ODVA 2014
Industry Conference
and 16th Annual Meeting

Review of the CIP Safety SafeMotion Profile Functionality

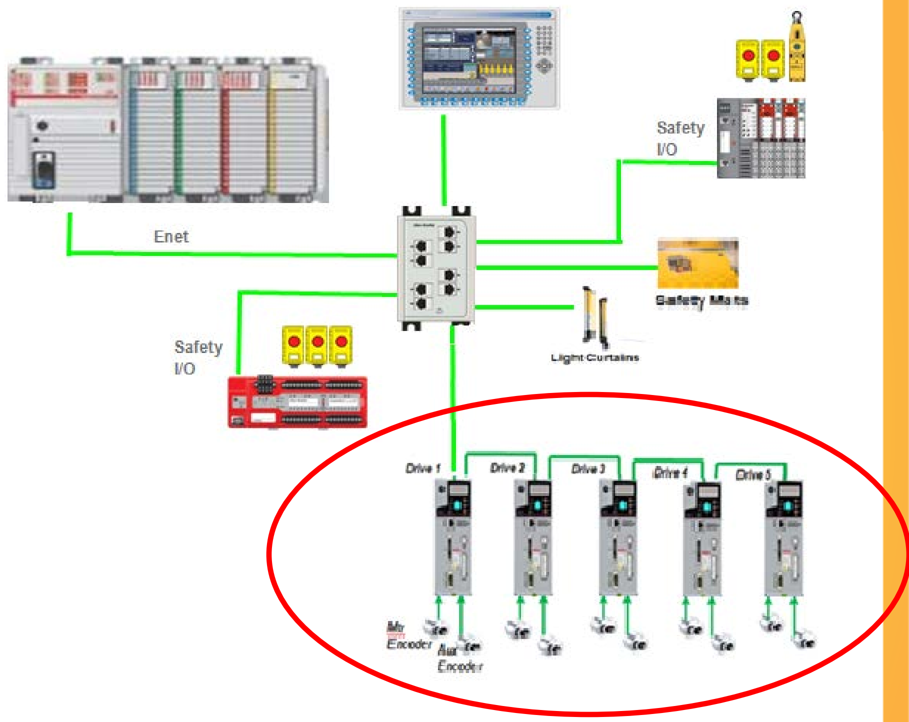
John Deinlein
Rockwell Automation

Mark Chaffee
Rockwell Automation

Technical Track

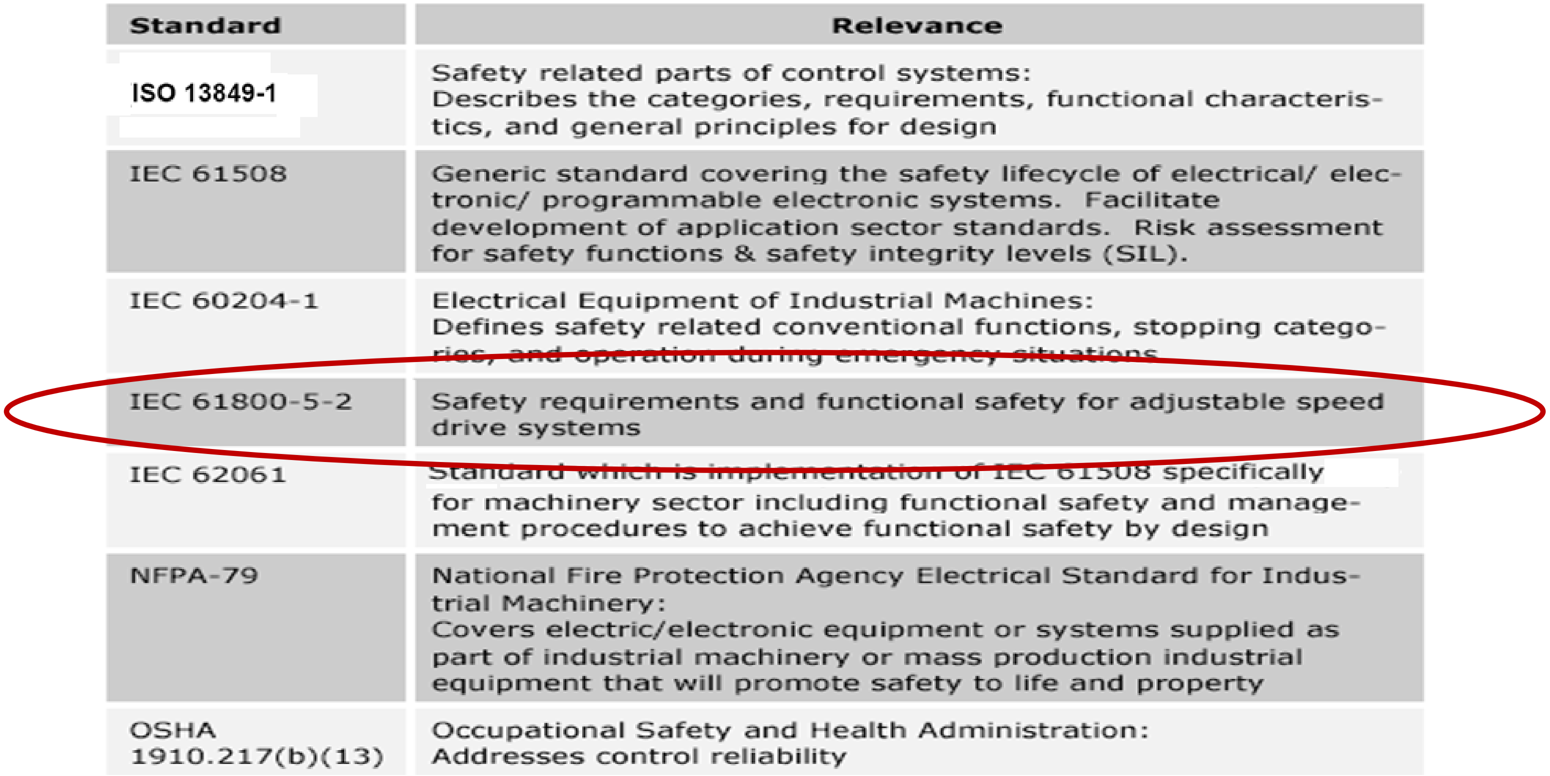
Safety Controller Architecture

- Networked Safety
- Based on EtherNet/IP
- Safety Controller/PLC
  - Safety Task
- Safety I/O Devices
  - Emergency Stop
  - Safety Relays
  - Light Curtains
  - Safety Mats
  - Door Lock Control
- New Safety Device ➔ CIP Safety Drives



