
# CIP Safety For Drives

Pascal Hampikian
Schneider Electric

Bob Hirschinger
Rockwell Automation

Ludwig Leurs
Bosch Rexroth

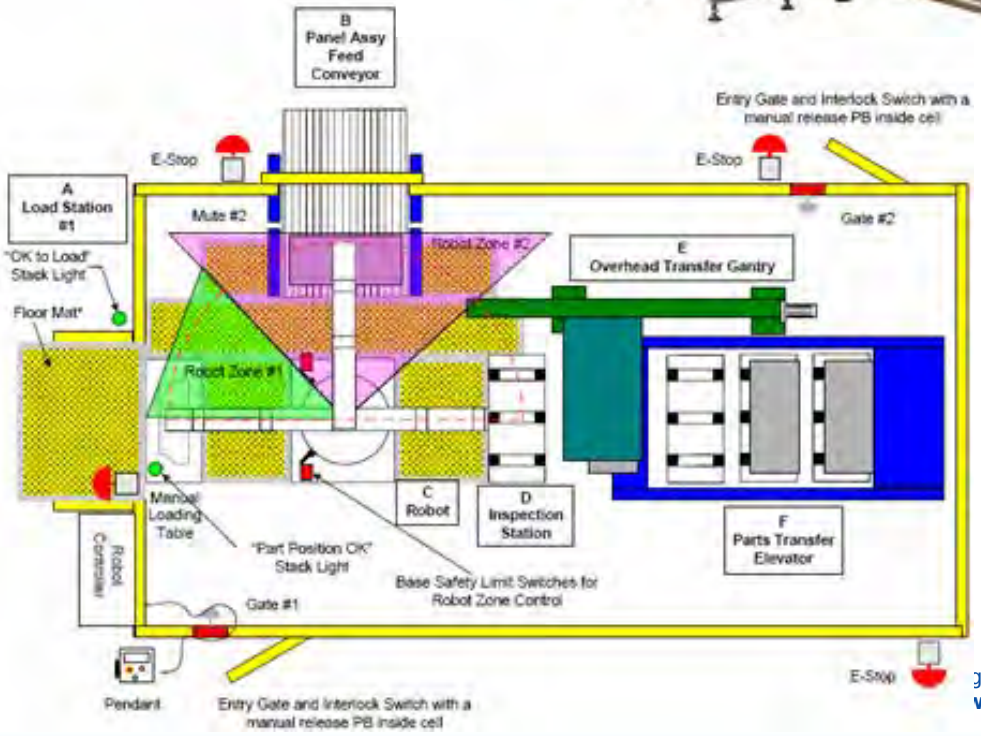
## Technical Track

www.odva.org

# 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

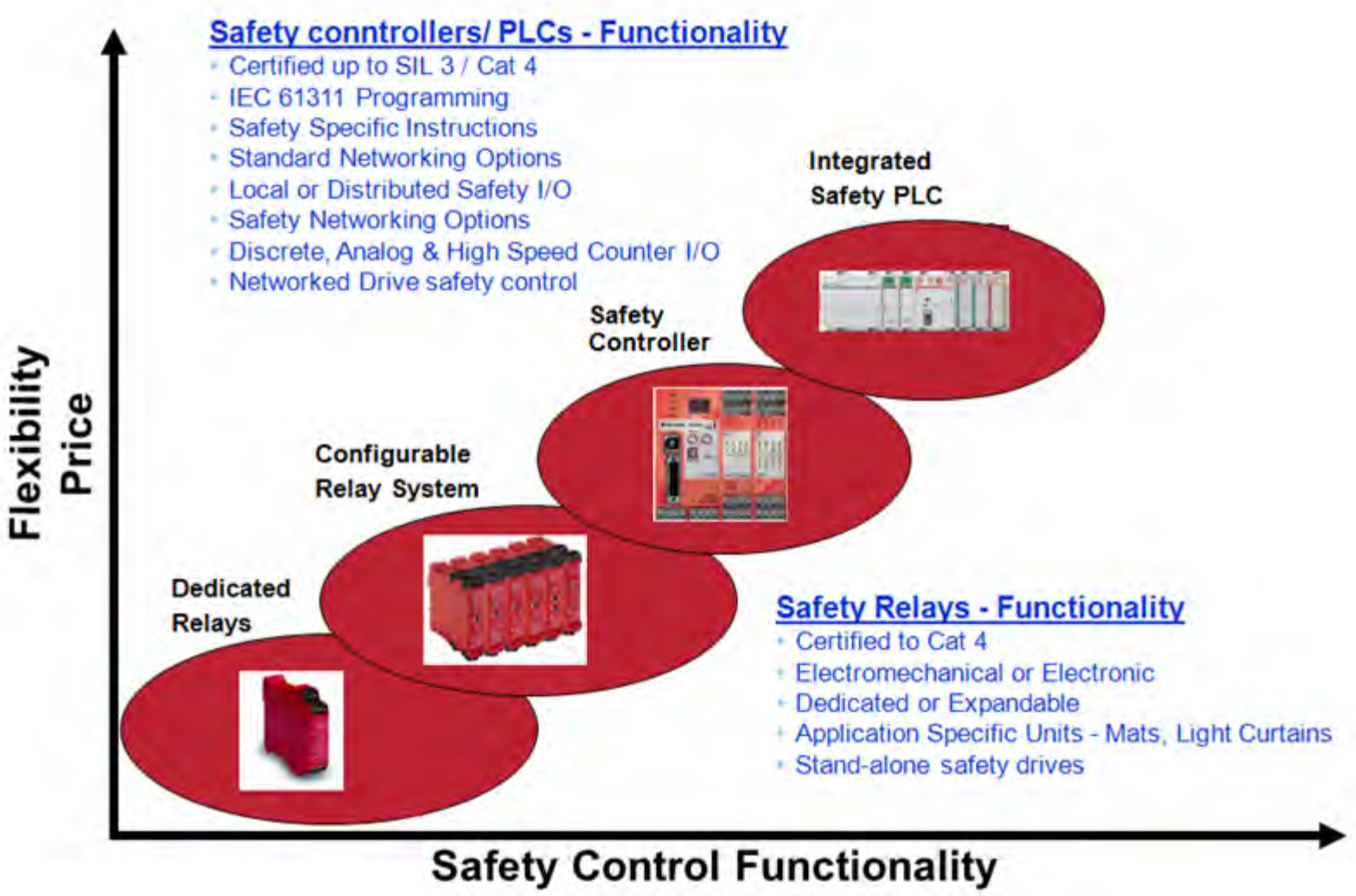
## Simple = Relay Focused

1. Achieving CAT 3 on small simple systems can be cost effective and relatively easily achieved without the use of a safety PLC
2. Hardwired safety devices with fixed or locally managed safety configuration
3. Modifications Difficult
4. Limited Special Functions
5. Limited Machine states / Zone Control
6. Hard Wired Diagnostics / LEDS Only
7. Home Run Wiring Device to Relay Inputs & Actuators
8. Single Panel Limited distance
