# Opensafety – the open source safety solution

Miodrag Veselic (Bernecker & Rainer)

**The safety requirements for mobile machinery have increased considerably since the introduction of the new Machinery Directive (2006/42/EC). The new standards have resulted in new approaches to the design of safety technology. Integrated safety solutions allow safety signals to be used for automation as well. New features increase machine availability, reduce the number of required sensors and decrease the overall complexity of safety solutions. Opensafety is the world's only open-source safety protocol that enables safety communication via any protocol available on the market. In addition, the Opensafety stack is pre-certified for SIL3 by TÜV-SÜD and TÜV-Rheinland. With no licensing costs and a free, pre-certified software stack, users benefit from greatly accelerated time-to-market.**

## Basic safety requirements

The failure of components – in vehicles for example – can be minimized through well-defined rules and regulations. The transformation of the Machinery Directive into the Product Safety Act (ProdSG) provides a solid technical basis and, in Germany, a legal framework as well.

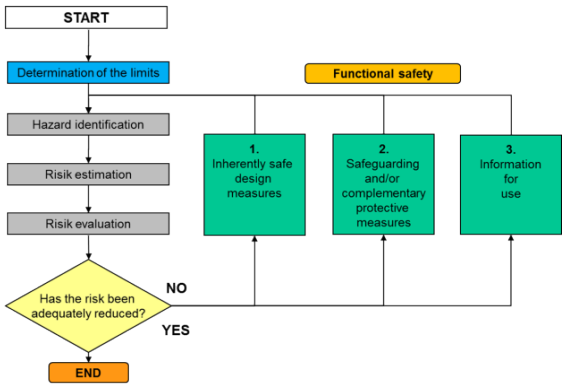


**Figure 1: EN ISO 12100**

In our case, the Product Safety Act regulates auxiliary equipment on tractors and considers additional risks not covered in Directive 2003/37/EC (the type-approval of agricultural or forestry tractors, their trailers and interchangeable towed machinery, etc.).

The procedure for reducing risk to an acceptable minimum is defined in EN ISO 12100 - Risk assessment and risk reduction - see also Figure 1.

In the first step, hazards and hazardous situations are evaluated on the bare machine. The assessment must be carried out throughout the entire life cycle of the machine (manufacture, transport, commissioning, etc.). In the second step, risk is estimated by determining the likely extent of damage and its probability of occurrence.

The last step, risk evaluation, involves an assessment of whether objectives for risk reduction have been achieved. If this is not the case, this step is followed by attempts to further reduce risk through constructive measures before repeating steps one through three. If the potential hazard presented by the machine is still too high, technical protective measures, known as "functional safety", are applied.

As a final measure to minimize residual risk, organizational measures such as signs, signals and instructions are implemented. If the goals have not been reached after this step, the machine must be redesigned.

## Functional safety

A number of different standards can be used for risk assessment, whereby IEC 61508 (Type A) represents the fundamental standard. Depending on the requirements, each individual standard has its advantages and disadvantages. For example, IEC 62061 includes a high level of documentation and validation overhead and is usually used by series machine manufacturers. It provides a very detailed risk assessment. Although ISO 13849 facilitates the switch from deterministic to probabilistic design, its risk assessment lacks sufficient detail.
The world of mobile machinery relies primarily on the following two standards:

- EN ISO 26262 – (Road vehicles – Functional safety), for vehicles up to 3.5 T. Classification of the required safety levels in “QM” or “ASIL A to D”.
- EN ISO 25119 – (Tractors and machinery for agriculture and forestry - Safety-related parts of control systems). Classification of the required safety levels in “AgPL a to e”.
- Both standards are relatively new, having taken effect in 2011, and have yet to find widespread acceptance in the agriculture industry.