Safety Standards

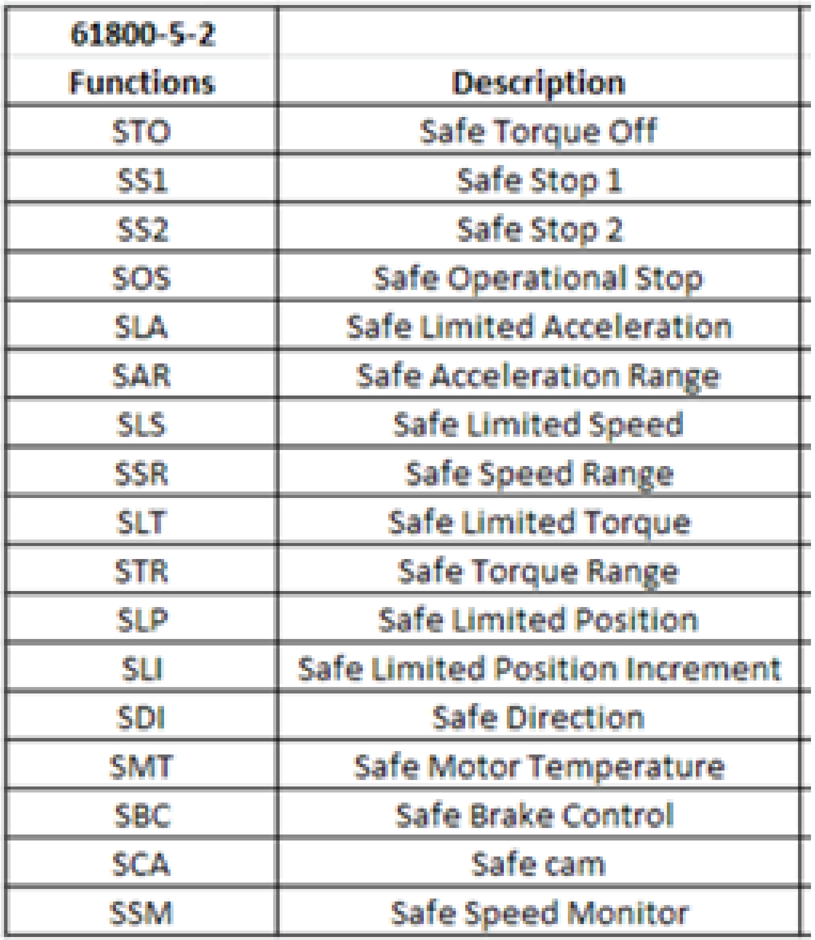
- There are many safety standards that provide guidelines for safety systems.
- CIP Safety Drive Profile design focuses on EN61800-5-2, which defines Safety Function requirements for adjustable speed drive systems.



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

EN61800-5-2 Drive Safety Functions

- EN61800-5-2 provides high level functional description of drive safety functions
- These are the safety functions that are targeted for CIP Safety Drive Profile support



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

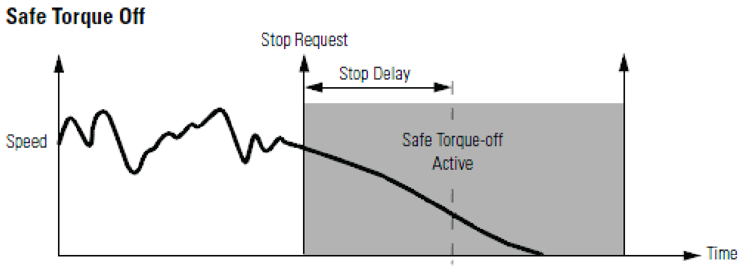
Functionality Grouping

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

Drive Safety Function Examples

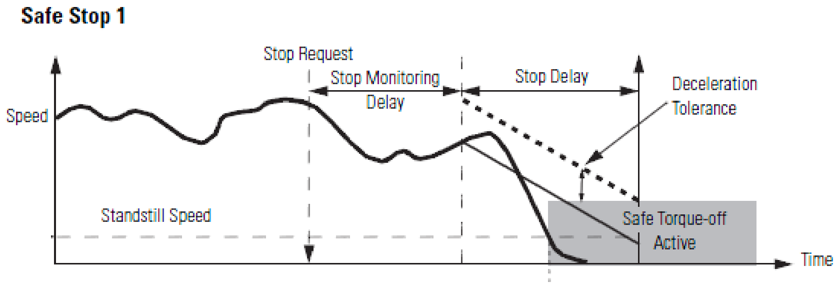
STO (Safe Torque Off)

- Stop Request
- Wait Stop Delay
- Disable Motor Power



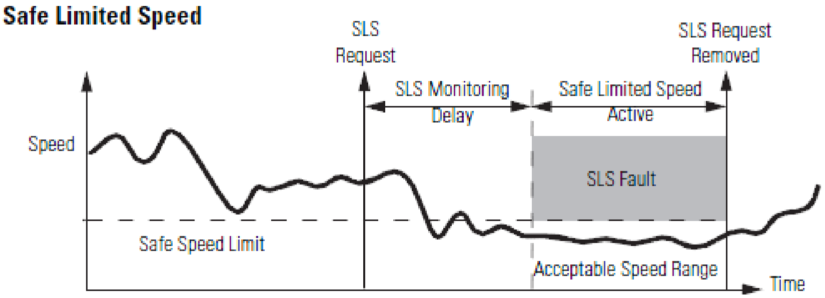
SS1 (Safe Stop 1)

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

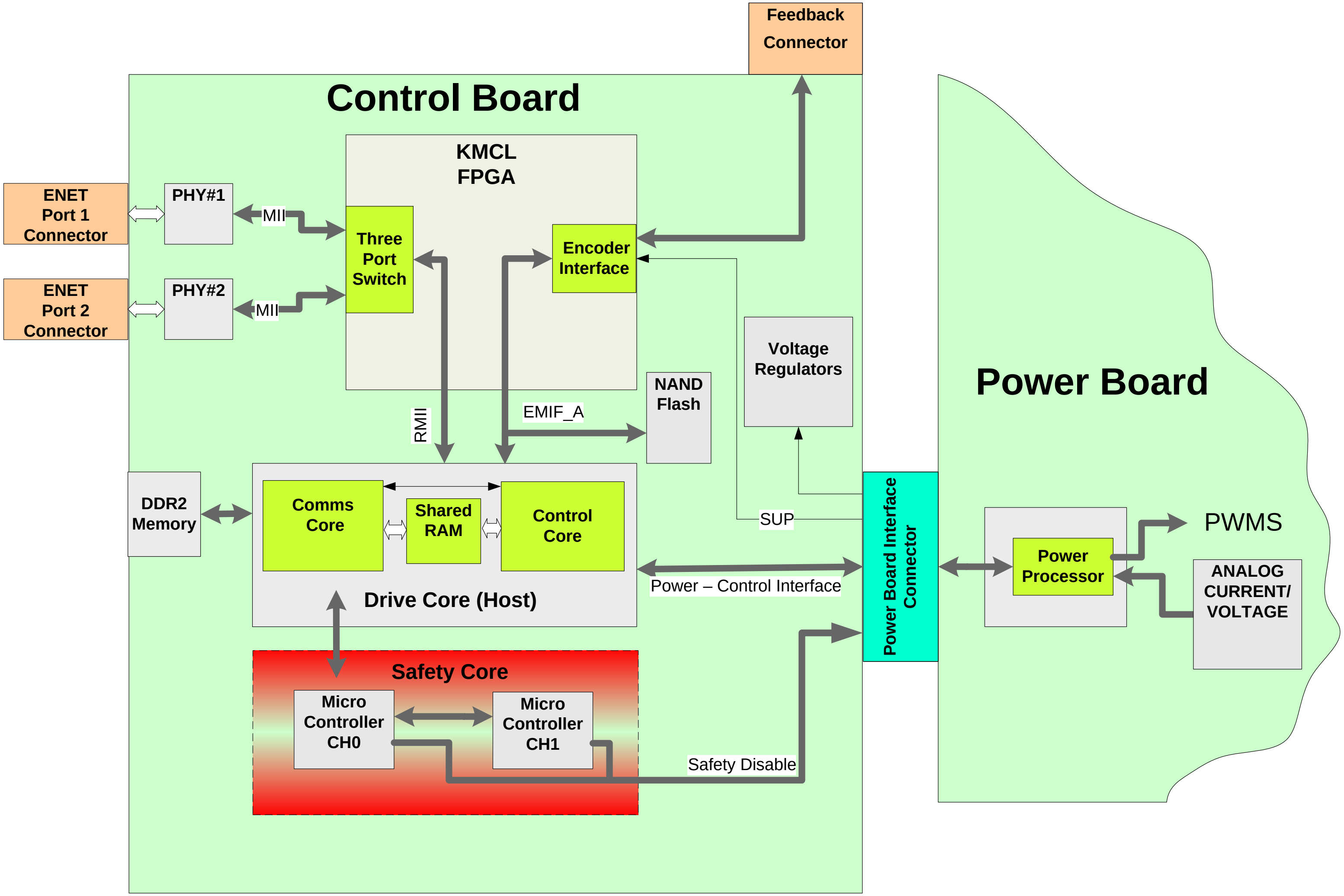


SLS (Safe Limited Speed)