9. Redundant to Control system
10. Panel space many components
11. Start Up / Check Out can be complex

## Complex = Safety Controller/PLC Focused

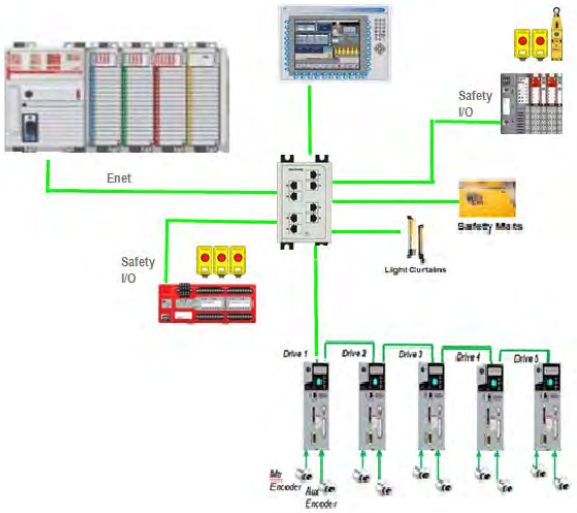
1. Achieving CAT 3 on a complex system is more difficult but can be made simpler by utilizing a safety controller/PLC.
2. Safety controller/PLC is a scalable solution that is easily, quickly modified when upgrades are desired
3. Wide range of networked safety devices
4. Many Special functions Including library for numerous applications
5. Unlimited machine states and Zones
6. Extensive diagnostics via HMI
7. Wire to nearest I/O Node
8. Long lines, Multi-panel / multi controller
9. Reuse infrastructure of control system
10. Reduced component count (space savings)

