CIP Safety for Drives

Pascal Hampikian
System Strategy & Architecture Marketing Leader
Schneider Electric

Bob Hirschinger
Principle Applications Engineer
Rockwell Automation

Ludwig Leurs
Project Director Ethernet Convergence
Bosch Rexroth AG

Presented at the ODVA
2012 ODVA Industry Conference & 15th Annual Meeting
October 16-18, 2012
Stone Mountain, Georgia, USA

Abstract

The implementation of safety functions on networks for drive applications is emerging as a critical requirement for industrial applications. This paper will propose the application of safety networking for use in systems deploying drives.

Introduction

Machine safety has been an important aspect of industrial automation for the last four decades. Once considered a cumbersome solution that not only reduced productivity but also promoted even more dangerous operator behaviors, contemporary safety solutions now offer the opportunity to protect people and equipment while enhancing machine performance. Recent studies conducted by the Aberdeen Group indicate that companies with the highest overall equipment effectiveness (OEE) also have the lowest incidence rate of lost work time injuries and lowest rate of repeat injuries. Characteristically, those companies have a strong safety culture and invest in contemporary safety technologies.

In many ways, safety technology is following a similar evolutionary curve as that experienced in standard control. Today safety innovations are focused on integrated safety, networked safety and rapid growth of networked safety devices. These innovations are paving the way for both design time and run time performance enhancements for machines. By providing easy configuration, extensive diagnostics and scalable solutions to fit the application, machine builders are able to design machines that provide the appropriate level of safety relative to the hazard and risk, while allowing operators, engineers, maintenance easy access.

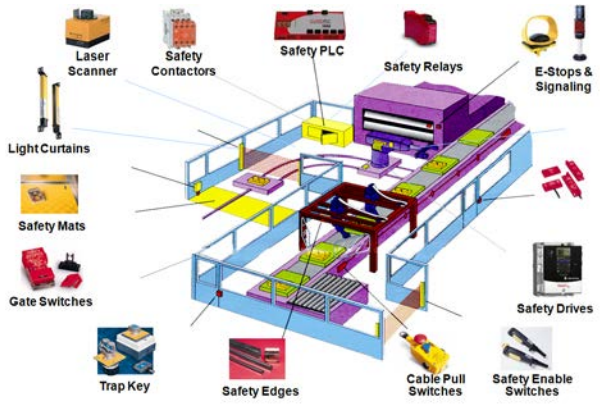

Figure 2 - 1 Safety Devices

To illustrate this evolution, please refer to Figure 2-1 which highlights the broad range of safety components found on a typical production line from simple devices like safety relays, to complex devices like drives and highly capable safety controllers/PLC's. In the past, many applications deployed safety devices in a standalone, hardwired mode where safety was managed locally at the device…..device safety network support was not required. For example safe drives required dedicated local safety I/O and supported a limited range of safety functions like safe torque off and safe stopping. The drives safety configuration was managed locally using web browsers or dedicated software tools and the drives require dedicated safety I/O to support the safety functions.

For larger, more complex safety solutions the current trend is to implement a fully programmable, flexible safety solution architecture using powerful safety PLC's with networked safety devices that are fully integrated into the machine process. The safety PLC based architecture is appropriate 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

This architecture requires safety devices with safety network capability supporting safety configuration, safety function activation, and safety status monitoring. Figure 2-2 shows the range of safety solution options.

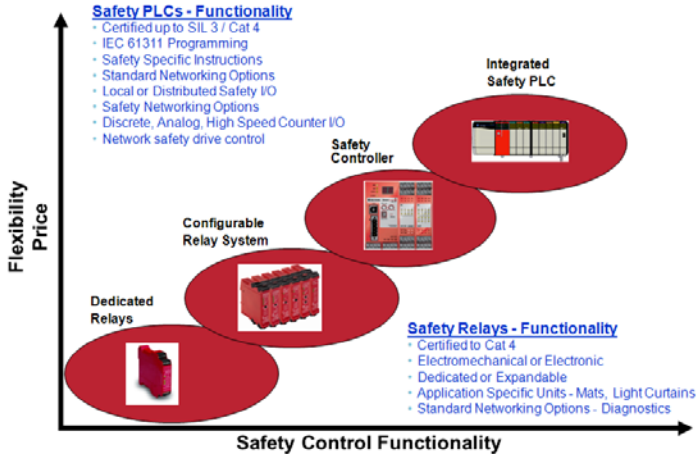

Figure 2 - 2 Safety System Options

An example of an Safety controller/PLC based controller architecture is shown in figure 2-3 below. Networked safety drives are often a critical safety component in the safety controller/PLC based architecture. Safety drives offer basic and advanced safety functions with safety configuration, safety function activation, and safety status monitoring support via a network safety connection. Modern network technology allows safety devices like safety discrete I/O, safety analog I/O, drives with safety core, and other safety devices with safety support to coexist with standard control devices on a common network

