Review of the CIP Safety SafeMotion Profile Functionality

Mark Chaffee
Senior Principal Engineer
Rockwell Automation

John Deinlein
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 2005 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 (fall-2013) Safety Motion Profile further integrates networked safety functionality into a broad range of drive products to greatly expand the scope of functional safety applications addressed through CIP Safety. This paper presents a detailed review of the Safety Motion Profile and four new objects introduced by the Safety Motion Objects SSE supporting motion safety functionality as defined in the IEC 61800-5-2 (Adjustable speed electrical power drive systems - Part 5-2: Safety Requirements - Functional) standard.

Keywords:

Safety Motion Profile, Safety Motion Objects

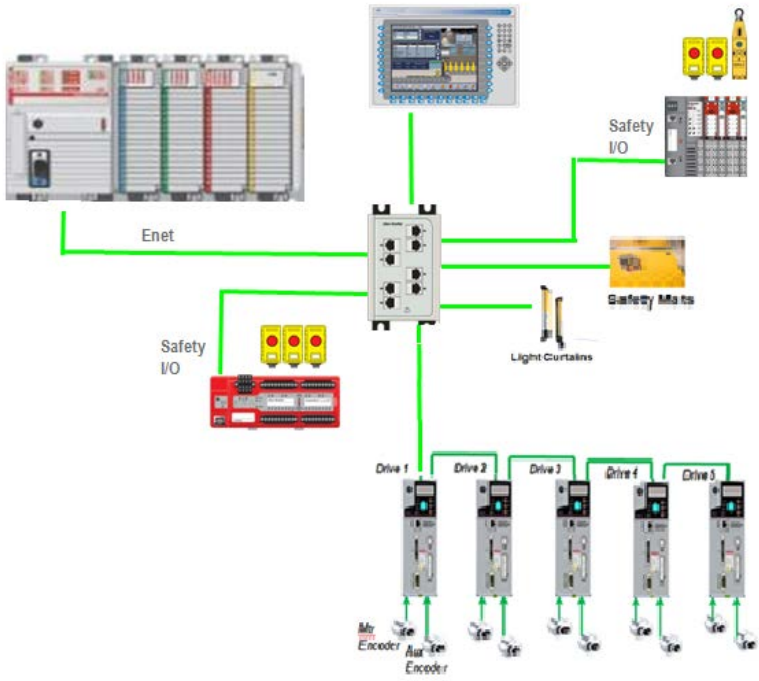
Introduction:

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 limited range of safety functions like safe torque off and safe stopping. Drive safety configuration was managed locally using web browsers or dedicated software tools.

Today, the current trend is to implement fully programmable, flexible safety solutions using safety controllers (PLCs) with networked safety devices that are fully integrated into the machine process. 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 a network safety connection. Modern safety 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.



Safety Controller Based Architecture

While there are published open CIP Safety profiles for *"Safety Discrete I/O"* and *"Safety Analog I/O"* available today, no open profiles were available for networked "*Safety Drives*". This was identified as a critical need at the 2012 ODVA Networking Conference. At that time, a Safe Motion Sub-committee was formed to construct SSEs for a new Safety Drive profile and supporting Safe Motion objects targeted for the Fall 2013 ODVA publication of the Volume 5 CIP Safety standard, Edition 2.8.

This paper reports on the fruit of the Safe Motion Sub-committee's work that includes a new Safety Motion Device Profile supporting Device Types for both CIP Motion Safety Drives as well as Safety Drives using the SERCOS III interface, and also includes four new Safe Motion objects.

Drive Safety Functions:

One of the key requirements for the Safety Motion Device Profile was to support a large subset of the drive safety functions defined by the EN61800-5-2 "Adjustable speed electrical power drive systems – Part 5.2 Safety Requirements - Functional" standard. This standard defines a broad range of drive safety functions as listed below.

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 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

EN61800-5-2 Drive Safety Functions

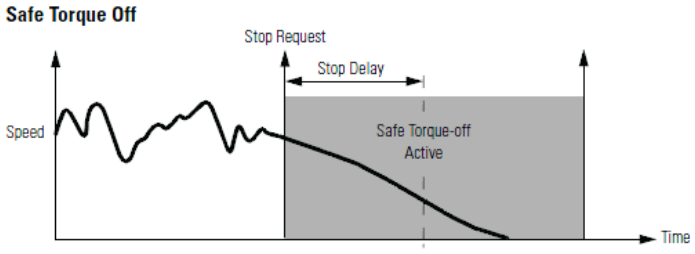
These 17 safety functions can be categorized into following general groups:

- 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. SLS)
- 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 more common drive safety functions is provided below.

Safe Torque-off (STO)

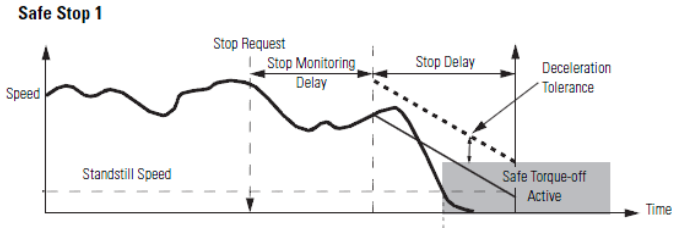
STO is used to disable the torque generating power feed to the motor. A typical implementation includes a safe torque off request input and stop delay parameter. On occurrence of a STO safe torque off request a STO will be initiated after the specified Stop Delay. The figure below shows a typical timing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



Safe Torque Off (STO) Timing Diagram

Safe Stop 1 (SS1)

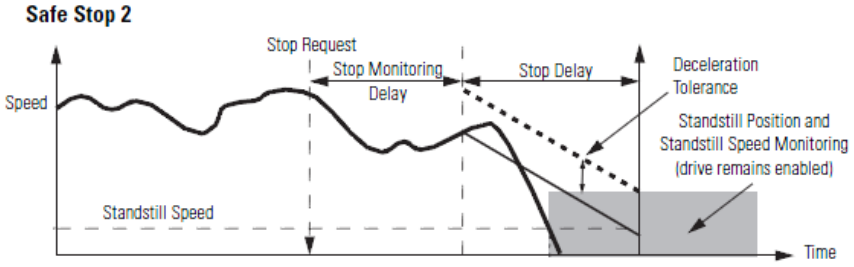
SS1 is used to decelerate the motor followed by an STO. A typical implementation includes the SS1 stop request input, stop monitoring delay parameter, stop delay parameter, deceleration tolerance parameter, and standstill speed parameter. On occurrence of a SS1 safe stop request the deceleration ramp 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. The figure below shows a timing diagram for a typical SS1 sequence.



Safe Stop 1 (SS1) Timing Diagram

Safe Stop 2 (SS2)

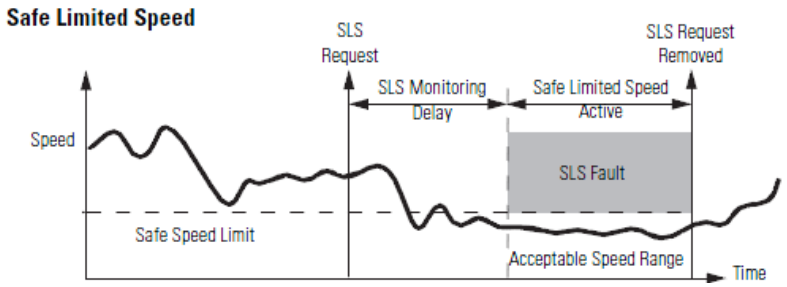
SS2 is used to decelerate the motor followed by safe operational stop (SOS) monitoring. A typical implementation includes the SS2 stop request input, stop monitoring delay parameter, stop delay parameter, deceleration tolerance parameter, and standstill speed parameter. On occurrence of a SS2 safe stop 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. The figure below shows a timing diagram for a typical SS2 sequence.