- Safe Limited Speed Request
- Wait Stop Monitoring Delay
- Monitor Speed < Safe Speed Limit



Typical Drive Safety Core



Drive Safety System Architecture Options

OPTION 1

Drive safety I/O activated drive safety functions

OPTION 2 ← Safe Motion Subcommittee Target

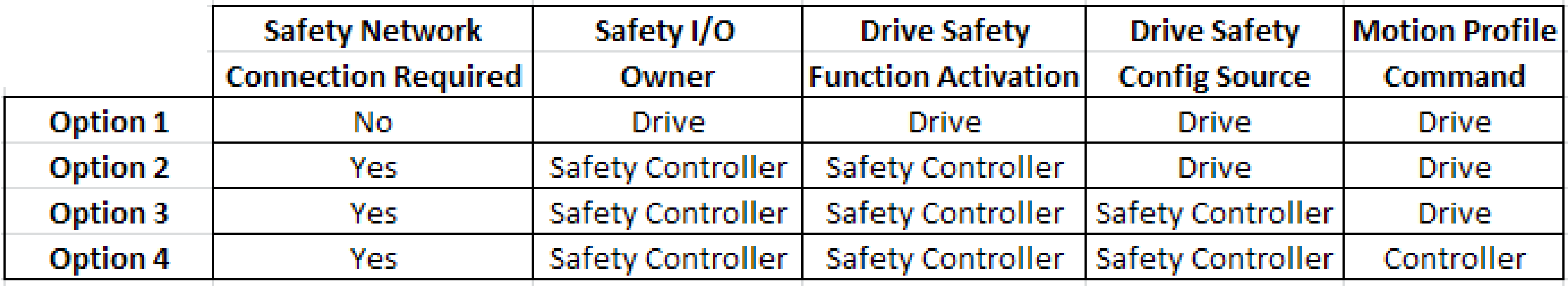
Safety controller activated drive safety functions

OPTION 3

Safety controller configured & activated drive safety functions

OPTION 4 ← Safe Motion Subcommittee Target

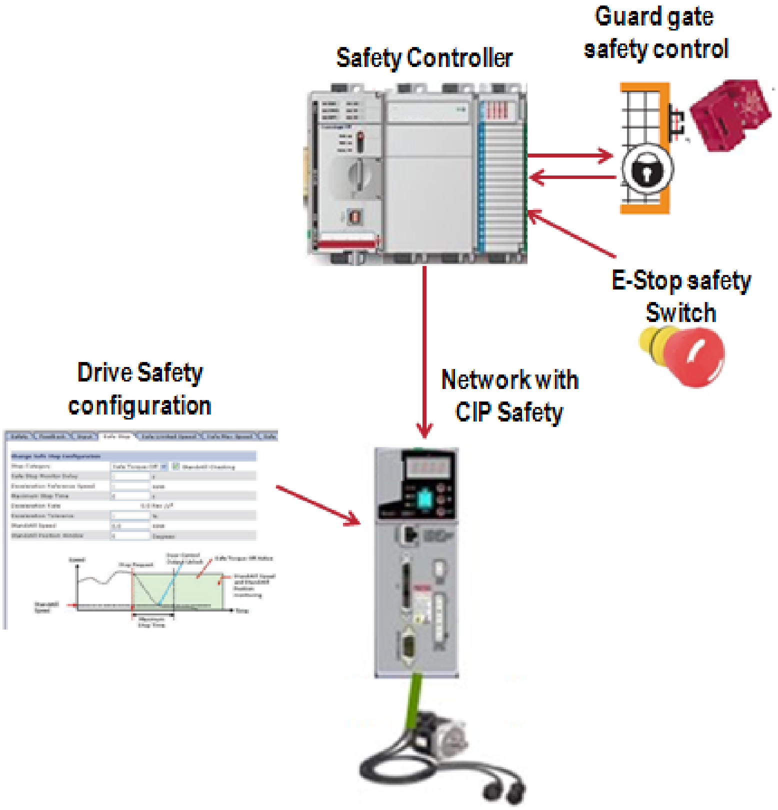
Safety controller executed drive safety functions



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

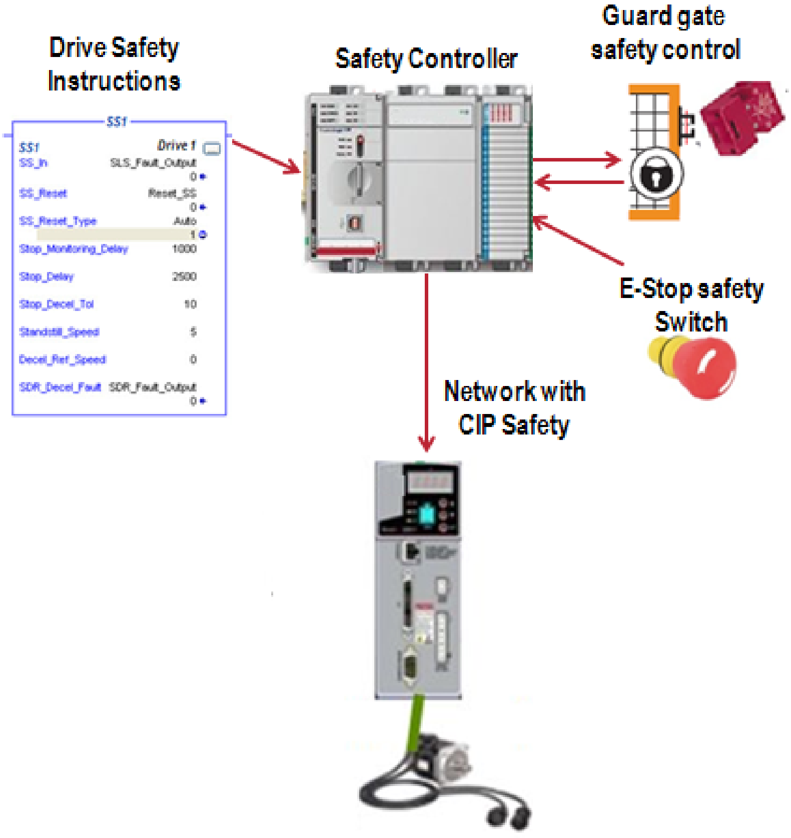
Safety Controller Activated Safety Functions (Option 2)

- CIP Safety network connection required.
- Safety Functions are executed in the Drive.
- Safety Function configuration data is stored in the Drive.
  - Local configuration tool with signature management.
- Safety Controller
  - Manages all safety I/O – local and distributed
  - Activates drive safety functions in drive & monitors drive safety status
  - User programmable safety logic with access to broad range of safety instructions and safety devices
- Benefits
  - Simple pre-defined Safety Functions in drive
  - Relatively Fast Safety Reaction Time.
  - Light impact on Safety Controller loading.
- Deficiencies
  - Drive safety function configuration is locked in drive, so limited drive setpoint control.
  - No Support for Multi-axis Coordination.



Safety Controller Executed Drive Safety Functions (Option 4)

- CIP Safety network connection required.
- Safety functions are executed in the safety controller (Except STO)
- Safety function configuration is stored in the Safety Controller.
  - Can be changed dynamically within Safety Program.
- Safety Controller
  - Manages all safety I/O – local and distributed
  - Executes drive safety functions in Safety Task using drive safety status data
  - User programmable safety logic with access to broad range of safety instructions and safety devices
- Benefits
  - Support for Multi-axis Coordination.
  - Programmable drive safety function set-point control.
  - Flexible implementation of drive safety functions via safety program.
- Deficiencies
  - Relatively Slow Safety Reaction Time.
  - Heavier impact on Safety Controller loading.
  - Additional Safety Function programming required.