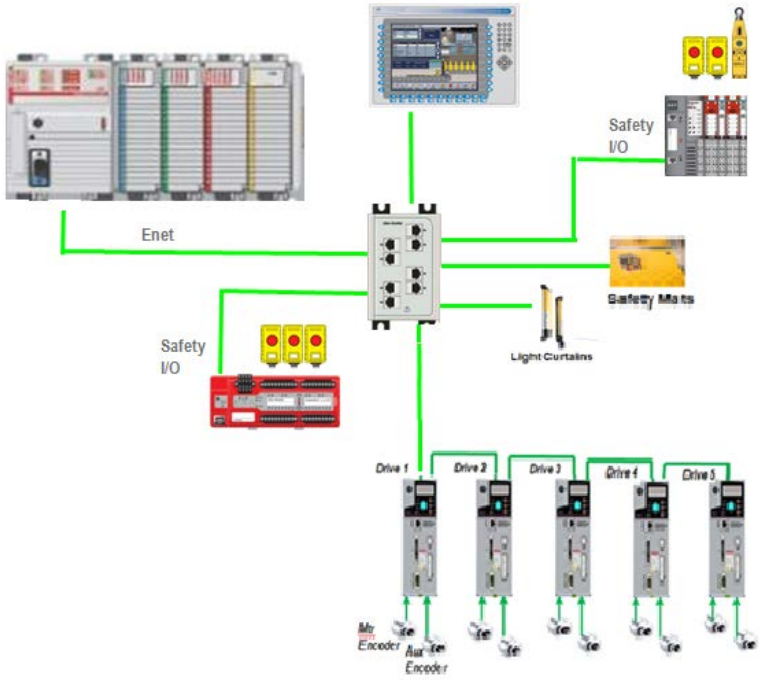

Figure 2 - 3 Safety Controller/PLC Based Architecture

This paper presents requirements and implementation considerations for networked drive safety support using CIP Safety. This includes CIP Networks (EtherNet/IP and DeviceNet), and SERCOS III. Specific subjects that will be covered include:

1. EN61800-5-2 drive safety functional review
2. Drive safety architecture option review
3. CIP Safety Safe Motion Sub-committee work plan and deliverables

Safety standards and drive safety functions

There are a range of standards which provide device and machine level safety requirements. Some of the relevant standards are shown in Figure 2-4 below.

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

Figure 2 - 4 Safety Standards

The EN61800-5-2 “Adjustable speed electrical power drive systems safety requirements functional” standard is of particular interest for drive systems. It defines a broad range of drive safety functions as listed in Figure 2-5.

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 initiates 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 devisting 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

Figure 2 - 5 EN61800-5-2 Drive Safety Functions

These safety functions can be categorized into general groups of:

- Disconnect Torque generating power feed to the motor (i.e. 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)

An overview of “typical” functionality associated with some of these safety functions is provided below.

Safe Torque-off (STO)

STO is used to disable the torque generating power feed to the motor. 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 2-6 shows a typical timing diagram for an STO sequence.

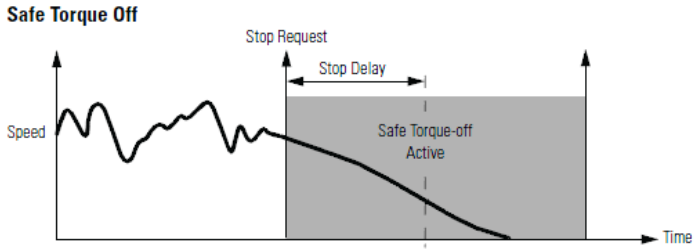

Figure 2 - 6 Safe Torque Off (STO) Timing Diagram

Safe Stop 1 (SS1)

SS1 is used to decelerate the motor followed by an STO. 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 2-7 shows a timing diagram for a typical SS1 sequence.

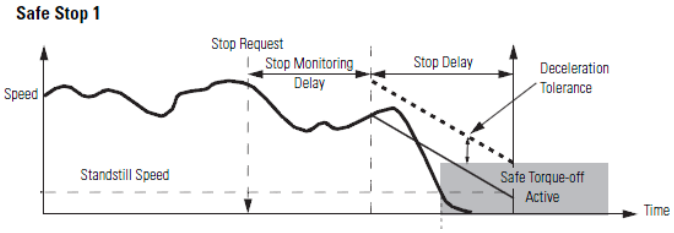

Figure 2 - 7 Safe Stop 1 (SS1) Timing Diagram

Safe Stop 2 (SS2)

SS2 is used to decelerate the motor followed by safe operational stop (SOS) monitoring. A typical implementation includes the SS2 stop request input, stop monitoring delay parameter, stop delay parameter, deceleration tolerance parameter, and standstill speed parameter. On occurrence of a SS2 safe stop request the deceleration ramp will be monitored after the stop monitoring delay expires. After the motor speed is below the Standstill speed then the position & velocity of the motor will be monitored to insure no movement (Safe Operational Stop - SOS). Unlike SS1 the motor torque producing power remains enabled unless a safety fault occurs. Figure 2-8 shows a timing diagram for a typical SS2 sequence.