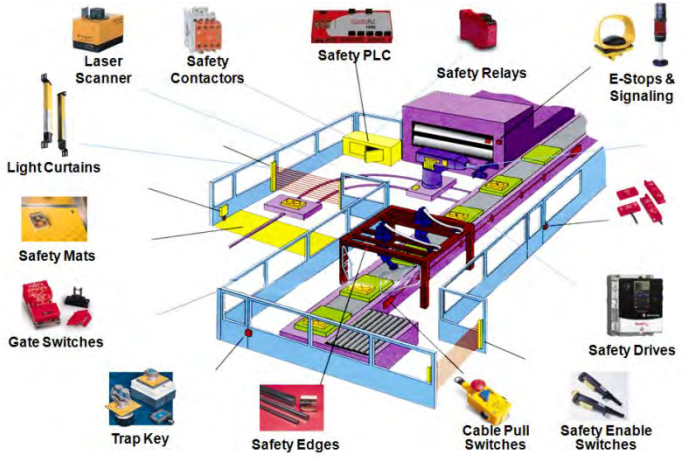
# Safety Control System Options

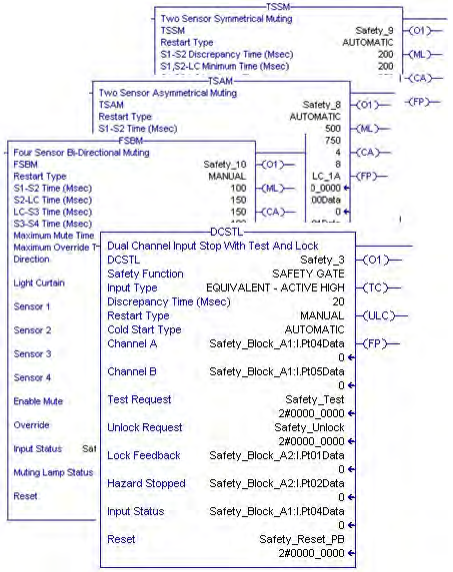


# Typical Safety Controller / PLC System

- **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

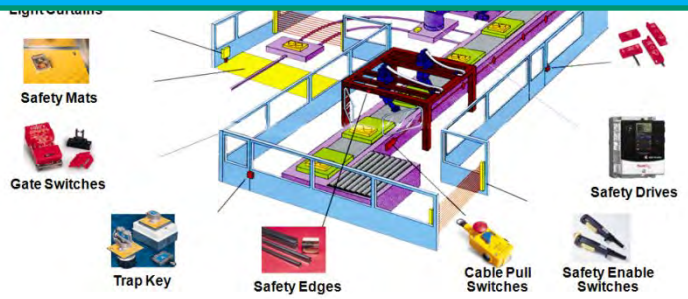
- **Full programmable with safety task support**
- **Wi**
-

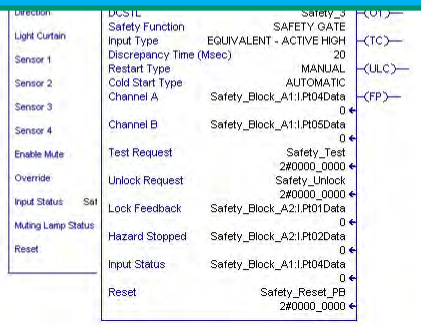

***Networked Safety Drives are a common device used in Safety Controller / PLC based safety solutions***

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

***<u>CIP Safety Profiles:</u>***

| | |
|---|---|
| ***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

| Standard | Relevance |
|---|---|
| ISO 13849-1 | Safety related parts of control systems: Describes the categories, requirements, functional characteristics, and general principles for design |
| IEC 61508 | Generic standard covering the safety lifecycle of electrical/ electronic/ programmable electronic systems. Facilitate development of application sector standards. Risk assessment for safety functions & safety integrity levels (SIL). |
| IEC 60204-1 | Electrical Equipment of Industrial Machines: Defines safety related conventional functions, stopping categories, and operation during emergency situations |
| IEC 61800-5-2 | Safety requirements and functional safety for adjustable speed drive systems |
| IEC 62061 | Standard which is implementation of IEC 61508 specifically for machinery sector including functional safety and management procedures to achieve functional safety by design |
| NFPA-79 | 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 |
| OSHA 1910.217(b)(13) | Occupational Safety and Health Administration: Addresses control reliability |

# 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

| 61800-5-2 Functions | Description |
|---|---|
| STO | Safe Torque Off |
| SS1 | Safe Stop 1 |
| SS2 | Safe Stop 2 |
| SOS | Safe Operational Stop |
| SLA | Safe Limited Acceleration |
| SAR | Safe Acceleration Range |
| SLS | Safe Limited Speed |
| SSR | Safe Speed Range |
| SLT | Safe Limited Torque |
| STR | Safe Torque Range |
| SLP | Safe Limited Position |
| SLI | Safe Limited Position Increment |
| SDI | Safe Direction |
| SMT | Safe Motor Temperature |
| SBC | Safe Brake Control |
| SCA | Safe cam |
| SSM | Safe Speed Monitor |

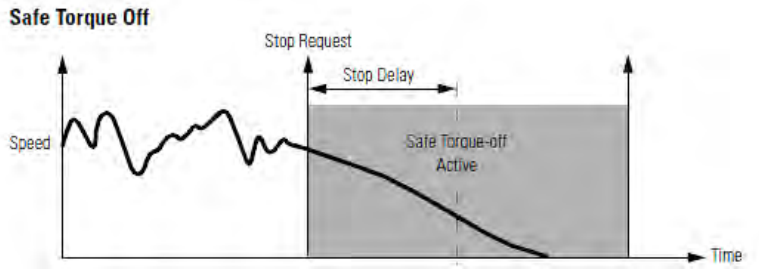
## Functionality Grouping

- 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)

