innotec GmbH

Michael Kieviet
michael.kieviet@innotec-safety.com
“Industrie 4.0”

1. Revolution Mechanization (Use of Steam Engines)
2. Revolution Electricity (Use of Assembly Lines)
3. Automation (Use of Computers, PLCs)
4. ’0’ Information Technology (Cyber Physical Systems)
Cyber Physical Systems (CPS)

Data Warehouse

Individual product assembly specification

Assembling

Product

Physical environmental condition
CPS: Challenges for the Functional Safety

S1: Door switch
A2: Door lock
Door
S2: Light curtain
work direction
workpiece
S3: Emergency stop
S4: Light curtain
A1: Robotic arm
S5: Operating mode selector
S6: Enable switch
S7: Start
MS11: Muting sensor
MS12: Muting sensor
MS21: Muting sensor
MS22: Muting sensor
Table
Conventional safety functions

**SF 1**
- Emergency Push Button
  - PFH / MTTF...
- Control Unit
  - PFH / MTTF...
- Robotic drive
  - (Safe Stop 1)
  - PFH / MTTF...

**SF 2**
- Door Switch
  - PFH / MTTF...
- Control Unit
  - PFH / MTTF...
- Robotic drive
  - (Safely Limited Speed)
  - PFH / MTTF...
Roboter standards

- ISO 10218 – 1 Robots and robotic devices -- Safety requirements for industrial robots -- Part 1: Robots

- ISO 10218 - 2 Robots and robotic devices -- Safety requirements for industrial robots -- Part 2: Robot systems and integration

- ISO 13482:2014 Robots and robotic devices -- Safety requirements for personal care robots (e.g Household)
### IEC61800-5.2 safe drive function

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>STO</td>
<td>Safe Torque Off</td>
</tr>
<tr>
<td>SS1</td>
<td>Safe Stop 1</td>
</tr>
<tr>
<td>SS2</td>
<td>Safe Stop 2</td>
</tr>
<tr>
<td>SOS</td>
<td>Safe Operating Stop</td>
</tr>
<tr>
<td>SLA</td>
<td>Safety –Limited Acceleration</td>
</tr>
<tr>
<td>SLS</td>
<td>Safety-Limited Speed</td>
</tr>
<tr>
<td>SLT</td>
<td>Safety-Limited Torque</td>
</tr>
</tbody>
</table>
IEC61800-5.2 safe drive function

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLP</td>
<td>Safety-Limited Position</td>
</tr>
<tr>
<td>SLI</td>
<td>Safety-Limited Increment</td>
</tr>
<tr>
<td>SDI</td>
<td>Safe Direction</td>
</tr>
<tr>
<td>SMT</td>
<td>Safe Motor Temperature</td>
</tr>
<tr>
<td>SBC</td>
<td>Safe Brake Control</td>
</tr>
<tr>
<td>SCA</td>
<td>Safe Cam</td>
</tr>
<tr>
<td>SSM</td>
<td>Safe Speed Monitor</td>
</tr>
</tbody>
</table>
Safe Torque off, STO)

The drive stops without any break moment.
This is similar to IEC 60204-1, Category 0.
Safe stop 1, SS1

time monitored

\[ n \]

request \hspace{10cm} t_{n0} \text{STO}

\[ t \]
Safe stop 1, SS1) (Controlled break ramp)
Sicherer Stopp 2 (Safe stop 2, SS2) (time monitoring)
Safe operating stop (SOS)

The SOS-Function avoids, that the Motor rotats more than a amount of movements around the stop position. The inverter controls the motor and adjust the position also if external torques exist.
Safe operating stop (SOS)
Safely-limited acceleration, SLA

The SLA-Function avoids the exceeding of the acceleration limit of the motor.
Safe acceleration range, SAR

The SAR-Function avoids the exceeding of the acceleration limits of the motor.
Safely limited speed, SLS

The SLS-Function avoids the exceeding of the speed limit of the motor.
Safe speed range, SSR

The SSR-Function avoids the exceeding of the speed limits of the motor.
Safely-limited torque, SLT

The SLTA-Function avoids the exceeding of the torque or force limit of the motor.
Safe torque range, STR

