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

Ludwig Leurs
Project Director Ethernet Convergence
Bosch Rexroth AG

Bob Hirschinger
Principal Engineer
Rockwell Automation

Presented at the ODVA
2014 ODVA Industry Conference & 16th Annual Meeting
March 11-13, 2014
Phoenix, Arizona, USA

Abstract
First released in 2003 to solve functional safety applications, 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. The recently published (November 2013) CIP Safety™ SafeMotion profile provides for inclusion of networked safe motion functionality in a broad range of functional safety applications, unique in covering this application space. This paper presents a range of CIP Safety Safe Motion application use case scenarios for both centralized and decentralized safety solutions. A detailed analysis of the safety architecture, functionality, programming, and commissioning is provided for each use case.

Keywords
Safety Motion Profile, Safety Motion Objects

Definition of terms (optional):
TCP Tool Center Point

Introduction
In the past, many applications deployed safety devices in a standalone, hardwired mode where safety was managed locally at the device and safety network support was not required. For example, safe drives were equipped with dedicated local safety I/O and supported a range of safety functions like safe torque off, safe stopping, and safe limited speed monitoring. Drive safety configuration was managed locally using web browsers or dedicated software tools, and the safety function activation was via safety I/O at the drive.

Today the trend is to implement fully programmable, flexible safety solutions using controllers with safety task support with networked safety devices that are fully integrated into the machine process [1]. This safety controller based architecture has distinct advantages over traditional standalone hardwired safety when:

1. Complex safety logic is required
2. Multiple safety zones have to be managed
3. Distributed safety I/O is required

4. A large area/footprint is to be safe-guarded
5. Machine modularity and scalability is important
6. Diagnostic safety information is required
7. Advanced drive safety control is required

Networked safety drives are a critical safety component in the safety controller based architecture. Networked safety drives can offer basic and advanced safety functions with safety configuration, safety function activation, and safety status monitoring support via network safety connections. Modern safety network technology allows safety devices like safety discrete I/O, safety analog I/O, drives with a safety core, and other devices with safety support to coexist with standard control devices on a common network which support both safety connections and standard connections.

Controllers are available that are dedicated safety controllers as well as controllers that offer both safety control and standard control support. A controller with safety and standard control support typically includes safety task(s), standard task(s), and network support for safety and standard connections. Figure 1 is example of an architecture utilizing a controller with safety and standard task support, safety and standard network connections, with support for both safety and standard devices.

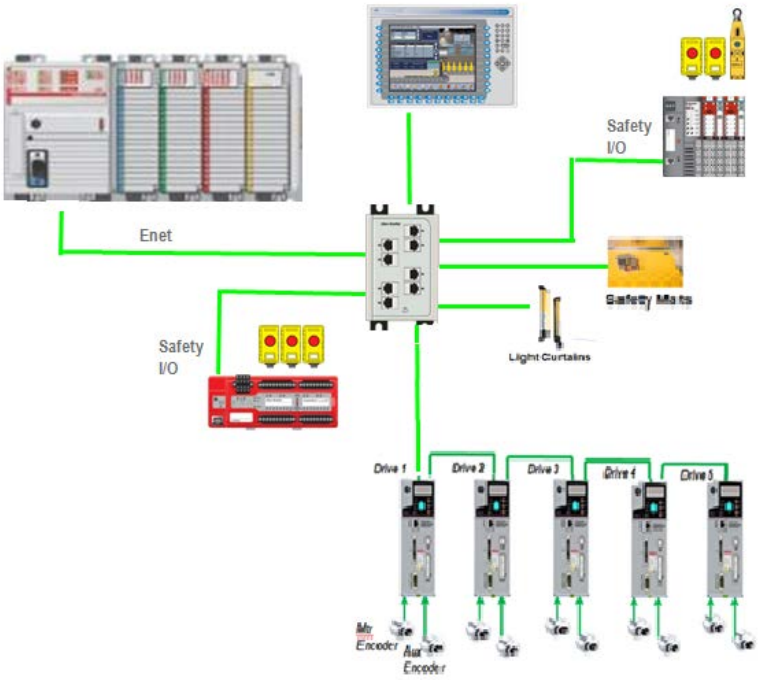


Figure 1 - Safety Controller Based Architecture

While there are published open CIP Safety profiles for *"Safety Discrete I/O"* and *"Safety Analog I/O"* available, open profiles were not available for networked "*Safety Drives*". This was identified as a critical need and as a result a CIP Safety Safe Motion Sub-committee was formed to construct safety specification enhancements (SSE) for a CIP Safety ***Safety Drive Profile*** and supporting ***Safe Motion objects*** Specification [2].

This paper examines functionality and architectures supported by the CIP Safety Safety Drive Profile and CIP Safety Motion Objects specification. A number of application use case scenarios will be examined based on the supported architectures.

Drive Safety Functions:
The CIP Safety Drive Profile and supporting CIP Safety Motion Objects support a broad range of drive safety functions as listed in the EN61800-5-2 "Adjustable speed electrical power drive systems safety requirements functional" standard [3]. Table 1 lists the drive safety functions.

EN61800-5-2 Function	Description	Definition
STO	Safe Torque Off	Power that can cause rotation (or motion in the case of a linear motor), is not applied to the motor. The drive will not provide energy to the motor which can generate torque (or force in the case of a linear motor).
SS1	Safe Stop 1	The drive either initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the STO function when the motor speed is below a specified limit; or initiates and monitors the motor deceleration rate within set limits to stop the motor and initistes the STO function when the motor speed is below a specified limit; or initiates the motor deceleration and initiates the STO function after an application specific time delay
SS2	Safe Stop 2	The drive either initiates and controls the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; or initiates and monitors the motor deceleration rate within set limits to stop the motor and initiates the safe operating stop function when the motor speed is below a specified limit; or initiates the motor deceleration and initiates the safe operating stop function after an application specific time delay.
SOS	Safe Operational Stop	The SOS function prevents the motor from deviating more than a defined amount from the stopped position. The drive provides energy to the motor to enable it to resist external forces.
SLA	Safe Limited Acceleration	The SLA function prevents the motor from exceeding the specified acceleration limit.
SAR	Safe Acceleration Range	The SAR function keeps the motor acceleration and/or deceleration within specified limits.
SLS	Safe Limited Speed	The SLS function prevents the motor from exceeding the specified speed limit.
SSR	Safe Speed Range	The SSR function keeps the motor speed within specified limits.
SLT	Safe Limited Torque	The SLT function prevents the motor from exceeding the specified torque (or force, when a linear motor is used) limit.
STR	Safe Torque Range	The STR function keeps the motor torque (or force, when a linear motor is used) within the specified limits.
SLP	Safe Limited Position	The SLP function prevents the motor shaft from exceeding the specified position limit(s).
SLI	Safe Limited Increment	The SLI function prevents the motor shaft from exceeding the specified limit of position increment.
SDI	Safe Direction	The SDI function prevents the motor shaft from moving in the unintended direction.
SMT	Safe Motor Temperature	The SMT function prevents the motor temperature(s) from exceeding a specified upper limit(s).
SBC	Safe Brake Control	The SBC function provides a safe output signal(s) to control an external brake(s).
SCA	Safe CAM	The SCA function provides a safe output signal to indicate whether the motor shaft position is within a specified range
SSM	Safe Speed Monitor	The SSM function provides a safe output signal to indicate whether the motor speed is below a specified limit

Table 1 - EN61800-5-2 Drive Safety Functions

These 17 safety functions can be categorized into following general groups:

- Disable power flow to the motor (i.e. STO)
- Safe brake control (i.e. SBC)
- 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)

An overview of “typical” functionality associated with a few of the common drive safety functions is provided in figure 2 through 4.

