Technical Article

A safety strategy for reliable components.

Functional safety: What is it? What do you need to know?

Anyone producing heavy duty or special vehicles in Europe needs a safety strategy for interaction between the subsystems and electronic components, whether for on-road or off-road vehicles. Designating a safety level for each safety-relevant application will enable you to ensure functional safety right across your supply chain – and the key to doing this lies in risk analyses that are performed in accordance with the appropriate standards. As expert partner, EAO prioritizes functional safety in all of its customer relationships, as there are great advantages in this area for users and manufacturers alike.

Traditional mechanisms are increasingly being replaced by smart electronics, and smart solutions are even replacing mechanical actuators and indicators in heavy duty and special vehicles. CAN (Controller Area Network) bus systems are able to connect more than hundred bus participants with one another: data and information are sent across shared cables, therefore reducing the number of wiring harnesses as well as the associated weight – and subsequent cost. At the same time, these data buses also expand vehicles' technical capabilities to the benefit of their users and operators; the downside is that the increasing complexity of these electronics can cause new types of malfunctions. All it takes to distort the intended information is for a bit to flip from 0 to 1 during digital data transfer, possibly switching the application to an unintended state – with potentially devastating consequences when safety components are affected. This is where functional safety comes in. Not only highly complex applications can benefit from this, but also simple or seemingly non-critical ones, such as window openers or light switches.

Immediate system response to random errors.

International standards define the handling of functionally safe products – from the concept phase to product development, manufacturing and operation of the products in use.

Functional safety reduces unacceptable risks caused by random electronic system errors to a level that is acceptable. The risks in question here are those that may cause injury to persons, i. e. not damage to property. Functional safety means applying and observing certain standards to ensure that the correct operation of safety functions is monitored. In the event of an error, the system will respond and switch the application to a safe state – for example by stopping it or by alerting the user.

When it comes to mechanics, it is important to apply appropriate development processes to prevent systematic errors. Increasingly complex electronics also require the systems to be monitored when in use – and random errors must be detected during this process. Random errors may be caused by external influences such as radiation, magnetic fields or simply the ageing of the electronics systems. In the event of malfunctions of this kind, it is vital that the system responds immediately, for example by switching a vehicle into a safe state. In these situations, systems switch themselves off or warn the driver, for example by causing a monitoring lamp to flash.

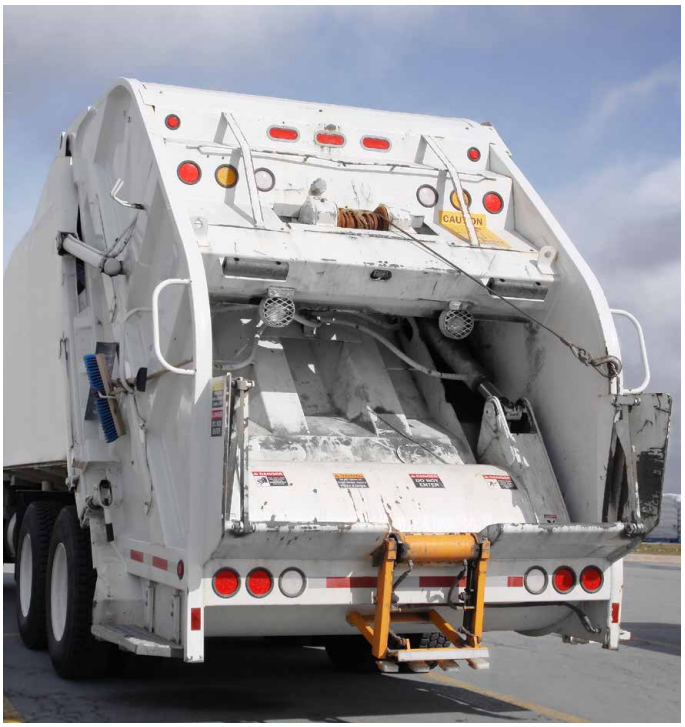
So although functional safety cannot prevent malfunctions, it can significantly reduce the potential damage they may cause. In summary, functional safety means limiting risks to a level that is acceptable. To this end, there are various standards that define development and production processes, regulate the monitoring of electronics and define what a safe state is. These standards also ensure the necessary protection for manufacturers of safety components, subsystems or entire heavy duty or special vehicles. The extensive documentation and certification relating to functional safety provides companies with proof that they are supplying their customers with “safe” products.