The STR-Function avoids the exceeding of the torque or force range of the motor.
Safely-limited position, SLP

The SLP-Function avoids the exceeding of a defined position.
The SLI-Function avoids the exceeding of a defined increment.
Safe direction, SDI

The SDI-Function avoids that the motor runs in the wrong direction.
Safe motor temperature, SMT

The SLI-Function avoids the exceeding of a defined motor temperature
Safe brake control, SBC

The SBC-Function provide a safe output for control a mechanical break.
The SCA-Funktion provide a safe output signal in relation to the axle angle of the drive.
Sichere Geschwindigkeitsüberwachung (Safe speed monitor, SSM)

Die SSM-Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Motordrehzahl unterhalb eines festgelegten Grenzwertes liegt.
CPS: Additional technical risks

From the safety point of view some technical risks have been added. For instance:

- RFID – Tag will authorize the wrong assembling specification and also to the wrong safety parameter set.

- The access to the date ware house is enabled and the current the safety parameter set isn’t the right one for the product.

- The safety parameter set can be manipulated in the data ware house (conscious or unconscious).
Collaborating Robotic means

Interaction with humans being

ISO/DTS 15066
Robots and robotic devices – Safety requirements for industrial robots – Collaborative operation
(still under development)
4 Concepts of ISO/DTS 15066

- Manually controlled (Hand in Hand Concept)
- Automatic controlled during production cycle
- Stop the movement at specified boarder points
- Manually controlled via Joystick or Enable-Switch

**Safety Function**
Safely Limited Speed (PL d, Cat. 3)
4 Concepts of ISO/DTS 15066

- Speed and Distance controlled (e.g. by Laserscanner)

**Safety Function**
Safely Limited Speed (PL d, Cat. 3)
Safe Distances according EN ISO 13855
4 Concepts of ISO/DTS 15066

- Stop in any kind of distance-limit exceeding (e.g. by Laserscanner)

Safety Function
Safely Limited Speed (PL d, Cat. 3)
Safe Operating Stop
Safe Distances according EN ISO 13855
No automatic restart
4 Concepts of ISO/DTS 15066

- Speed and Distance controlled (e.g. by Laserscanner)

**Safety Function**

- Safely Limited Speed (PL d, Cat. 3)
- Safe Distances according EN ISO 13855
4 Concepts of ISO/DTS 15066

- Power an Force reduced (Intrinsic Safety)
- Max. 80W or 150N

Safety Function
Safely Limited Torque (PL d, Cat. 3)
Safely Limited Speed (PL d, Cat. 3)
Superposition in collaborating Systems

protection area

vehicle

arm speed

vehicle speed
Safety Functions

Safely Limited Speed (SLS)

Safe Operating Stop

rpm

SLS request

t

speed limit

rpm

SOS request

rpm

0

0+Δrpm

0-Δrpm

0

t
Combination of Safety Function

SF 1 Agent 1

Scanner
PFH / MTTF...

Control Unit
PFH / MTTF...

Vehicle drive
(SLS)
PFH / MTTF...

SF 1 Agent 2

Scanner
PFH / MTTF...

Control Unit
PFH / MTTF...

Vehicle drive
(SLS)
PFH / MTTF...

SF 2 Agent 1

Scanner
PFH / MTTF...

Control Unit
PFH / MTTF...

Vehicle drive
(SOS)
PFH / MTTF...

SF 2 Agent 2

Scanner
PFH / MTTF...

Control Unit
PFH / MTTF...

Vehicle drive
(SOS)
PFH / MTTF...
Combination of Safety Functions

Combinations of safety functions

SF1 A2 ^ SF2 A2

✓ SF2 A2 ^ SF2A1

✓ SF1 A1 ^ SF2A2

✓ SF1 A1 ^ SF2A1

SF: Safe Function
A: Agent
Collaborative Cluster

Data Ware House

Agent

Agent

Agent

Agent

Agent

Agent

Agent

Agent

Critical area

entry request

vertical communication

horizontal communication

Basic Safety Functions
Safety characteristic values

Safety Parameter Agent x
Thank you for your attention!