



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

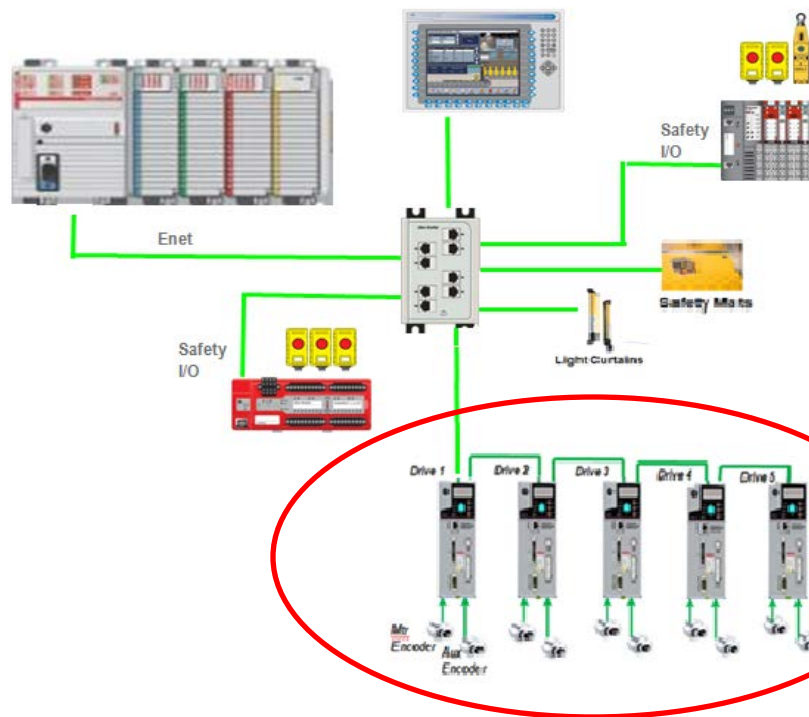
Drive Safety System Architecture Option Review

**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.

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

Functionality Grouping

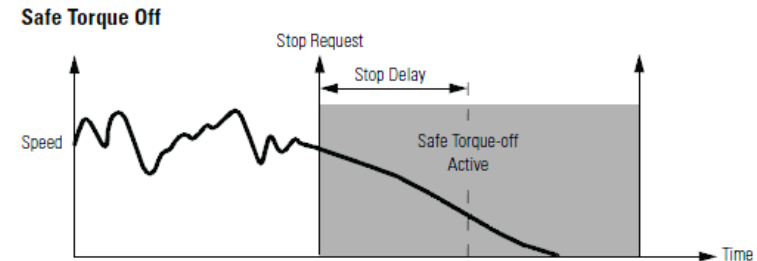
- ▶ Disconnect Torque generating power to the motor (STO)
- ▶ Safe stop (i.e. SS1, SS2)
- ▶ Safe speed monitoring (i.e. SSM)
- ▶ Safe acceleration monitoring (i.e. SLA)
- ▶ Safe torque monitoring (i.e. SLT)
- ▶ Safe position monitoring (i.e. SLP)
- ▶ Safe brake control (i.e. SBC)

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

Drive Safety Function Examples

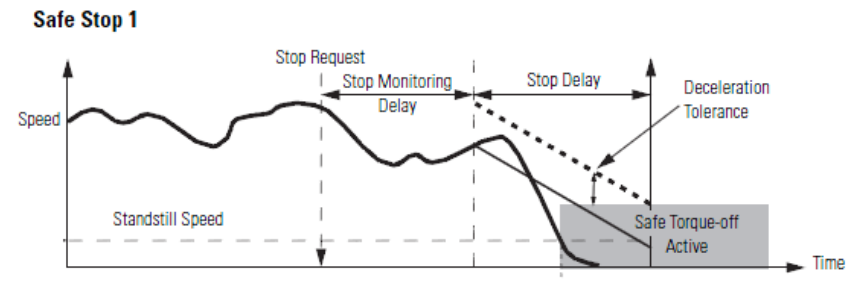
STO (Safe Torque Off)

- ▶ Stop Request
- ▶ Wait Stop Delay
- ▶ Disable Motor Power



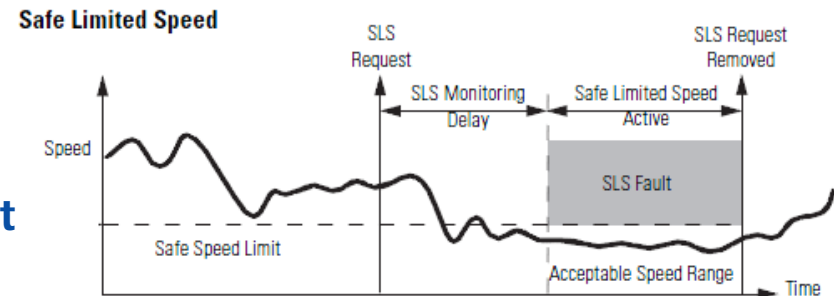
SS1 (Safe Stop 1)

