Application of CIP Safety for functional safety in motion applications - analysis of CIP Safety motion application use case scenarios

Ludwig Leurs  
Bosch Rexroth AG

Bob Hirschinger  
Rockwell Automation

Technical Track

www.odva.org
Agenda

Safety Architecture and Standards Review

Drive Safety System Architecture Option Review

Safety Controller Activated Drive Safety Function Overview and Application Use Cases

Safety Controller Executed Drive Safety Function Overview and Application Use Cases
Safety Controller Architecture

- Networked Safety
- Based on EtherNet/IP
- Safety Controller/PLC
  - Safety Task
- Safety I/O Devices
  - Emergency Stop
  - Safety Relays
  - Light Curtains
  - Safety Mats
  - Door Lock Control
- New Safety Device ➔ CIP Safety Drives
## Safety Standards

- There are many safety standards that provide guidelines for safety systems.
- CIP Safety Drive Profile design focuses on EN61800-5-2, which defines Safety Function requirements for adjustable speed drive systems.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 13849-1</td>
<td>Safety related parts of control systems: Describes the categories, require</td>
</tr>
<tr>
<td></td>
<td>ments, functional characteristics, and general principles for design</td>
</tr>
<tr>
<td>IEC 61508</td>
<td>Generic standard covering the safety lifecycle of electrical/ electronic/</td>
</tr>
<tr>
<td></td>
<td>programmable electronic systems. Facilitate development of application sector</td>
</tr>
<tr>
<td></td>
<td>standards. Risk assessment for safety functions &amp; safety integrity levels</td>
</tr>
<tr>
<td>IEC 60204-1</td>
<td>Electrical Equipment of Industrial Machines: Defines safety related</td>
</tr>
<tr>
<td></td>
<td>conventional functions, stopping categories, and operation during</td>
</tr>
<tr>
<td></td>
<td>emergency situations</td>
</tr>
<tr>
<td>IEC 61800-5-2</td>
<td>Safety requirements and functional safety for adjustable speed drive</td>
</tr>
<tr>
<td>IEC 62061</td>
<td>Standard which is implementation of IEC 61508 specifically for machinery</td>
</tr>
<tr>
<td></td>
<td>sector including functional safety and management procedures to achieve</td>
</tr>
<tr>
<td></td>
<td>functional safety by design</td>
</tr>
<tr>
<td>NFPA-79</td>
<td>National Fire Protection Agency Electrical Standard for Industrial</td>
</tr>
<tr>
<td></td>
<td>Machinery: Covers electric/electronic equipment or systems supplied as</td>
</tr>
<tr>
<td></td>
<td>part of industrial machinery or mass production industrial equipment that</td>
</tr>
<tr>
<td></td>
<td>will promote safety to life and property</td>
</tr>
<tr>
<td>OSHA 1910.217(b)(13)</td>
<td>Occupational Safety and Health Administration: Addresses control</td>
</tr>
<tr>
<td></td>
<td>reliability</td>
</tr>
</tbody>
</table>
EN61800-5-2 Drive Safety Functions

- EN61800-5-2 provides high level functional description of drive safety functions
- These are the safety functions that are targeted for CIP Safety Drive Profile support

Functionality Grouping
- Disconnect Torque generating power to the motor (STO)
- Safe stop (i.e. SS1, SS2)
- Safe speed monitoring (i.e. SSM)
- Safe acceleration monitoring (i.e. SLA)
- Safe torque monitoring (i.e. SLT)
- Safe position monitoring (i.e. SLP)
- Safe brake control (i.e. SBC)

<table>
<thead>
<tr>
<th>Functions</th>
<th>Description</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 Operational Stop</td>
</tr>
<tr>
<td>SLA</td>
<td>Safe Limited Acceleration</td>
</tr>
<tr>
<td>SAR</td>
<td>Safe Acceleration Range</td>
</tr>
<tr>
<td>SLS</td>
<td>Safe Limited Speed</td>
</tr>
<tr>
<td>SSR</td>
<td>Safe Speed Range</td>
</tr>
<tr>
<td>SLT</td>
<td>Safe Limited Torque</td>
</tr>
<tr>
<td>STR</td>
<td>Safe Torque Range</td>
</tr>
<tr>
<td>SLP</td>
<td>Safe Limited Position</td>
</tr>
<tr>
<td>SLI</td>
<td>Safe Limited Position Increase</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>
Drive Safety Function Examples

**STO (Safe Torque Off)**
- Stop Request
- Wait Stop Delay
- Disable Motor Power

**SS1 (Safe Stop 1)**
- Stop Request
- Wait Stop Monitoring Delay
- Monitor Decel Until Standstill
- Disable Motor Power

**SLS (Safe Limited Speed)**
- Safe Limited Speed Request
- Wait Stop Monitoring Delay
- Monitor Speed < Safe Speed Limit
Drive Safety System Architecture Options