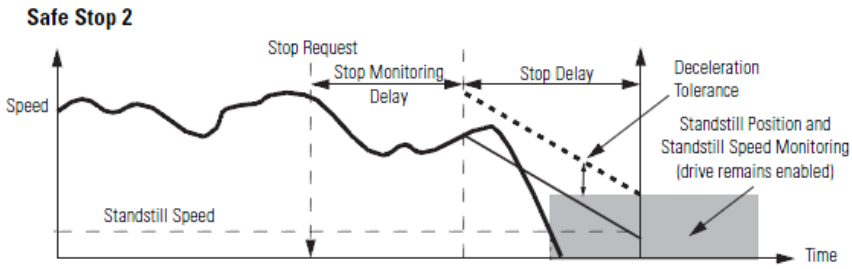

Figure 2 - 8 Safe Stop 2 (SS2) Timing Diagram

Safe Limited Speed (SLS)

SLS is used to insure the speed of the motor does not exceed a minimum value. 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 2-9 shows a timing diagram for a typical SLS.

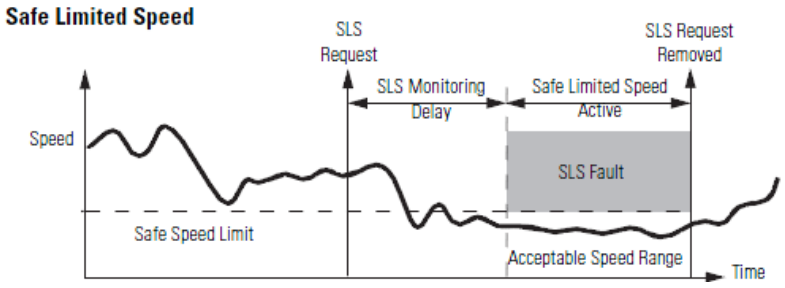

Figure 2 - 9 Safe Limited Speed (SLS) Timing Diagram

Drive Safety Core

Drives may support all or a subset of the 61800-5-2 safety functions with STO being a minimum requirement. To support these safety functions a 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 EN61508 SIL 3 levels. An example of a typical drive safety core is shown in Figure 2-10.

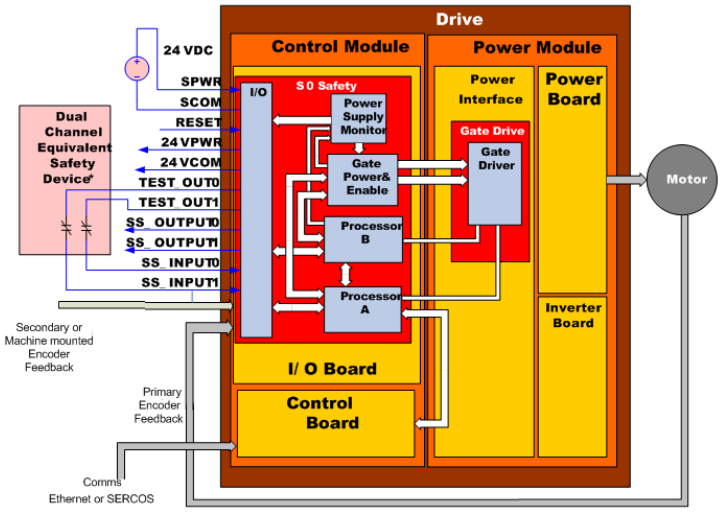

Figure 2 - 10 Typical Drive Safety Core

The typical drive safety core includes dual channel safety I/O (safety I/O is optional for drives with a safety network interface), safety network interface, primary and secondary position/velocity feedback, dual redundant processor safety core with gate drive interface to disable torque producing current to the motor, and firmware to support a range of 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 safety functions, and the safety interface to the drive.

Drive Safety Architecture Options

In this paper, four different Drive safety architecture options are defined below and summarized in Figure 2-11.

OPTION 1 - Drive safety I/O activated drive safety functions
OPTION 2 - Safety controller activated drive safety functions via drive network safety connection
OPTION 3 - Safety controller configured and activated drive safety functions via drive network safety connection
OPTION 4 - Safety controller executed drive safety functions - drive safety data via drive network safety connection

	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

Figure 2 - 11 Safety Architecture Option Summary

A description of each option is provided below. To illustrate the differences between the four options a safety application example *"**safe stop (SS1) with guard gate lock control**"* operation is shown for each option.