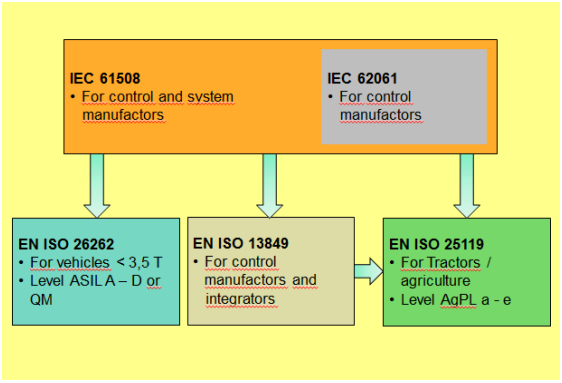


**Figure 2: Safety standards overview**

## Requirements for functional safety

In the years since introduction of the new Machinery Directive, requirements on safety technology have increased significantly. According to the newly introduced standards (see Figure 2), safety concepts must be designed to serve the protection of both human and machine.
The availability of new safety components on the market has resulted in new approaches in the design of safety technology. Intelligent safety functions now allow human–machine interaction during operation. Simple diagnostic functions allow errors to be resolved more quickly, and central data storage provides shorter recovery times, which in turn increases the availability of the machine.
Implementation of an integrated safety system brings several significant advantages. The number of components can be decreased, the complexity of wiring can be reduced and configuration and parameterization can be automated (see Figure 3).


**Figure 3: Application example**

These new features are made possible by:

- Safety sensors linked directly to the network
- Direct read-out of component data
- Simplified maintenance due to automated component parameter setting across the network
- Safer operating mode switching due to runtime parameter setting
- Decreased response time through elimination of relay-induced latency

**Black channel principle**

Opensafety functions on the so-called "black channel principle", also known as "black or gray channel". This principle enables the transmission of standard and fail-safe data over the same bus line. Regardless of the underlying network channel (transport layer / fieldbus), safety-related components can transmit their data via whatever protocol is used. This is also called "data tunnelling". The available bandwidth and the cycle times depend on the transport protocol, since the safe fieldbuses are pure application protocols (see Figure 4).

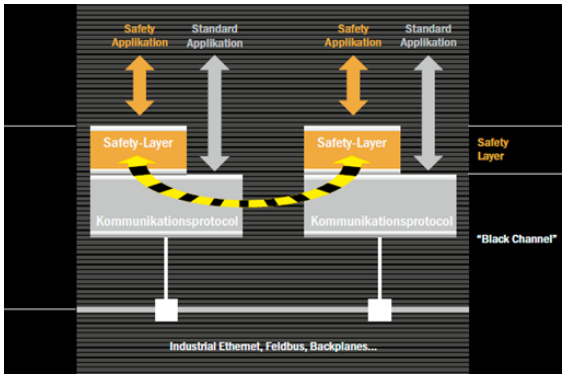


**Figure 4: Black channel principle**

Communication risks that may arise include, duplication, loss, insertion, incorrect sequences and more. The specific errors and corresponding corrective measures are specified in the relevant standards – IEC61784-3 (Functional Safety Fieldbuses) – see Figure 5.
The quality, or bit error rate1, of verification depends on the Safety Level to be achieved.

*[1] Bit error rate (BER) - Typical value 1 bit errors at 1000 bits transmitted.*

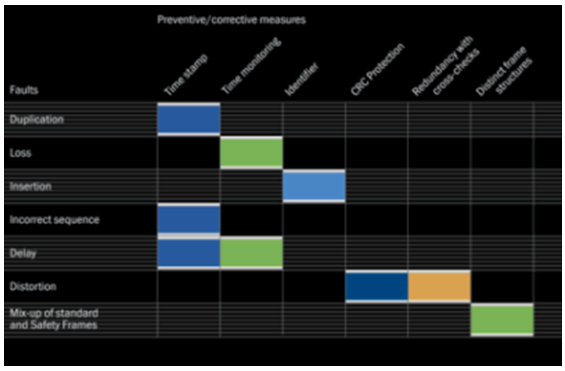


**Figure 5: Communication risks according to the IEC 61784-3**

**Opensafety - the open source safety standard**

Opensafety is the only open source safety protocol in the world. The software stack is developed under the Berkeley Software Distribution (BSD) license. This license states only that copyright must be noted in the source code. Otherwise, the Opensafety stack can be used free of charge and royalty. Using the black channel principle, the stack can be implemented on any fieldbus. Currently, specifications are available for implementation on:

- Ethernet TCP/UDP/IP
- EtherNet/IP
- Modbus TCP/IP
- Powerlink
- Sercos III
- Profinet

The advancement of Opensafety technology is driven by the members of the Ethernet Powerlink Standardization Group (EPSG).
Stack certification has been completed for implementation up to SIL 3 by TÜV-Rheinland and TÜV-Süd. To ensure that users can benefit from this pre-certification, the EPSG provides a review of Opensafety stack integration. After verification, the user receives a certificate of conformance to the EPSG specification, which can then simply be submitted to the certification authority.


**Opensafety functionality**

Opensafety was designed to transmit safety-related data over any fieldbus or network. It can be used on all fieldbus systems, Ethernet-based or not.
For the transmission of safety data, the producer-consumer model is used. The advantage of this model is that all consumers in an Opensafety network can receive and subsequently process the messages sent by the producer. Each Opensafety node has a Unique Device Identification number (UDID). This is a combination of the MAC address and the manufacturer's device number.
During the booting process, the Safety Configuration Manager (SCM) checks the device type and the UDID, allowing it to automatically detect replaced devices. In such a case, the required parameters are automatically transferred to the safe nodes (SNs). Analogous to other communication protocols, the SCM can be viewed as an Opensafety master that uses services to manage the network.
The Opensafety Object Dictionary (SOD) manages all parameters, which are then transferred to the safe nodes using Safety Service Data Objects (SSDO). Upon completion of node configuration and the booting phase, cyclic data transfer between producer and consumer commences. Safety Process Data Objects (SPDOs) are used to transfer safety-critical process data. The Opensafety frame consists of two sub-frames. It can transport a maximum of 254 bytes of safety data, using CRC 8 for payloads from 1 to 8 bytes and CRC 16 for payloads from 9 to 254 bytes (see Figure 6).

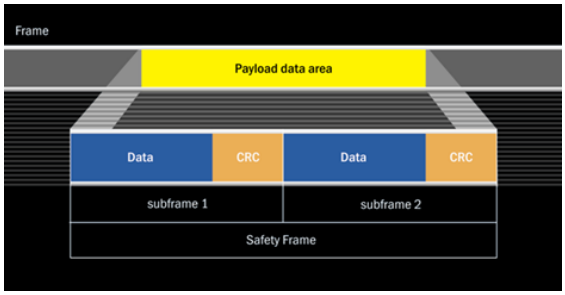


**Figure 6: Opensafety frame**

Opensafety makes it possible to create very large networks. For each Opensafety domain (SD), up to 1023 safe nodes can be connected. As they are addressed by the SCM, no additional hardware switches are required.
The largest Opensafety network that can be configured has 1023 Opensafety domains with a total of more than a million safe nodes. Communication between the individual domains is performed by the Opensafety Domain Gateway (SDG).
Automatic configuration, detection of device replacements and centralized data management make it possible to map multiple machine options. This permits auxiliary equipment to be switched out without requiring any additional manual intervention (see Figure 7).

