Gerhard Henninger, Frankfurt am Main

Safety-related Parts of Control Systems in Mobile Farm Machinery

The increasing „electronisation" of farm machinery and the changeover from electromechanical to electronic control systems (µC) makes it also necessary to revise the standards themselves[2] and in their relationship to agricultural machinery. In this contribution, the relevant existing standards are briefly illustrated, and the draft standard based on the results of the Working Group Safety of the VDMA Technical Committee Electronics is explained.

Dipl.-Ing. (TU) Gerhard Henninger is Secretary of ISO Sub-Committee ISO/TC 23/SC 19 Agricultural Electronics at the VDMA Agricultural Machinery Association, Lyoner Straße 18, 60528 Frankfurt / Main; e-mail: *gerhard.henninger@vdma.org*

Keywords

Lifecycle, probabilistic, risk analysis, safety culture

The Mother of Safety Standards: IEC 61508

The standard IEC 61508 [3], which was published in 1998, applies to the machinery and process industry and includes all aspects of functional safety during the entire life cycle of a machine or a plant. It has developed into a basic, comprehensive standard for virtually all kinds of safety-technological questions in the areas of electric systems and electronics.

IEC 61508 caused a structural change in the world of standards. In addition to the deterministic (defined, clear) approach, the consideration of the entire life cycle additionally as a probabilistic approach were introduced.

Its high degree of complexity (more than 450 pages, divided into seven parts) is an important disadvantage of this non-harmonized standard, which means that it has no presumption of conformity with the Machinery Directive. For this reason, this standard in its present form cannot be applied in practice by small and medium-sized agricultural machinery manufacturers.

EN 954-1 and its Successors

Since 1996, EN 954-1 [4] has been one of the most widely used standards for machines with safety control.

The establishment of electronic systems, however, resulted in the necessity to revise this standard. In particular, additional measures were called for, which reduce the remaining risk when risks grow. This also includes the fact that EN 954-1 does not provide any sufficient requirements for the consideration of reliability values.

Two new standards are "competing" as successors of EN 954-1: First, ISO 13849-1 [5], which was developed as direct successor of EN 954-1. Second, the IEC 62061 standard [6], a sector-specific derivative of IEC 61508 for machinery construction, is "competing" as a successor of EN 954-1.

With both standards, probability calculus and reliability engineering are becoming an additional part of the design of safety-relevant parts of machinery control systems. The approach of EN 954-1, however, is mainly based on the consideration of structures (control categories). Insofar, downward compatibility does not exist, or it is insufficient.

The standard ISO 13849-1 tries to strike a balance between proven principles of EN 954-1 and new approaches of IEC 61508. This means that deterministic and probabilistic considerations in the design of safety-relevant parts of machine control systems are combined. The new aspect of the probabilistic approach is reduced to an extent, which is necessary and practicable for the "average user" of ISO 13849-1. ISO 13849-1 exclusively deals with the design of safety control and does not define any organizational requirements.

ISO 13849-1 continues to use a risk graph. However, the consideration of the risk parameters no longer leads to a control category like in EN 954-1, but to a performance level (PL). The PL describes the capability of a safety-relevant part of a machine control system to carry out a safety function in order to reach the required risk reduction. This approach integrates both quantitative and qualitative aspects. As compared with EN 954-1, the individual risk parameters (severity of injury, frequency of exposure to the hazard, and possibilities of avoiding the hazard) have remained unchanged in ISO 13849-1.

The Standardization Approach for Agricultural Machinery

Given the changes in standardization and the growing necessity, the question arose how agricultural engineering could react to this development. Therefore, the development of a product standard for agricultural and forestry as well as municipal machinery was initiated at the level of the association. The starting point was EN ISO 13849.

The goal of this initiative was to propose a standard which can be easily applied in our industry, which is particularly characterized by medium-sized companies. This objective was reached with the aid of a simple structure, examples, and an order of the standard