OPTION 1 Architecture

Drive safety I/O activated drive safety functions

With this option the drive safety functions are activated and safety status is monitored using local drive safety I/O. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is managed locally at the drive using a web browser, software utility, or similar. This option does not require a drive network safety connection.

Figure 2-12 shows the drive with safety core with the safety I/O connected to the drive including the E-Stop safety switch, and Guard gate safety control. Also shown is a typical wiring diagram for the drive safety I/O. A typically drive safety configuration GUI is shown which is used to configure the operation of the safety I/O and the SS1 stop and the safety guard lock sequencing.

Safe stop with guard gate control sequence description

1. Safe Stop (SS1) is activated via a E-Stop safety switch input on the drive
2. SS1 is managed by the drive safety core as defined by the drive SS1 safety configuration
3. After successful SS1 completion the guard gate is unlocked by the drive safety core via the Guard gate safety control output

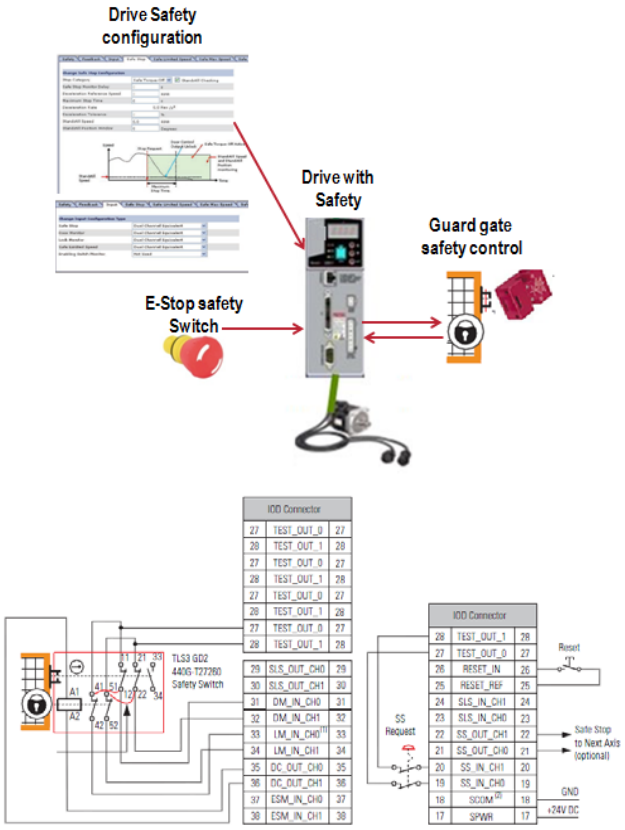

Figure 2 - 12 Safety Stop With Guard Door Interlock – Option 1 Architecture

OPTION 2 Architecture

Safety control activated drive safety functions via drive network safety connection

With this option the drive safety functions are activated and safety status is monitored by the safety controller using the drive network safety connection. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is managed locally at the drive using a web browser, software utility, or similar.

Figure 2-13 shows the drive with safety core and the Safety control with safe network connection to the drive. All safety I/O is managed by the safety controller including the E-Stop safety switch input, and Guard gate safety control output. A typically drive safety configuration GUI is shown which is used to configure the SS1 operation.

Safe stop with guard gate control sequence description

1. Safe Stop request (SS1) is detected by the safety controller E-Stop Safety Switch input and a SS1 request is sent to the drive via safety network connection.

2. SS1 stop is initiated and controlled by the safety core of the drive as defined by the drive SS1 safety configuration
3. The drive SS1 stop status is monitored by the Safety controller via status data returned over the safety network connection from the safety core of the drive.
4. After stop and disable of motor power the guard gate is unlocked by the Safety controller via a safety discrete output (Guard gate safety control)

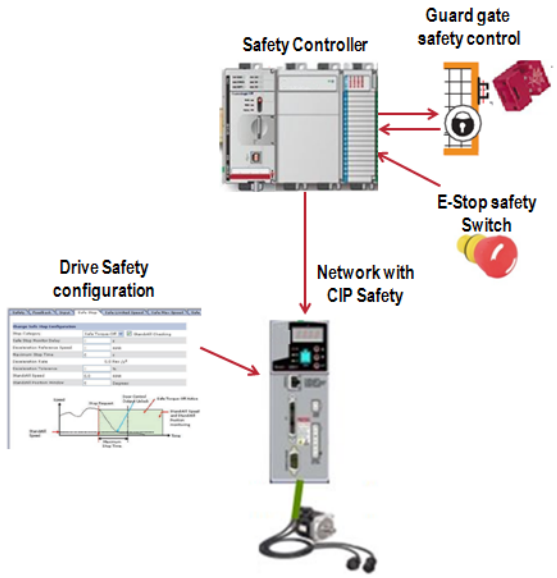

Figure 2 - 13 Safety Stop With Guard Door Interlock – Option 2 Architecture

OPTION 3 Architecture

Safety control configured and activated drive safety functions via drive network safety connection

With this option the drive safety functions are initiated and status is monitored using the drive network safety connection. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is managed at the Safety controller and sent to the drive safety core as runtime parameters along with the safety function activation request.

