Introduction

Technology Trends

- Hydraulics and Electronics belong together

Example: Electro / hydraulic circuit diagram of a mobile machine
Functional Safety and Diagnostics
Murphy:  
“Whatever can go wrong will go wrong, and at the worst possible time, in the worst possible way.”
Functional Safety and Diagnostics
Correspondingly the legal and standards situation has reacted to this development.
Functional Safety and Diagnostics

- Increasing of functionality and productivity means for the system and the system components:
  - higher complexity
  - higher safety requirements
  - more diagnostics

System / Application
Software
Sensors
Controllers
Visualization

Hydraulic
Functional Safety and Diagnostics

Standards, principles and implementation

- Relevant directives

**DO 178B / 254**
Example: Design Assurance Level DAL 2

**ISO 26262**
Example: Automotive SIL ASIL 2

**ISO 25119**
Example: Agricultural SIL AgSIL 2

**EN ISO 13849**
Example: Performance Level PL d

**IEC 61508**
Example: Safety Integrity Level SIL 2

**EN 15000**

- IEC 61508
- EN ISO 13849
- ISO 25119
- EN 15000
- ISO 26262
- DOE 178B / 254
- Relevant directives
The manufacturer confirms to comply with the following guidelines:

- Machinery Directive – 2006/42/EC
- Noise Emission Standards – 2000/14/EC
- Electromagnetic Compatibility Standards – 2004/108/EC
All machinery that are put in circulation in the European Economic Union, have to satisfy the requirements of the Machinery Directive.

Some key principles:
- The machinery has to be built in such a way that no person is exposed to a hazard during
  - Operation
  - Mounting/Service
  - Predictable misuse
- Principles for risk reduction
  - Elimination or minimization of risks as far as possible
  - Take protective measures against risks which cannot be eliminated
  - Information of users of remaining risks
- Controls need to be designed in such a way, that hazard situations are avoided, specifically considering:
  - Predictable usage scenarios and external influences
  - Defects in hardware or software
  - Errors in logic
  - Predictable misuse
Harmonized standards for Machinery Directive 2006/42/EC

EN ISO 13849 and other safety standards as a part of the machinery directive

Presumption of conformity: “Where products have been designed in accordance with suitable harmonized Standards, market surveillance authorities are obliged to assume that the essential requirements of the applicable directive(s) which are covered by these Standards have been fulfilled. The products are deemed to comply with the directives (presumption of conformity).”
Risk for the manufacturer

However, there is also a certain risk for the manufacturer: an accident which could have been avoided by following the EN ISO 13849-1, can turn into a problem for the manufacturer and the responsible persons involved.

Essential for the clarification of liability is the state of technology which is no longer represented by EN 954-1 based on deterministic approaches or the choice of the control architecture, but by the broader defined EN 13849.
In contrast to the civil Compensation Laws, in criminal law, the injuring party is always called to account personally, a corporate liability is not possible in this case. As, in general, the managing director and the technical director are out of responsibility, the investigations are often directed against the design engineers. "In many cases, it is difficult to find the guilty party for an accident." a prosecutor from Cologne said. “Often enough, there is sufficient suspicion of a criminal act – due to design faults or to non-conformity with the safety regulations. “

In civil right, it is very realistic that design engineers become personally liable. Still, the principle set up by the federal labour court applies that employees can only be made fully responsible in case of intentional act or gross negligence. Nevertheless, gross negligence, i.e. the ignorance of the most apparent things, is not very difficult to prove.
The most effective way to build in globally relevant safety is to design for standards like (EN) ISO 13849 and (EN) IEC 62601. Note that The EN ISO 13849 and IEC 62061 safety standards for machinery control are scheduled to merge into one global standard, IEC/ISO 17305, by 2016 (see cover story on page 20). Industrial equipment shipped to or from Europe must comply with one of these two standards. A U.S. court has held an OEM liable for building to international standards for EU machinery users, while using less stringent benchmarks for U.S. customers.
Legal Environment and Terminology
Current Standards: IEC 61508 und EN ISO 13849-1