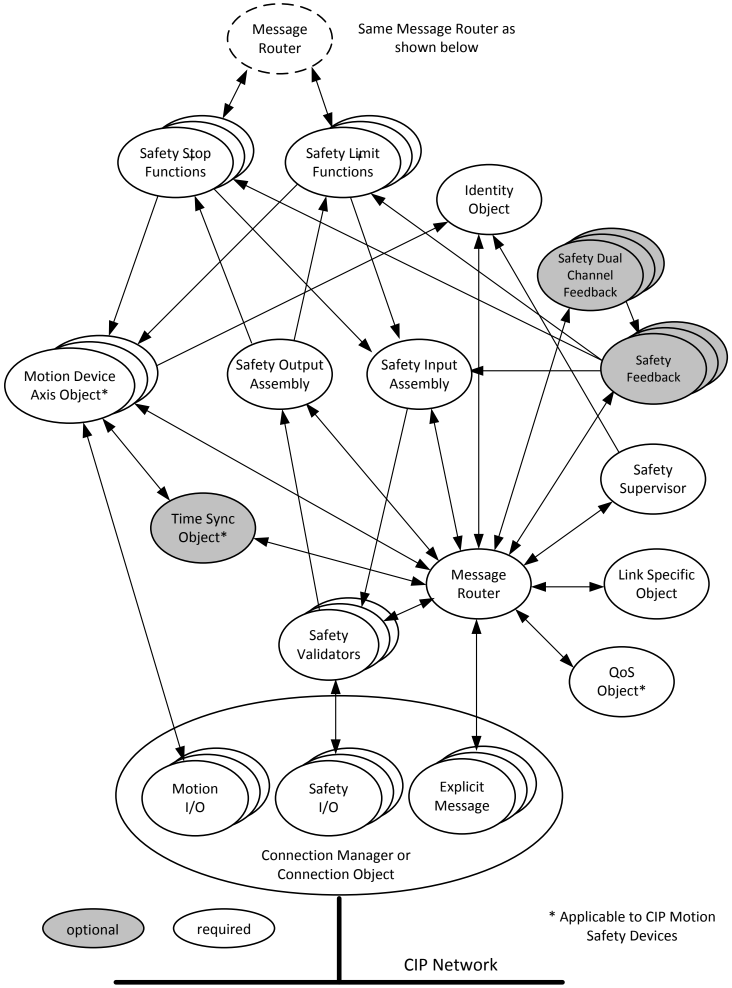


Safety Motion Device Profile

- New Profile Targets 2 Distinct Drive Types
  - CIP Motion Drives
  - Non-CIP Drives (SERCOS III)
- Profile Adds 2 New Safety Drive Device Types
  - CIP Motion Safety Drive Device Type: $2D_{hex}$
  - Safety Drive Device Type: $2E_{hex}$
- Both Drive Device Types...
  - Support CIP Safety Connections to Safety Controller.
  - Share Common Safe Motion Objects.
  - Share Common Safety I/O Assembly Definitions.
  - Share Common Safety Supervisor State Model

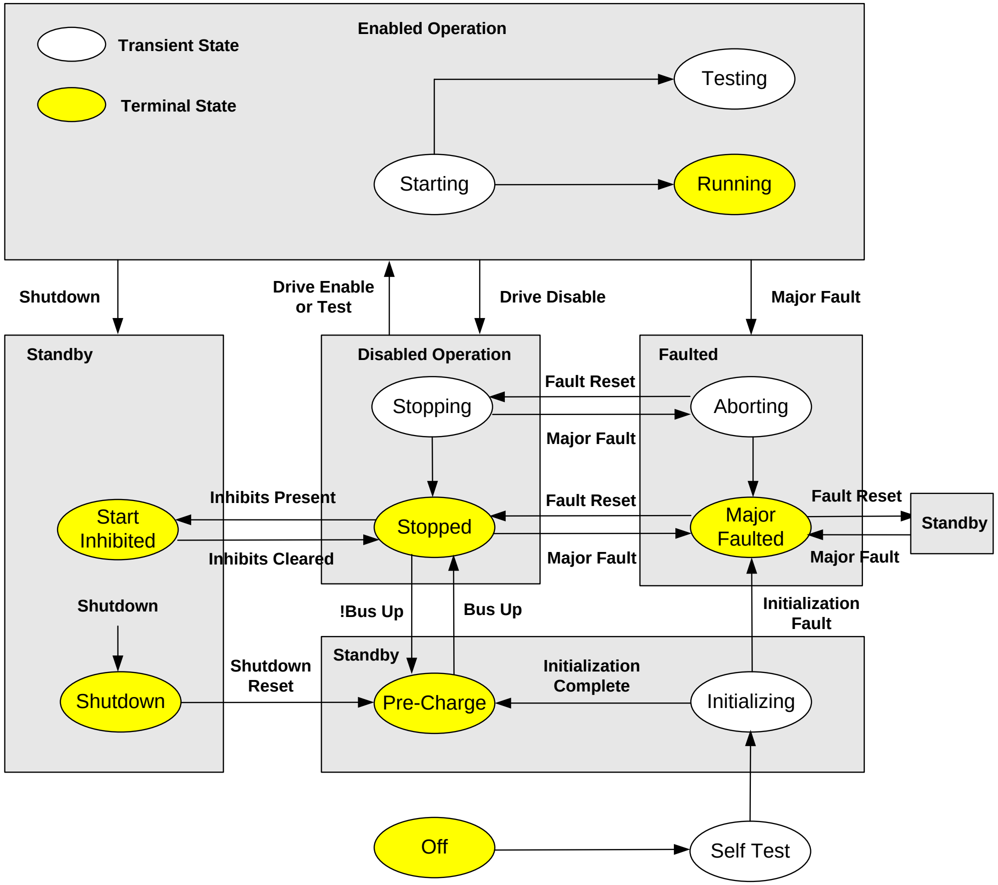
Object Model for CIP Motion Safety Drive Device

- New Safe Motion Objects:
  1. Safety Stop Functions Object
  2. Safety Limit Functions Object
  3. Safety Feedback Object
  4. Safety Dual Channel Feedback Object
- Basic CIP Safety Objects:
  1. Safety Validator Object
  2. Safety I/O Assembly Object
  3. Safety Supervisor Object
- CIP Motion Objects:
  1. Motion Device Axis Object
  2. Time Sync Object
  3. QoS Object
- Basic CIP Objects:
  1. Identity Object
  2. Message Router