Safe Torque-off (STO)

STO is used to disable the torque generating power feed to the motor [3]. A typical implementation includes a safe torque off request input and stop delay parameter. On occurrence of a STO safe torque off request a STO will be initiated after the specified Stop Delay. Figure 2 shows a typical timing diagram for an STO sequence.

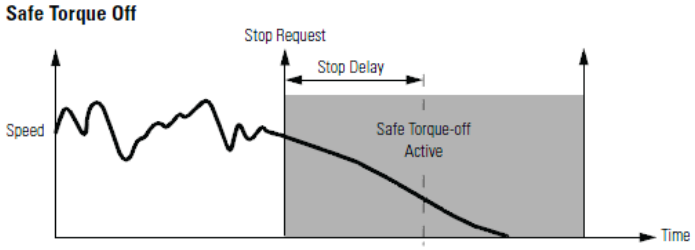


Figure 2 - Safe Torque Off (STO) Timing Diagram

Safe Stop 1 (SS1)

SS1 is used to decelerate the motor followed by an STO [3]. A typical implementation includes the SS1 stop request input, stop monitoring delay parameter, stop delay parameter, deceleration tolerance parameter, and standstill speed parameter. On occurrence of a SS1 safe stop request the deceleration ramp will be monitored after the stop monitoring delay expires. An STO will be initiated as soon as the motor speed is below the Standstill speed or the stop delay time expires. Figure 3 shows a timing diagram for a typical SS1 sequence.

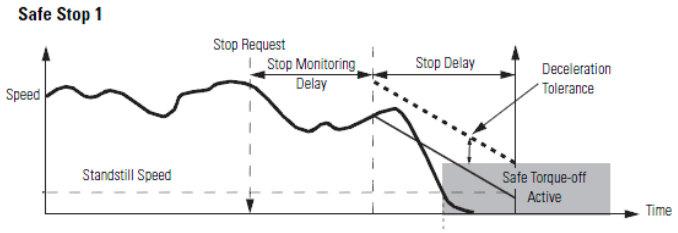


Figure 3 - Safe Stop 1 (SS1) Timing Diagram

Safe Limited Speed (SLS)

SLS is used to insure the speed of the motor does not exceed a minimum value [3]. A typical implementation includes the SLS monitoring request input, SLS monitoring delay parameter, and safe speed limit parameter. On occurrence of a SLS monitoring request the motor speed will be monitored after the SLS monitoring delay expires to insure it does not exceed the safe speed limit value. If the limit is exceeded a SLS fault will occur and an STO is initiated. Figure 4 shows a timing diagram for a typical SLS.

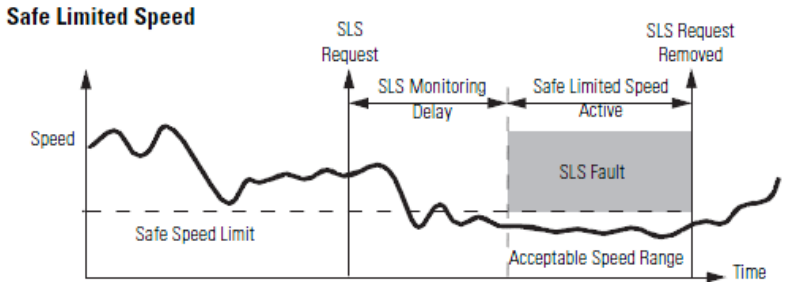


Figure 4 - Safe Limited Speed (SLS) Timing Diagram

Drives may support a subset of the 61800-5-2 safety functions with STO being a minimum requirement. The drive includes a Safety Core to manage the safety function operation. The Safety Core is typically designed to meet EN-ISO 13849-1 PLe and up to and including EN61508 SIL 3.

The typical drive Safety Core includes the safety network interface, primary and secondary position/velocity feedback, redundant processors with gate drive interface to disable torque producing current to the motor, and firmware to support a range of drive safety functions. Single motor mounted feedback is typically used for SIL 2, PLd while an additional secondary feedback is required for SIL 3, PLe (typically driven on the load side). The functionality provided by the drive safety core differs based on the supported drive safety functions, and the safety interface to the drive.

Drive Safety Architecture Deployment Options:
In the 2012 ODVA Conference paper "CIP Safety for Drives", four different drive safety architecture deployment options were defined. Key factors in differentiating these options are based on the following attributes:

1) Safety I/O owner – Drive or Safety Controller
2) Drive Safety function activation source – Drive Safety I/O or Safety Controller
3) Drive Safety Configuration – Drive configuration or Safety Controller based configuration/programming
4) Motion Profile Command – Drive or Motion Controller

The key attributes for the four options are listed in the table 2.

	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

Table 2 - Safety Architecture Deployment Options

This paper will focus on use case analysis for Option 2 and Option 4. These will be referred to as Option 2 –*Drive Managed Motion Safety Functions*, and Option 4 – *Safety Controller Managed Motion Safety functions*.

A review of the Option 2 and Option 4 control architecture is provided below:

Option 2 – Drive Managed Motion Safety Functions
With option 2 the drive safety functions are activated and safety status is monitored by the safety controller using the drive network safety connections. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is entered and stored locally at the drive using a web browser, software utility, or similar.

The safety controller activates and monitors safety functions in the drive via the safety network input and output connections using one or more assemblies as defined in the Safety Motion Device Profile. Multiple input and output assembly options are available depending on the safety functionality supported in the drive. Examples of safety input/output assemblies supporting STO, and STO with safe stop/limit functions are shown in table 3 through 8.

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

Table 3 - Safety Output Data with STO

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
$1A0_{hex}$	0	Reset Required	Safety Fault	Reserved	Reserved	Reserved	Reserved	Reserved	Torque Disabled

Table 4 - Safety Input Data with STO

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
183_{hex}	0	Reset Request	Reserved	SMT Request	SOS Request	SS2 Request	SS1 Request	SBC Output	STO Output
	1	Reserved	Reserved	SDI– Request	SDI+ Request	Reserved	SLA Request	SLS Request	SSM Request

Table 5 - Safety Output Data with Safe Stop/Limit Functions

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
$1A3_{hex}$	0	Reset Required	Safety Fault	Safe Motor Temp	Safe Standstill	SS2 Active	SS1 Active	Brake Engaged	Torque Disabled
	1	Reserved	Reserved	Motion Negative	Motion Positive	SDI Active	SLA Active	SLS Active	Safe Speed

Table 6 - Safety Input Data with Safe Stop/Limit Functions

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
184_{hex}	0	Reset Request	Reserved	SMT Request	SOS Request	SS2 Request	SS1 Request	SBC Output	STO Output
	1	Reserved	Reserved	Reserved	Reserved	Group Select			

Table 7 - Safety Output Data with Safe Stop and Safe Limit Groups

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
$1A4_{hex}$	0	Reset Required	Safety Fault	Safe Motor Temp	Safe Standstill	SS2 Active	SS1 Active	Brake Engaged	Torque Disabled
	1	Reserved	Reserved	Reserved	Reserved	Group Active			

Table 8 - Safety Input Data with Safe Stop and Safe Limit Groups

Table 3 and table 4 apply to the simplest drive with STO only support. Table 5 and Table 6 apply to drives that support STO and safe stop and safe limit functions. Table 7 and table 8 apply to drives that support preconfigured sets of safe limit functions.