- IEC 61508
- EN 954
- EN 13849
- IEC 62061
- ISO 26262
- ISO 25119

IEC 61508

Probabilism

EN 13849

Determinism

“Safety of Machinery“

Harmonized according to

Machinery Directive 2006/42/EC

Automotive

Agricultural

Machinery Industry
# Comparison ISO EN 13849-1 and IEC 62061

<table>
<thead>
<tr>
<th>Technology Type</th>
<th>EN ISO 13849-1</th>
<th>IEC 62061</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non electrical, e.g. hydraulics</td>
<td>Covered</td>
<td>Not covered</td>
</tr>
<tr>
<td>Electromechanics, e.g. relays, or non complex electronics</td>
<td>All architectures and up to PL = e</td>
<td>All architectures and up to SIL 3</td>
</tr>
<tr>
<td>Complex electronics, e.g. programmable</td>
<td>All architectures and up to PL = e</td>
<td>Up to SIL 3 when designed according to IEC 61508</td>
</tr>
<tr>
<td>Embedded software (SRESW)</td>
<td>Up to PL = e (PL = e without diversity: design according to IEC 61508-3, clause 7)</td>
<td>Design according to IEC 61508-3</td>
</tr>
<tr>
<td>Application software (SRASW)</td>
<td>Up to PL = e</td>
<td>Up to SIL 3</td>
</tr>
<tr>
<td>Combination of different technologies</td>
<td>Restrictions as above</td>
<td>Restrictions as above, non electrical parts acc. to EN ISO 13849-1</td>
</tr>
</tbody>
</table>
Functional Safety and Diagnostics
Standards, principles and implementation

Typical Implementation of the Standards / Regulations
**Functional Safety and Diagnostics**

- **Hazard and Risk analysis**

**First step**

List of machine functions
- Example -

<table>
<thead>
<tr>
<th>Machine function</th>
<th>Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H&amp;R Analysis</strong></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List of machine functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Driving functions</strong></td>
</tr>
<tr>
<td>1. Speed control (foot throttle)</td>
</tr>
<tr>
<td>2. F/N/R control (forward, neutral, reverse)</td>
</tr>
<tr>
<td>3. Indicator control</td>
</tr>
<tr>
<td>4. Transmission shift</td>
</tr>
<tr>
<td>5. Cruise control</td>
</tr>
<tr>
<td>6. Inch</td>
</tr>
<tr>
<td>7. Parking brake</td>
</tr>
<tr>
<td>8. Steering / auxiliary steering</td>
</tr>
<tr>
<td><strong>Release functions</strong></td>
</tr>
<tr>
<td>1. Safety lever</td>
</tr>
<tr>
<td>2. Road travel switch</td>
</tr>
<tr>
<td><strong>Work functions</strong></td>
</tr>
<tr>
<td>1. Lifting / lowering</td>
</tr>
<tr>
<td>2. Rotating</td>
</tr>
<tr>
<td>3. Telescopic function</td>
</tr>
<tr>
<td>4. Auxiliary attachments</td>
</tr>
<tr>
<td><strong>Automatic functions</strong></td>
</tr>
<tr>
<td>1. Parallel lift control</td>
</tr>
<tr>
<td>2. Continuous path control</td>
</tr>
<tr>
<td><strong>Further functions</strong></td>
</tr>
<tr>
<td>1. Fan drive speed control</td>
</tr>
<tr>
<td>2. Suspension functions</td>
</tr>
<tr>
<td>3. Levelling</td>
</tr>
</tbody>
</table>
Required risk minimisation and Performance Level:

Severity of injury:
- **S1** slight (usually reversible injury)
- **S2** serious (usually irreversible injury which may include death)

Frequency and / or duration of exposure to danger:
- **F1** rarely up to not very frequently and / or the time of exposure to danger is short
- **F2** frequently up to continuously and / or the time of exposure to danger is long

Probability of avoiding the exposure [P]
- **P1** possible under certain conditions
- **P2** rarely possible
Basic structure of a component or a system

Input / Sensor → Processing / Logic → Output / Actuator
Designated Architectures for Categories B, 1 and 2:

Architecture of **Category B and 1**
Design with “basic safety level”