Figure 2-14 shows the drive with safety core and the Safety controller with network safety connection to the drive. All safety I/O is managed by the safety controller including the E-Stop safety switch input, and Guard gate safety control output.

Safe stop with guard gate control sequence description

1. Safe Stop request (SS1) is detected by the safety controller E-Stop safety switch input and an SS1 activation request along with the SS1 configuration data is sent to the drive via the drive network safety connection.
2. SS1 stop is initiated and controlled by the drive safety core as defined by the drive SS1 safety configuration sent from the safety controller
3. The drive SS1 stop status is monitored by the Safety controller via status data returned over the safety network connection from the safety core of the drive.
4. After SS1 is complete, the guard gate is unlocked by the Safety controller via the Guard gate safety control safety output

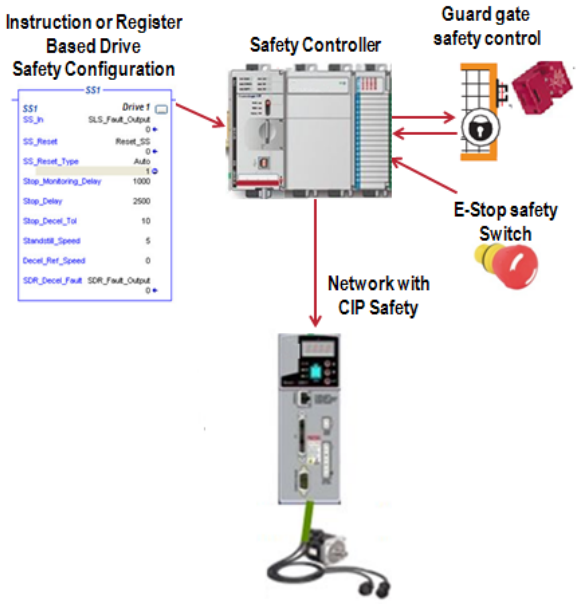

Figure 2 - 14 Safety Stop With Guard Door Interlock – Option 3 Architecture

OPTION 4 Architecture

Safety controller/PLC execution of drive safety functions - drive safety data via drive network safety connection

With this option only the STO safety function is directly managed in the drive. The drive safety functions are directly executed in the safety controller using safety instructions (i.e. SS1 instruction) and safety status data from the drive safety core via the drive network safety connection. Safety status data includes STO status, safety feedback data – position, velocity, acceleration. With this approach the safety feedback data for the drive safety core is used in the Safety Controller safety task to perform the safe speed, safe position monitoring functions. An example of the feedback data is shown below.

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

Figure 2-15 shows the drive with safety core and the Safety control with drive network safety connection. All safety I/O is managed by the safety controller including the E-Stop safety switch input, and Guard gate safety control output.

Safe stop with guard gate control sequence description

1. Safe Stop request (SS1) is detected by the safety control E-Stop safety switch input and an SS1 command is executed in the safety controller.
2. SS1 stop is managed by the safety controller using safety status data from the drive.

3. STO is sent to the drive safety core via the drive network safety connection as appropriate as part of the SS1 execution.
4. After STO is complete, the guard gate is unlocked by the Safety controller via the Guard gate safety control safety output

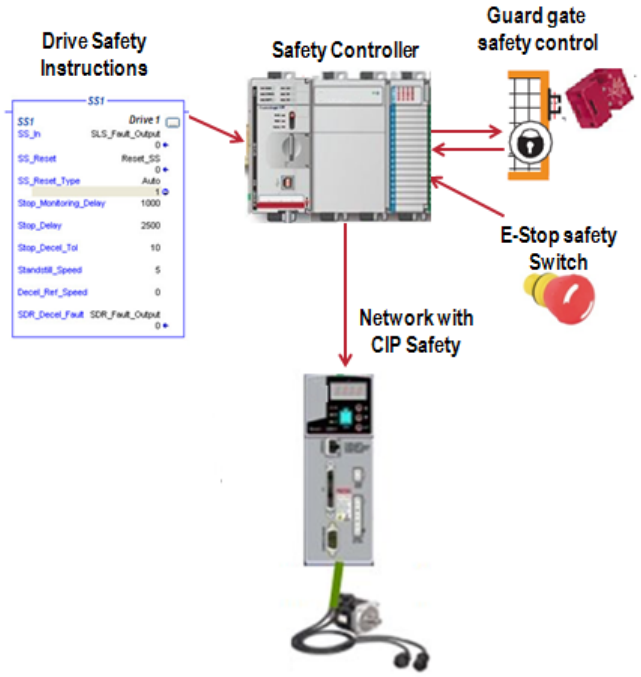

Figure 2 - 15 Safety Stop With Guard Door Interlock – Option 4 Architecture

Use Case Examples

Use case examples are provided below for the Option 2 architecture and the Option 4 architecture.