# Safety Function Examples

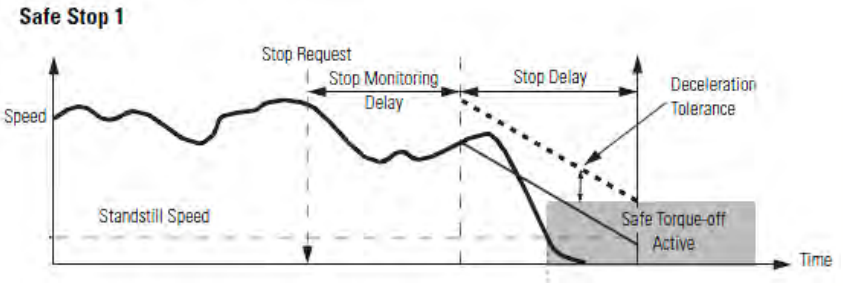
## STO

- Stop Request
- Wait Stop Delay
- Disable Motor Power



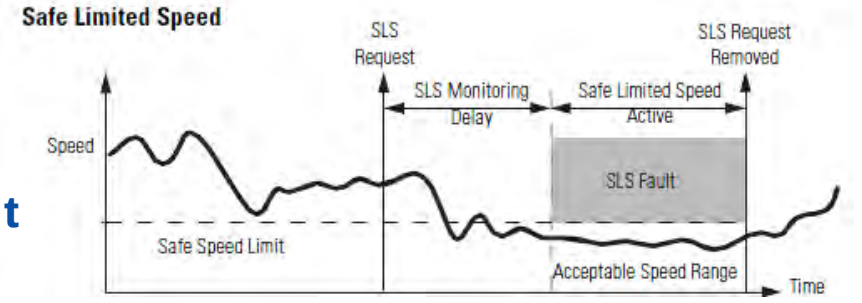

## SS1

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



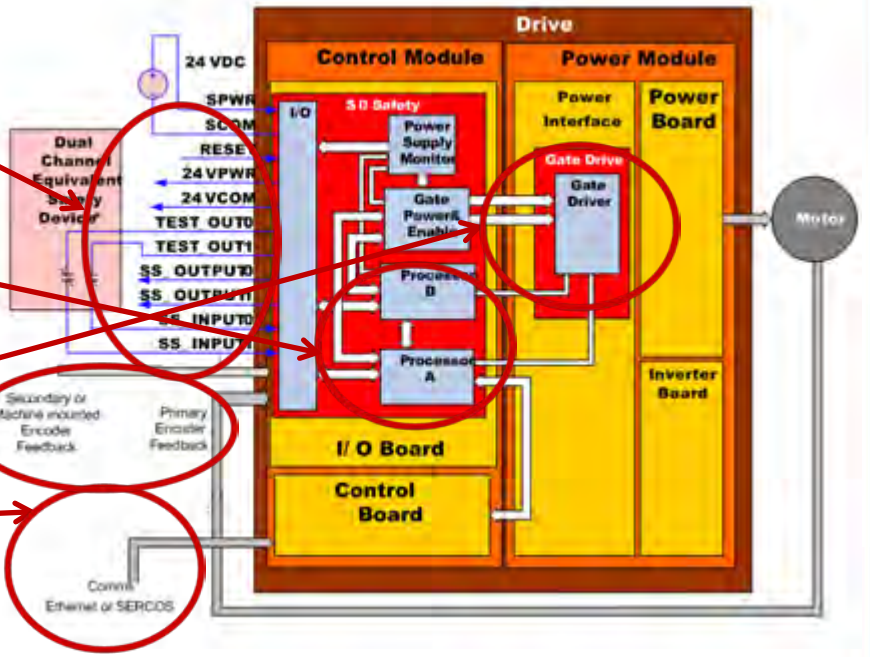

## SLS

- 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

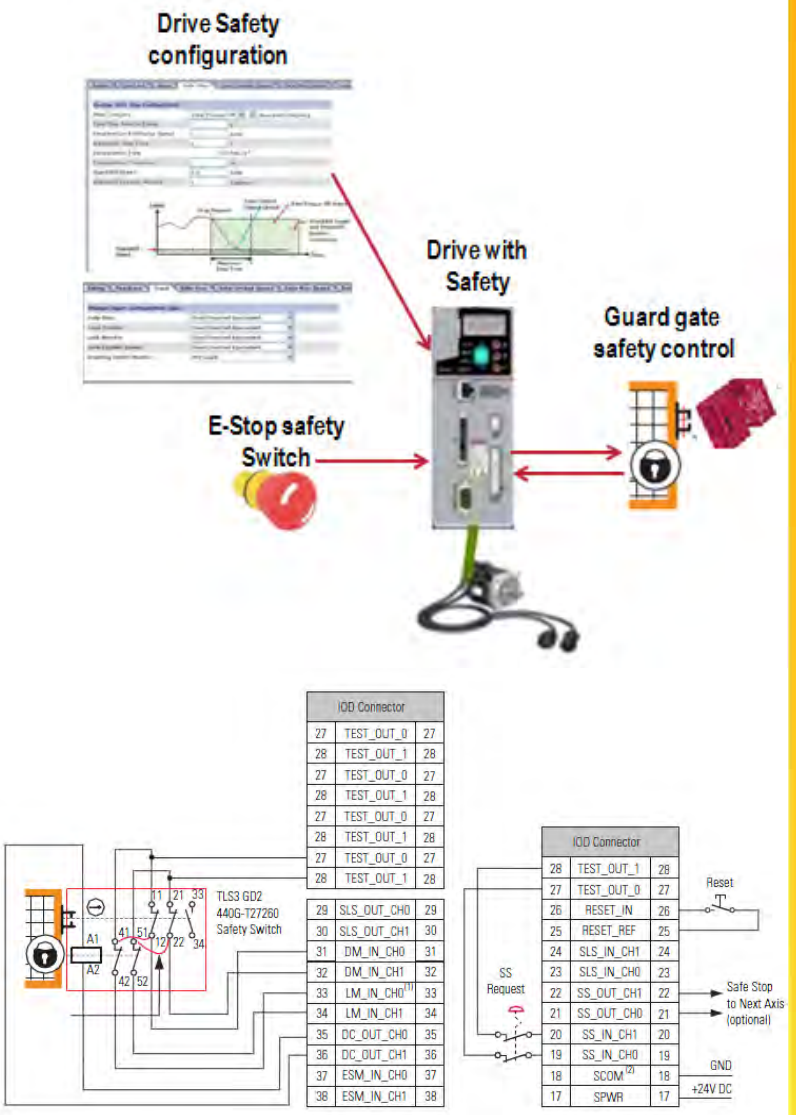
**OPTION 4**

Safety controller executed drive safety functions