- ▶ 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

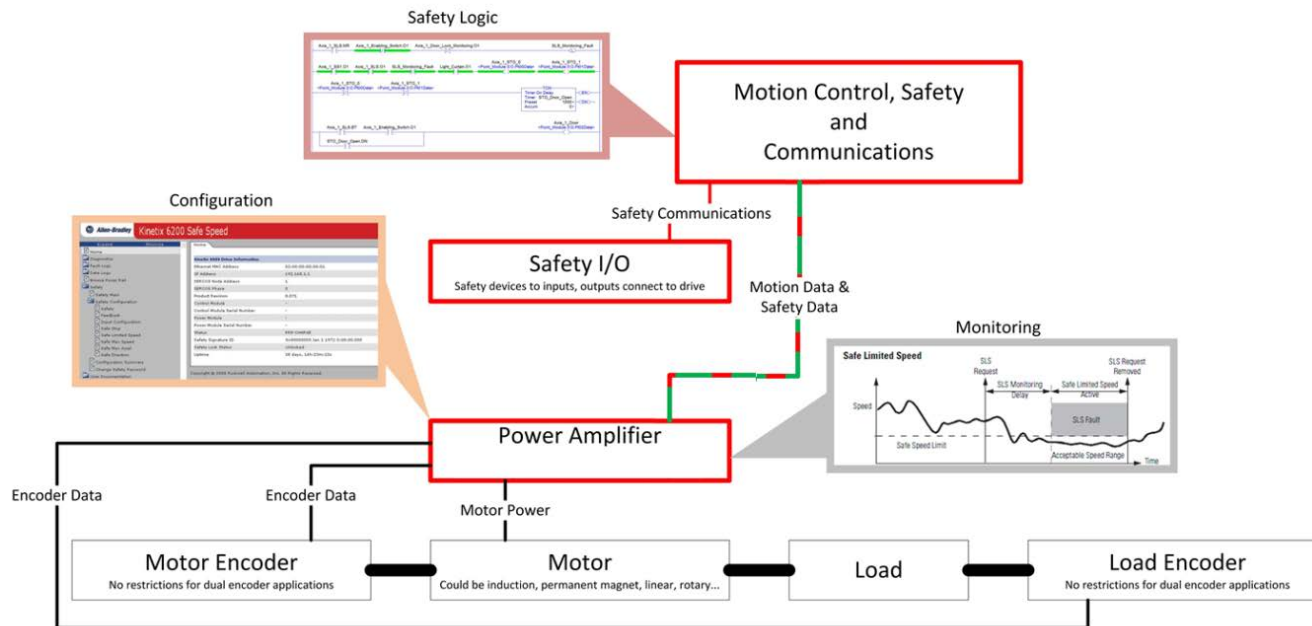
Safety controller configured & activated drive safety functions

OPTION 4 ← Detail & application use case examples focus

Safety controller executed drive safety functions

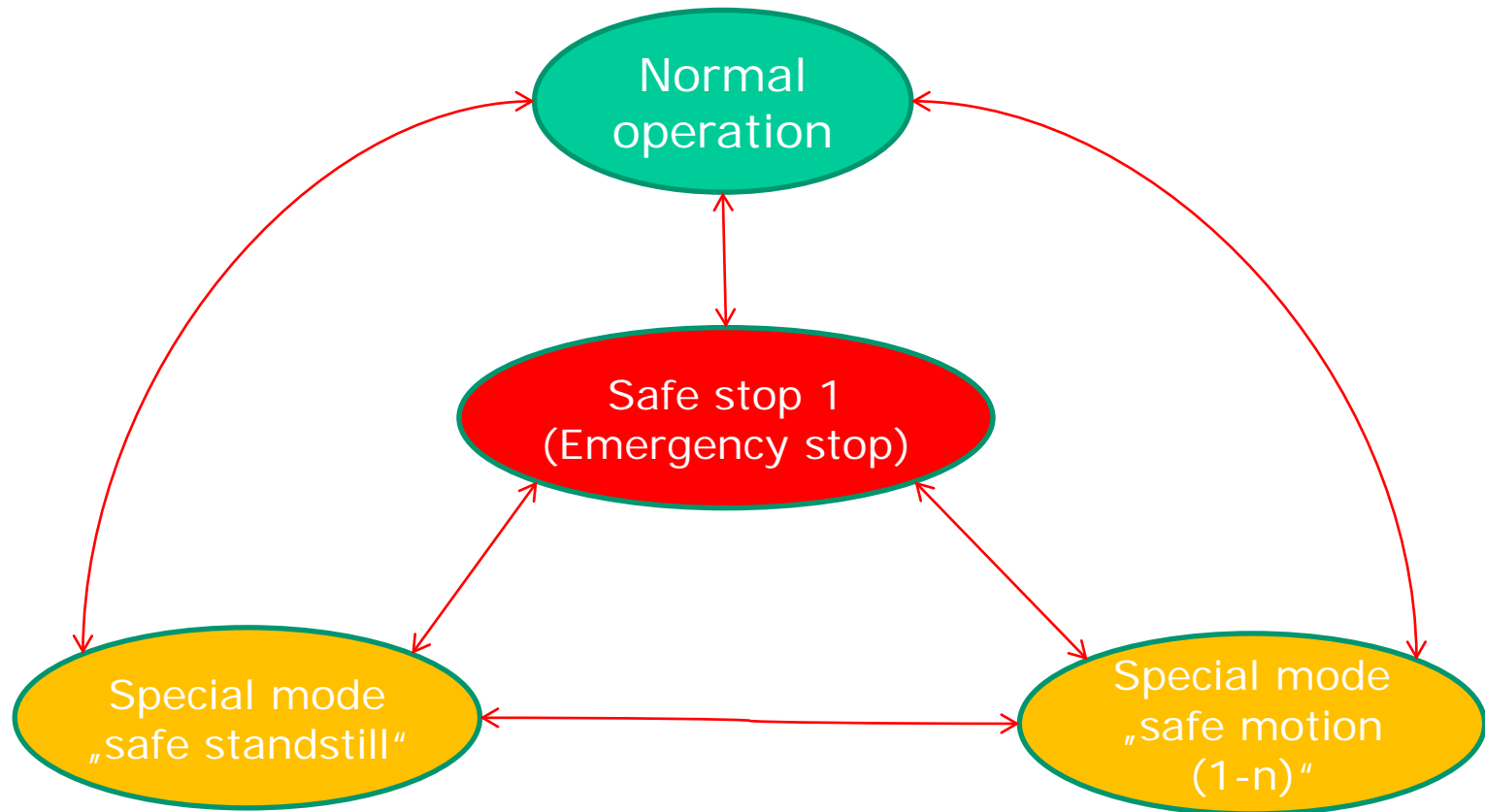
	Safety Network Connection Required	Safety I/O Owner	Drive Safety Function Activation	Drive Safety Config Source	Motion Profile Command
Option 1	No	Drive	Drive	Drive	Drive
Option 2	Yes	Safety Controller	Safety Controller	Drive	Drive
Option 3	Yes	Safety Controller	Safety Controller	Safety Controller	Drive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

