784-3 "Functional safety fieldbuses" is referred to the principles of which have been implemented in the CANopen Safety standard EN 50325-5, for example. It is important at this point that the systems which should communicate with each other reliably must comply with the requirements of the standard. For Black-Channel transmission this means that at least the software has to be developed according to IEC 61508-3 and executed in a safe context.

In summary, it can be said that the manufacturers of mobile machines are indeed currently managing well with ISO 13849, but that the additional use of IEC 61508 brings many advantages for future challenges. With control components which have been certified accordingly, manufacturers can secure their investments long-term, because the systems can be supplied to different sectors without having to be developed compliant to different standards. ◀

Author

Philipp Luger
Sensor-Technik Wiedemann
info@sensor-technik.de
www.sensor-technik.de