CIP Safety for Drives Agenda

Safety Controller/PLC Safety Solution
Architecture Overview

EN61800-5-2 Drive Safety Function Review

Drive Safety System Architecture Option
Review

CIP Safety Safe Motion Sub-Committee
Deliverables
Range of Safety Systems – Simple to Complex
## Simple Vs. Complex Systems

<table>
<thead>
<tr>
<th>Simple = Relay Focused</th>
<th>Complex = Safety Controller/PLC Focused</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Achieving CAT 3 on small simple systems can be cost effective and relatively easily achieved without the use of a safety PLC</td>
<td>1. Achieving CAT 3 on a complex system is more difficult but can be made simpler by utilizing a safety controller/PLC.</td>
</tr>
<tr>
<td>2. Hardwired safety devices with fixed or locally managed safety configuration</td>
<td>2. Safety controller/PLC is a scalable solution that is easily, quickly modified when upgrades are desired</td>
</tr>
<tr>
<td>3. Modifications Difficult</td>
<td>3. Wide range of networked safety devices</td>
</tr>
<tr>
<td>4. Limited Special Functions</td>
<td>4. Many Special functions Including library for numerous applications</td>
</tr>
<tr>
<td>5. Limited Machine states / Zone Control</td>
<td>5. Unlimited machine states and Zones</td>
</tr>
<tr>
<td>8. Single Panel Limited distance</td>
<td>8. Long lines, Multi-panel / multi controller</td>
</tr>
<tr>
<td>9. Redundant to Control system</td>
<td>9. Reuse infrastructure of control system</td>
</tr>
<tr>
<td>10. Panel space many components</td>
<td>10. Reduced component count (space savings)</td>
</tr>
<tr>
<td>11. Start Up / Check Out can be complex</td>
<td></td>
</tr>
</tbody>
</table>
Safety Control System Options

Safety Controllers/PLCs - Functionality
- Certified up to SIL 3 / Cat 4
- IEC 61511 Programming
- Safety Specific Instructions
- Standard Networking Options
- Local or Distributed Safety I/O
- Safety Networking Options
- Discrete, Analog & High Speed Counter I/O
- Networked Drive safety control

Safety Relays - Functionality
- Certified to Cat 4
- Electromechanical or Electronic
- Dedicated or Expandable
- Application Specific Units - Mats, Light Curtains
- Stand-alone safety drives
Typical Safety Controller/PLC System

- Fully programmable with safety task support
- Wide range of safety instruction support
  - Basic Logic
  - Dual channel I/O
  - Muting control
  - Safety mat
  - Drive safety
  - Application specific
- Network connectivity for a broad range of standard and safety devices
Typical Safety Controller/PLC System

- Full programmable with safety task support
- Wide range of safety instruction support
- Dual channel
- Muting control
- Safety mat
- Drive safety
- Application specific
- Network connectivity for a broad range of standard and safety devices

Networked Safety Drives are a common device used in Safety Controller/PLC based safety solutions

CIP Safety Drive Safety Profile standards are under development for use on networks that deploy CIP Safety

CIP Safety Profiles:
- Discrete safety I/O (Available)
- Analog safety I/O (Available)
- Drive safety (May 2013)
Safety Standards

- There are a number of safety standards that provide guidelines for safety systems
- EN61800-5-2 provides safety 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, requirements, functional characteristics, and general principles for design</td>
</tr>
<tr>
<td>IEC 60204-1</td>
<td>Electrical Equipment of Industrial Machines: Defines safety related conventional functions, stopping categories, and operation during emergency situations.</td>
</tr>
<tr>
<td>IEC 61800-5-2</td>
<td>Safety requirements and functional safety for adjustable speed drive systems</td>
</tr>
<tr>
<td>IEC 62061</td>
<td>Standard which is implementation of IEC 61508 specifically for machinery sector including functional safety and management procedures to achieve functional safety by design</td>
</tr>
<tr>
<td>NFPA-79</td>
<td>National Fire Protection Agency Electrical Standard for Industrial Machinery: Covers electric/electronic equipment or systems supplied as part of industrial machinery or mass production industrial equipment that 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 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 feed to the motor (STO)
- Safe stop (i.e. SS1)
- Safe speed monitoring (i.e. SLS)
- 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 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>
Safety Function Examples