- **I**: Input device e.g. Sensor
- **L**: Logic
- **O**: Output device e.g. Actuator

Architecture of **Category 2**
Design with “increased safety level”

- **I**: Input e.g. Sensor
- **L**: Logic
- **O1/O2**: Output e.g. Actuator
- **TE**: Test equipment
Designated Architectures for Categories 3 and 4:

Architecture of **Category 3**
Design with “increased safety level”

Architecture of **Category 4**
Design with “increased safety level”

I1, I2: Inputs e.g. Sensors
L1, L2: Logic
O: Outputs e.g. Actuator
Classification of the MTTFd values according to standard:

Total period: 3 up to 100 years:
- 3 up to 10 years = low
- 10 up to 30 years = medium
- 30 up to 100 years = high

MTTFd values exceeding 100 years will be considered with max. 100 years in their safety calculation

MTTFd is a measure for the quality of the component
Typical values according to practical experience:

| Component Type                                      | Basic and well-tried safety principles to EN ISO 13849-2:2003 | Other relevant standards | Typical values:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical components</td>
<td>Tables A.1 and A.2</td>
<td>—</td>
<td>MTTFd = 150</td>
</tr>
<tr>
<td>Hydraulic components</td>
<td>Tables C.1 and C.2</td>
<td>EN 982</td>
<td>MTTFd = 150</td>
</tr>
<tr>
<td>Pneumatic components</td>
<td>Tables B.1 and B.2</td>
<td>EN 983</td>
<td>B10d = 20,000,000</td>
</tr>
<tr>
<td>Relays and contactor relays with negligible load</td>
<td>Tables D.1 and D.2</td>
<td>EN 50205 IEC 61810 IEC 60947</td>
<td>B10d = 20,000,000</td>
</tr>
<tr>
<td>Relays and contactor relays with maximum load</td>
<td>Tables D.1 and D.2</td>
<td>EN 50205 IEC 61810 IEC 60947</td>
<td>B10d = 400,000</td>
</tr>
<tr>
<td>Proximity switches with negligible load</td>
<td>Tables D.1 and D.2</td>
<td>IEC 60947 EN 1088</td>
<td>B10d = 20,000,000</td>
</tr>
<tr>
<td>Proximity switches with maximum load</td>
<td>Tables D.1 and D.2</td>
<td>IEC 60947 EN 1088</td>
<td>B10d = 400,000</td>
</tr>
</tbody>
</table>

MTTFd = \( \frac{B_{10d}}{0.1 \cdot n_{op}} \)

\( n_{op} = \frac{d_{op} \cdot h_{op}}{t_{Zyklus}} \cdot 3600 \)

\( MTTF_d = \frac{1}{\lambda_d} \)
MTTFd HYDAC Electronic Products

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Products</th>
<th>HYDAC Electronic</th>
</tr>
</thead>
</table>

**Note:**

1 Mio h = 114 years

i.e., all MTTFd-Values are classified “high”

<table>
<thead>
<tr>
<th>MTTF</th>
<th>MTBF</th>
<th>MTTFd</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Mean Time To Failure]</td>
<td>[Mean Time Between Failures]</td>
<td>[Mean Time To Dangerous Failure]</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>HDA 3800</td>
<td>&gt; 2 Mio h</td>
<td>&gt; 2 Mio h</td>
</tr>
<tr>
<td>HDA 4000</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>HDA 7000</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>HDA 8000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>EDS 300</td>
<td>&gt; 2 Mio h</td>
<td>&gt; 2 Mio h</td>
</tr>
<tr>
<td>EDS 3000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>EDS 8000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>EDS 1700</td>
<td>&gt; 1,2 Mio h</td>
<td>&gt; 1,2 Mio h</td>
</tr>
<tr>
<td>EDS 4000</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>EDS 601</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>EDS 410</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>EDS 810</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>ETS 300</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>ETS 3000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>ETS 1700</td>
<td>&gt; 1,2 Mio h</td>
<td>&gt; 1,2 Mio h</td>
</tr>
<tr>
<td>ETS 4000</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>ETS 7000</td>
<td>&gt; 1,5 Mio h</td>
<td>&gt; 1,5 Mio h</td>
</tr>
<tr>
<td>TFP 100</td>
<td>&gt; 2 Mio h</td>
<td>&gt; 2 Mio h</td>
</tr>
<tr>
<td>EVS 3000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>HDA 5500</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>AS 1000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>HLB 1000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>ENS 3000</td>
<td>&gt; 750,000 h</td>
<td>&gt; 750,000 h</td>
</tr>
<tr>
<td>HMG 500</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
<tr>
<td>HMG 3000</td>
<td>&gt; 1 Mio h</td>
<td>&gt; 1 Mio h</td>
</tr>
</tbody>
</table>
Diagnostic Coverage