Methods for error prevention

Mechanisms and electronics	Prevent systematic errors	through defined processes in concept phase, during product development and manufacturing.
Electronics	Detect random errors	through monitoring during use.
	Respond to random errors	with safe states during operation.

In addition to the Machinery Directive, specific standards may apply.

“If you neglect functional safety, you – yes, you personally – are therefore putting your company at great risk, not to mention the users of your products.”



For example, a refuse truck and its compactor should be considered as separate applications.

Who absolutely needs to address functional safety? To put it simply: all manufacturers are responsible for ensuring that nobody comes to any harm because of their products. The European Directive on general product safety requires that all products sold on EU markets must be safe. This EU Directive will become binding in the corresponding countries when it is transposed into national product safety legislation. Accordingly, product manufacturers must comply with specific standards or uphold the state of the art in their products. This includes the principle of functional safety. The ISO 26262 standard is one of the standards that applies to vehicles containing safety electronics.

This standard was expanded to explicitly include all road vehicles in its Second Edition in December 2018. Machinery and vehicles should be considered separate applications and specific technical standards must be taken into account. Functional safety matters, or rather the currently applicable standards in this area are now often the subject of legal disputes. Anyone who fails to respect them may be found to have acted in gross negligence and is therefore liable if people experience injury. If you neglect functional safety, you – yes, you personally – are therefore putting your company at great risk, not to mention the users of your products.

Addressing the issue of functional safety is a corporate obligation.

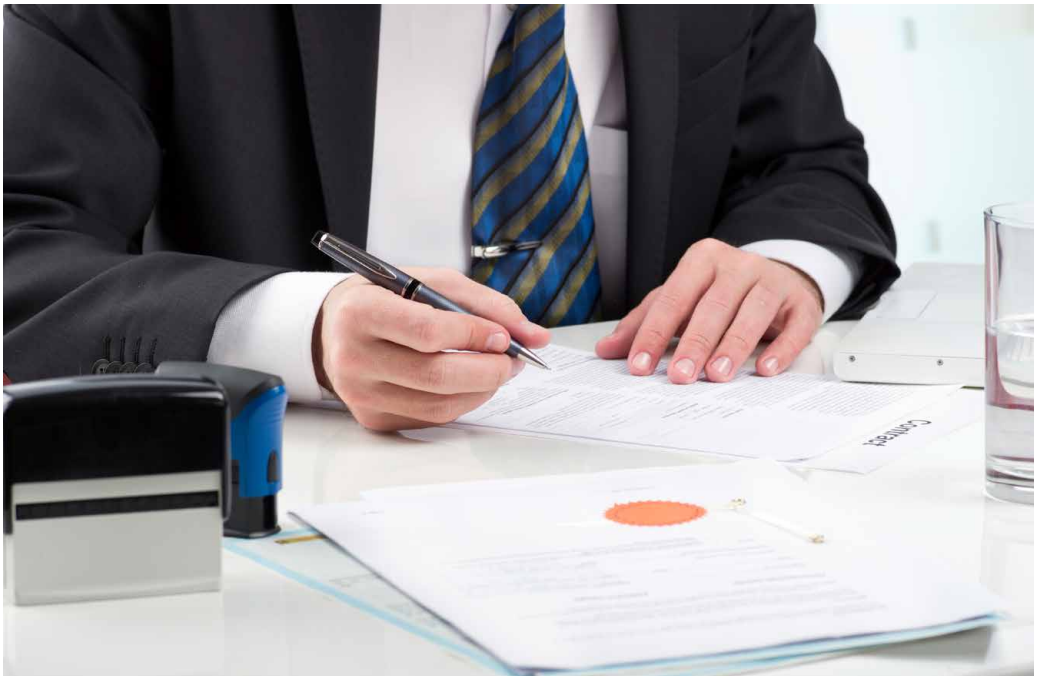
“Applying the relevant standards can reduce the risk of legal ramifications and financial damage for the manufacturer.”

“It is not just companies that may be prosecuted, but also employees, such as a development manager deemed responsible for a failure.”

Special purpose and other vehicles and components of vehicles that do not ensure functional safety therefore pose a big risk to their users and their environment as well as their manufacturers. Conversely, functional safety in vehicles protects manufacturers from legal ramifications and financial damages. In this respect, it is not just companies that may be prosecuted, but also employees, such as a development manager deemed responsible for a failure. Lawmakers provide for compensation payments or even prison sentences in such cases. Products with insufficient functional safety can result in costly recalls, while reputational damage will inevitably cause long-term financial losses. Addressing the issue of functional safety is therefore a corporate obligation. For manufacturers of safety applications, this means developing a safety culture that also intervenes in management and support processes: functional safety management. At the same time, applying the relevant standards and certifications presents an opportunity that goes beyond product safety and avoiding legal ramifications: the application of the relevant standards increases the quality standards. In actuators and indicators, for example, this affects their switching safety and reliability.