An option 2 control architecture example is shown in figure 5. The Safety controller owns and manages the safety I/O and activates and monitors execution of drive safety functions via the drive network safety output/input connections. After activation of a drive safety function, execution of the safety function is managed in the drive using the drive safety configuration data and drive based safety feedback.

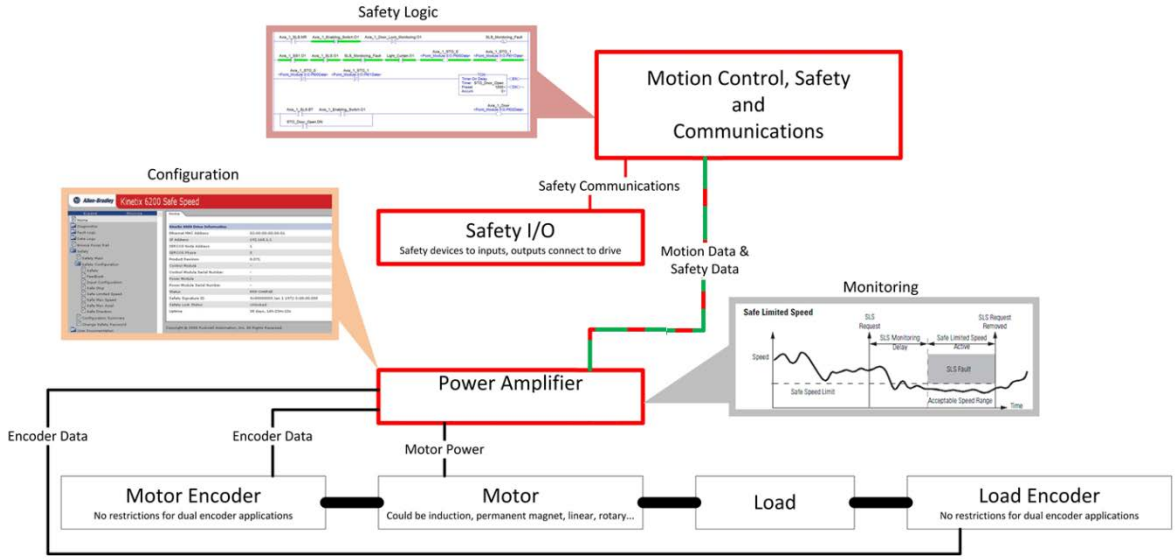


Figure 5 - Option 2 Architecture

An example safety function is SLS using the output assembly in table 5 and input assembly in table 6. The execution sequence is:

1. Safety controller sets the *SLS request* bit
2. On receipt of the *SLS request* bit the drive safety core activates the SLS monitoring function
3. The drive safety core manages the SLS monitoring function execution using the SLS configuration data stored in the drive (i.e. monitoring delay, safe speed limit) and the drive safety feedback data (single or dual channel position, speed, and acceleration)
4. The safety controller monitors the SLS status using the SLS Active, Safe Speed, and Safety Fault bits via the network safety input connection to the drive.

Some applications require safety limit functions with different limit setpoints at different operating conditions. As an example the speed limit for the safe limited speed could vary or could be combined with the Safe Direction function. The implementation of this functionality in the drive (option 2) while still using a compact data interface to the safety controller can be accomplished by grouping the safety functions regarding the operating cases.
In the hardwired case (option 1) all safety functions and the governing states have to be implemented in the drive controller. The typical states are shown in Figure 6.

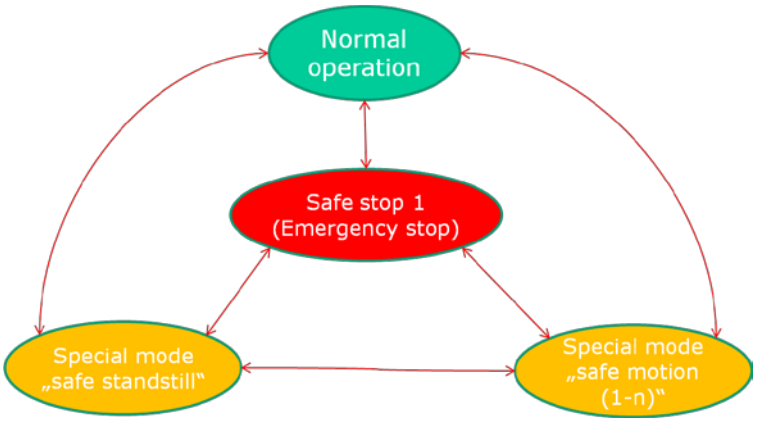


Figure 6 - Safety technology operating states of a drive

These modes are:

1. "Normal operation" is the production state of the machine. Safety is usually guaranteed by locked doors, but optionally some safety monitoring may be on.
2. "Safe stop 1" means that all actuators are disconnected from power. This inhibits the actuators from starting to move. This mode has previously been the standard for safe manual interaction with machines. In case of an error the devices go to the "safe stop 1" mode, where the actuators go to standstill with maximum deceleration and power is cut off from the actuators.
3. "Safe standstill" means all actuators are stopped but still powered. This is used in case of some manual interaction which should only cause minimal interruption of production. Special care must be taken to monitor the actors in this state.
4. "Safe Motion" state: if there is manual interaction needed while still some parts of the machine need to move, there are usually speed or position limits defined to guarantee safety. The limits depend on the operating conditions of the machine. So there can be several safe motion modes necessary for a machine.

Table 9 shows the safety functions of a drive applicable in each operating state of the machine.

Operating state	Safety Functions	Comment
Normal mode	Safe direction Safe maximum speed Safely-limited position	On top of locking out users from dangerous machine parts in Normal mode can have these safety functions which are implemented in the drive safety controller in oprion 2.
Safe standstill	Safe stop 1 Safe stop 2 Safe break control	Depending on machine type different stop functions can guarantee standstill
Emergency stop	Safe stop 1	Emergency stop is activated by the Emergency stop button or any safety monitoring function detecting an error.
Safe motion	Safely-limited speed Safe direction Safely-limited increment Safely-monitored position Safe maximum speed Safely-limited position	These safety functions can be combined and parameterized to form a set of 16 safe motion groups.