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



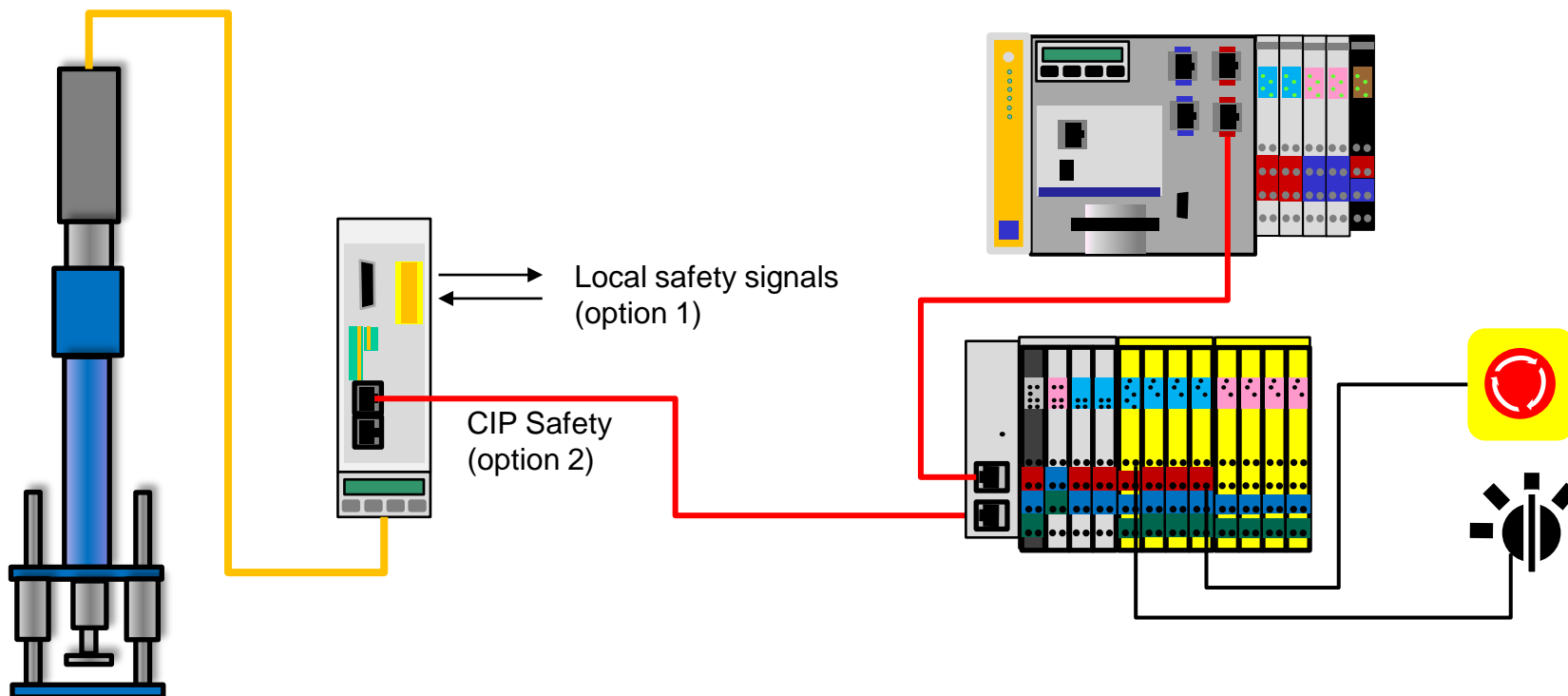
Safety modes and functions

Operating state	Safety Functions	Mode Selector
Normal mode	Safe direction Safe maximum speed Safely-limited position	Normal mode select
Safe standstill	Safe stop 1 Safe stop 2 Safe brake control	Special mode select
Emergency stop	Safe stop 1	Emergency stop button
Safe motion	Safely-limited speed Safe direction Safely-limited increment Safely-monitored position Safe maximum speed Safely-limited position	Special mode select + enabling control button

Benefits - Safety Controller Activated Drive Safety Functions (Option 2 Architecture)