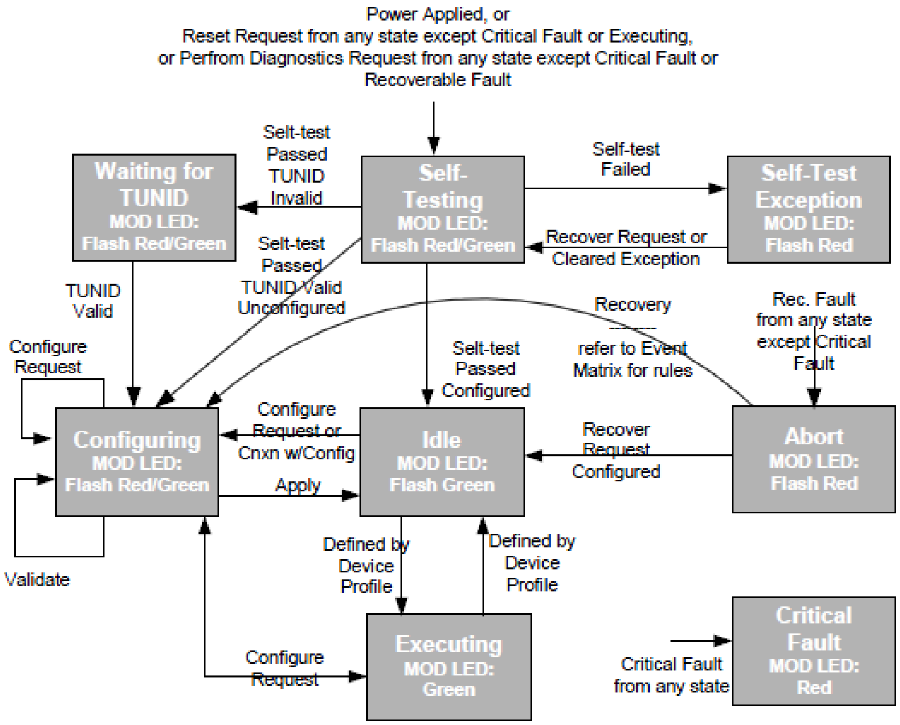
Motion Device Axis Object State Model

- CIP Motion Drive behavior is governed by the Motion Device Axis Object State Model.
- Axis Object states are mapped to Identity Object states.
- Identity Object states govern Module Status LED Behavior.



Safety Supervisor State Model

- CIP Safety Device behavior is governed by the Safety Supervisor State Model.
- Safety Supervisor states are mapped to Identity Object states.
- Safety Supervisor states govern Module Status LED Behavior.
- Problem: A CIP Motion Safety Drive has only 1 Identity Object and 1 Module Status LED. How do we reconcile behavior?


Power Applied, or
Reset Request fron any state except Critical Fault or Executing,
or Perfrom Diagnostics Request fron any state except Critical Fault or Recoverable Fault
Self-test Passed TUNID Invalid
Self-test Failed
Waiting for TUNID MOD LED: Flash Red/Green
Self-Testing MOD LED: Flash Red/Green
Self-Test Exception MOD LED: Flash Red
Recover Request or Cleared Exception
Self-test Passed TUNID Valid Unconfigured
TUNID Valid
Recovery
refer to Event Matrix for rules
Rec. Fault from any state except Critical Fault
Configure Request
Self-test Passed Configured
Configure Request or Cnxn w/Config
Recover Request Configured
Configuring MOD LED: Flash Red/Green
Idle MOD LED: Flash Green
Abort MOD LED: Flash Red
Apply
Validate
Defined by Device Profile
Defined by Device Profile
Critical Fault MOD LED: Red
Configure Request
Executing MOD LED: Green
Critical Fault from any state

Safety Drive State Precedence

- Identity state and Module Status LED behavior can be reconciled by applying state precedence rules to determine the drive’s Governing State:

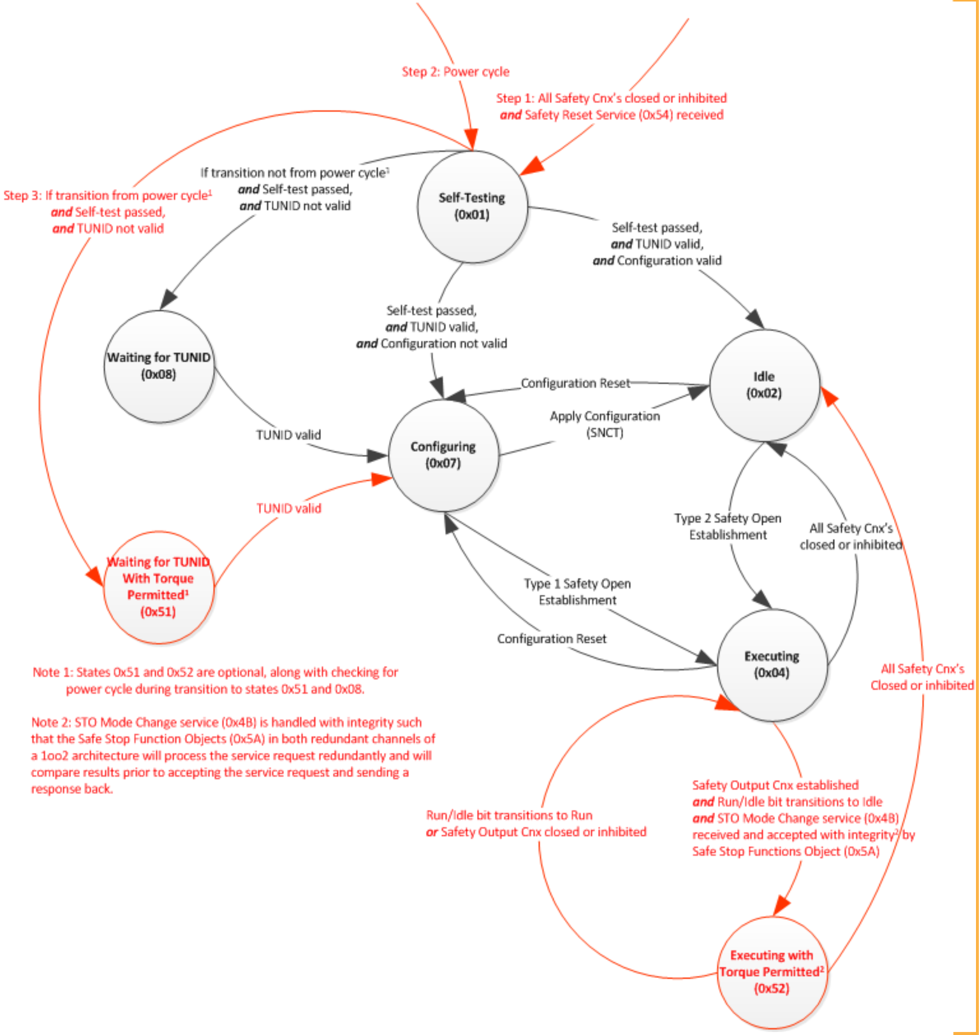
1. Self-Test
2. Unrecoverable Fault
3. Recoverable Fault
4. Safety Configuring
5. Safety Idle
6. Axis Standby
7. Axis Operational
8. Safety Executing
9. Safety Waiting for TUNID (Out of Box)

Safety Drive State Mapping

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, Executing, Executing with Torque Permitted	Initializing Pre-Charge Shutdown Start Inhibit	Motion Axis	Standby	Flashing Green
	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

New Safety Supervisor States for Commissioning & Maintenance

- Unlike Safety I/O devices, Safety Drives are sophisticated devices that require commissioning and maintenance.
- Commissioning requires the safety drive be operational "Out of the Box" when there is no Safety Configuration.
  - Add "Waiting for TUNID with Torque Permitted state".
- Maintenance requires the safety drive be permitted to operate when the Safety Output Connection is Idle.
  - Add "Executing with Torque Permitted state".


Step 2: Power cycle
Step 1: All Safety Cnx's closed or inhibited *and* Safety Reset Service (0x54) received
Self-Testing (0x01)
If transition not from power cycle[1] *and* Self-test passed, *and* TUNID not valid
Step 3: If transition from power cycle[1] *and* Self-test passed, *and* TUNID not valid
Self-test passed, *and* TUNID valid, *and* Configuration valid
Waiting for TUNID (0x08)
Self-test passed, *and* TUNID valid, *and* Configuration not valid
Idle (0x02)
Configuration Reset
Apply Configuration (SNCT)
TUNID valid
Configuring (0x07)
TUNID valid
Waiting for TUNID With Torque Permitted[1] (0x51)
Type 2 Safety Open Establishment
All Safety Cnx's closed or inhibited
Type 1 Safety Open Establishment
Configuration Reset
Executing (0x04)
All Safety Cnx's Closed or inhibited
Run/Idle bit transitions to Run *or* Safety Output Cnx closed or inhibited
Safety Output Cnx established *and* Run/Idle bit transitions to Idle *and* STO Mode Change service (0x4B) received and accepted with integrity[2] by Safe Stop Functions Object (0x5A)
Executing with Torque Permitted[2] (0x52)

Note 1: States 0x51 and 0x52 are optional, along with checking for power cycle during transition to states 0x51 and 0x08.