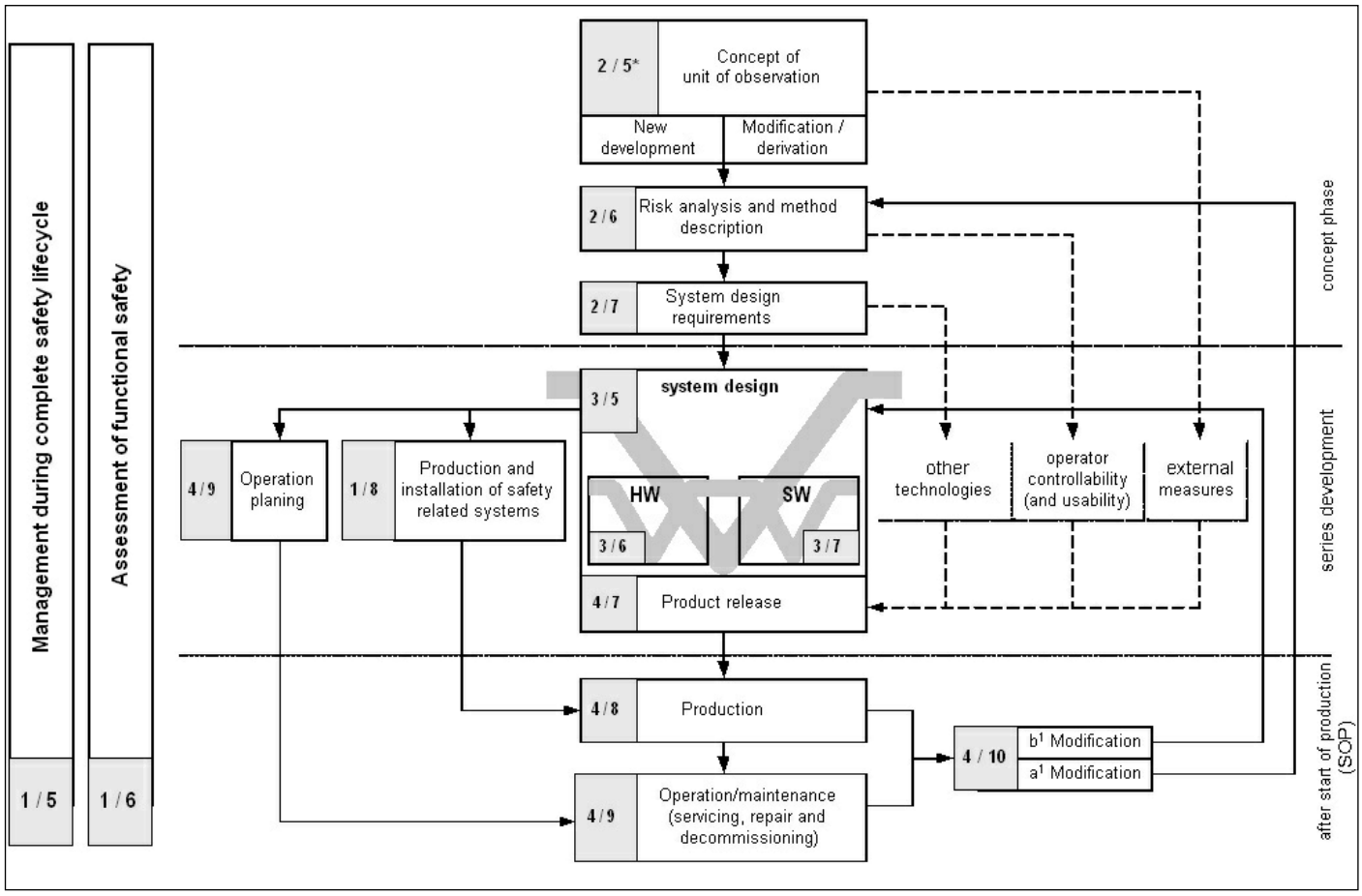

Fig. 1: Safety lifecycle

which follows the existing processes within the companies. The new ISO/CD 25119 standard [7] focuses on electric, electronic, and programmable electronic systems. The classic disciplines of mechanical engineering, such as mechanics, hydraulics, and pneumatics are not considered in the overall concept. However, they must be taken into account in the risk assessment of the safety-relevant functions.

ISO/CD 25119 covers all areas from the idea until scrapping (*Fig. 1*). In general, no other safety standard must be used, except for EN ISO 12100, parts 1-2 [8] and ISO 14121 [9], which are directly referred to in the new Machinery Directive 2006/42/EC. *Table 1* shows the parts of ISO 25119.

An important aspect is the "performance level" approach including the AgPLr (required agricultural performance level), which was taken over from EN ISO 13849 and upgraded.

Based on risk analysis, the developer has several possibilities to reach the AgPLr. Together with the newly introduced "SRL" (software requirement level), the failure detection rate, which is termed "DC" (diagnostic coverage), and the MTTFdC (mean time to dangerous failure for one channel), different "categories" meet the required AgPLr. The "categories" describe different kinds of hardware architecture from a very simple structure to a fully redundant design. Together with a high dangerous failure rate of the components of a channel and good monitoring, a simple structure can provide a solution which is as safe as a more complex, redundant structure with lower MTTFac and simple monitoring. This approach gives every developer (company) the possibility to adapt to the specific requirements of the machine, the project, and/or the company.