Having a safety strategy allows manufacturers to take responsibility.

“The safety level must be broken down for each individual component and its respective application.”



The task is to perform a risk analysis for the overall product, to determine the necessary safety level and to derive and implement risk-minimising measures.

When it comes to functional safety with respect to end customers, the responsibility lies with the company that brings a product to the market. The company is therefore dependent on using components that will not cause injury. The task of such companies is to perform a risk analysis for their overall product as a whole and determine the necessary safety level for it. To this end, the relevant standards define what are known as Safety Integrity Levels (SIL) or Performance Levels (PL) for machine applications (see box on page 2). The safety level must be broken down for each individual component and its respective application. Specific requirements for supplier components can then be derived accordingly. The safety level required for the same component from a supplier for customer A may differ from that for customer B. In each particular case, the application determines the safety level. For this reason, a safety strategy is required. All manufacturers of heavy duty and special vehicles must determine the following: Which components require which safety level? How do they need to respond to random errors? For some applications it is sufficient to inform the user that a workshop visit is necessary – for other applications, an emergency strategy is implemented in parallel. In other cases, a response must be triggered. This response will then ensure, for example, that a heavy duty or special vehicle can then only be manoeuvered at a limited speed. In the case of particularly critical errors, it may even be necessary to stop the vehicle moving altogether.

For every application the safety level must be determined.

Standards show manufacturers how to achieve the Safety Integrity Levels (SIL) and define risk classification parameters. Risk classification focuses on the questions: How serious are the consequences of the various errors? How often do these errors arise? How successfully can they be managed? The answers to these questions determine the “severity” of the risk classification (see example on page 2). As mentioned above, each application must be considered separately; for example, the braking system as a whole will have a high safety level, while another safety level may be adequate for one of its subsystems. Such as the anti-locking system. The risk assessment covers levels 1 to 4, and the designations may differ slightly depending on the standard being applied. For example, machinery standard EN ISO 13849 defines Performance Levels, classified from a to e. Meanwhile, the ISO 26262 standard, applicable to vehicles, has Automotive Safety Integrity Levels (ASIL) ranging from A as the lowest safety level to D as the highest. Independent test laboratories or other assessment procedures are prescribed depending on the safety level.

Example: Determining the safety level (ASIL) for a vehicle application

What injuries (S for Severity) will an error cause?

- S0: none
- S1: mild to moderate
- S2: severe, survival likely
- S3: very severe, survival unlikely

How likely is it (E for Exposure) that the error will occur?

- E1: very low probability
- E2: low probability
- E3: medium probability
- E4: high probability

How easy to control (C for Controllability) is the error?

- C0: controllable in general
- C1: easy (99 % of drivers)
- C2: normal (90 % of drivers)
- C3: difficult (by under 90 % of drivers)

The safety level can now be taken from the risk table:

Risk matrix ISO/DIS 26262-3		C - Controllability		
S - Severity	E - Exposure	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Discipline-specific standards serve as the basis.

Various discipline-specific standards have been derived from the IEC 61508 basic standard.

Functional safety and the related standards require management systems with defined development processes. The V model can be used to organise these processes into different phases – starting with risk analysis. In this respect, functional safety requires further-reaching, more laborious analysis than conventional development processes: fault tree analyses (FTAs) assess the reliability of technical systems and the likelihood that they will fail, and form the basis for the safety strategy. The inspection and documentation of the processes is equally labour-intensive: a company must be able to prove that it is implementing all the requirements. This means that all steps must be traceable in great detail.

IEC 61508 is the basic functional safety standard, and discipline-specific detailed standards have since been derived from it for various sectors. The ISO 26262 standard focuses on road vehicles (Automotive Norm) and components that control driving functions. ISO 13849, on the other hand, applies to machine functions such as tippers, compactors and turntable ladders, which are mounted on vehicles.