Note 2: STO Mode Change service (0x4B) is handled with integrity such that the Safe Stop Function Objects (0x5A) in both redundant channels of a 1oo2 architecture will process the service request redundantly and will compare results prior to accepting the service request and sending a response back.

Safety Output Assemblies

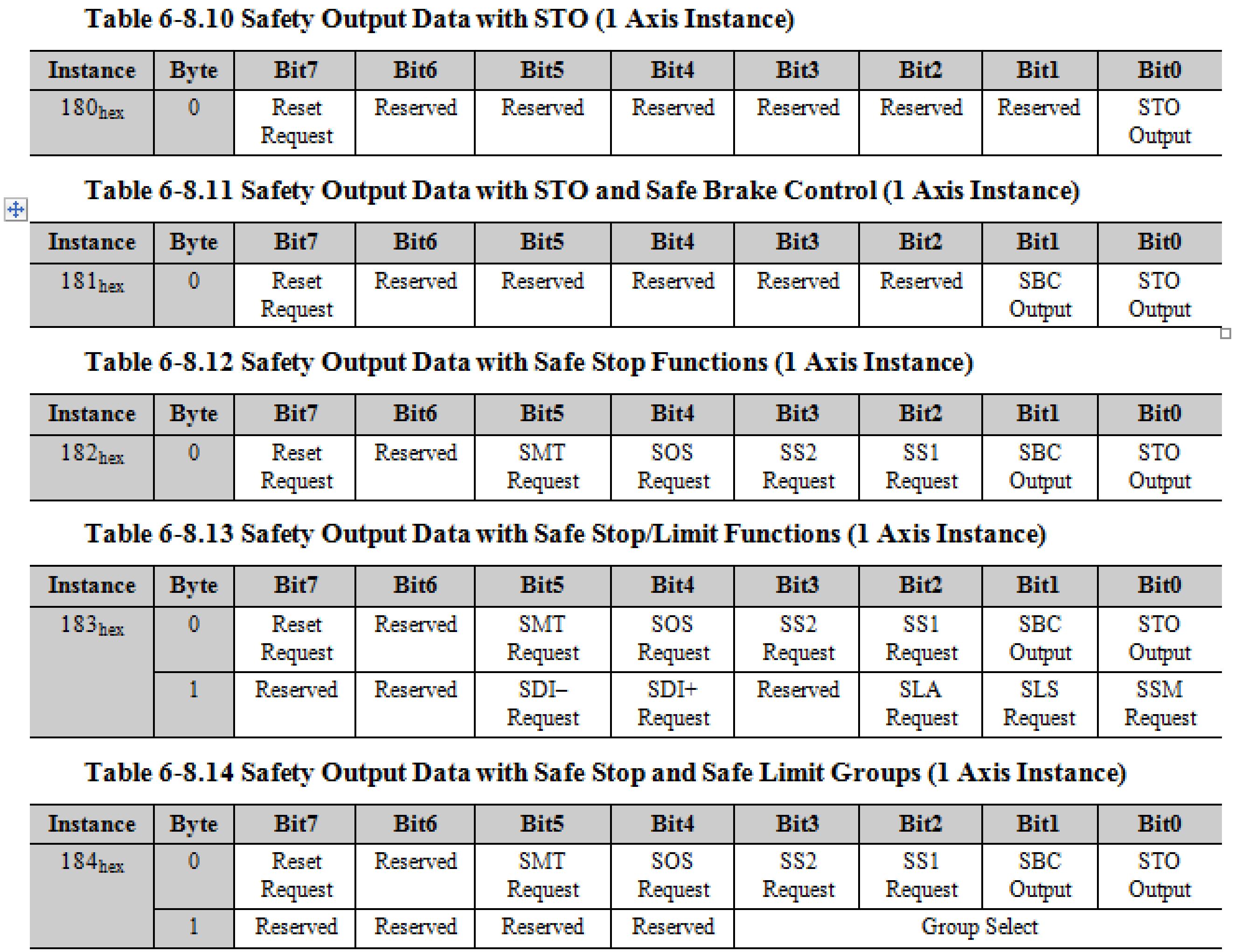


Table 6-8.10 Safety Output Data with STO (1 Axis Instance)

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 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 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

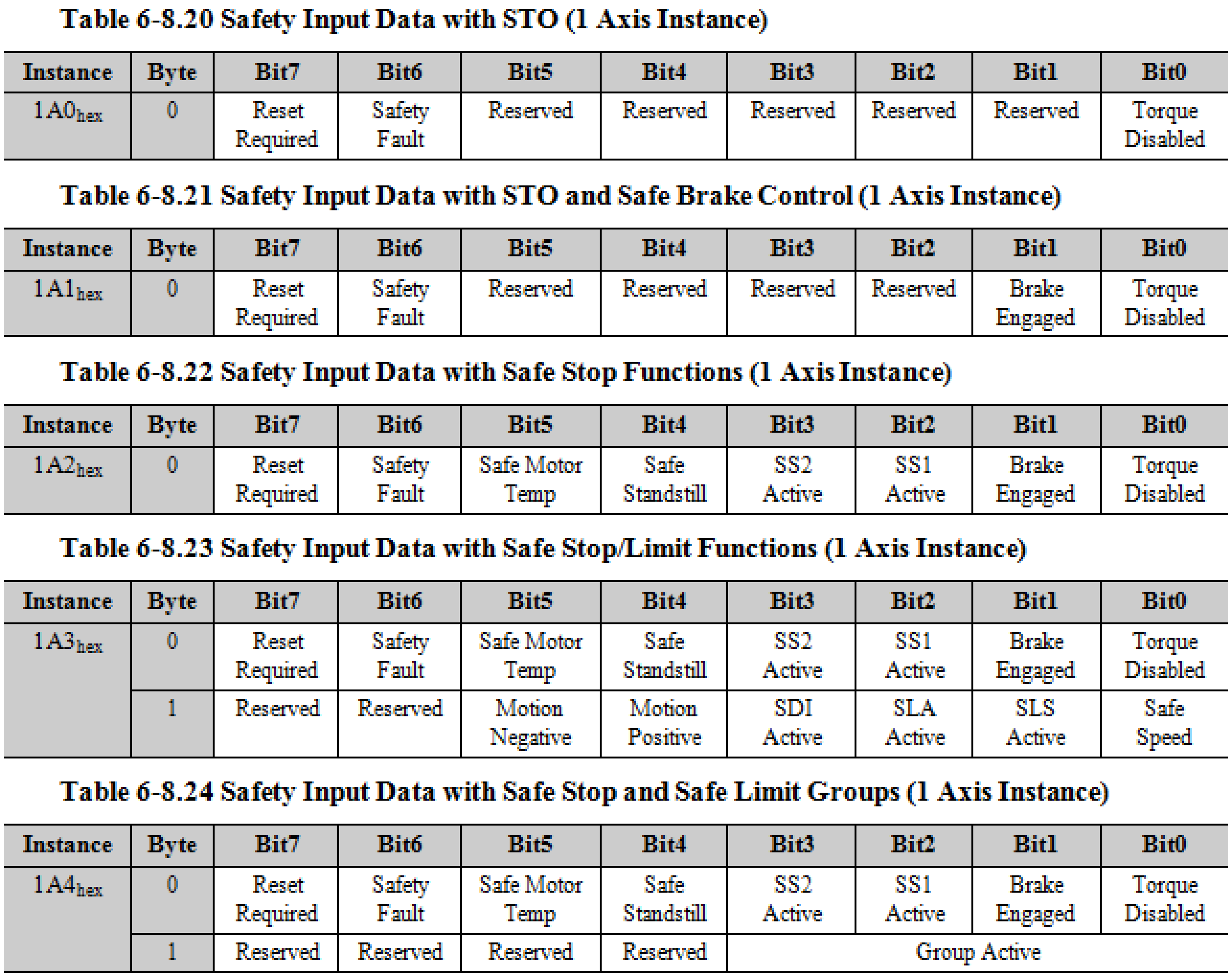


Table 6-8.20 Safety Input Data with STO (1 Axis Instance)