**STO**
- Stop Request
- Wait Stop Delay
- Disable Motor Power

**SS1**
- Stop Request
- Wait Stop Monitoring Delay
- Monitor Decel Until Standstill
- Disable Motor Power

**SLS**
- Safe Limited Speed Request
- Wait Stop Monitoring Delay
- Monitor Speed < Safe Speed Limit
Drive Safety Core

- Manages drive safety functions
- Dual channel safety I/O interface
- Primary and secondary motor/load feedback interface
- Dual redundant processor safety core
- Gate driver interface to disable torque producing current to the motor
- Safety input/output network connection support
- Firmware support for a range of safety functions
Drive Safety System Architecture Options

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

**OPTION 2**
Safety controller activated drive safety functions

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

**OPTION 4**
Safety controller executed drive safety functions

<table>
<thead>
<tr>
<th>Network Safety Connection Required</th>
<th>Safety I/O Owner</th>
<th>Drive Safety Function Activation</th>
<th>Drive Safety Config Source</th>
<th>Motion Profile Command</th>
</tr>
</thead>
<tbody>
<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>Drive</td>
</tr>
<tr>
<td>Option 4</td>
<td>Yes</td>
<td>Safety Controller</td>
<td>Safety Controller</td>
<td>Controller</td>
</tr>
</tbody>
</table>
Hardwired Drive Safety (Option 1)

- Safety network connection not required
- Safety functions are managed in the drive
  - EN61500-5-8 and safety I/O sequencing
- Safety configuration is stored in the drive
  - Local configuration tool with signature management
  - Drive specific and canned safety functions
- Safety I/O is connected to the drive
  - Safety function activation (input)
  - Safety device status monitoring (input)
  - Drive safety status (output)
  - Safety device control (output)
- Considerations
  - Safety network connection is not required
  - Limited “general” safety functions
  - Locked safety configuration (limited drive setpt control)
  - Extra/redundant wiring
  - Limited support for advanced safety functions
    - Machine states and zone control
    - Coordinated line control
    - Complex safety logic
Safety Controller Activated Safety Functions (Option 2)

- **Safety network connection required**
- **Safety functions are managed in the drive**
  - EN61500-5-8
- **Safety configuration is stored in the drive**
  - Local configuration tool with signature management
- **Safety Controller**
  - Manages all safety I/O – local and distributed
  - Activates drive safety functions & monitors drive safety status
  - User programmable safety logic with access to broad range of safety instructions and safety devices
- **Considerations**
  - Safety network connection is required
  - Broad range of “general” safety functions via safety controller
  - Locked drive safety configuration with limited drive setpt control
  - Broad support for advanced safety functions
    - Machine states and zone control
    - Coordinated line control
    - Runtime “configured” safety functions
Safety Controller Configured and Activated Safety Functions (Option 3)

- **Safety network connection required**
- **Safety functions are managed in the safety controller (Except STO)**
  - EN61500-5-8
- **Safety configuration is stored in the drive**
  - Local configuration tool with signature management
- **Safety Controller**
  - Manages all safety I/O – local and distributed
  - Activates drive safety functions & monitors safety status
  - User programmable safety logic with access to broad range of safety instructions and safety devices
- **Considerations**
  - Safety network connection is required
  - Broad range of “general” safety functions via safety controller
  - Programmable drive safety set-point control – managed in the safety controller
  - Broad support for advanced safety functions
    - Fully programmable drive safety function setpt control
    - Machine states and zone control
    - Coordinated line control
    - Runtime “configured” safety functions
Safety Controller Executed Drive Safety Functions (Option 4)

- Safety network connection required
- Safety functions are managed in the drive
  - EN61500-5-8
- Safety configuration is stored in the safety controller
  - Via safety application program parameters
- Safety Controller
  - Manages all safety I/O – local and distributed
  - Executes drive safety functions using drive safety status data
  - User programmable safety logic with access to broad range of safety instructions and safety devices
- Considerations
  - Safety network connection is required
  - Broad range of “general” and “drive” safety functions via safety controller
  - Broad support for advanced safety functions
    - Fully programmable drive safety function execution
    - Machine states and zone control
    - Coordinated line control
    - Runtime “configured” safety functions
Option 2 – Light Curtain SS1 Application Example