EAO: Your expert partner for Human Machine Interfaces
Functional safety is by no means a new topic, and has already been applied in mechanical components to a certain extent. Striving for safe states is a fundamental requirement in product development. What's more, the first CAN bus systems were implemented in private vehicles as early as the late 1980s. It is important that companies now hone their awareness with respect to functional safety, and apply the standards that are required. At EAO, functional safety has been integrated into our development processes in the form of smart components. Customers are increasingly requesting components with defined safety levels. As expert partner, EAO has always thought from the perspective of its customers and as a result has ensured that they all have functional safety on their radar, as well as the related risks.

Series 09 Rugged CAN Keypads – Designed for E1 applications with functional safety.

Series 09 Rugged CAN Keypads for applications with functional safety
The Rugged CAN Keypads feature high reliability and are designed for functional safety in accordance with the EN ISO 13849 PL d and ISO 26262 ASIL B standards. These robust control units with flexible illumination are ideally suited for use in heavy duty and special vehicle applications.

Further information is available at www.eao.com/09

EAO Headquarters in Olten (Switzerland).
Errors and changes possible.

EAO Contact.
Your centre of excellence.

Headquarters

EAO Holding AG
Tannwaldstrasse 88
CH-4600 Olten
Telephone +41 62 286 92 00
info@eao.com

Manufacturing Companies

Switzerland
EAO AG
Tannwaldstrasse 88
CH-4600 Olten
Telephone +41 62 286 91 11
info@eao.com

EAO Systems AG
Tannwaldstrasse 88
CH-4600 Olten
Telephone +41 62 286 91 11
sales.esy@eao.com

China
EAO (Guangzhou) Ltd.
3/F, Block G4, South China
New Materials Innovation Park
31 Kefeng Road
Guangzhou Science City
CN-Guangzhou, PRC
Telephone +86 20 3229 0390
sales.ecn@eao.com

Germany
EAO Automotive GmbH & Co. KG
Richard-Wagner-Straße 3
DE-08209 Auerbach/Vogtland
Telephone +49 3744 8264 0
sales.esa@eao.com

North America
EAO Corporation
One Parrott Drive
Shelton
US-CT 06484
Telephone +1 203 951 4600
sales.eus@eao.com

Sales Companies

China
EAO (Guangzhou) Ltd.
3/F, Block G4, South China
New Materials Innovation Park
31 Kefeng Road
Guangzhou Science City
CN-Guangzhou, PRC
Telephone +86 20 3229 0390
sales.ecn@eao.com

EAO (Shanghai) Office
Rm.401, Lihpao Plaze,
NO.159 Shenwu Road,
Minhang District,
CN-Shanghai, 201106.
PRC
Telephone +86 21 6095 0717
sales.ecn@eao.com

France
EAO France SAS
Bâtiment Silex
15 rue des Cuirassiers
CS 33821
FR-69487 Lyon Cedex O3
Telephone +33 9 74 18 93 41
sales.efr@eao.com

Germany, Austria, Czech Republic, Poland, Slovakia
EAO GmbH
Langenberger Straße 570
DE-45277 Essen
Telephone +49 201 8587 0
sales.ede@eao.com

Hong Kong (Asia Pacific)
EAO (Far East) Ltd.
Unit A1, 1/F, Block A
Tin On Industrial Building
777 Cheung Sha Wan Road
Lai Chi Kok, Kln
HK-Hong Kong
Telephone +852 27 86 91 41
sales.ehk@eao.com

Italy
EAO Italia S.r.l.
Centro Direzionale Summit –
Palazzo D1
Via Brescia 28
IT-20063 Cernusco sul Naviglio (MI)
Telephone +39 029 247 0722
sales.eit@eao.com

Japan
EAO Japan Co. Ltd.
Net 1 Mita Bldg. 3F
3-1-4 Mita Minato-ku
JP-Tokyo 108-0073
Telephone +81 3 5444 5411
sales.ejp@eao.com

Netherlands, Belgium
EAO Benelux B.V.
Kamerlingh Onnesweg 46
NL-3316 GL Dordrecht
Telephone +31 78 653 17 00
sales.enl@eao.com

North America
EAO Corporation
One Parrott Drive
Shelton
US-CT 06484
Telephone +1 203 951 4600
sales.eus@eao.com

Switzerland
EAO Schweiz AG
Tannwaldstrasse 86
CH-4600 Olten
Telephone +41 62 286 95 00
sales.ech@eao.com

United Kingdom, Denmark, Finland, Ireland, Norway, Sweden
EAO Ltd.
Highland House
Albert Drive
Burgess Hill
GB-West Sussex RH15 9TN
Telephone +44 1444 236 000
sales.euk@eao.com

EAO_TA_Functional_Safety_V1.0/4.2021