Indicator of how many dangerous failures/ outages are detected

\[ DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_d} \]

Outage rate: detected dangerous failures
Outage rate: all dangerous failures

Regulations for the medium DC for the entire system by approximation formula:

<table>
<thead>
<tr>
<th>Term</th>
<th>Value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>DC &lt; 60%</td>
</tr>
<tr>
<td>low</td>
<td>60% ≤ DC &lt; 90%</td>
</tr>
<tr>
<td>medium</td>
<td>90% ≤ DC &lt; 99%</td>
</tr>
<tr>
<td>high</td>
<td>99% ≤ DC</td>
</tr>
</tbody>
</table>

Formula for DCavg in Standard according to fig. 28

\[ DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + ... + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + ... + \frac{1}{MTTF_{dN}}} \]

Out of all DCs of the single components, the DC avg for the controller is defined.
## Diagnostic Coverage

<table>
<thead>
<tr>
<th>Output device</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring of outputs by one channel without dynamic test</td>
<td>0 % to 99 % depending on how often a signal change is done by the application</td>
</tr>
<tr>
<td>Cross monitoring of outputs without dynamic test</td>
<td>0 % to 99 % depending on how often a signal change is done by the application</td>
</tr>
<tr>
<td>Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)</td>
<td>90 %</td>
</tr>
<tr>
<td>Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)</td>
<td>99 %</td>
</tr>
<tr>
<td>Redundant shut-off path with no monitoring of the actuator</td>
<td>0 %</td>
</tr>
<tr>
<td>Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment</td>
<td>90 %</td>
</tr>
<tr>
<td>Redundant shut-off path with monitoring of the actuators by logic and test equipment</td>
<td>99 %</td>
</tr>
<tr>
<td>Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)</td>
<td>90 % to 99 %, depending on the application</td>
</tr>
<tr>
<td>Fault detection by the process</td>
<td>0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!</td>
</tr>
<tr>
<td>Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)</td>
<td>99 %</td>
</tr>
</tbody>
</table>
CCF - Common Cause Failures

Causes for outage of channel 1

CCF

Causes for outage of channel 2
In multi-channel controller structures starting from category 2, an observation of the CCF must be effected. This means, measures are to be taken so that both channels in a safety system can not break down due to a common cause.

For this purpose, there is a table of points in the EN 13849-1 standard.

Of 100 available points at least 65 points shall be reached.
Safety related parts of machine controls
Functional Safety and Diagnostics

Standards, principles and implementation

The achieved safety level is the result (balance) from the combination of the parameters:

- Architecture
- Reliability of used components
- Recognisability (diagnosibility) of safety relevant failures
Summary characteristics

- The achieved safety level (= PL) is the result of the combination of:
  - Architecture (= category)
  - Quality of components (= MTTFd)
  - Capability to detect safety relevant failures (= DC)
  - For safety functions of category 2 or higher CCF need to be considered
PL column chart according to EN ISO 13849-1 illustrates the relationship between PL, MTTFd, category and DC.
Example 1:

Performance Level “PLr c” for a machine function is required.