Safe Stop 2 (SS2) Timing Diagram

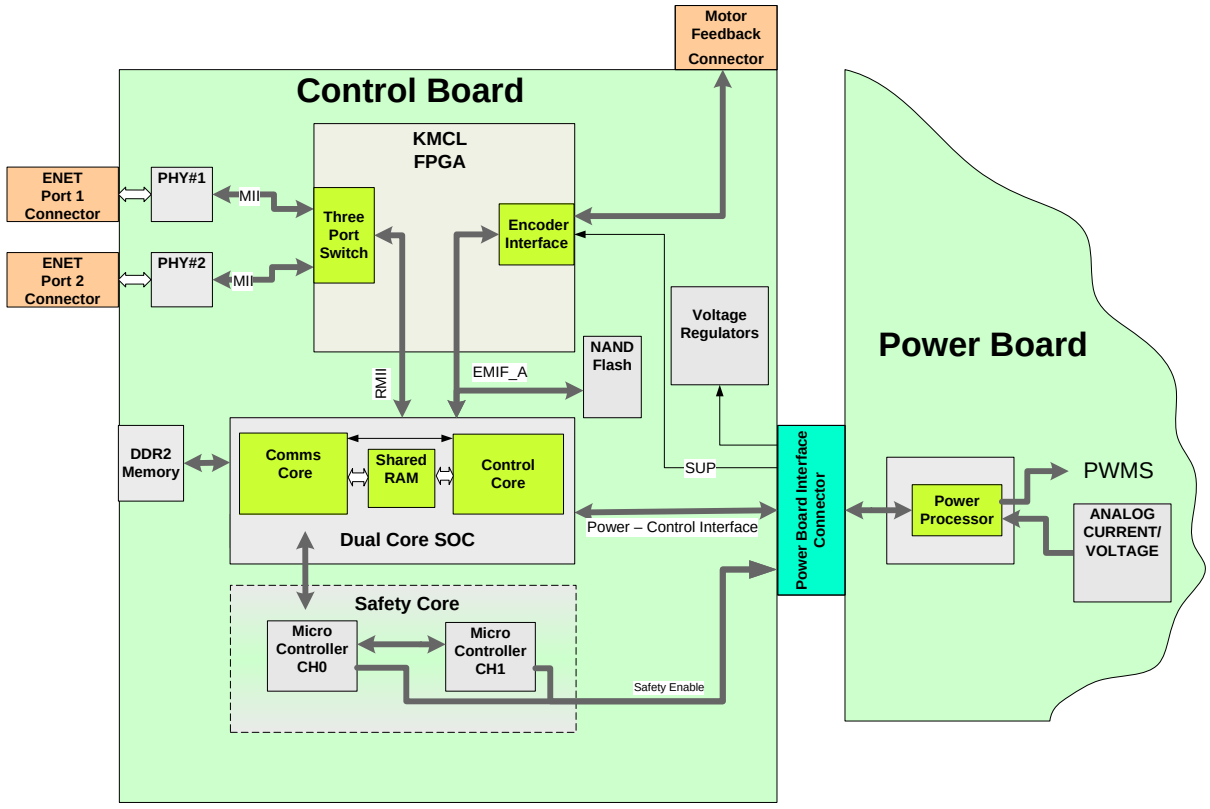
Safe Limited Speed (SLS)

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. The figure below shows a timing diagram for a typical SLS.



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 EN61508 SIL 3 levels. An example of a typical drive Safety Core is shown in the figure below.



Typical Drive Safety Core

The typical drive Safety Core includes safety network interface, primary and secondary position/velocity feedback, dual 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 whether the controller or drive, 1) owns the safety I/O, 2) activates the drive safety functions, 3) configures the drive safety functions, and 4) generates the motion profile.

Option 1 – Local drive safety I/O activated drive safety functions
Option 2 - Safety controller activated drive safety functions
Option 3 - Safety controller configured and activated drive safety functions
Option 4 - Safety controller executed drive safety functions using drive STO

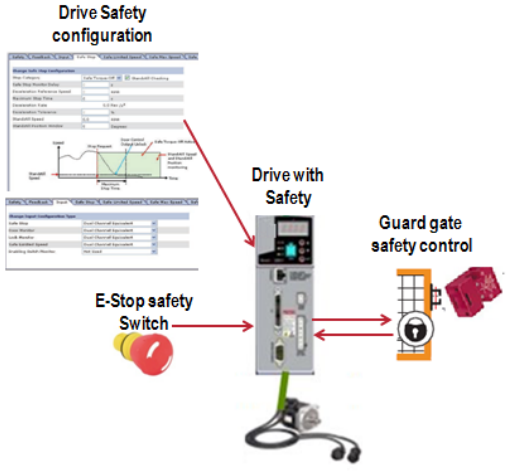
	Safety Network Connection Required	Safety I/O Owner	Drive Safety Function Activation	Drive Safety Config Source	Motion Profile Command
Option 1	No	Drive	Drive	Drive	Drive
Option 2	Yes	Safety Controller	Safety Controller	Drive	Drive
Option 3	Yes	Safety Controller	Safety Controller	Safety Controller	Drive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

Safety Architecture Deployment Options

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

Option 1 - Local drive safety I/O activated drive safety functions

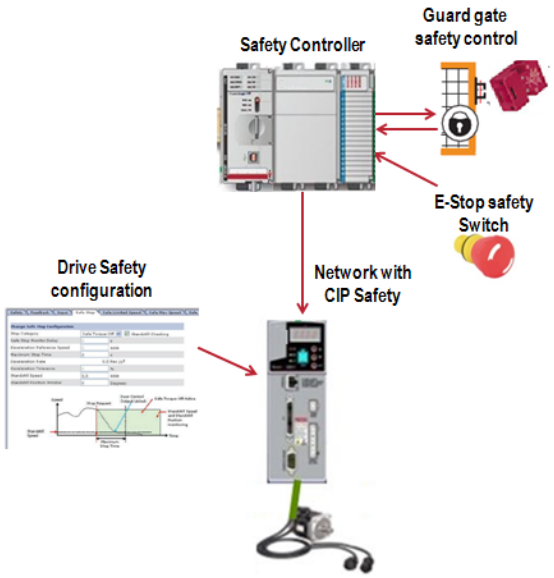
With this option the drive safety functions are activated and safety status is monitored using local drive safety I/O. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is managed locally at the drive using a web browser, software utility,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



Option 1 Architecture

Option 2 - Safety controller activated drive safety functions

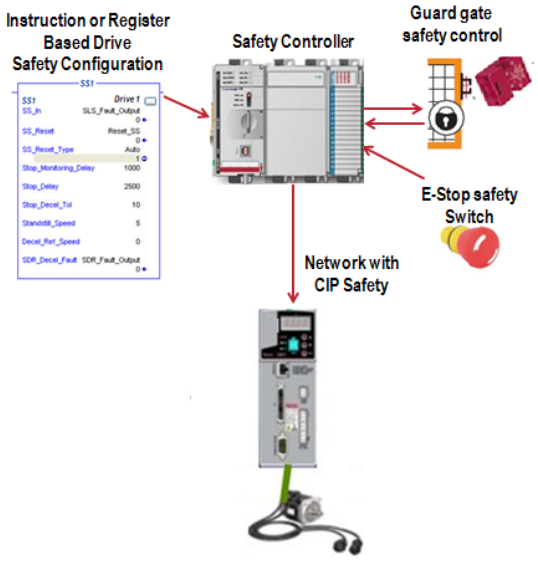
With this option the drive safety functions are activated and safety status is monitored by the safety controller using the drive network safety connection. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is managed locally at the drive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