Instance	Byte	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
1A0hex	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
1A1hex	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
1A2hex	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
1A3hex	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
1A4hex	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			

Safety Input Assembly with Feedback Data

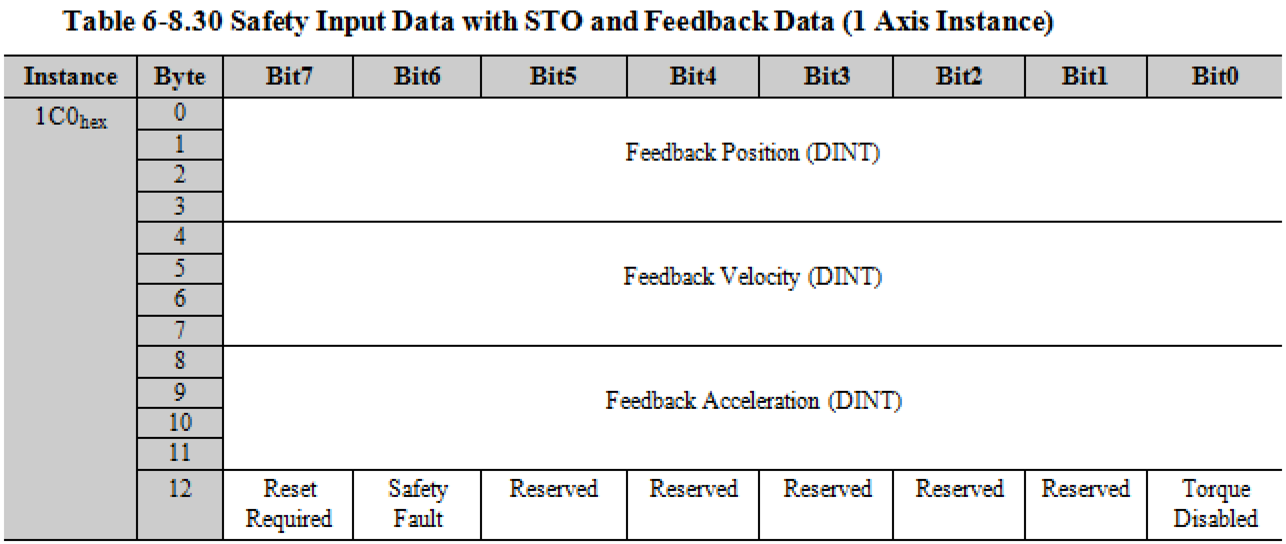


Table 6-8.30 Safety Input Data with STO and Feedback Data (1 Axis Instance)

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

Safety Input Assemblies with 2 Axis Instances

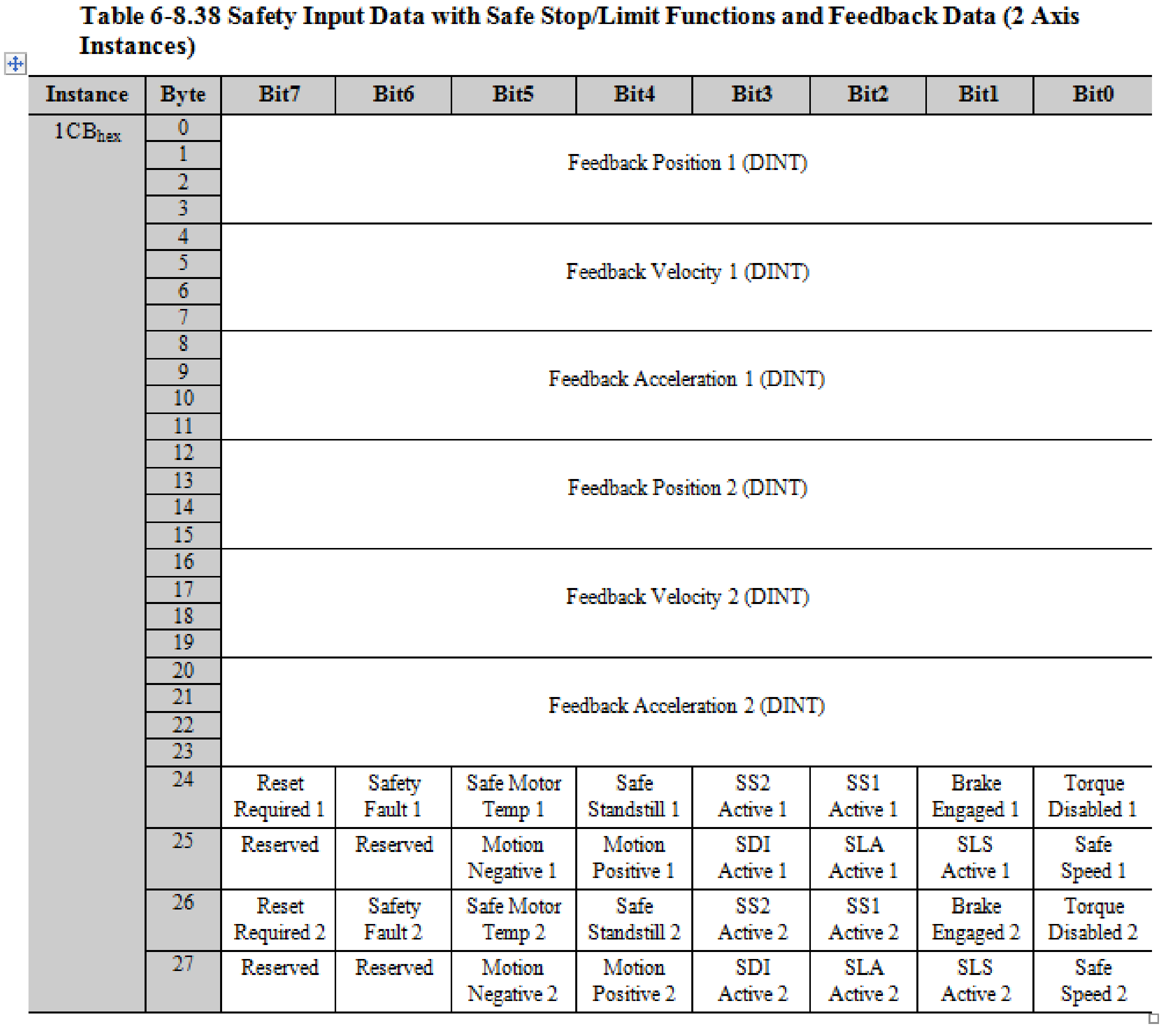
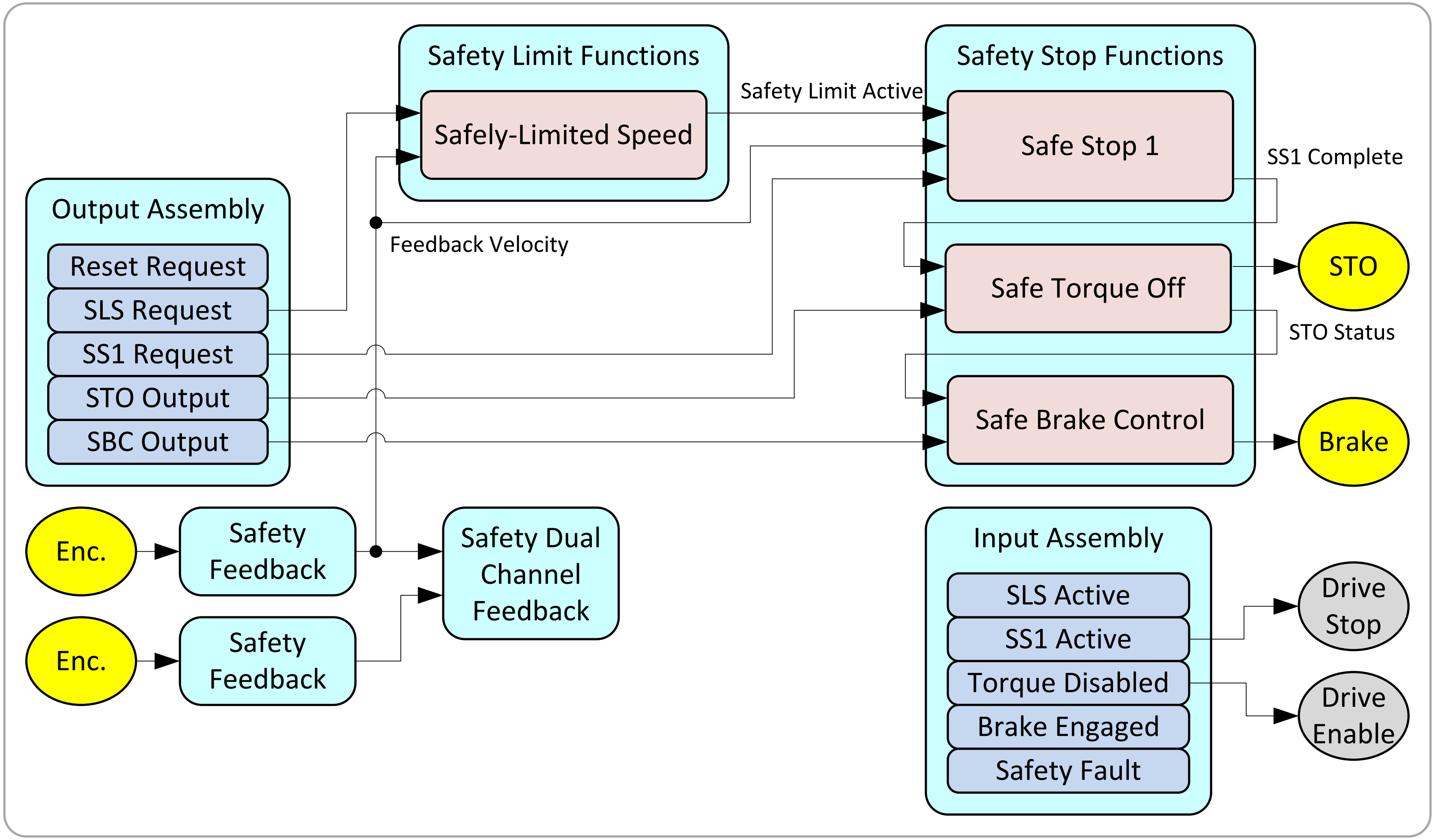