For MTTFdC, MTTF data bases as well as the conversion of switching cycles (relay, switches, etc.) into hours are mentioned. It is very important that only those parts must be considered which can lead to a dangerous failure. Example: A relay contact can be short-circuited (glued) or open. Depending on the circuit design, only one situation is potentially dangerous. This means that in this case the MTTFdC for the channel to be examined corresponds to 50 % of the MTTF. Thus, the values in the calculation double.

For hardware and software, separate, complete sections were developed. There, methods, tools, and procedures for every development phase (planning, design, implementation) including verification and validation are described in detail. The individual requirements for the different AgPLr (a to e) are shown. Since several sections are combined in one part of the standard, a design engineer can focus exclusively on this part and does not have to occupy ("burden") himself with the others.

Another approach of ISO/CD 25119 with far-reaching consequences for business practice is the integration of necessary management activities (functional safety management assessment) over the entire life cycle of the electronic functions/components. As compared with current standards governing the safety of electronic systems, the naming of responsible institutions at the level of the manufacturers (and suppliers) is another new (and demanding) approach.

All supporting processes are listed. Instructions and requirements for cooperation with suppliers as well as procedures in the service sector are described, and organizational instructions are given. In all respects and in particular with regard to documenta-

Table 1: Standard ISO 25119 Part 1- 4

ISO 25119 Parts:	
Part 1:	General principles for design and development
Part 2:	Concept phase
Part 3:	Series development, Hardware, Software
Part 4:	Production, Operation, Modification and supporting processes

tion, the existing procedures/structures in companies were taken into consideration.

Companies which work according to ISO/CD 25119 not only manufacture safe electronic systems, but also automatically produce high quality.

Each section in ISO/CD 25119 is structured such that first general considerations, objectives and conditions are stated (informative part). Afterwards, the requirements are defined (normative part). Thus, a design engineer can work on each section in the same way.

With regard to the total perspective, the implementation of a safety philosophy in the company and consistency (the same solutions for the same functions) in all projects are important aspects [13].

The new standard ISO/CD 25119 Part 1 to 4 is available as CD (committee draft) since September 2007. The DIS survey is intended to begin at the second quarter of 2008.

Activities in Other Industries

For construction machines, ISO-CD 15998 [10] is applied. This standard is suitable as a guideline for electronics with EMC and environmental requirements as well as risk assessment according to IEC 61508. This means that no product-specific adaptations were made with regard to safety.

For the automotive industry, a product-specific standard for passenger cars is being developed and is currently at the draft stage (ISO WD 26262 part 1-8 Road Vehicles – Functional Safety [11]). Like in the agricultural and municipal machinery sector, the standard focuses on the design of safety-relevant parts of electronic control systems for passenger cars of certain classes (M, N, and O). The standardization activities of the VDMA and FAKRA have been harmonized.

Summary

With ISO CD 25119, a draft standard has been presented which makes it easer for agricultural machinery manufacturers to develop safety-relevant functions for their machines and thus to fulfil the requirements of legal regulations and product liability. After the standardization process has been completed, products with steer by wire or other by-wire solutions are expected to appear on the market. The standard allows safe electronic systems to be developed. In addition, uniform regulations can be provided for the competent authorities with regard to the proof of safety for road traffic approval.

Literature

Books are marked by •

[1] • *Böttinger, S., R. Buschmeier und P. Hieronymus*: Jahrbuch Agrartechnik 2004, Band 16, Kapitel 2.3 Kommunikationssysteme

[2] • *Gehlen, P.*: Funktionale Sicherheit von Maschinen und Anlagen. 1. Auflage, Erlangen, Publucis KommunikationsAgentur GmbH, 2007, ISBN-13: 978-3-89578-281-7

[3] IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems

[4] EN 954 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

[5] ISO 13849 Safety of machinery – Safety-related parts of control systems

[6] IEC 62061 Safety of machinery – Functional safety of electrical, electronic and programmable control systems for machinery

[7] ISO/CD 25119 Teil 1-4, Safety related parts of control systems

[8] ISO 12100 Safety of machinery – Basic concepts, general princiles for design

[9] ISO 14121 Safety of machinery – Principles of risk assessment

[10] ISO 15998 Earth-moving machinery – Machine-control systems using electronic components – Performance criteria and tests

[11] ISO WD 26262 Part 1-8 Road vehicles – Functional Safety