Option 2 Architecture

Option 3 - Safety controller configured and activated drive safety functions

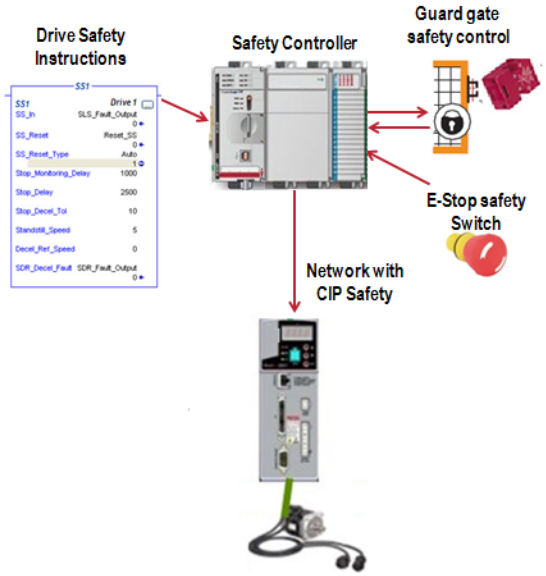
With this option the drive safety functions are initiated and status is monitored using the drive network safety connection. All safety functions are managed locally within the safety core of the drive. Drive safety function configuration is managed at the Safety controller and sent to the drive safety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



Option 3 Architecture

Option 4 - Safety controller executed drive safety functions using drive STO

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.



Option 4 Architecture

The Safe Motion Sub-committee agreed to focus their efforts on providing support for Option 2 and 4. This is the functionality that was delivered in the Safety Motion Profile SSE and the companion Safety Motion Objects SSE.

Safety Motion Device Profile:

Construction of the Safety Motion Device Profile began with the recognition that there were two distinct types of drives we were targeting, CIP Motion Drives and a non-CIP (SERCOS III) Drives. While these drives would share a common Safety Core interface, the behavior of the drives is quite different. Two separate Device Types were needed to differentiate these drives, so the Safety Motion Device Profile defined the following:

CIP Motion Safety Drive Device Type: $2D_{hex}$
Safety Drive Device Type: $2E_{hex}$

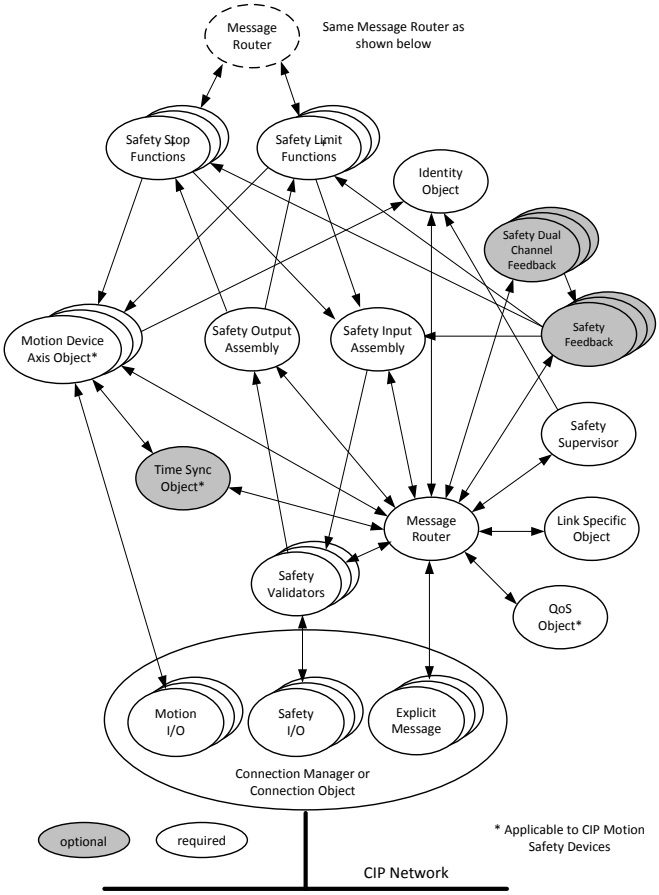
A **CIP Motion Safety Drive** device provides all the functionality associated with a CIP Motion Drive device as described in the CIP Motion Device Profile (see Volume 1, Section 6-41) while also providing a CIP Safety network connection to a safety controller to exchange safety input and output data associated with the safety functionality of the CIP Motion Safety Drive.

A **Safety Drive** device does not support CIP Motion but does provide a CIP Safety network connection to a safety controller to exchange safety input and output data associated with the safety functionality of the Safety Drive. This profile is applicable to non-CIP Motion drives such as those using the SERCOS III interface.

The more challenging of the two device types to define was the CIP Motion Safety Drive due to the fact that a CIP Motion drive already has a rich set of attributes and state behavior that must be merged with the specified behavior of a CIP Safety device. There was no precedent for this kind of safety device nor was this kind of a device anticipated when the CIP Safety specification was constructed. (All CIP Safety devices defined thus far in Volume 5 are relatively simple Safety I/O devices.) We have begun to refer to this kind of device, where both a standard CIP function and CIP safety function must coexist on the network as a single device profile with a single identity state, as a Hybrid Safety device.

Object Model:

Another distinct characteristic of the CIP Motion Safety Drive is that it supports both standard and safety CIP connections, specifically a bidirectional CIP Motion connection and the bidirectional CIP Safety connection. The Object Model for the CIP Motion Safety Drive diagram below shows these two connections and how the objects from the CIP Motion Drive device profile have been merged with CIP Safety objects.



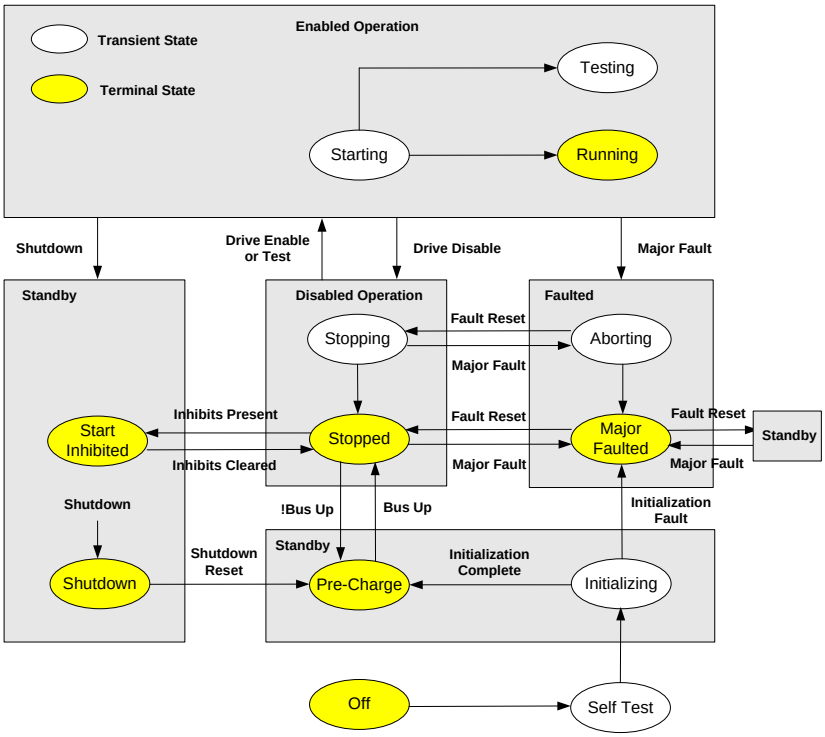
Object Model for CIP Motion Safety Drive device

Safety Drive device types would follow the same Object Model but without the CIP Motion connection and all CIP Motion related objects, marked with an "*" in diagram. Instead of the CIP Motion connection, these drives would have a non-CIP SERCOS III network connection to operate the drive.