| | Network Safety Connection Required | Safety I/O Owner | Drive Safety Function Activation | Drive Safety Config Source | Motion Profile Command |
|---|---|---|---|---|---|
| Option 1 | No | Drive | Drive | Drive | Drive |
| Option 2 | Yes | Safety Controller | Safety Controller | Drive | Drive |
| Option 3 | Yes | Safety Controller | Safety Controller | Safety Controller | Drive |
| Option 4 | Yes | Safety Controller | Safety Controller | Safety Controller | Controller |

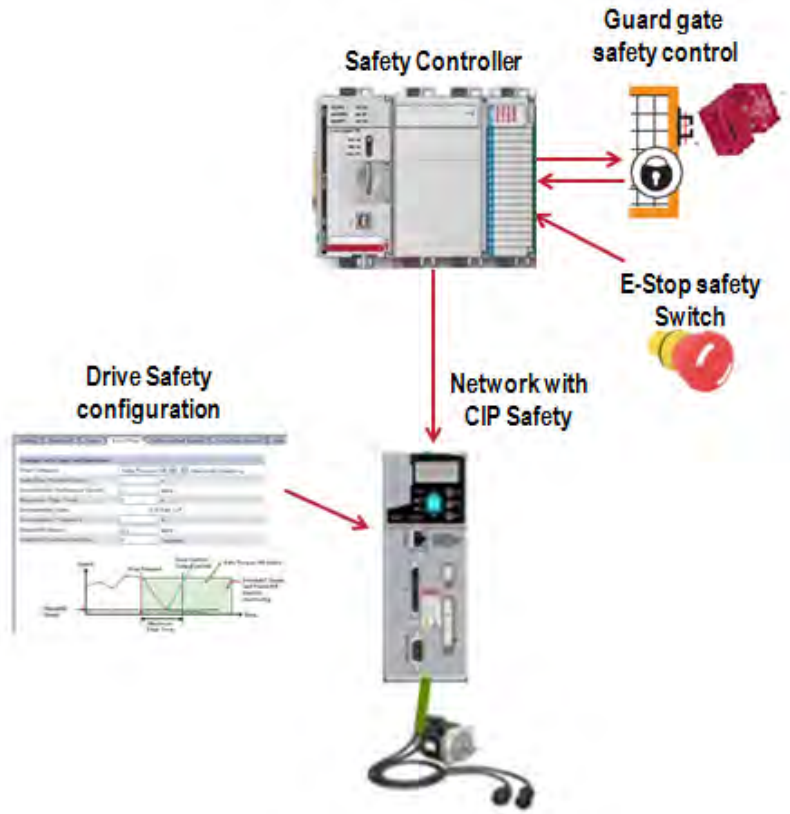
# Hardwired Drive Safety (Option 1)