Option 2 Use Case Example

Light curtain input Safe Stop 1 (SS1) on Drive 1

Description:

This application includes a safety controller with an Ethernet network connection to 4 drives and a safety I/O block. The safety controller has a standard task for user application logic execution and a safety task for user safety application logic execution. Each drive has an Ethernet standard connection and an Ethernet CIP Safety connection via a single physical network port. The standard connection is used to manage the drive motion and the safety connection is used to activate safety functions in the drive safety core and provide drive safety status data to the safety controller.

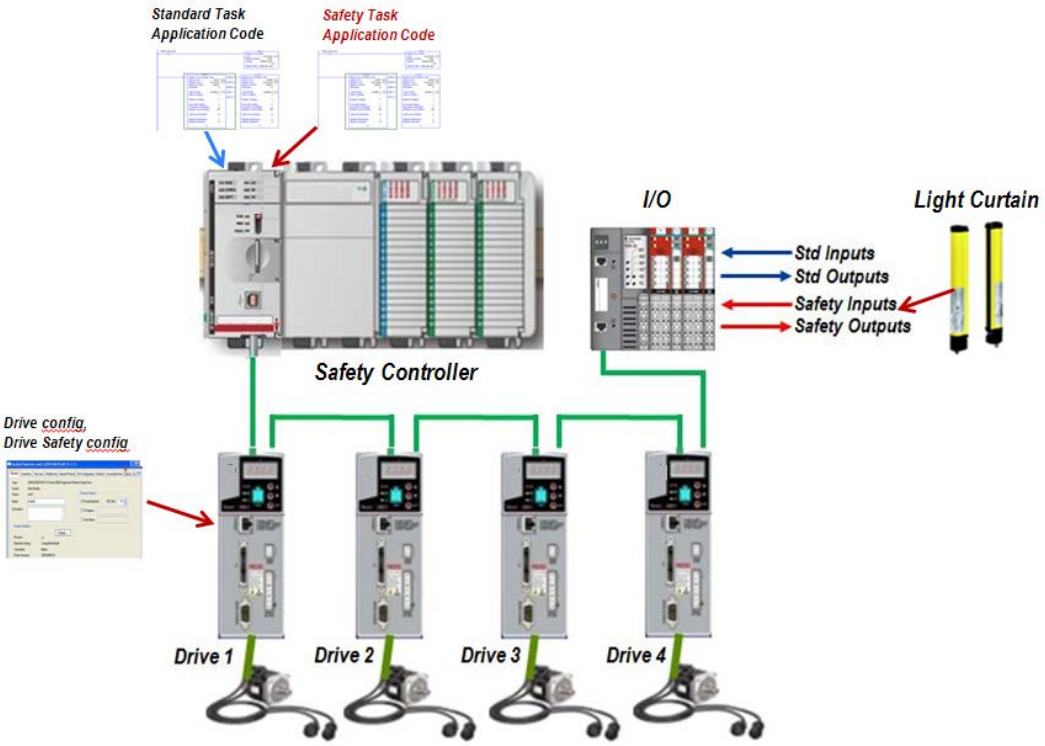

Figure 2 - 16 Option 2 Use Case Example Architecture

Safety Requirement:
When light curtain safety input transitions from on to off a safe stop 1 (SS1) on drive 1 is executed. The SS1 status is available for use in the safety controller application program safety task user application logic.

Figure 2 - 17 SS1 Timing Diagram

Sequence – Light curtain safety input triggered SS1 stop of Drive 1:

1. Light curtain safety input transition detected in the Safety controller Safety Task (safety input via CIP Safety connected safe I/O block)
2. The Safety controller safety task application code sends an SS1 request to drive 1 using the CIP Safety drive safety output assembly (safety activation code = SS1)
3. The SS1 request is detected by the drive safety core and it initiates/manages an SS1 stop as configured in the drive. (Configuration parameters -> stop monitoring delay, stop delay, deceleration tolerance, standstill speed)

4. The drive safety core returns safety status via CIP Safety drive input assembly to be used in the safety task user application logic.