Note that there is an Identity Object and a Safety Supervisor Object represented in the Object Model. Both are required. The Identity Object is critical to the standard side operation of the device, while the Safety Supervisor Object is critical to the safety operation of the device.

Device State Mapping:

A CIP Motion compliant drive is governed by the following Motion Device Axis State Model.



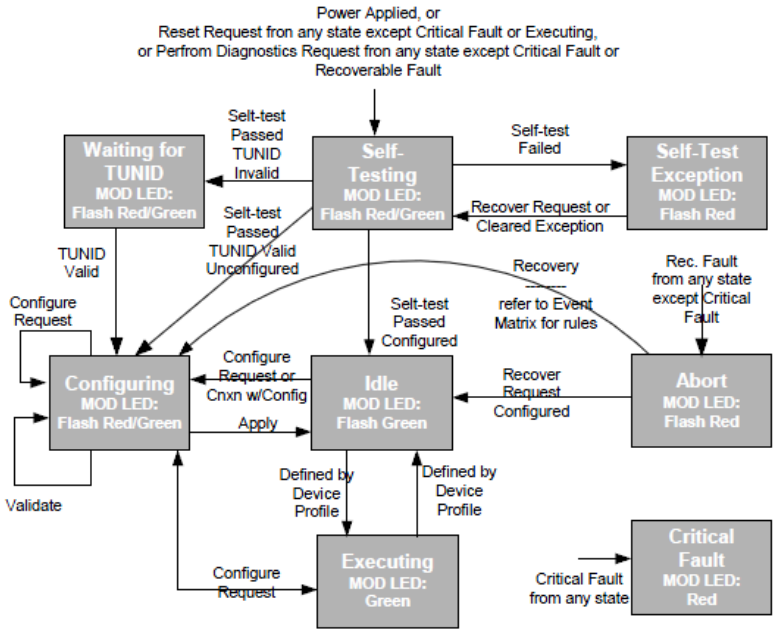
Motion Device Axis Object State Model

The Motion Device Axis Object specification in Volume 1 of the CIP standard defines a relationship between the Motion Axis Object states of a CIP Motion Drive and the Identity Object states. As with all standard CIP devices, the Identity Object state dictates the Module Status LED behavior for the device.

Axis State	ID Object State	Module Status LED
Off	Nonexistent – Power Off	Off
Self-Test	Device Self-Testing	Flash Red/Green
Initialization – Bus not Up	Standby	Flashing Green
Initialization – Bus Up		
Shutdown – Bus not Up		
Shutdown – Bus Up		
Pre-Charge - Bus not Up		
Start Inhibit		
Stopped	Operational	Solid Green
Stopping		
Starting		
Running		
Testing		
Aborting	Major Recoverable Fault	Flashing Red
Major Faulted		
Aborting	Major Unrecoverable Fault	Solid Red
Major Faulted		

Axis State to Identity Object Mapping

A CIP Safety compliant Safety I/O device, on the other hand, is governed by the following Safety Supervisor State Model.



Safety Supervisor State Model

The Safety Supervisor Object specification in Volume 5 of the CIP standard defines the relationship between the Safety Supervisor states of a CIP Safety I/O device and the Identity Object states. The specification also states that the Safety Supervisor state determines the behavior of the Module Status LED, superseding the traditional role of the Identity Object.

Table 5-4.28 State Mapping of Safety Supervisor to Identity

Safety Supervisor	Identity
Self-Testing	Device Self-Testing
Self-Test Exception	Major Unrecoverable
Idle	Standby
Configuring	Standby
Waiting for TUNID	Standby
Executing	Operational
Abort	Major Recoverable
Critical Fault	Major Unrecoverable

Safety Supervisor State to Identity Object Mapping

It should now be apparent that integrating a CIP Safety compliant Safety Core into a CIP Motion Drive creates a significant system design issue in that we have only one Identity Object and one Module Status LED to reflect the condition of the drive, Axis and Safety. With Axis states and Safety states that are almost completely independent of each other, it is no longer possible to satisfy both CIP Motion and CIP Safety specifications with respect to the Identity Object. Note that there is a Module Status LED conflict as well. Identity Object “Standby” states are always Flashing Green, while some of the "Standby" states of Safety Supervisor, like "Configuring" and "Waiting for TUNID" are Flashing Red/Green.

The key to resolving these design issues was establishing state precedence rules to dictate the overall state of the safety drive. This is similar to how the Module Status LED behavior was established for a Multi-axis CIP Motion drive. The object whose state has the highest precedence dictates the overall state of the device. The state precedence rules, starting with the highest precedence, are as follows:

1. Self-Test
2. Unrecoverable Fault
3. Recoverable Fault
4. Safety Configuring
5. Safety Idle
6. Axis Standby
7. Axis Operational
8. Safety Executing
9. Safety Waiting for TUNID (Out of Box)

Based on this hierarchy, the object that governs the Identity Object state is shown in the Governing State column in the table below.

Safety State	Axis State	Governing State	Identity State	Module Status LED
Self-Testing	Any State	Safety Supervisor	Device Self-Testing	Flashing Red/Green
Any State*	Self-Test	Motion Axis	Device Self-Testing	Flashing Red/Green
Self-Test Exception	Any State*	Safety Supervisor	Major Unrecoverable	Solid Red
Waiting for TUNID	Any State*	Safety Supervisor	Standby	Flashing Red/Green
Configuring	Any State*	Safety Supervisor	Standby	Flashing Red/Green
Idle	Any State*	Motion Axis	Standby	Flashing Green
Waiting for TUNID with Torque Permitted,	Initializing Pre-Charge Shutdown Start Inhibit	Motion Axis	Standby	Flashing Green
Executing, Executing with Torque Permitted	Stopped Stopping Starting Running Testing	Motion Axis	Operational	Solid Green
Any State*	Aborting	Motion Axis	Major Recoverable or Major Unrecoverable	Flashing Red or Solid Red
Any State*	Major Faulted	Motion Axis	Major Recoverable or Major Unrecoverable	Flashing Red or Solid Red
Abort	Any State*	Safety Supervisor	Major Recoverable	Flashing Red
Critical Fault	Any State*	Safety Supervisor	Major Unrecoverable	Solid Red

* "Any State" = any state that with lower precedence.

The Governing Object in the above table not only determines the Identity Object state, but also determines the Module Status LED behavior. If the Safety Supervisor is the governing object, then the Module Status LED follows the rules specified by the Safety Supervisor Object specification. If the Motion Device Axis is the governing object, then the Module Status LED follows the rules of the Identity Object specification.