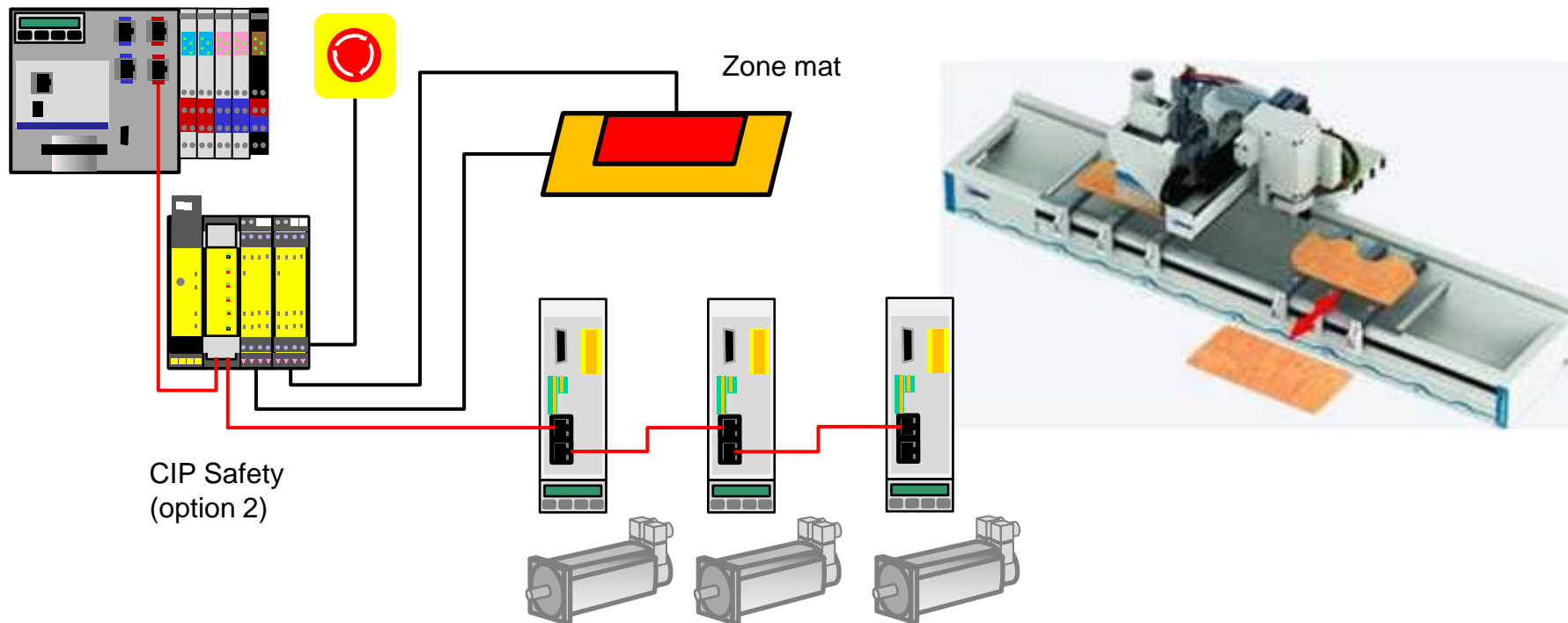
- ▶ Safety functions pre-configured and pre-tested without a safety controller
- ▶ Easy migration path between option 1 (safety I/O hardwired to the drive) and option 2
- ▶ Less CPU power needed in the safety controller. Valuable in machines using a large number of safe drives
- ▶ Less data used for 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



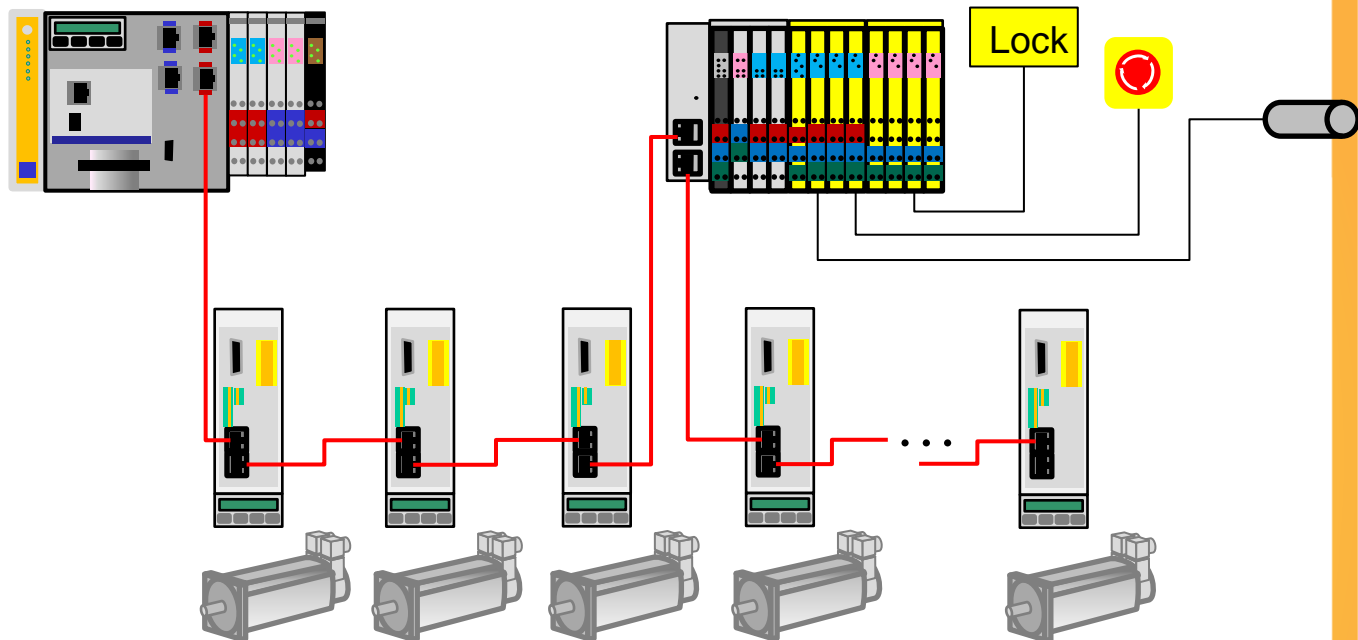
- ▶ **Independent axis configuration**
- ▶ **Flexible system integration**