Option 4 Use Case Example:
Machine line stop input coordinated line stop with Safe Stop 2 (SS2) on drives 1-4

Description:
This application includes a Safety Controller with an Ethernet connection to 4 drives and a safety I/O block. The Safety Controller has a standard task for user application logic execution and a safety task for user safety application logic execution. Each drive has an Ethernet standard connection and a CIP Safety connection via a single physical Ethernet port. The standard connection is used to manage the drive motion from the safety controller standard task and the safety connection is used to activate safety functions (STO) in the drive and provide safety status data to the safety controller. The SS2 function is completely managed in the safety controller. This application is a web feed line where drives 1-5 are coordinated via gearing to a common virtual axis line master.

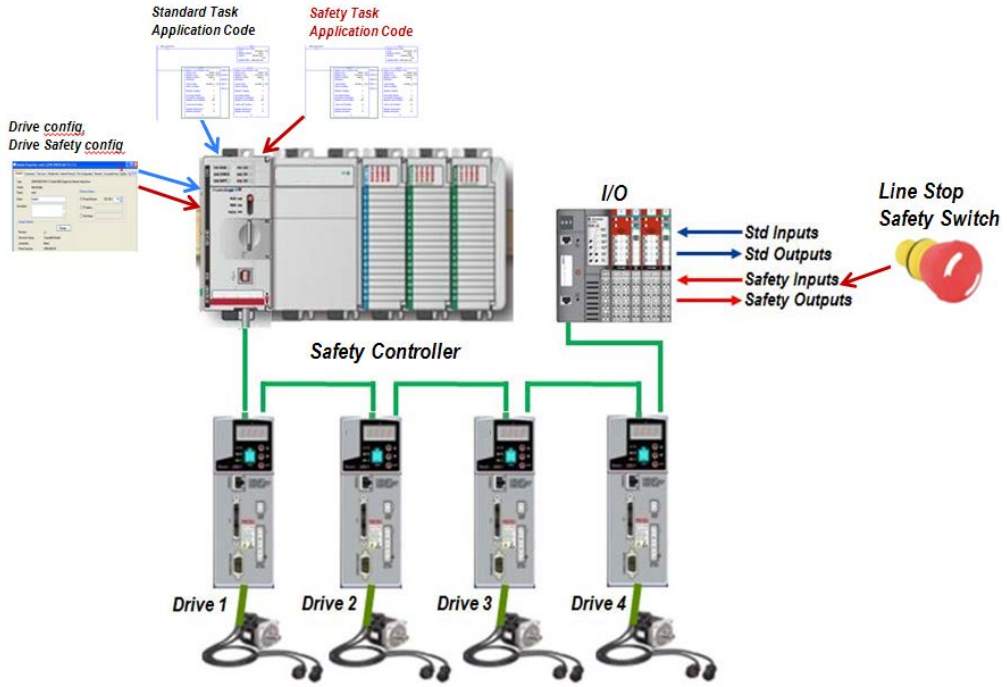

Figure 2 - 18 Option 4 Use Case Example Architecture

Safety Requirement:
When the machine line stop safety input transitions from on to off, initiate a SS2 (safe stop 2) on drive 1 through drive 5 using a coordinated/controlled line stop. This is a converting machine with a continuous web and a coordinated line stop is required to insure the web is not broken.

SS2 Instruction Description:
An instruction and timing diagram example is shown below for SS2. The SS2 instruction is called and executed in the safety task of the safety controller as part of the user safety task application program and initiates the safe SS2 monitoring functions. The user application program in the standard task works in conjunction with the SS2 instruction in the safety task to execute the required stopping action. In this

application the SS2 safety function provides safe stop monitoring only, it does not provide direct control of the drive motion profile.

SS2 Safety Controller Instruction

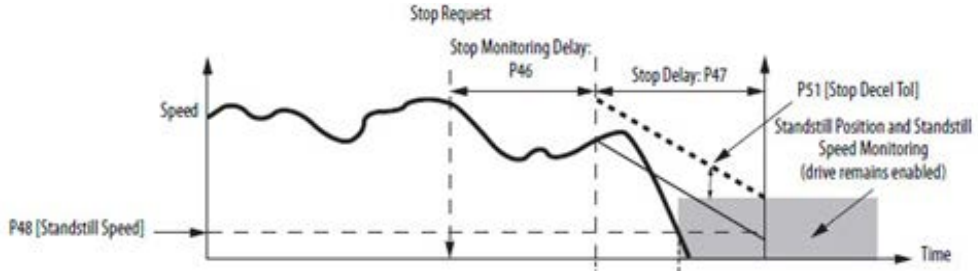

Figure 2 - 19 SS2 Timing Diagram

Sequence – Machine line stop safety input triggered coordinated line stop with SS2 monitoring of Drive 1 through Drive 5:

1. Machine line safety input transition detected in the safety controller Safety Task (safety input via CIP Safety)
2. An SS2 instruction per drive with user defined input parameters is executed in the safety task application program. The SS2 instruction input parameters define the SS2 operation including Stop_Monitoring_Delay, Stop_Delay, Stop_Decel_Tol, and Standstill_Speed. There is one SS2 instruction instance for each drive 1 through 5.
3. The safety controller safety task application code handshakes with the standard task application code to initiate a coordinated line stop from the standard task.
4. The Standard task user application program logic initiates a coordinated line stop of drive 1 through drive 5 by performing a ramped stop of the virtual master axis (drives 1-5 are geared to the virtual master) with a given deceleration profile and decel rate
5. The Safety task performs the SS2 monitoring on drives 1-5 per the SS2 instruction.
6. Assuming no faults, the line comes to a controlled stop through the virtual axis stop, and the SS2 monitoring of drives 1-5 is satisfied, resulting in a SOS stop condition for drives 1-5.

CIP Safety Safe Motion Sub-committee Work Plan

As discussed in this paper there is increasing adoption of flexible safety solutions using a safety controller/PLC with networked safety device connectivity. CIP Safety technology allows safety devices like safety discrete I/O, safety analog I/O, drives with safety core, and other safety devices with safety support to coexist with standard control devices on a common network. While there are published open CIP Safety profiles for *"Safety Discrete I/O"* and *"Safety Analog I/O"* available today, published, open profiles are not available for drives with a safety core. To that end a CIP Safety Safe Motion Sub-committee has been formed to develop a *"drive safety profile(s)"* to be voted on by May 2013 in time for publication in the fall 2013 CIPSE edition.

The Safe Motion Sub-committee deliverables include:

- Data model for safe motion
  - Mapping of a safe motion data model to objects
  - Services required to support safe motion
  - Development of the device profile
    - Set of objects, interfaces, and data assemblies.

The focus of the Safe Motion Sub-committee will be on the "Option 2" architecture described in this paper. This includes support over the network safety connection for (1) drive safety function activation, and (2) drive safety status monitoring for the safety functions listed in the EN61800-5-2 standard. The profile will be available for networks that utilize CIP Safety including SERCOS III and CIP networks (EtherNet/IP, DeviceNet). An example of the option 2 architecture with CIP Safety safe function activation and safe status monitoring is shown in Figure 2-20.

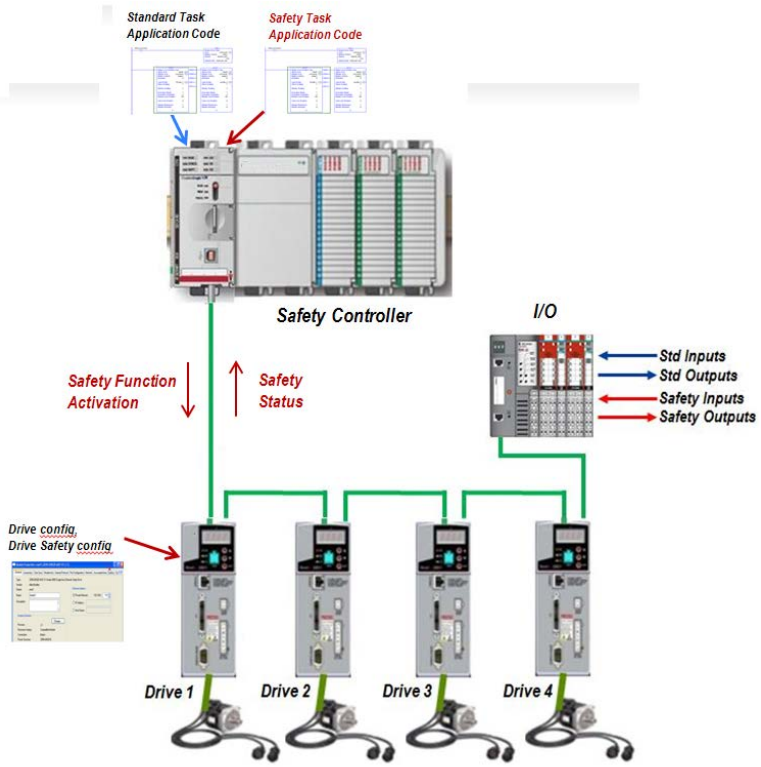

Figure 2 - 20 Option 2 Architecture with CIP Safety

Conclusion

This paper discussed the migration from simple, hardwired safety solutions which provide basic machine guarding/shutdown solutions to flexible, safety PLC based safety solutions that are an integral part of the machine process. Drives with network safety connection support are a key component in the safety controller based safety architecture. A review of the EN 61800-5-2 safety functions along with some "typical" timing diagrams was provided as a summary of key safety functionality that is expected in drives with networked safety support. A number of different drive safety architecture options were defined and reviewed. Finally, a summary of the CIP Safety Safe Motion Sub-committee work plan to support CIP Safety safe motion network based drive safety was described.

****