- **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



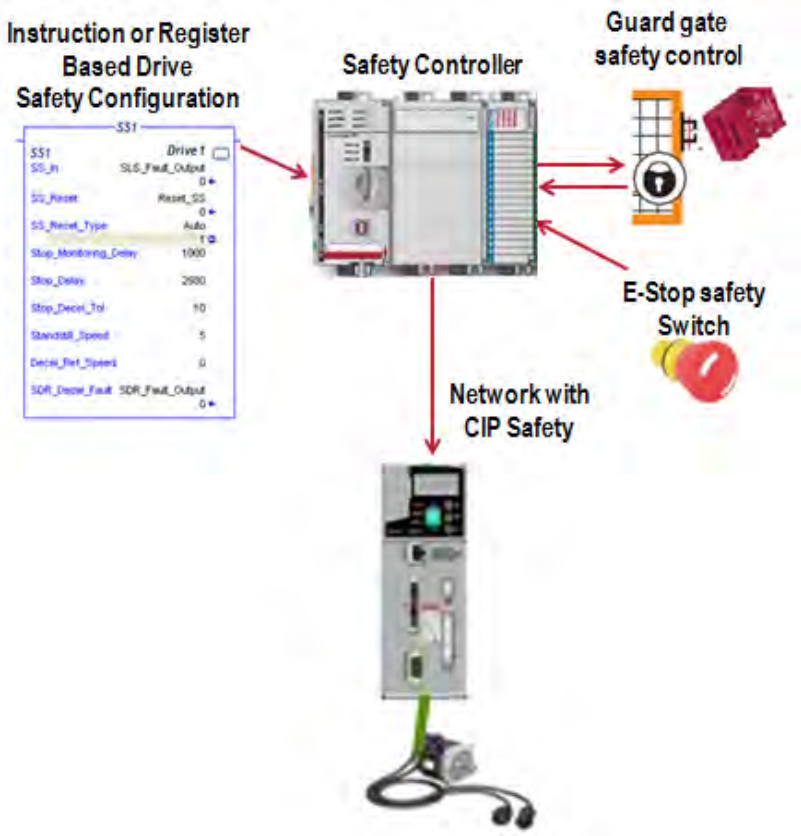
# Safety Controller Activated Safety Functions (Option 2)

- **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



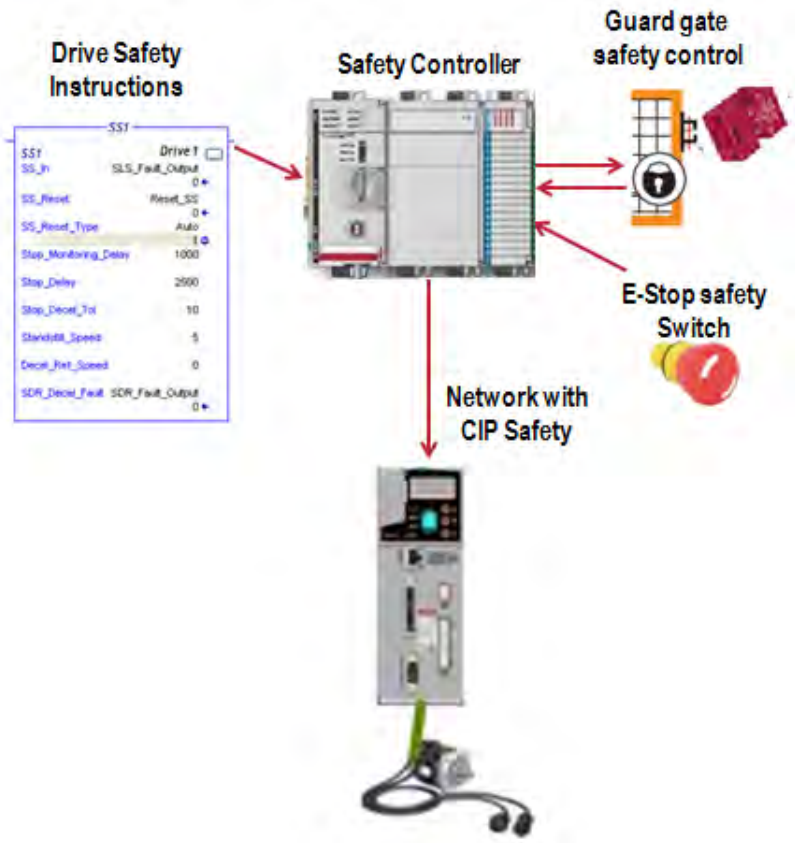
# Safety Controller Configured and Activated Safety Functions (Option 3)