Table 9 - Operating state and safety function

Converting a safety drive solution for such a machine from option 1 to option 2 requires moving the safety state machine and the governing safety signals to a safety controller. The safety limits configuration stays in the drive.

The assembly interface defined by the profile in Table 7 and Table 8 show that all stop functions stay at the same bit positions as the direct select interface shown in Table 5 and Table 6. The 4 bit Group Select field enables the selection of 16 different safe motion modes.

Benefits of Drive Managed Motion Safety Functions – Option 2

1. Safety functions can be configured and pre-tested without a safety controller.
2. Easy migration path between option 1 (safety I/O hardwired to the drive) and option 2. Allows sophisticated safety functions in the drive using statically configured combinations which are dynamically selected.
3. As use cases exclude TCP monitoring no tight coupling to the motion controller is needed. The safety controller (Originator) can be a separate device on the network or integrated into the motion controller.
4. No calculation of analogue values is needed in the safety controller. All position and speed calculations are done in the drive device. This is valuable in machines using a large number of safe drives, allowing a lower class of safety controller being used.
5. Less data used for safety communication. If more than 2 bytes are used the inverse data and a larger checksum has to be exchanged. This adds load to the communication interface and is relevant in applications using a large number of safe drives.
6. Shortest possible reaction time to events exceeding limits. Especially for hydraulic applications this is in many cases the only possible solution.

Use Case example #1 - Single axis press-fit module

Description

In this example an OEM builds press-fit modules which implement a lot of functions including functional safety using an intelligent drive. These modules are used by machine builders for a variety of applications. As cost does not allow a separate safety controller for this module, the drive integrated safety functions (option 1 or option 2) are used. The module can be completely tested at the OEM site and responsibility for module safety can be kept separate from total machine safety. Different application dependent safety functions can be implemented by the OEM and need only be selected by the local safety signals at the drive.

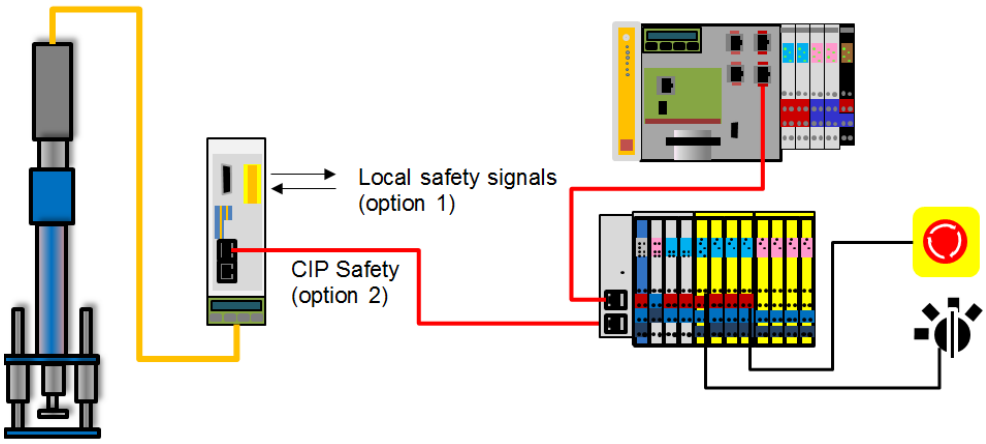


Figure 7 - Single axis press-fit module

Solution
The single axis press-fit unit is controlled by a drive with integrated safety stop and limit functions. The machine safety I/O is owned by the safety module of the PLC controlling the whole machine.
Safe Stop SS2 and Safe Limited Speed SLS functions are implemented in the drive. The safety PLC sends stop and SLS Signals when the condition of the machine requires this.

Use case example #2 - Woodworking machinery

Description
Woodworking machines usually have no housing or one open side. So there is need of safety functions under the constraint of maximum productivity. A mat detects a person standing in the dangerous area. Depending on the area the machine has to reduce speed or even do a full stop. As modern machines are operating at high speed, every ms from detection of the person to finally reaching the reduced speed counts. Drive integrated functional safety allows the signals to directly take effect on the control loop of the drive controller. This avoids delays of network and safety controller cycles. Depending on the distance of the person to the dangerous machine part the group select can choose the appropriate safety reaction (e.g. different reduced speed levels, also depending from axis position).

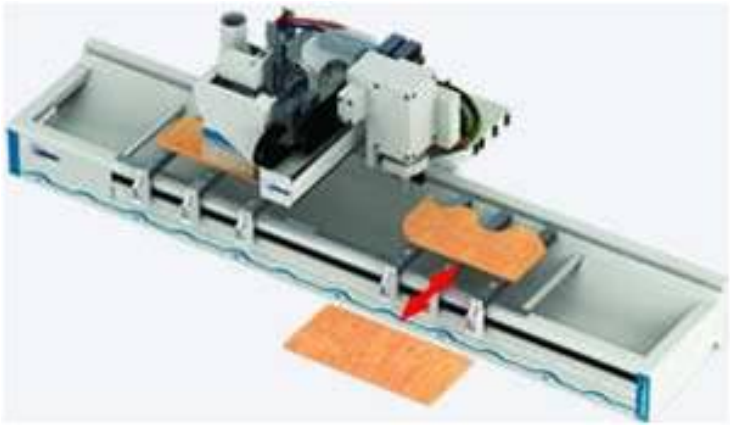


Figure 8 - Woodworking machine

Solution
The machine is controlled by a CNC. The safety controller is a separate unit and communicates safety signals to the network using CIP Safety. Safety I/O is connected locally to the safety controller but could also be connected remotely via CIP Safety. Speed limiting and safe stopping functions are configured in the drives. The two zones of the detection mat map to different safe limit group selects. In machines capable of high acceleration and needing a safe operational stop (SS2) it is essential to detect problems and react fast to guarantee no motion. If some problem in the motion controller leads to restart motion by command values, the drive detects this and can react within a position control loop. If a speed limit is violated the drive can react performing a SS1.

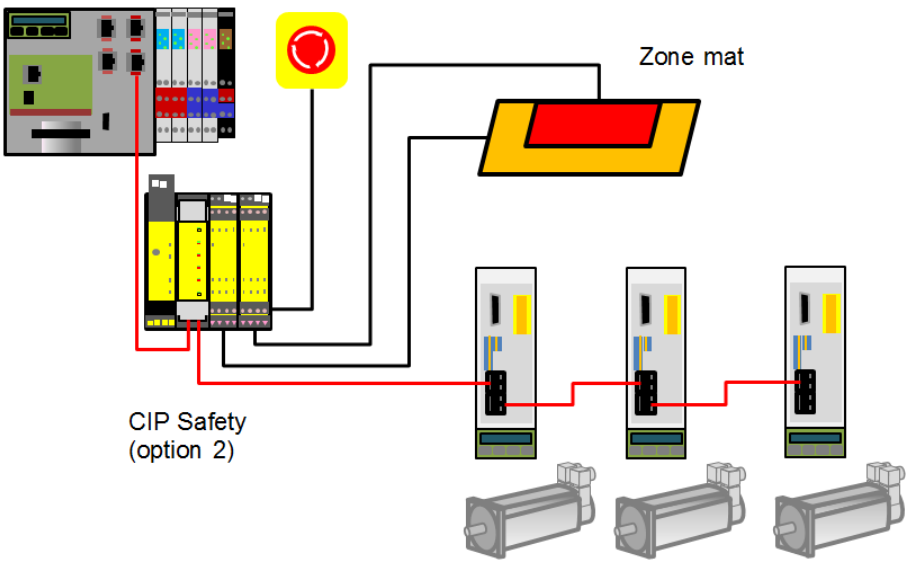


Figure 9 - Example structure of a woodworking machine

Use case example #3 - Printing machines

Description

Printing machines need manual interaction for exchange of printing plates, introducing a new paper web or cleaning the roller. Depending on the situation there are different constraints as moving only in one direction and different allowable speeds. Grouping the selected functions allows combinations of limiting functions for the operating conditions e.g.:

- Monitoring a maximum speed limit (SMS) for certain products at normal operation
- Monitoring direction (SDI-) and speed limit (SLS) for cleaning cylinders
- Monitoring a lower speed limit while changing printing plates. The speed limit is dependent on the direction of the motion.

Figure 10 - Change of printing plate

Solution
One printing unit usually consist of many cylinders each driven by an electric drive and some auxiliary drives. A (non-safe) motion controller controls via virtual axis line shafting application. Its add-on safety controller module owns the safety I/O. Due to the number of drive axis and limited performance of the safety controller, Safe Stop and limiting functions are chosen to be implemented in the drive controllers. The different limit functions map to the group selection of safety functions.

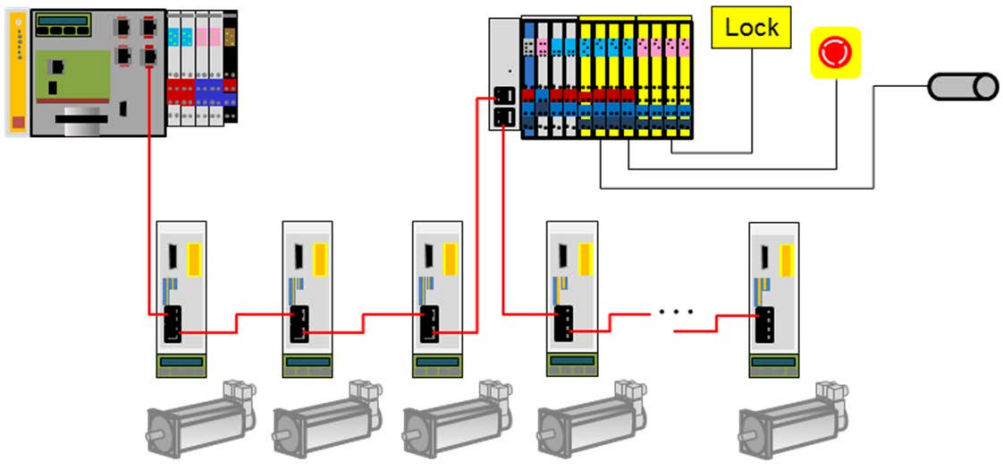


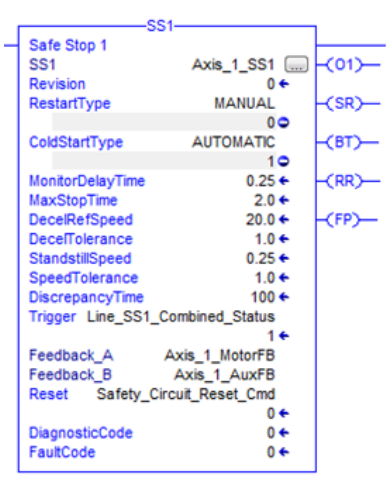
Figure 11 - Control structure of printing unit

Option 4 – Safety Controller Managed Motion Safety functions

With option 4 the STO safety function is activated and drive safety status is monitored by the safety controller using the drive network safety connections. Unlike Option 2 where the motion safety function execution is managed in the drive, the motion safety functions with the exception of STO are executed directly in the safety controller safety task application program using one or more motion safety instructions. Depending on the capability of the safety controller one or more safety instructions maybe available to support motion safety functions in the following categories:

- Disable power flow to the motor (i.e. STO)
- Safe brake control (i.e. SBC)
- 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)

An example of a typical motion safety instruction is shown in figure 12 for safe stop 1 (SS1)



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).

Figure 12 – SS1 Motion Safety Instruction

Safety data which may originate from a multitude of safety devices including the drive safety core and safety controller owned safety I/O is used during execution of the safety instructions. Safety data may include single or dual channel position, velocity, and acceleration information.

The safety controller sends STO activation request, monitors the drive safety status, and acquires drive safety data via the drive safety network input and output connections using the assemblies as defined in the Safety Motion Device Profile.

Examples of input/output assemblies supporting STO with drive supplied safety feedback position, velocity, and acceleration data are shown in table 10 and table 11.

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

Table 10 - 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

Table 11 - Safety Input Data with STO and Feedback Data

An option 4 controller architecture example is shown in figure 13. The Safety controller owns and manages the safety I/O. The safety controller executes the safety functions directly via the safety task application code using

safety instructions. Safety feedback data from the drive safety core and/or other safety feedback devices is used in the safety instructions. If the drive safety core is the source of the safety data then the drive network safety input connection with an input assembly as shown in table 10 would be used.