Use Case - Woodworking Machinery



- ▶ **Speed limit monitored in drive → fast reaction time**
- ▶ **Example shows separate safety controller**
 - Easily implemented using CIP Safety

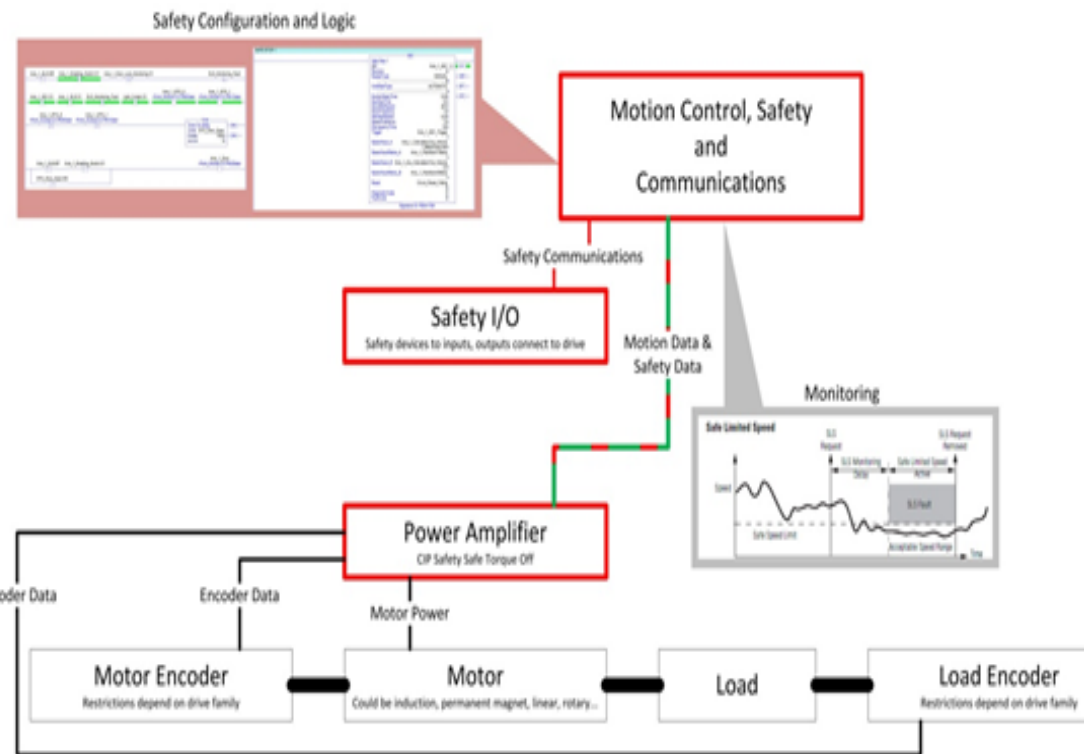
Use Case - Printing Machine



- ▶ 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

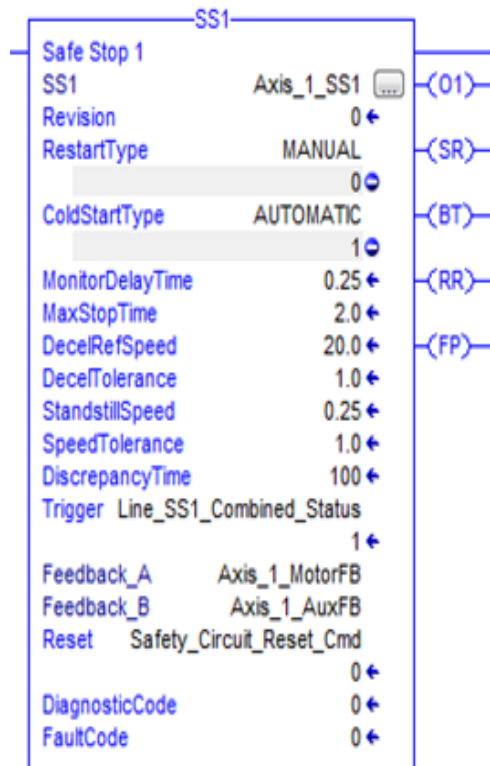
Safety Controller Executed Drive Safety Functions (Option 4 Architecture)