- **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



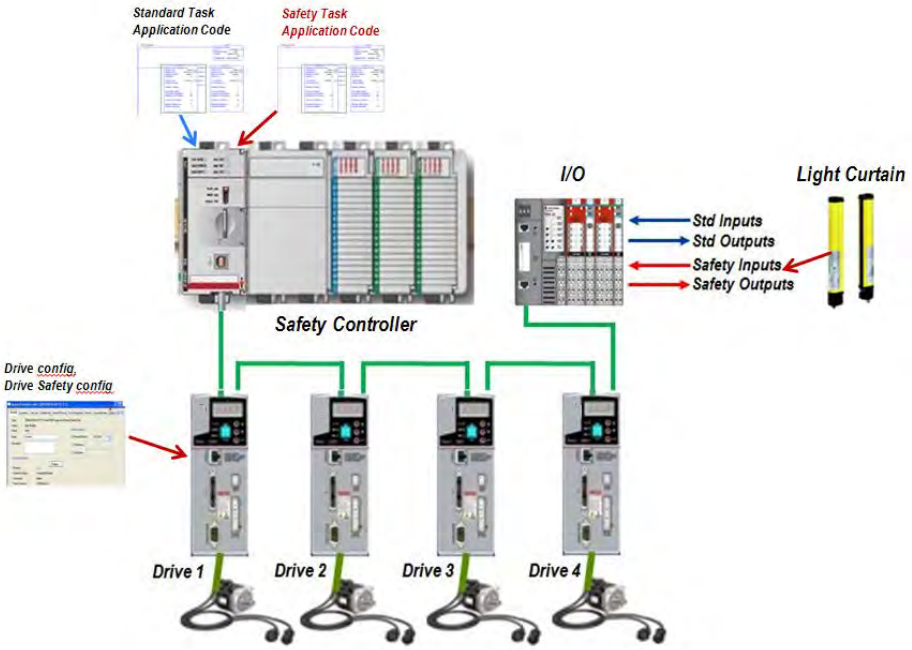
# Safety Controller Executed Drive Safety Functions (Option 4)

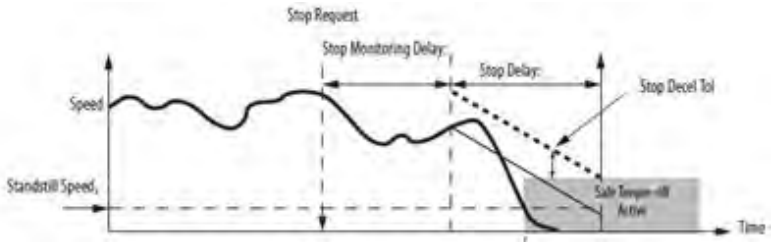
- **Safety network connection required**
- **Safety functions are managed in the drive**
  - EN61500-5-8
- **Safety configuration is stored in the safety controller**
  - Via safety application program parameters
- **Safety Controller**
  - Manages all safety I/O – local and distributed
  - Executes 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

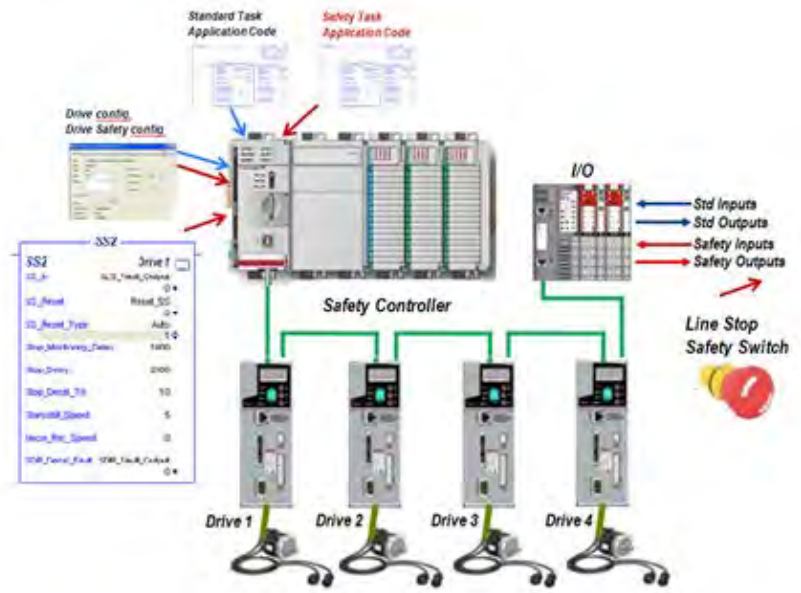
- **Drive SS1 stop request management**
  - Safety task application code recognizes and processes SS1 stop request
  - Light curtain transition = SS1 request to drive 1 through drive 4 via network safety CIP Safety input connection safety function activation object
- **SS1 stop management**
  - SS1 request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