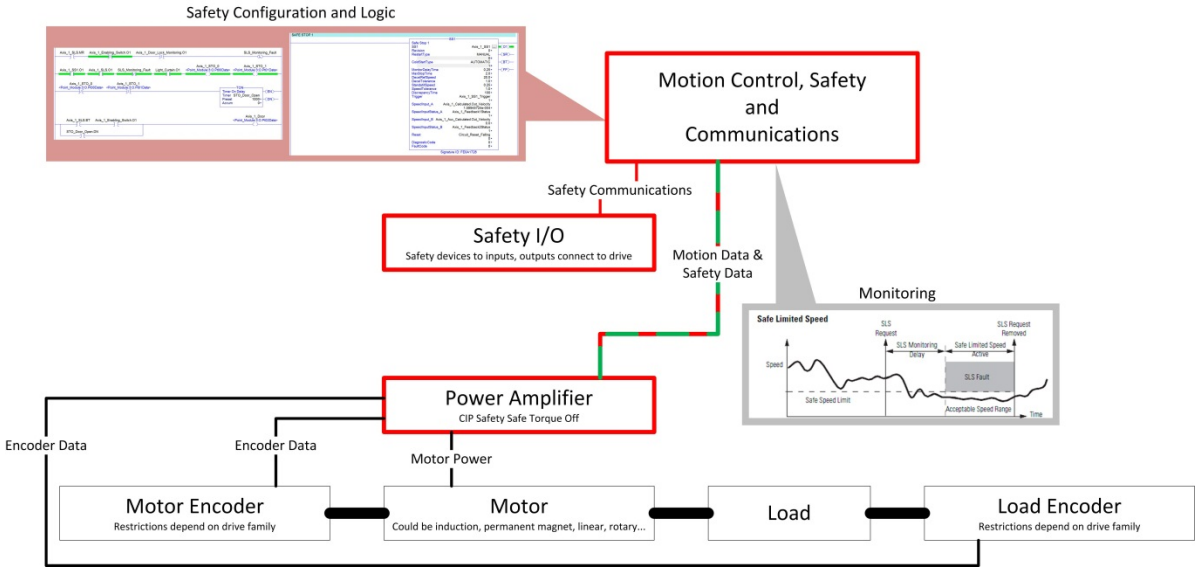
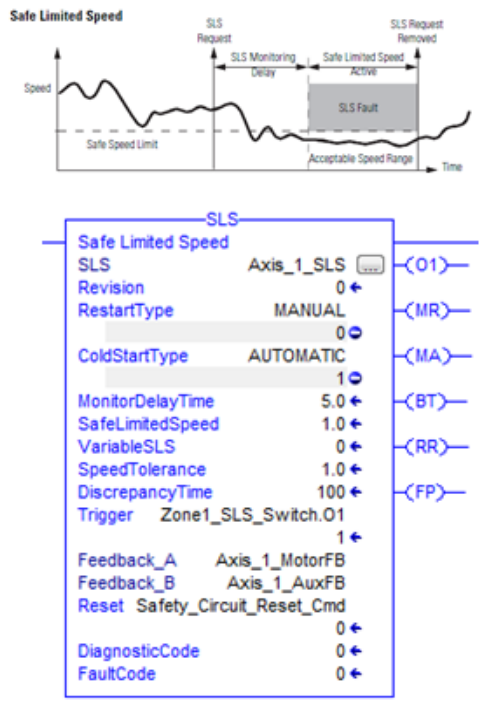


Figure 13 - Option 4 Control Architecture

An example safety function is SLS using the output assembly table 10, and input assembly in table 11. In this case the safe feedback data source is the drive safety core. The sequence is:

1. SLS safety instruction is executed in the safety controller application program (Example SLS instruction is shown in figure 14)
2. An SLS request handshake is received by the drive motion controller application program (there are multiple options for implementing the handshaking between the safety controller and Motion controller…or safety task and standard task) which is interpreted as a request to ramp down to a speed below the SLS monitoring speed setpoint
3. The safety controller manages the SLS monitoring function execution using the instruction input parameter data (i.e. monitoring delay, safe speed limit, speed tolerance, discrepancy time) and the safety feedback data from the drive (single or dual channel position, speed, acceleration)
4. If a safety fault is detected by the safety controller as the result of the SLS monitoring a STO activation request is sent to the drive safety core
5. Drive safety core executes a STO
6. Safety controller monitors the STO status



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. 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.
Monitor Requested (MR)	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 specified restart process has completed or a fault occurs.
Monitor Active (MA)	This output is energized when the Monitor Delay Time has expired. It will stay energized until the specified restart process has completed or a fault occurs.
Below Threshold (BT)	This output is energized when the Velocity values for Feedback A and Feedback B are both below the Safe Limited Speed configuration value and the monitor sequence is active. This output must energize before the Monitor Active (MA) output or else a fault will be generated.
Reset Required (RR)	This output is energized when the Reset input needs to be toggled to resume normal operation. This can occur with Restart Type Manual after 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).

Figure 14 - Option 4 SLS Instruction Example

Benefits of Safety Controller Managed Motion Safety Functions – Option 4

1. Single software package for managing safety – configuration, programming, commissioning, diagnostics, maintenance
2. Eliminates the need for individual drive/device safety configuration …safety configuration is unified in the safety controller
3. Flexible, centralized safety function execution supports complex safety logic
4. Coordinated safety function execution for an unlimited number of drives
5. Dynamic, runtime calculated or operator specification of safety function parameters for maximum flexibility and adapting to changing conditions and requirements…i.e. speed, acceleration, torque , position limit setpoints
6. Flexible safety feedback options – drive based feedback, network based device feedback, local I/O connected feedback or any combination can be used to achieve PLd and PLe.
7. “Path” based safe functions…i.e. robot TCP safety monitoring which requires multi-axis kinematics functions
8. Support for safe stopping and safe limiting functions for drives/devices that only support the minimum STO capability

Use Case Examples for Option 4 – Safety Controller Managed Motion Safety functions

Use Case Example #1 – SLS for variable diameter wind/unwind roll

Description

This use case is SLS monitoring of the surface speed of a winder roll. This is a PLd rated solution with a single motor mounted safety feedback device.

The Motor drives the winder roll at a variable speed to maintain a constant surface feet per minute (SFPM) as the web is wound onto the winder roll. As the web is wound, the winder roll diameter increases. The instantaneous winder roll diameter is used to derive the required motor speed to maintain the required SFPM web speed.

There are scenarios where the machine operator has to perform maintenance operations in the vicinity of the winder roll with the guard doors open. The maintenance operation requires jogging the winder roll with SLS monitoring of the roll circumference speed (web speed).

The control architecture is shown below. The controller provides both standard control (standard control task) and safety control (safety control task) of the drive/motor which rotates the winder roll. The standard control task manages the position/velocity/acceleration profile of the drive while the safety control task manages the safety monitoring functions. Safety I/O owned by the safety controller includes two analog inputs which are used to determine the roll diameter for the SLS speed setpoint calculation.

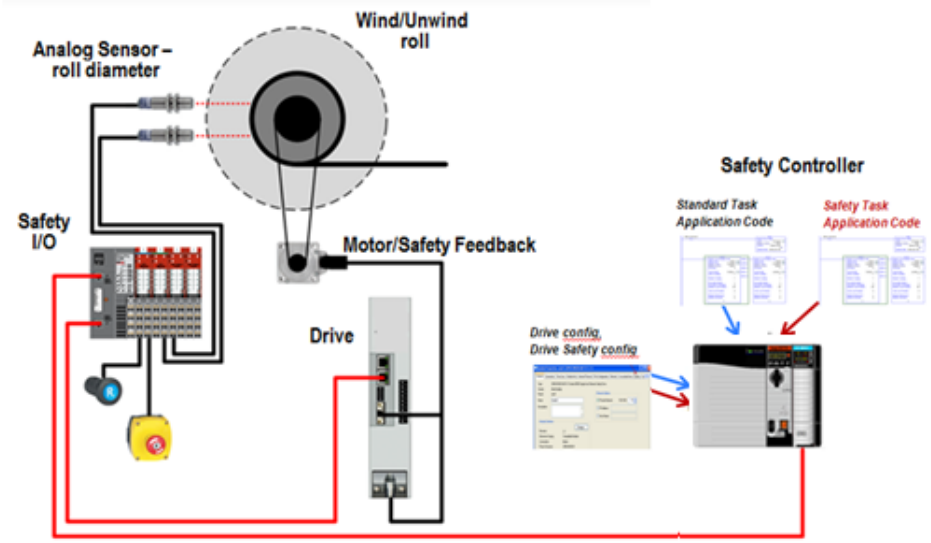


Figure 15 - Winder Control Architecture

Solution

The controller application program provides dynamic SLS monitoring of the winder roll circumference speed. The basic sequence in the controller safety task application program is:

1. Open guard door state is detected (safety task)

2. SLS setpoint is calculated using analog inputs for the roll diameter calculation….the setpoint calculation can be executed as a one-time event on request or on a continuous basis at some specific update rate (safety task)
3. SLS request with the SLS setpoint is sent to the standard task (safety task/standard task)
4. The drive is ramped to speed < SLS speed setpoint calculated in (2) (standard task)
5. SLS monitoring instruction is executed with the following key parameters (safety task):
    a. Safe limited speed
    b. Monitoring delay time
    c. Variable SLS mode enabled
    d. Speed tolerance
    e. Discrepancy time

    NOTE: Steps 4 and 5 are concurrent…SLS monitoring is active while the drive speed is being ramped down, the monitoring delay time can be used to coordinate the two operations.
6. If after the monitoring delay time out the speed exceeds the SLS Speed Setpoint the Fault Present output will be set (safety task)
7. Fault Present output generates an STO activation request to the drive (safety task)

Typical safety task application code for calculating the safe limited speed setpoint and enabling the SLS monitoring is shown figure 16. Typical standard task application code for changing the speed of the windup roll is shown in figure 17.

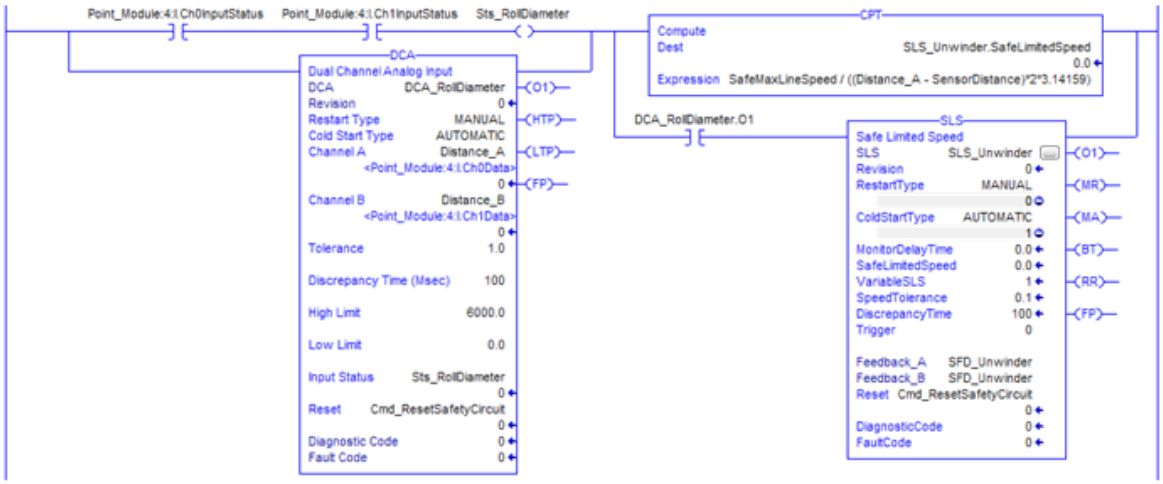


Figure 16 - Typical Logic for calculating the SLS setpoint using measured roll diameter and enabling SLS monitoring

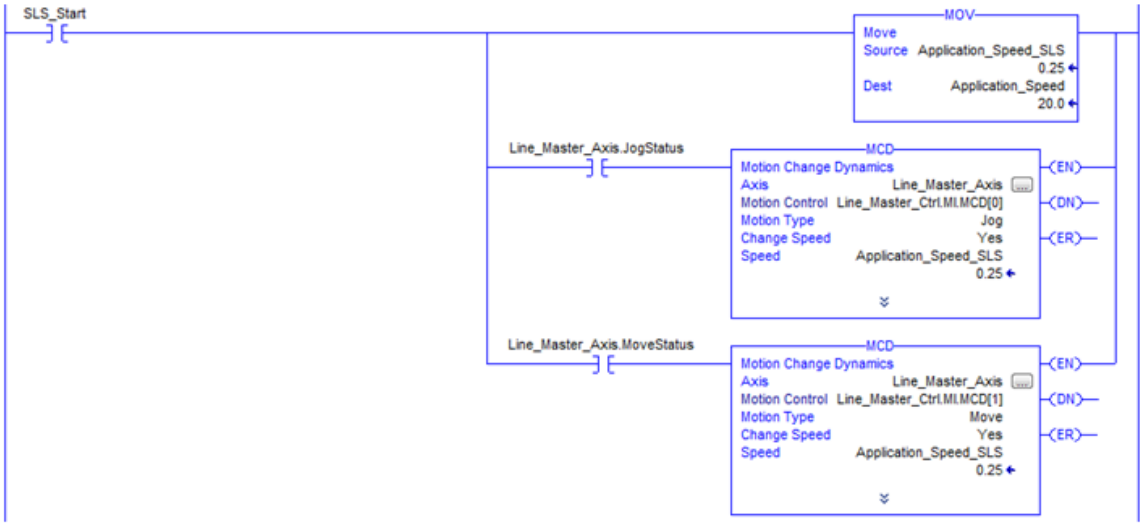


Figure 17 - Typical Logic for coordinating action between the standard task motion profile control (windup roll speed) and the safety task safety monitoring functions

Use Case Example #2 – Coordinated safe line stop (SS1)

Description

This use case is a coordinated safe line stop (SS1) of a web line.

There are four drives that are geared to a line master axis (typically a virtual axis) which propel the web. When the operator pushes the line stop safety switch button the line will ramp to a coordinated, controlled stop, with SS1 safety monitoring in place for each of the four drives. The line ramp rate can be changed by the operator using an operator interface or via a downloaded setpoint recipe.

The control architecture is shown in figure 18. The controller provides both standard control (standard control task) and safety control (safety control task) of the four drives and the virtual line master axis. The standard control task manages the position/velocity/acceleration profile of the drives while the safety control task manages the safety monitoring functions for the drives. The four drives are geared to the line master axis, performing a controlled stop of the line master axis will result in the four drives stopping in full coordination with the line master axis and with each other. Safety I/O is owned by the safety controller and includes the safety line stop switch input. The operator is used to enter/change the line start/stop ramp rate and line speed.