PL column chart according to EN ISO 13849-1 illustrates the relations between PL, MTTFd, category and DC.
PL column chart according to EN ISO 13849-1 illustrates the relations between PL, MTTFd, category and DC

Example 1:
Performance Level “PL c” for a machine function is required
Example for an „increased safety hydraulic design“
Sensors and Controllers for Applications with Increased Functional Safety
Functional Safety and Diagnostics
Standards, principles and implementation

Overview of control architectures (categories)

Kategorie B und 1:

Kategorie 2:

Kategorie 3

Achievable safety level

Costs

design for “normal safety level”

design with “increased safety level”
Functional Safety and Diagnostics

Sensors with increased Functional Safety and Diagnostics

- **Sensors for pressure, position and distance**

- **Pressure transducer** HDA 8000
  - Category 2
  - MTTFd: high (190 years)
  - DC: low (87%)
  - Safety level: PL d, SIL 2

- **Pressure transducer** HDA 4000
  - Category 3
  - MTTFd: high (976 years)
  - DC: low (84%)
  - Safety level: PL d

- **Position switch** HLS 100
  - Category 2
  - MTTFd: high (419 years)
  - DC: low (88%)
  - Safety level: PL d, SIL 2

- **Linear position sensor** HLT 1000
  - Category 2
  - MTTFd: high (83 years)
  - DC: low (91%)
  - Safety level: PL d, SIL 2

- **Valve position switch** HLS 200
  - Category 2
  - MTTFD hoch / high (110 Jahre/ years)
  - DC: medium (91%)
  - Safety level: PL d
Functional Safety and Diagnostics

Sensors with increased Functional Safety and Diagnostics

- Pressure transducer
Functional Safety and Diagnostics

Sensors with increased Functional Safety and Diagnostics

Linear position sensor, magnetostrictive
Functional Safety and Diagnostics

Sensors with increased Functional Safety and Diagnostics

- Function principle, standard version
Functional Safety and Diagnostics

Sensors with increased Functional Safety and Diagnostics

- Functional principle of a magnetostrictive sensor
  - version with increased functional safety and diagnosis
Functional Safety and Diagnostics

Sensors with increased Functional Safety and Diagnostics

- Functional principle of a magnetostrictive sensor
  - version with increased functional safety and diagnosis
Characteristics for HY-TTC 90 with PLd, Excerpt from TUV certificate

Architecture: Category 2

MTTFd: high
DC: low ⇒ PL d
Safety Controller Key Features

**Flexibility and Usability**
- Up to 96 I/Os with multiple configuration options
- Open programming environments i.e. C and CODESYS 3 SIL 2

**Safety & Availability**
- EN ISO 13849 PL d & IEC 61508 SIL 2 TÜV certified
- ISO 25119 AgPL d certifiable
- CODESYS Safety SIL 2
- CANOpen Safety
- Separation of safety / non-safety software
- Output shut-off in groups

**Connectivity**
- Up to 7 CAN interfaces
- Automatic baudrate detection
- Configurable CAN termination
- Ethernet

**Robustness**
- Automotive style aluminium housing for rough operating conditions
- Total current up to 60A

**Performance**
- Up to 32-bit 180MHz dual-core lockstep
- Floating-Point-Unit
- Up to 2.3MB RAM / 11 MB Flash
Safety I/O Module Key Features

Flexibility
- Extensive I/O set with small form factor
- 30 I/Os with multiple configuration options per pin
- 5 variants offer flexible building blocks

Safety
- EN ISO 13849 PL c certified
- CANopen Safety

Usability
- Easy integration and usage
- CANopen compliant
- Auto-baudrate-detection
- CAN termination configurable via connector pins
- Node-ID configuration via dedicated input pins

Robustness
- Automotive style aluminium housing for rough operating conditions
- High maximum current
Displays

Why Displays?

- Rising demand for visualization, driven by automotive and consumer industry
- Used for
  - Diagnostics
  - User Manuals
  - Configuration (Parameterization)
  - Video cameras

Target Applications
Displays Key Features

Features:
- High CPU Performance
- Fast Boot Up Time
- Excellent Sunlight Readability
- Robust and Easy to Clean
- Touch Screen
- Flexible graphical developer interface

Target Applications
Summary
Functional Safety and Diagnostics - Sensors, Controllers, Displays, Systems...

Pressure sensors
Controller
Displays
Linear position sensors
Angle sensors
Inclination sensors

ISO 26262
ISO 25119
EN ISO 13849
IEC 61508