- **Drive SS1 stop request management**
  - Safety task application code recognizes and processes SS1 stop request
  - Light curtain transition = SS1 request to drive 1 through drive 4 via network safety CIP Safety input connection safety function activation object

- **SS1 stop management**
  - SS1 request is received and managed by the drive(s) safety core
  - SS1 stop as configured with stop monitoring delay, stop delay, deceleration tolerance, standstill speed parameters
  - Drive safety status returned via network safety output connection CIP Safety drive safety status object
  - Drive safety status is monitored in the Safety Controller safety task application code
  - Additional functions can be executed as defined in the Safety Controller safety task application code
Option 4 – Safe Coordinated Line Stop with SS2 Application Example

**Line Stop request management**
- Safety task application code recognizes and processes safe coordinated line stop request
- Line Stop input transition = coordinated line stop, SS2 monitoring request for drive 1 through drive 4
- Event sent to standard task – coordinated line stop request

**Coordinated line stop management**
- Virtual axis is ramped to a stop in the standard task application code
- Drive 1 through drive 4 are geared to the virtual axis and will follow...coordinated line stop

**SS2 drive monitoring**
- Safety task application code provides SS2 monitoring of drive 1 through drive 4
- SS2 instruction per drive with appropriate parameters - stop monitoring delay, stop delay, deceleration tolerance, standstill speed parameters
- Drive speed/position feedback is provided for use in the safety task application code SS2 via network safety output connection CIP Safety feedback object
CIP Safety Safe Motion Sub-Committee

- Industry brief released 4/2012
  - New area of technical investigation – “Safe Motion”
  - CIP Safety Safe Motion Sub-committee formed
- CIP Safety Safe Motion Sub-committee goals
  - Develop “Drive Safety Profile(s)”
  - To be voted on by May 2013
  - Published in the fall 2013 CIPSE edition
- Focus on the option 2 architecture
  - Safety function activation and drive safety status monitoring
- Deliverables include:
  - Data model for drives safety
    - Object interface and data assembly definition
    - Device profile
- CIP Safety Profiles
  - Discrete I/O (Available Today)
  - Analog I/O (Available Today)
  - Drive Safety (Fall 2013 CIPSE edition)
Option 2 Object Concepts

Drive Safety Function Activation

<table>
<thead>
<tr>
<th>Basic Control Word (Safety Function Activation) - Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Res</td>
</tr>
</tbody>
</table>

Drive Safety Status

<table>
<thead>
<tr>
<th>Basic Status Word (Safety Function Status) - Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Res</td>
</tr>
</tbody>
</table>

Drive Safety Feedback

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Description of Attribute</th>
<th>Semantics of Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Time</td>
<td>ULINT</td>
<td>System Time when Feedback Position was sampled</td>
<td>Nanoseconds (CIP Sync absolute)</td>
</tr>
<tr>
<td>Feedback Position</td>
<td>DINT</td>
<td>Actual position of the feedback device</td>
<td>Feedback Counts</td>
</tr>
<tr>
<td>Feedback Velocity</td>
<td>REAL</td>
<td>Actual filtered velocity</td>
<td>Feedback Units / Sec</td>
</tr>
<tr>
<td>Feedback Acceleration</td>
<td>REAL</td>
<td>Actual filtered acceleration</td>
<td>Feedback Units / Sec²</td>
</tr>
</tbody>
</table>

Diagram of Drive Safety Feedback
Conclusion

• There is increasing adoption of flexible safety solutions using a safety controller/PLC with networked safety device connectivity
• A drive with safety core and network safety connection is a critical safety device in this type of safety solution
• The EN61800-5-2 provides a comprehensive list of drive safety functions
• Four different safety architectures can be considered based on safety network connection support and drive safety function execution and status monitoring approach
• A CIP Safety “safe motion” sub-committee has been formed to develop a safe drive profile
  • Targeted for publication in the Fall 2013 CIPSE
  • Applicable to any network that deploys CIP Safety – including SERCOS III and CIP Networks (EtherNet/IP, DeviceNet)
  • Focus on option 2 drive safety architecture
    • Drive Safety function activation
    • Drive Safety status monitoring