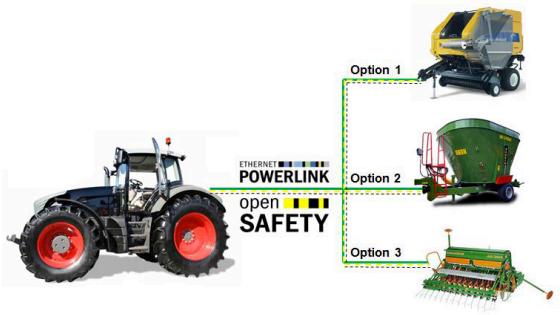


**Figure 7: Safety machine options Powerlink**

"Powerlink is CANopen over Ethernet" – although this statement simplifies the matter by ignoring Powerlink 's real-time capabilities – it nonetheless captures an essential feature of this communication system, which gives users the benefits of both protocols in a single package. Powerlink is also available as open-source technology under a BSD license, allowing the source code to be used free of charge and royalty. Powerlink can be implemented on a variety of real-time capable operating systems such as VxWorks, Linux, QNX, Windows CE, and more. Furthermore, the stack can be ported to any FPGA. One thus needs no special ASICs and remains manufacturer-independent.

## Powerlink functionality

Powerlink uses a mixture of timeslot and polling procedures to achieve isochronous data transfer. In order to ensure coordination, a PLC or an industrial PC is designated as the Managing Node (MN). This manager enforces the cycle timing that serves to synchronize all devices and controls cyclic data communication. All other devices operate as Controlled Nodes (CN). In the course of one clock cycle, the MN sends poll requests to one CN after another in a fixed sequence. Each CN replies immediately to this request with a poll response, to which all other nodes can listen in.

A Powerlink cycle consists of three periods. During the "Start Period" the MN sends a "Start of Cycle" (SoC) frame to all CNs to synchronize the devices. Jitter amounts to about 20 nanoseconds. Cyclic isochronous data exchange takes place during the second period ("Cyclic Period"). Multiplexing allows for optimized bandwidth utilization in this phase. The third period marks the start of the asynchronous phase, which enables the transfer of large, non-time-critical data packets. Such data, including user data or TCP/IP frames, is distributed across the asynchronous phases of several cycles. Powerlink distinguishes between real-time and non-real-time domains. Since data transfer in the asynchronous period supports standard IP frames, routers separate data safely and transparently from the real-time domains.
Powerlink is very well suited to all sorts of automation applications, including I/O, motion control, robotics tasks, PLC-to-PLC communication and visualization.

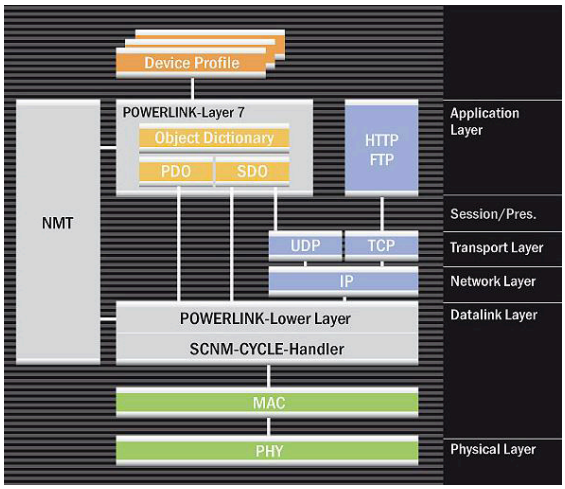


**Figure 8: Diagram of Powerlink stack**

**Ethernet Powerlink Standardization Group**

The Ethernet Powerlink Standardization Group (EPSG) was founded in 2003 as an independent organization of companies in the drives and automation sector. The group's goal is the standardization and ongoing development of the Powerlink and Opensafety protocols. The EPSG cooperates with standardization organizations such as CAN in Automation (CiA) and the IEC.

**Biography**

Following an apprenticeship at the company Getzner Textil AG, Miodrag Veselic went through various industries such as Food & Beverage, Custom Machine Engineering and Renewables. During the last nine years he focused on topics involving functional safety. Since 2011 he has worked in B&R's Open Automation Technologies business unit with responsibility for sales and marketing of Powerlink and Opensafety technologies.

Miodrag Veselic
Bernecker & Rainer
B&R Strasse 1, 5142 Eggelsberg, Austria
+43 7748 6586 - 0
+43 7748 6586 - 26
miodrag.veselic@br-automation.com
www.br-automation.com