New Safety States for Commissioning and Maintenance:

CIP Motion Safety Drives, unlike Safety I/O devices, must be allowed to operate with the safety function disabled. This allows the user to perform commissioning and major maintenance operations on drives associated with various motion components of the machine without interference from the safety function. The ability to operate the drive

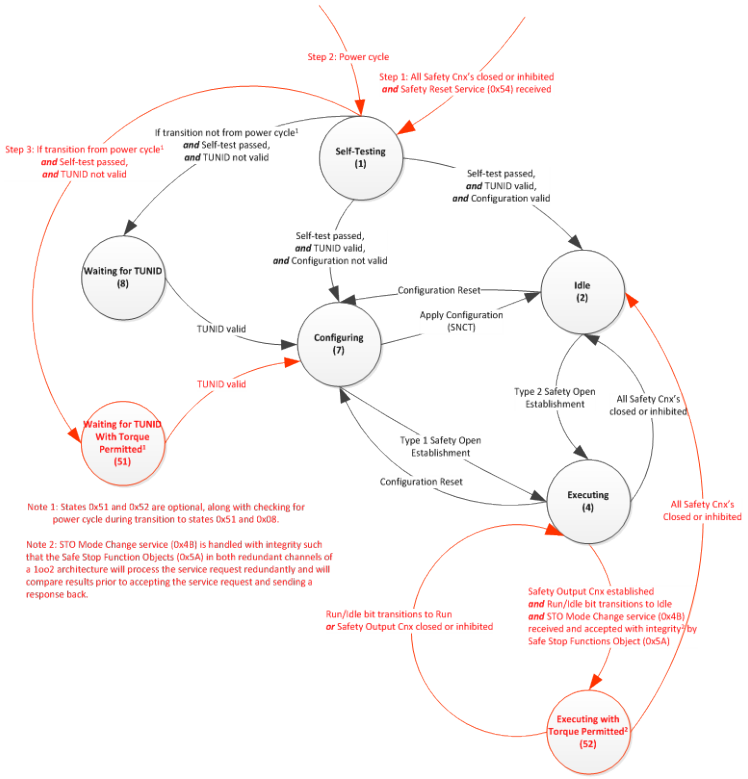
with the safety function disabled is particularly important during initial commissioning of the drive, and is also desirable when performing a machine maintenance activity.

Since the Safety Core embedded in the drive functions much like a CIP Safety I/O device, the drive's safety function is only operational after a CIP Safety connection has been made to the drive and the Safety Core has been configured. For Safety I/O devices the CIP Safety connection is the only connection to the device so the device simply cannot operate until the Safety connection is opened and the device is configured. But Hybrid Safety devices, like the CIP Motion Safety Drive, support multiple connections, Safety and Standard, so device operation via the Standard connection prior to establishing a Safety connection is possible, and desirable for easy commissioning.

To manage the dual safety/standard connection aspect of a CIP Motion Safety Drive, the controller's device profile should be designed to select among three different connection configurations, 'Safety', 'Motion', and 'Motion and Safety'. This functionality allows the user to handle the cases where this device profile is applied by separate Safety and Standard controllers.

To commission a CIP Motion Safety Drive, the user configures the controller's device profile for a 'Motion' Connection. When downloaded, the drive would operate as a standard CIP Motion drive without any connection being made to the drive's Safety Core. Since the drive's Safety Core is still in its "Out of Box" state and not owned by a Safety Controller, the drive is totally controlled by the standard CIP Motion connection. When commissioning is complete, the user simply re-configures the drive with the controller's device profile set for 'Motion and Safety' Connection. This transforms the commissioned CIP Motion Drive into a CIP Motion Safety Drive with a fully operational Safety Core where standard drive functions are controlled by the CIP Motion connection and safety functions are controlled via the CIP Safety connection.

To make this operational Out of Box state clear from a Safety Supervisor state perspective, an additional device profile specific state was added for CIP Motion Safety Drives, "Waiting for TUNID with Torque Permitted". The existing safety state, "Waiting for TUNID", shall continue to apply to traditional Out of Box behavior where the safety device is forced to safe state.



New Safety Supervisor States for CIP Motion Safety Drives

With an operational Safety Core, safety demands can occur at any time due to safety instruction execution in the safety controller. These safety demands could potentially disable the drive during a maintenance session. For this reason, it is desirable to perform maintenance operations with the safety controller in Program Mode (not Run Mode) were safety program execution is disabled. However, current Safety I/O device behavior forces the device to safe state when the safety controller is in Program Mode as indicated by the Safety Output connection's Run/Idle bit being Idle. In this condition the Safety I/O device is inoperable. A mechanism was therefore needed to allow the CIP Motion Safety Drives to operate when the safety controller is in Program Mode.

Again, referencing the above Safety Supervisor State diagram, a new state was defined, "Executing with Torque Permitted", to allow drive operation in Program Mode. To enter this state, an "STO Bypass" is initiated via an unconnected STO Mode Change service request to the CIP Motion Safety Drive. If the safety controller is in Program Mode (Safety Output Connection Run/Idle bit is Idle) the STO Mode Change bypasses the drive's STO safety function to permit drive operation in the "Executing with Torque Permitted" state. This allows the drive to operate during the maintenance procedure using the CIP Motion connection as long as the following conditions hold true:

1. Drive Safety core is operational without faults / errors.
2. CIP Safety connection is Open without faults / errors.
3. CIP Safety Output connection Run/Idle bit remains in Idle.

Normal machine operation is restored by transitioning the safety controller from Program Mode to Run Mode. This sets the Run/Idle bit to Run, automatically transitioning the Safety Supervisor State from "Executing with Torque Permitted" to "Executing", restoring STO safety function operation.

Safety Motion Device Assemblies:

The Safety Motion Device Profile defines a set of Safety Input and Safety Output Assemblies to support a wide range of drive safety functions ranging from simple Safe Torque Off only implementation to full feature Safety Stop and Safety Limit Monitoring implementations. These assemblies are defined with or without Safety Feedback data and support for one or two Axis instances.

Here is a summary of the Safety Output Assemblies defined in the Safety Motion Device Profile showing the progression of drive safety function support starting with a simple STO only assembly.

Table 6-8.10 Safety Output Data with STO (1 Axis Instance)

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

Table 6-8.11 Safety Output Data with STO and Safe Brake Control (1 Axis Instance)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
181_{hex}	0	Reset Request	Reserved	Reserved	Reserved	Reserved	Reserved	SBC Output	STO Output

Table 6-8.12 Safety Output Data with Safe Stop Functions (1 Axis Instance)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
182_{hex}	0	Reset Request	Reserved	SMT Request	SOS Request	SS2 Request	SS1 Request	SBC Output	STO Output

Table 6-8.13 Safety Output Data with Safe Stop/Limit Functions (1 Axis Instance)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
183_{hex}	0	Reset	Reserved	SMT	SOS	SS2	SS1	SBC	STO

		Request		Request	Request	Request	Request	Output	Output
	1	Reserved	Reserved	SDI– Request	SDI+ Request	Reserved	SLA Request	SLS Request	SSM Request

Table 6-8.14 Safety Output Data with Safe Stop and Safe Limit Groups (1 Axis Instance)

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			

Safety Input assemblies follow the same bit pattern as the Safety Output assemblies, with safety function request bits in the Safety Output assemblies aligning generally with safety function status bits in the Safety Input assemblies.

Table 6-8.20 Safety Input Data with STO (1 Axis Instance)

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 6-8.21 Safety Input Data with STO and Safe Brake Control (1 Axis Instance)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
$1A1_{hex}$	0	Reset Required	Safety Fault	Reserved	Reserved	Reserved	Reserved	Brake Engaged	Torque Disabled

Table 6-8.22 Safety Input Data with Safe Stop Functions (1 Axis Instance)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
$1A2_{hex}$	0	Reset Required	Safety Fault	Safe Motor Temp	Safe Standstill	SS2 Active	SS1 Active	Brake Engaged	Torque Disabled

Table 6-8.23 Safety Input Data with Safe Stop/Limit Functions (1 Axis Instance)

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 6-8.24 Safety Input Data with Safe Stop and Safe Limit Groups (1 Axis Instance)

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			

When safety function monitoring is performed by the safety controller rather than the drive, the drive must pass safety feedback data back to the safety controller via the Safety Input connection. To support this architecture (Deployment Option 4), the above Safety Input assemblies are augmented with Safety Feedback Data. Below is an example of the STO Only assembly with Safety Feedback data.