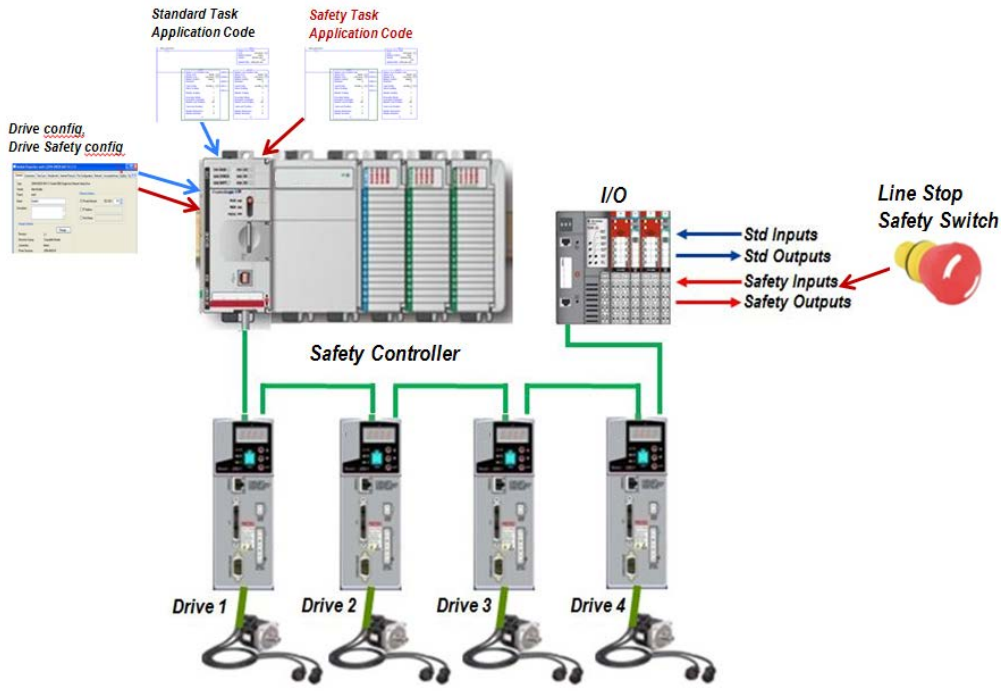


Figure 18 - Coordinated Line Control Architecture

Solution

The controller safety task application program provides SS1 monitoring of drives 1-4 in response to a safe line stop request. The controller standard task application program provides a coordinated ramp down of the line in response to the safe line stop request. The sequence in the safety task and standard task application program is:

1. Line stop safety switch input is detected (safety task)
2. SS1 request is sent to the controller standard task (safety task/standard task)…initiate line stop
3. A line master axis ramped stop is initiated…drives 1 through 4 will follow based on their geared relationship to the line master axis resulting in a coordinated stop of the drives (standard task)
4. SS1 monitoring instruction is executed for each drive with the following key parameters (safety task):
    a. Monitor delay time
    b. Maximum stop time
    c. Deceleration reference speed
    d. Standstill speed

    NOTE: Steps 3 and 4 are concurrent…SS1 monitoring is active while the drive speeds are being ramped down, the monitoring delay time can be used to coordinate the two operations.

5. Once standstill speed is detected on a drive a STO activation request is sent to that drive (safety task)
6. Assuming no safety faults, the line comes to a controlled stop via the line master axis stop, and the SS1 monitoring of drives 1-4 is satisfied, resulting in a STO final state for drives 1-4 (safety task)

Typical safety task application code for initiating SS1 monitoring for the 4 drives is shown in figure 20. Typical standard task application code for ramping the line to a controlled stop is shown in figure 19.

Figure 19 - Typical standard task application program logic for initiating a controlled line stop via the line master axis (Standard Task)

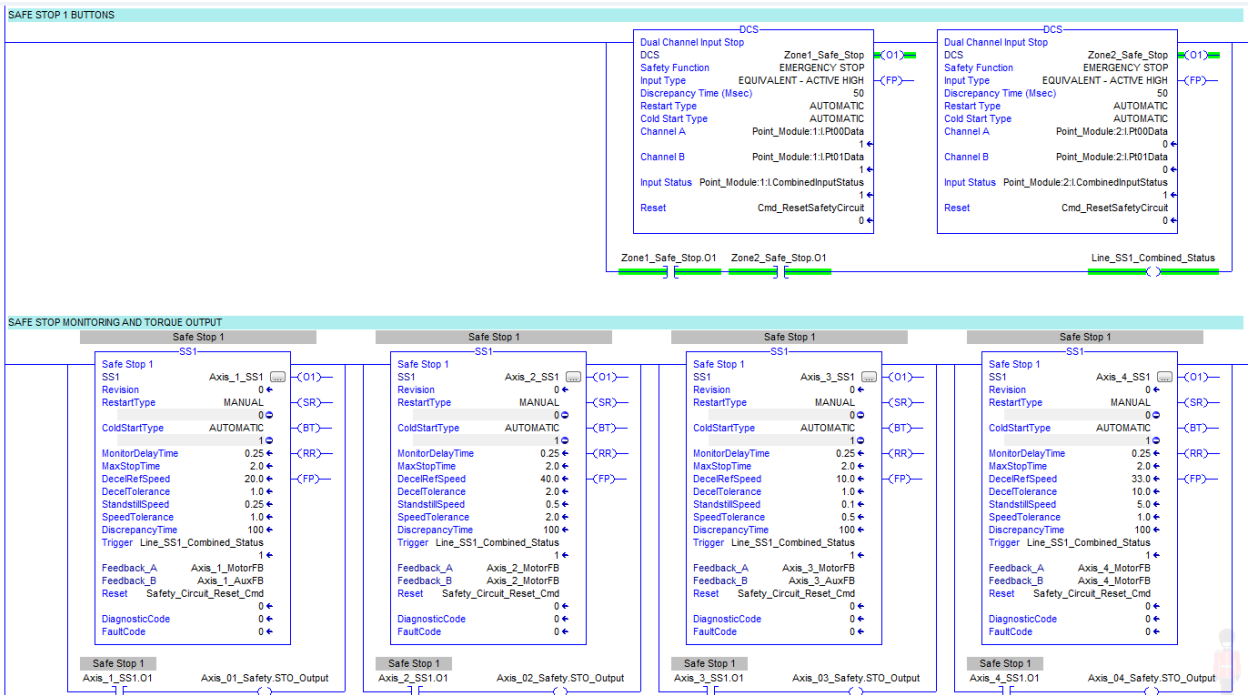


Figure 20 - Typical safety task logic for enabling SS1 monitoring on drives 1-4 (Safety Task)

Comparison:
A summary of option 2 and option 4 key attributes is provided in Table 12.

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

Table 12 – Option 2 and Option 4 Safety Architecture Comparison

Conclusion:
This paper discussed the migration from simple, hardwired safety solutions which provide basic machine guarding/shutdown solutions to flexible, safety controller based safety solutions in which drives with networked safety support are a key component. A review of the recently developed CIP Safety drive Profile and supporting safe motion objects specification support for the EN 61800-5-2 safety functions was presented. Four different motion safety architecture options were defined and reviewed with a more in-depth analysis of the option 2- Drive managed motion safety functions, and option 4- Safety controller managed motion safety function architectures. A number of application use cases were presented to illustrate typical system solution implementation characteristics for the option 2 and option 4 architectures.

References:

[1] P. Hampikian, B. Hirschinger und L. Leurs, *CIP Safety for Drives*, Stone Mountain: ODVA Industry Conference, 2012.

[2] ODVA, *The CIP Networks Library, Volume 5, CIP Safety, Edition 2.8,* Ann Arbor: ODVA, 2013.

[3] IEC, *EN61800-5-2 "Adjustable speed electrical power drive systems - safety requirements - functional"*, IEC, 2008.

****