- ▶ **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

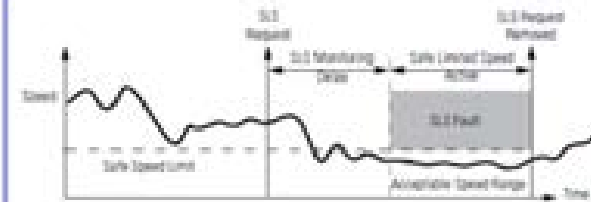
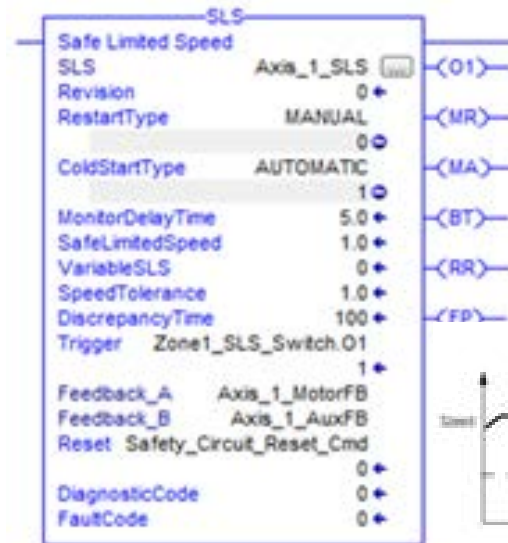
- ▶ **Safe Torque Off**
- ▶ **Safe Brake Control**
- ▶ **Safe stop**
 - i.e. SS1
- ▶ **Safe speed monitoring**
 - i.e. SSM
- ▶ **Safe acceleration monitoring**
 - i.e. SLA
- ▶ **Safe torque monitoring**
 - i.e. SLT
- ▶ **Safe position monitoring**
 - i.e. SLP



Parameter	Description
Output 1 (O1)	This output is energized when the input conditions have been satisfied. OFF (0): Unhealthy or inactive ON (1): Healthy and active The output become de-energized when the following occurs: 1.The rung is no long energized. 2.Any fault has occurred. 1.The monitoring sequence has completed. If item 1 occurs and monitoring has not been requested, only making the input conditions true is required to restart the instruction. If item 2 occurs, then a Reset command will need to be issued. If item 3 occurs, the restart action is dependent on the state of the Trigger and the Restart Type.
SS1 Requested (SR)	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.
Below Threshold (BT)	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.
Reset Required (RR)	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.
Fault Present (FP)	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).

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**



Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
180 _{hex}	0	Reset Request	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	STO Output

Safety Output Data with STO

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
1C0 _{hex}	0	Feedback Position (DINT)							
	1								
	2								
	3								
	4	Feedback Velocity (DINT)							
	5								
	6								
	7								
	8	Feedback Acceleration (DINT)							
	9								
	10								
	11								
	12	Reset Required	Safety Fault	Reserved	Reserved	Reserved	Reserved	Reserved	Torque Disabled

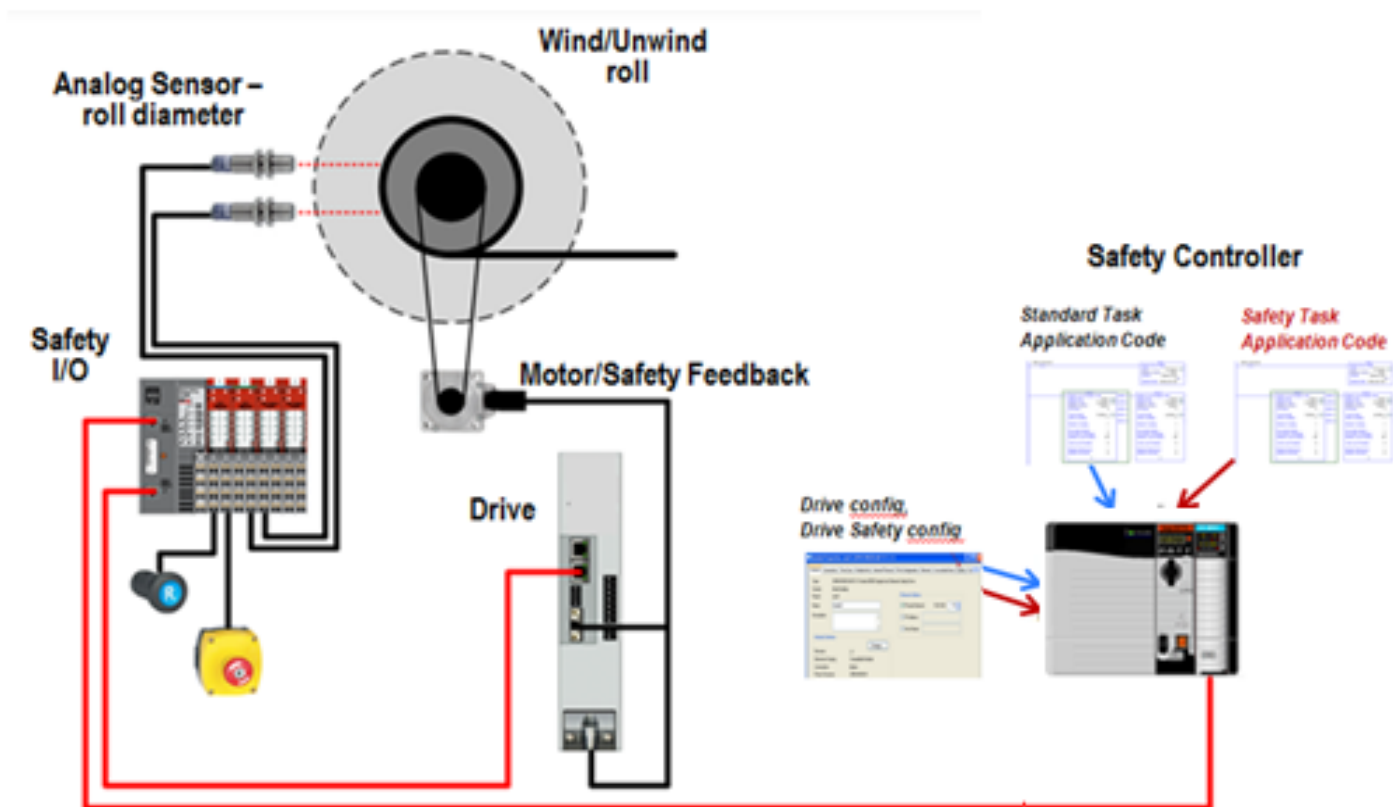
Safety Input Data with STO and Feedback Data