Table 6-8.30 Safety Input Data with STO and Feedback Data (1 Axis Instance)

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

For each of the above single axis instance assemblies, the Safety Motion Device Profile also defines assemblies that support data for 2-axis instances. Below is an example of a 2-axis instance Safety Input assembly that includes Feedback Data.

Table 6-8.38 Safety Input Data with Safe Stop/Limit Functions and Feedback Data (2 Axis Instances)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
$1CB_{hex}$	0	Feedback Position 1 (DINT)							
	1								
	2								
	3								
	4	Feedback Velocity 1 (DINT)							
	5								
	6								
	7								
	8	Feedback Acceleration 1 (DINT)							
	9								
	10								
	11								
	12	Feedback Position 2 (DINT)							
	13								
	14								
	15								
	16	Feedback Velocity 2 (DINT)							
	17								
	18								
	19								
	20	Feedback Acceleration 2 (DINT)							
	21								
	22								
	23								
	24	Reset Required 1	Safety Fault 1	Safe Motor Temp 1	Safe Standstill 1	SS2 Active 1	SS1 Active 1	Brake Engaged 1	Torque Disabled 1
	25	Reserved	Reserved	Motion Negative 1	Motion Positive 1	SDI Active 1	SLA Active 1	SLS Active 1	Safe Speed 1
	26	Reset Required 2	Safety Fault 2	Safe Motor Temp 2	Safe Standstill 2	SS2 Active 2	SS1 Active 2	Brake Engaged 2	Torque Disabled 2
	27	Reserved	Reserved	Motion Negative 2	Motion Positive 2	SDI Active 2	SLA Active 2	SLS Active 2	Safe Speed 2

Safe Motion Object Overview:

The Safety Stop Functions Object encapsulates drive safety functions focused on stopping the motor. Safety functions in this object include Safe Torque Off, Safe Brake Control, Safe Stop 1, and Safe Stop 2. One instance of the Safety Stop Functions Object is required for each Motion Device Axis Object instance supplying power to a motor.

The Safety Limit Functions Object encapsulates drive safety functions related to monitoring the dynamics of the motor against configured safe limits. Safety functions in this object include Safe Limited Speed, Safe Limited Acceleration, Safe Limited Torque, Safe Direction, and Safe Speed Monitor. At least one instance of the Safe Limit Functions is required per Motion Device Axis Object instance supplying power to a motor. More instances can be implemented if the drive supports multiple limits per safety function.

The Safety Feedback Object encapsulates Safe Position, Safe Velocity, and Safe Acceleration data associated with a safety feedback device such as safety capable encoder. One instance of the Safety Feedback Object is required per safety feedback device.

The Safety Dual Channel Feedback Object encapsulates the feedback discrepancy checking function used to achieve SIL 3, PLe safety certification level using two feedback devices. One instance of the Safety Dual Channel Feedback Object is required per pair of safety feedback device.

The Safety Stop Functions Object and Safety Limit Functions Object are intended to be used in systems where the "Safe State" in the case of a fault is the Safe Torque Off function in Torque Disabled state and, if implemented, the Safe Brake Control in Brake Engaged state.

Safety Feedback Objects

To promote consistency in definition of safety objects; the "design pattern" for the Safety Feedback Object (Class Code: 58_{hex}) was the Safety Analog Input Point Object (49_{hex})

Configuration attributes for feedback devices are based on the Feedback Configuration Attributes defined for the Motion Device Axis Object (42_{hex}).

The design pattern for the Safety Dual Channel Feedback Object (Class Code: 59_{hex}) is the Safety Dual Channel Analog Input Object ($4B_{hex}$).

Important Note: Speed Feedback Object definition requires that diagnostic tests appropriate to the defined Safety Integrity Level and the configured Feedback Type must be performed. Details of the diagnostic tests to meet the requirements are Vendor Specific.

Reset and Restart

Fault Reset behavior is significantly different for the Safe Motion Objects when compared to previously defined safety objects.

For objects such as Safety Discrete Point, Output Point, and Analog Input Point; the object is reset from its "fault state" when the cause of the fault is corrected and a configurable "Latch Error Time" has expired.

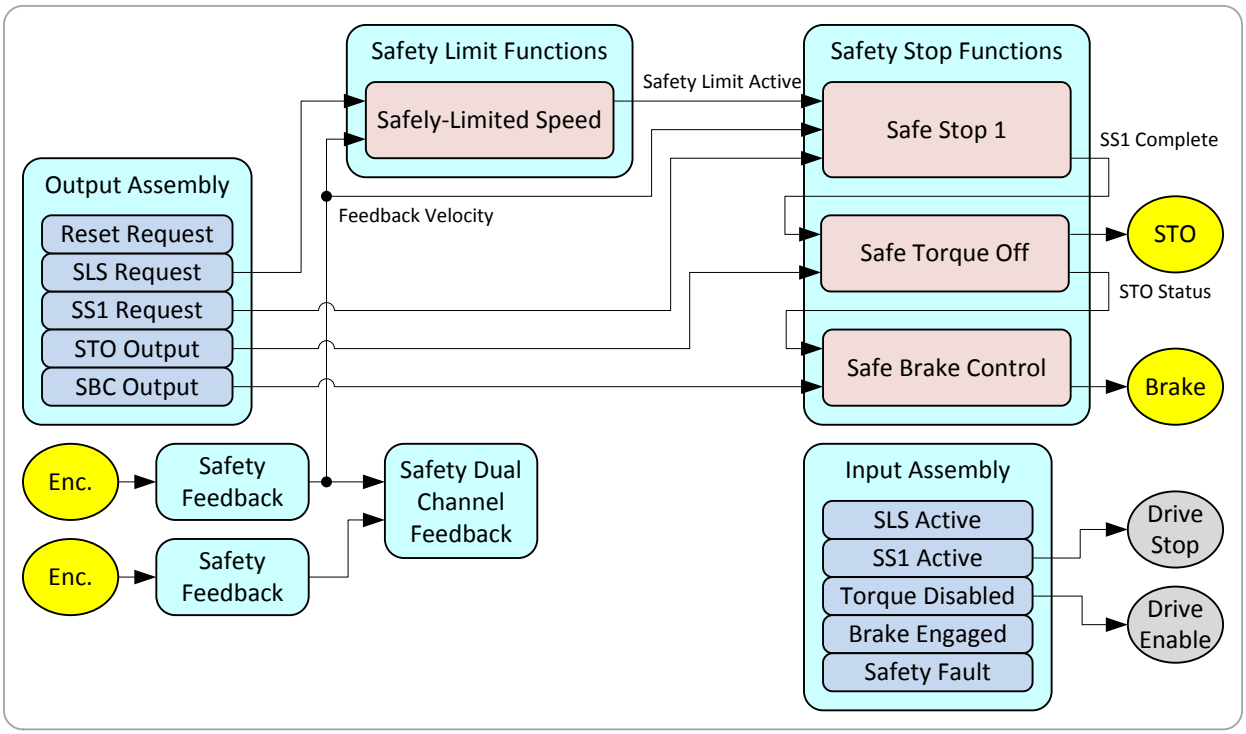
The possible fault cases for the Safety Motion Object are complex and in many cases it is not possible to define when a fault has "cleared". For instance, over-speed of Safety feedback is a fault because aliasing of the feedback signals means a high speed may be indistinguishable from low speed. Therefore a fault reset always requires correcting the cause of that fault followed by a 0 to 1 transition of the Function Reset attribute.