**OPTION 1**
Drive safety I/O activated drive safety functions

**OPTION 2** 
Detail & application use case examples focus
Safety controller activated drive safety functions

**OPTION 3**
Safety controller configured & activated drive safety functions

**OPTION 4** 
Detail & application use case examples focus
Safety controller executed drive safety functions

<table>
<thead>
<tr>
<th>Safety Network</th>
<th>Safety I/O</th>
<th>Drive Safety</th>
<th>Drive Safety</th>
<th>Motion Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Required</td>
<td>Owner</td>
<td>Function Activation</td>
<td>Config Source</td>
<td>Command</td>
</tr>
<tr>
<td>Option 1</td>
<td>No</td>
<td>Drive</td>
<td>Drive</td>
<td>Drive</td>
</tr>
<tr>
<td>Option 2</td>
<td>Yes</td>
<td>Safety Controller</td>
<td>Safety Controller</td>
<td>Drive</td>
</tr>
<tr>
<td>Option 3</td>
<td>Yes</td>
<td>Safety Controller</td>
<td>Safety Controller</td>
<td>Safety Controller</td>
</tr>
<tr>
<td>Option 4</td>
<td>Yes</td>
<td>Safety Controller</td>
<td>Safety Controller</td>
<td>Controller</td>
</tr>
</tbody>
</table>
Safety Controller Activated Drive Safety Functions (Option 2 Architecture)

- Drive safety configuration is stored in the drive
  - Use case: preconfigured safety functions
- Safety function (SF) activation is performed in the safety controller
  - Safety IO owned by Safety Controller
  - SF activation transmitted via network
- SF execution is performed in the drive
  - Safety functions are controlled locally
- Safety Controller safety input and safety output network connection to the drive(s)
Safety modes for Drive operation

- Normal operation
- Safe stop 1 (Emergency stop)
- Special mode "safe standstill"
- Special mode "safe motion (1-n)"
# Safety modes and functions

<table>
<thead>
<tr>
<th>Operating state</th>
<th>Safety Functions</th>
<th>Mode Selector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal mode</td>
<td>Safe direction&lt;br&gt;Safe maximum speed&lt;br&gt;Safely-limited position</td>
<td>Normal mode select</td>
</tr>
<tr>
<td>Safe standstill</td>
<td>Safe stop 1&lt;br&gt;Safe stop 2&lt;br&gt;Safe brake control</td>
<td>Special mode select</td>
</tr>
<tr>
<td>Emergency stop</td>
<td>Safe stop 1</td>
<td>Emergency stop button</td>
</tr>
<tr>
<td>Safe motion</td>
<td>Safely-limited speed&lt;br&gt;Safe direction&lt;br&gt;Safely-limited increment&lt;br&gt;Safely-monitored position&lt;br&gt;Safe maximum speed&lt;br&gt;Safely-limited position</td>
<td>Special mode select + enabling control button</td>
</tr>
</tbody>
</table>
Benefits - Safety Controller Activated Drive Safety Functions (Option 2 Architecture)

- Safety functions pre-configured and pre-tested without a safety controller
- Easy migration path between option 1 (safety I/O hardwired to the drive) and option 2
- Less CPU power needed in the safety controller. Valuable in machines using a large number of safe drives
- Less data used for safety communication.
  - Less load on the communication interface
  - Less bandwidth on network used
  - Relevant in applications using a large number of safe drives
- Shortest possible reaction time to events exceeding limits. Especially for hydraulic applications this is in many cases the only possible solution
Use Case - Single Axis Press-fit Module

- Independent axis configuration
- Flexible system integration
Use Case - Woodworking Machinery

- Speed limit monitored in drive → fast reaction time
- Example shows separate safety controller
  - Easily implemented using CIP Safety
Use Case - Printing Machine

- Speed limit monitored in drive → fast reaction time
- Group select enables flexible safety solution for a limited number of monitoring combinations
  - E.g. Changing print plates, speed limit depends on direction of motion
Safety Controller Executed Drive Safety Functions (Option 4 Architecture)

- Drive safety configuration is stored in the safety controller
  - Minimal safety configuration required

- Safety function activation is performed in the safety task
  - User safety task application program with embedded safety instructions
  - Library of drive safety instructions for a range of safety functions

- Safety function execution is performed in the safety controller – Except STO
  - Runtime execution of the safety functions is managed in the safety controller
  - Drive safety status data is used in the instruction runtime

- Safety Controller safety input and safety output network connection to the drive(s)
Drive Safety Instructions

- Safe Torque Off
- Safe Brake Control
- Safe stop
  - i.e. SS1
- Safe speed monitoring
  - i.e. SSM
- Safe acceleration monitoring
  - i.e. SLA
- Safe torque monitoring
  - i.e. SLT
- Safe position monitoring
  - i.e. SLP