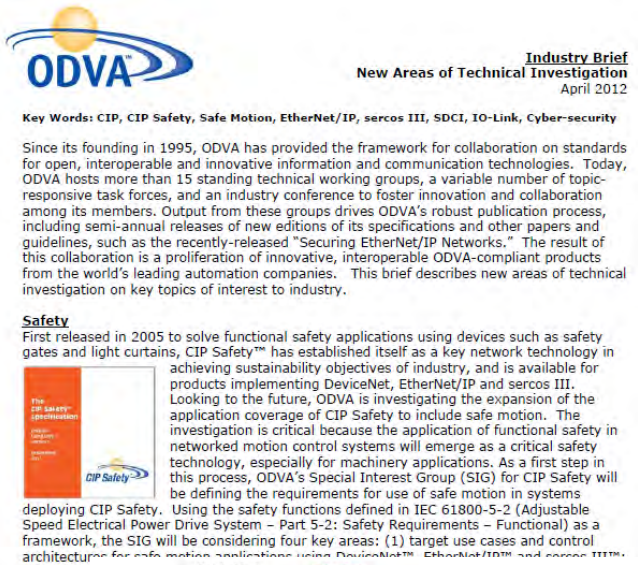
# Option 4 – Safe Coordinated Line Stop with SS2 Application Example

- **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)



ODVA

**Industry Brief**
**New Areas of Technical Investigation**
April 2012

**Key Words: CIP, CIP Safety, Safe Motion, EtherNet/IP, sercos III, SDCI, IO-Link, Cyber-security**

Since its founding in 1995, ODVA has provided the framework for collaboration on standards for open, interoperable and innovative information and communication technologies. Today, ODVA hosts more than 15 standing technical working groups, a variable number of topic-responsive task forces, and an industry conference to foster innovation and collaboration among its members. Output from these groups drives ODVA's robust publication process, including semi-annual releases of new editions of its specifications and other papers and guidelines, such as the recently-released "Securing EtherNet/IP Networks." The result of this collaboration is a proliferation of innovative, interoperable ODVA-compliant products from the world's leading automation companies. This brief describes new areas of technical investigation on key topics of interest to industry.

**Safety**

First released in 2005 to solve functional safety applications using devices such as safety gates and light curtains, CIP Safety™ has established itself as a key network technology in achieving sustainability objectives of industry, and is available for products implementing DeviceNet, EtherNet/IP and sercos III. Looking to the future, ODVA is investigating the expansion of the application coverage of CIP Safety to include safe motion. The investigation is critical because the application of functional safety in networked motion control systems will emerge as a critical safety technology, especially for machinery applications. As a first step in this process, ODVA's Special Interest Group (SIG) for CIP Safety will be defining the requirements for use of safe motion in systems deploying CIP Safety. Using the safety functions defined in IEC 61800-5-2 (Adjustable Speed Electrical Power Drive System – Part 5-2: Safety Requirements – Functional) as a framework, the SIG will be considering four key areas: (1) target use cases and control

# Option 2 Object Concepts

## Drive Safety Function Activation

**Basic Control Word (Safety Function Activation) - Mandatory**

| 15 | 14 | 13 | 12 | 11 | 10 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Res | Res | STO | SS1 | SS2 | SOS | SDI+ | SDI- | SBC | SLS 1 | SLS 2 | SLS 3 | SLS 4 | Activate | Reset |

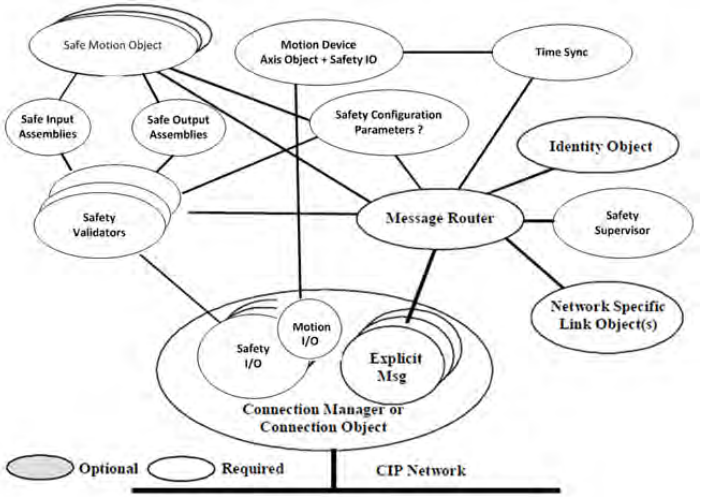
## Drive Safety Status

**Basic Status Word (Safety Function Status)- Mandatory**

| 15 | 14 | 13 | 12 | 11 | 10 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Res | Res | STO | SS1 | SS2 | SOS | SDI+ | SDI- | SSM | SLS 1 | SLS 2 | SLS 3 | SLS 4 | Err1 | Err2 |

## Drive Safety Feedback

| Name | Data Type | Description of Attribute | Semantics of Values |
|---|---|---|---|
| Sample Time | ULINT | System Time when Feedback Position was sampled | Nanoseconds (CIP Sync absolute) |
| Feedback Position | DINT | Actual position of the feedback device | Feedback Counts |
| Feedback Velocity | REAL | Actual filtered velocity | Feedback Units / Sec |
| Feedback Acceleration | REAL | Actual filtered acceleration | Feedback Units / $Sec^2$ |



# 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