The Function Reset attribute may also be configured as a manual Restart. Note the terminology; a "Reset" enables the transition out of a "Fault" state while a "Restart" enables transition out of a "Stopped" state. Restart behavior is configurable. For example: If Restart Type = Manual (default), the transition of STO Status from Disable Torque

to Permit Torque requires STO Output set to Permit Torque AND a 0 to 1 transition of Function Reset. If Restart Type = Automatic, STO Status is simply the inverse of STO Output.

Safe Motion Object Example:

In the figure below a Safety Feedback Object instance processes encoder input to determine motor velocity. A second Safety Feedback object instance and a Safety Dual Channel Feedback Object instance enable discrepancy testing to achieve a high SIL rating.



Safety Function Object Interaction

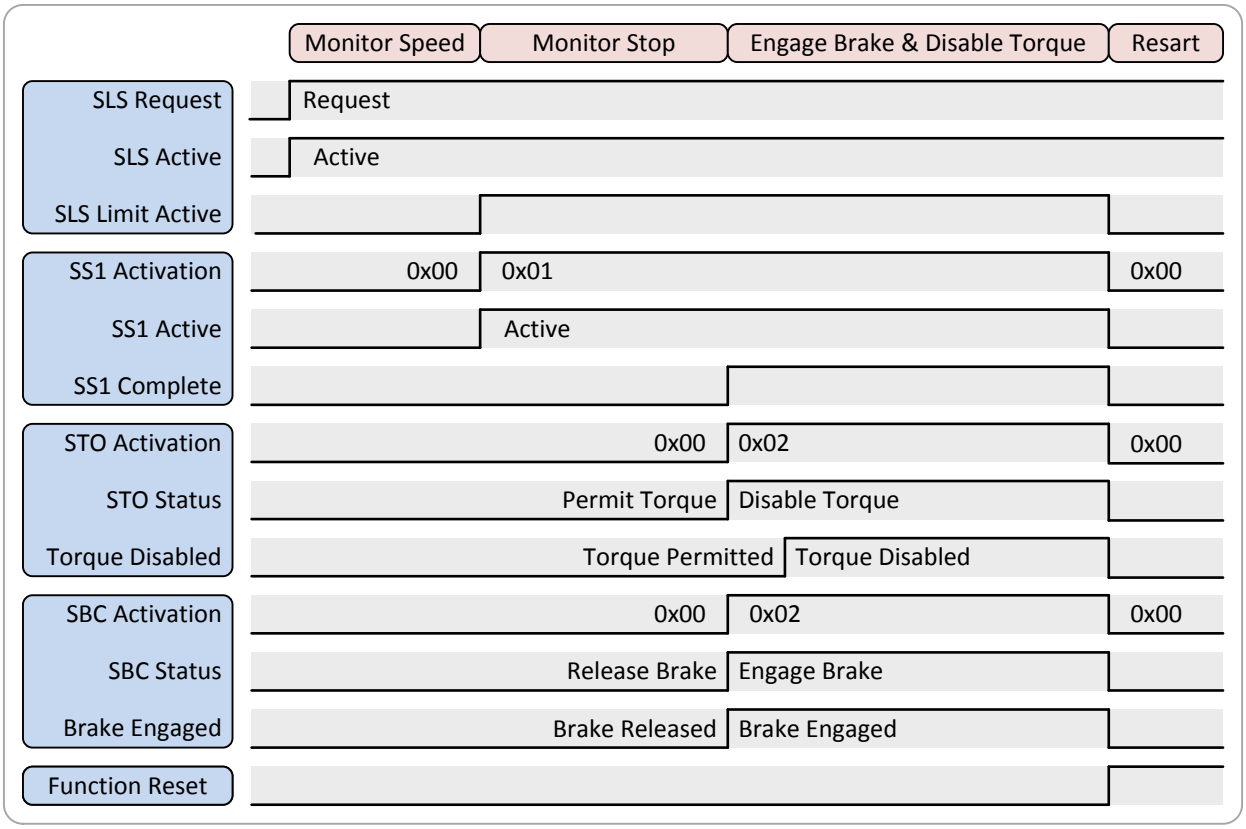
A Safely-Limited Speed function in the Safety Limit Functions Object instance is enabled by SLS Request in an Assembly Object instance from a Safety Controller. If the measured motor speed exceeds the configured speed limit this example is configured to initiate Safe Stop 1.

The drive control monitors SS1 Active and sets its internal state to stop. The SS1 function monitors deceleration to stop then sets SS1 Complete. SS1 Complete commands the Safe Torque Off function to set the drive's STO circuits to Torque Disabled. The drive control monitors Torque Disabled and sets its internal state to disabled.

NOTE: SS1 could also be initiated at any time by SS1 Request in the Output Assembly.

The above example system includes a Safe Brake Control function configured to engage a motor brake when STO is active. A slight time delay for the brake to engage before torque is disabled is configured. The safety control functions are reset by 0→1 edge on Reset Request.

The timing diagram below illustrates the configurable delay from Engage Brake to Torque Disabled. The signed configurable delay also supports the case where there is a delay between Disable Torque to Brake Engaged.



Safe Limited Speed Timing Diagram

Safety Limit Functions Setpoints

For the Safety Limit Functions typically have a "setpoint" that establishes the "limit". For example: For Safely Limited Speed, the limit value is set by SLS Active Limit or by SLS Default Limit.

In cases where the limit value may be a configuration parameter: The value is stored in SLS Default Limit (Set and NV) and copied to SLS Active Limit (Set and V) for the actual speed comparison.

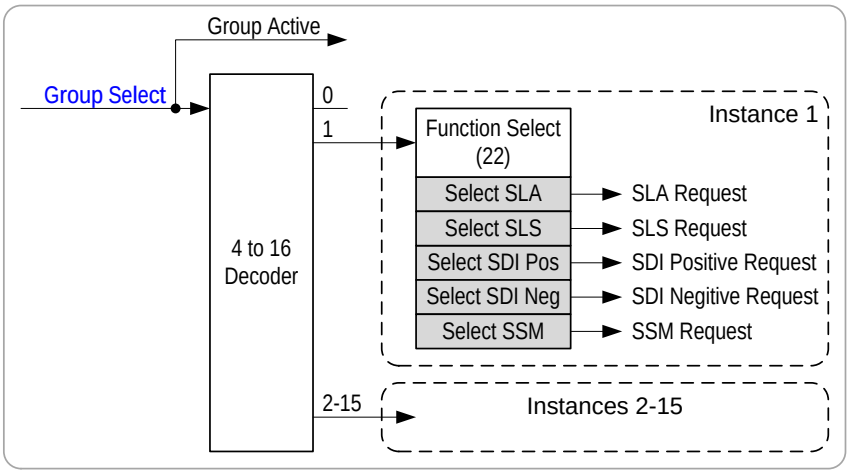
It is also possible to define an Output Assembly to drive SLS Active Limit. If that Assembly is selected, the Safety controller can dynamically change the limit setpoint.

It is also possible to implement an instance of Safety Limit Functions instance and then the limit function "Mode" attributes to always enable selected functions. This is intended for the case where exceeding some maximum setpoint should always be checked.

For example: Many safety controllers provide a Safely-Limited Speed that is activated only when a input is active and a "maximum" Safely-Limited Speed that should always be in effect.