#### Table: Parameter and Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SS1$</td>
<td>This output signifies that the monitor sequence is active. It will energize when the initialization of the instruction has completed after the Trigger transitions from ON (1) to OFF (0). It will stay energized until the process completes or a fault occurs.</td>
</tr>
<tr>
<td>$SS1$ Requested</td>
<td>This output is energized when Speed Input A and Speed Input B are both below the Standstill Speed configuration value. This output will continue to operate until a reset or a fault occurs.</td>
</tr>
<tr>
<td>Below Threshold</td>
<td>This output is energized when the Reset input needs to be toggled to restart the instruction. This can occur with Restart Type Manual after the monitor sequence completes and the Trigger is returned to the ON (1) state, or when a fault is present, or when Cold Start Type Manual is chosen.</td>
</tr>
<tr>
<td>Fault Present</td>
<td>This output is energized when a fault occurs and will stay energized until the fault is cleared and the Reset input transitions from OFF (0) to ON (1).</td>
</tr>
</tbody>
</table>
Safe Limited Speed Example

- SLS instruction is executed in the safety task
  - Safety task logic enables SLS instruction

- SLS request handshake received by the standard task
  - Request to command drive to SLS setpoint.

- Safety task executes SLS monitoring function
  - As defined by SLS instruction input parameters -> Monitoring delay, safe speed limit, speed tolerance, discrepancy time
  - Safety feedback data from the drive (single or dual channel position, speed, acceleration)

- If a SLS fault occurs a STO activation request is sent to the drive
Benefits - Safety Controller Executed Drive Safety Functions (Option 4 Architecture)

- Single software package for managing safety
  - configuration, programming, commissioning, diagnostics, maintenance
  - safety configuration is unified in the safety controller for all drives
- Flexible, centralized safety function execution supports complex safety logic
- Coordinated safety function execution for an unlimited number of drives
- Runtime calculated or operator entered safety function parameters
  - i.e. speed, acceleration, torque, position limit setpoints
- Support for safe stopping and safe limiting functions on drives that only support STO
- “Path” based safe functions
  - i.e. robot TCP safety monitoring which require multi-axis kinematic functions
Use Case – SLS Wind/Unwind Roll

- SLS monitoring of the surface speed on a Wind/Unwind roll
Solution

1. Open guard door input detected (safety task)
2. SLS setpoint is calculated using the analog inputs for roll diameter calculation – one time event or continuous (safety task)
3. SLS request with calculated setpoint handshake (safety task/standard task)
4. Drive ramped to speed < SLS setpoint (standard task)
   SLS instruction is executed (safety task)
5. > monitoring delay time out & speed exceeds the SLS setpoint = fault present
   output is set & STO activation request (Safety Task)
Use Case– Coordinated Web SS1

Coordinated safe line stop (SS1)
Solution

1. Line stop safety switch input detected (safety task)
2. SS1 request handshake (safety task/standard task)
3. Line master axis ramped stop is initiated – drives 1-4 follow (standard task)
Solution

4. SS1 monitoring instruction is executed for each drive (safety task)

5. STO activation request @ Standstill speed for each drive (safety task)
## Conclusion

- Drives with network safety connection support are a key component in emerging safety controller based safety architectures.
- Recently published Safety Motion Device Profile addresses critical need for a networked “Safety Drive” CIP Safety standards
- Reviewed Option 2 (Drive based) and Option 4 (Safety controller based) architectures and use case examples

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Option 2</th>
<th>Option 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration / Parameterization</td>
<td>Controller and each device separately</td>
<td>Controller only</td>
</tr>
<tr>
<td>Multi-axis kinematics (TCP)</td>
<td>Not possible</td>
<td>Possible</td>
</tr>
<tr>
<td>Safety limit setpoints</td>
<td>15</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Dynamic safety limit calculation</td>
<td>Not possible</td>
<td>Possible</td>
</tr>
<tr>
<td>Drive functionality</td>
<td>STO, safe stop, safe limiting functions</td>
<td>STO</td>
</tr>
<tr>
<td>Safety feedback</td>
<td>drive primary and auxiliary port connected safety feedback devices</td>
<td>Drive primary and auxiliary port safety feedback devices and/or local or network connected safety feedback</td>
</tr>
<tr>
<td>Safety PLC CPU power</td>
<td>Low</td>
<td>Medium to high - increases with number of axes</td>
</tr>
<tr>
<td>Safety response time</td>
<td>&lt;1ms</td>
<td>&gt;10ms</td>
</tr>
<tr>
<td>Network bandwidth</td>
<td>Low</td>
<td>Medium to High</td>
</tr>
</tbody>
</table>