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

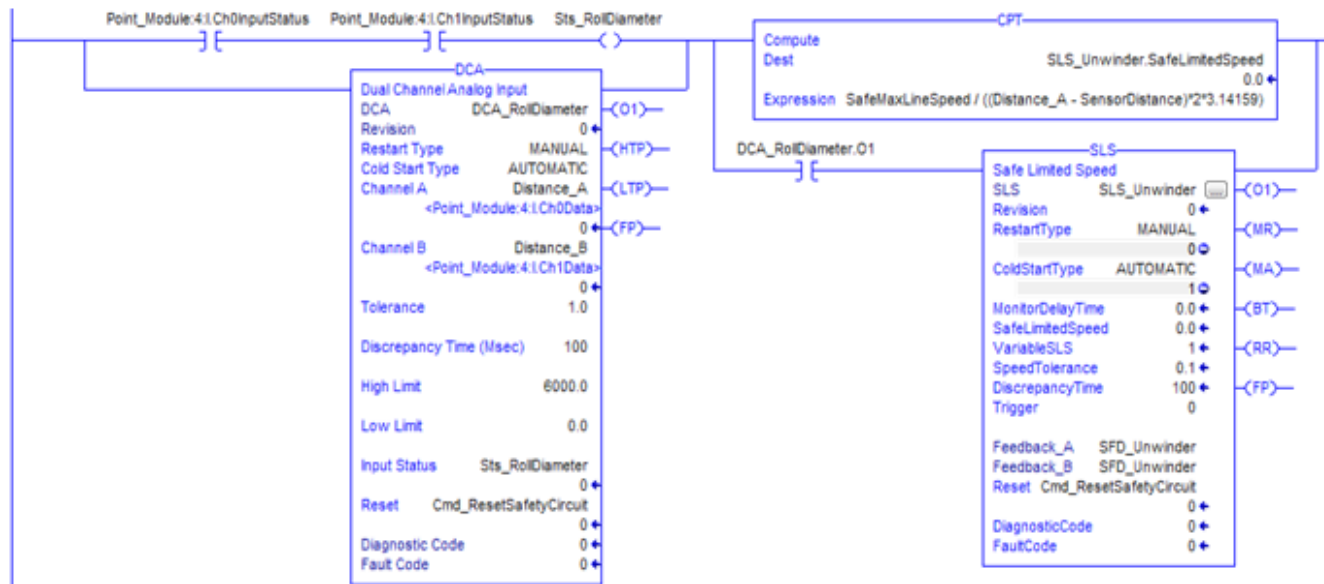
Use Case– SLS Wind/Unwind Roll

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



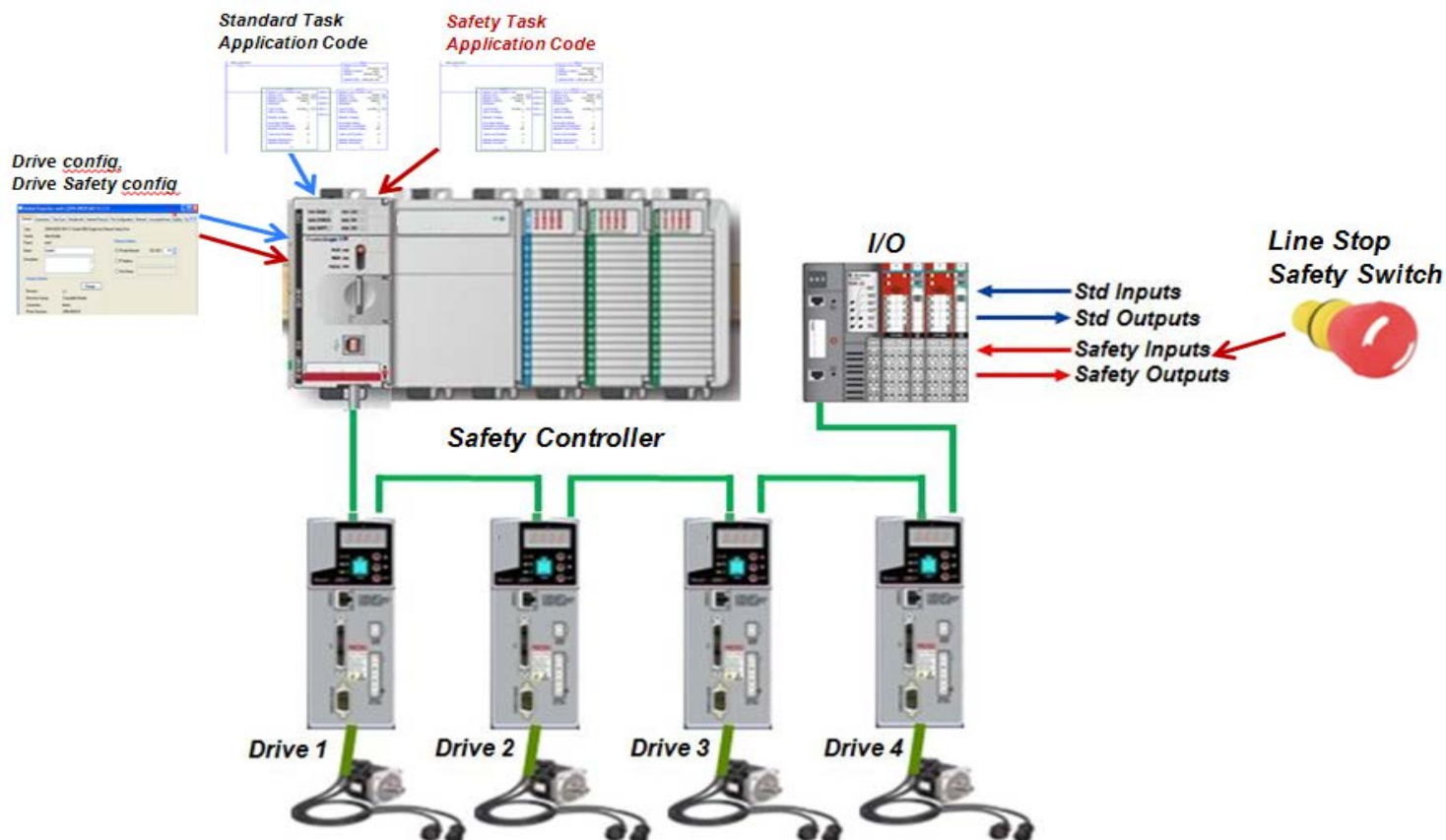
Solution