Safety Limit Functions Group Select

Understanding selection of Safety Limit Functions using Group Select needs some explanation of the background. It is anticipated that for certain applications of safety to machines, there would be cases where the machine has certain "machine states" or "modes of operation." Each state or mode might need activation of a different selection of Limit Functions and/or different limit setpoints for each.



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**			

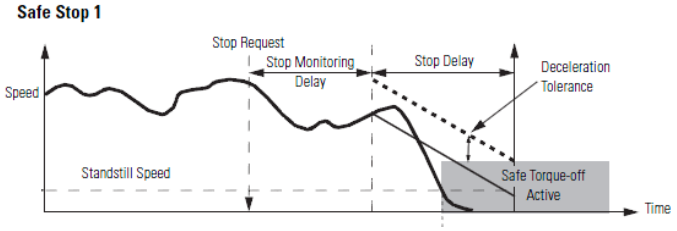
Group Safety Limit Function Selection

To use Group Select, an Output Assembly that includes Group Select is selected. Each value 1 through 15, selects a Safety Limit Functions instance and then the Function Select attribute in that instance selects which safety functions are active. (For Group Select = 0, all functions are disabled.)

Since each of the Safety Limit Functions instances has its own setpoint configuration attributes (Set and NV), this mechanism can be used to select from up to 15 different setpoints for each Limit Function as well as allowing a pattern of which functions are active.

New Motion Device Axis Object Attributes:

During normal operation the Motion Device Axis Object and the various Safety Functions Objects operate independent of each other. However, when safety demands occur, it is important that there be coordination between the drive safety functions and the motion controller. For example, when a Safe Stop 1 safety function is activated, the motion controller must decelerate the motor to a stop. To initiate the deceleration, the motion control system must have an awareness of the Safe Stop 1 activation.



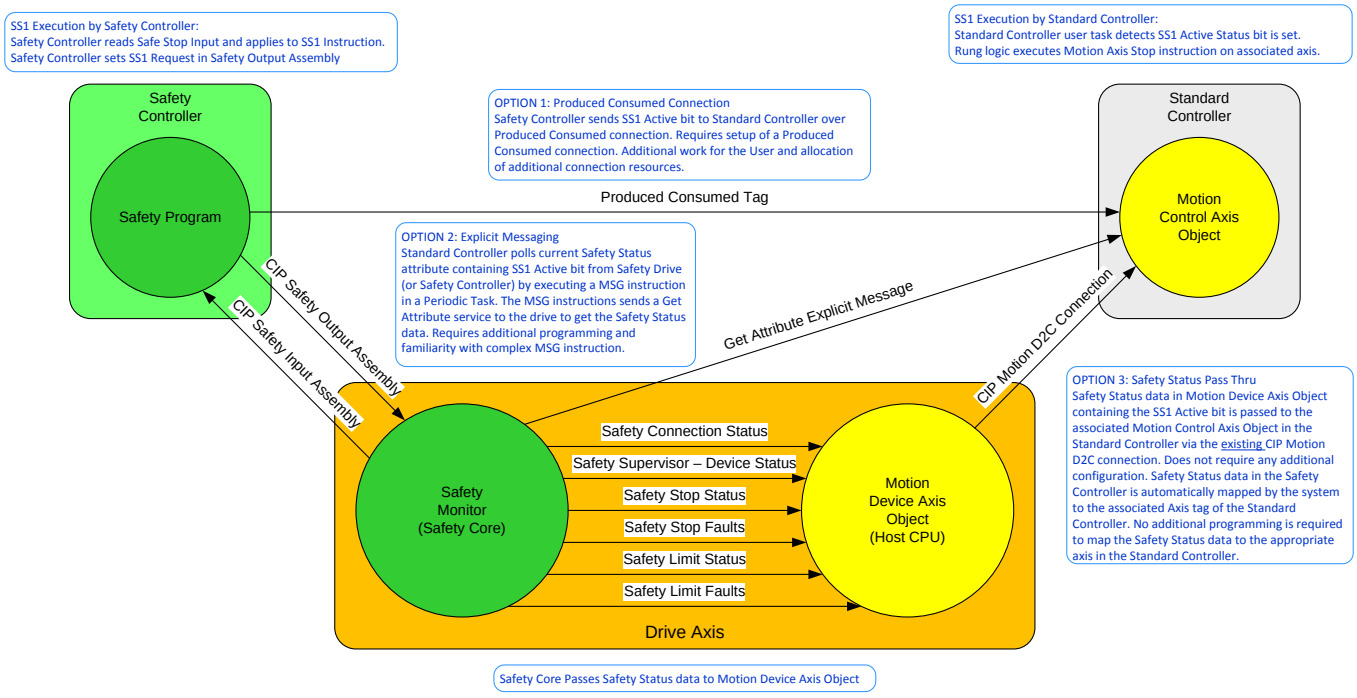
Safe Stop 1 (SS1) Timing Diagram

There are at least three different ways for the motion controller to recognize that Safe Stop 1 has been activated by the safety controller as illustrated in the diagram below.

Option 1 is where the safety controller sends the SS1 Request bit to the motion controller via a Produced-Consumed controller connection. This option would require a separate connection resource, connection configuration, and programming.

Option 2 is where the motion controller polls the drive's Safety Core for the SS1 Active bit using a Get Attribute service. Polling the drive for safety status information would be a very inefficient use of network resources and would also require programming to initiate the Get Attribute service.

Option 3 is by far the best option. The Safety Core in this case would pass the safety status information to the associated Motion Device Axis Object instance managed by the Host CPU. This safety status data would then be transmitted to the corresponding Motion Control Axis Object of the motion controller through the regular CIP Motion D2C connection update. No additional connections are required, and no addition programming is needed to access the safety status data. Note that the safety status data of the drive's Safety Core is automatically associated with the correct Axis instance in the motion controller using this Safety Status Pass Thru mechanism.



Accessing Safety Status Data

To support coordination between the various safety functions and the motion control functions, three new Motion Device Axis Object attributes were defined as part of Edition 3.15 of Volume 1 coincident with the release of Edition 2.8 of Volume 5 supporting CIP Motion Safety Drives.

1. Axis Safety State – passes the current Safety Supervisor State
2. Axis Safety Status – passes the current status of each drive safety function
3. Axis Safety Faults – passes any active safety fault conditions

Conclusion:

Drives with network safety connection support are a key component in emerging safety controller based safety architectures. While there are published CIP Safety profiles for *"Safety Discrete I/O"* and *"Safety Analog I/O"* available today, a critical need was identified at the last ODVA conference for a networked "*Safety Drive*" profile. This paper describes the recently published Safety Motion Device Profile that directly addresses that need. The paper began with a review of the EN 61800-5-2 safety functions and different drive safety architecture deployment options. Two new safety drive device types were defined, one serving CIP Motion drives and one for non-CIP (SERCOS III) drives. Merging existing CIP Motion behavior with CIP Safety behavior created significant design challenges with respect to state behavior, commissioning, and maintenance. The paper described how these design issues were resolved, setting a pattern for Hybrid Safety devices to come. Safety Motion Device Profile assemblies and Safety Motion Objects were the reviewed. Finally, mechanisms to coordinate motion control functions with drive safety functions were discussed, introducing the concept of Safety Status Pass Thru.

References:

EN61800-5-2 "Adjustable speed electrical power drive systems – Part 5.2 Safety Requirements - Functional"
Volume 1: Common Industrial Protocol, Edition 3.15
Volume 5: CIP Safety, Edition 2.8