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)

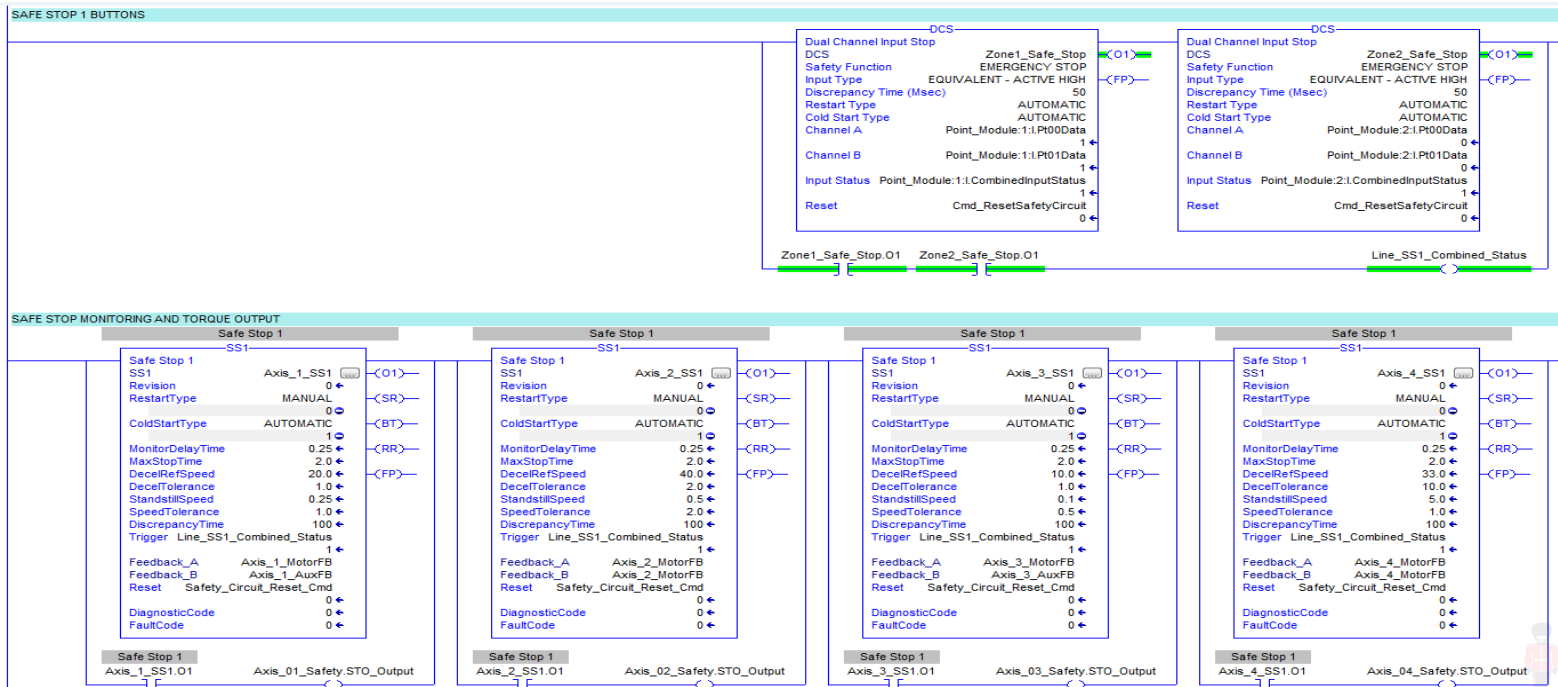


Solution

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)



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

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