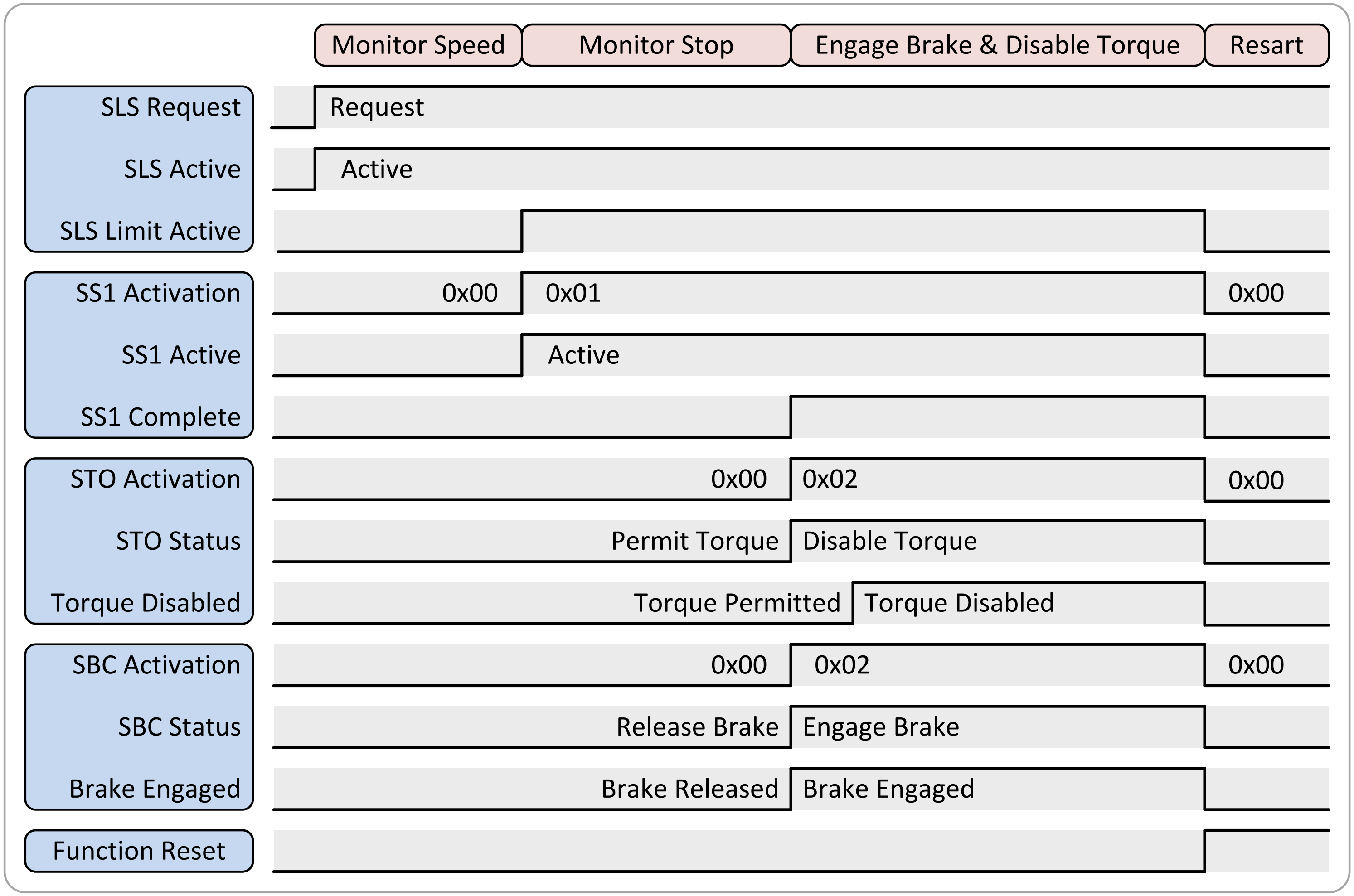
Table 6-8.38 Safety Input Data with Safe Stop/Limit Functions and Feedback Data (2 Axis Instances)

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

Safety Function Object Interaction



Safe Limited Speed Timing Diagram



Monitor Speed | Monitor Stop | Engage Brake & Disable Torque | Resart

SLS Request: Request

SLS Active: Active

SLS Limit Active

SS1 Activation: 0x00 | 0x01 | 0x00

SS1 Active: Active

SS1 Complete

STO Activation: 0x00 | 0x02 | 0x00

STO Status: Permit Torque | Disable Torque

Torque Disabled: Torque Permitted | Torque Disabled

SBC Activation: 0x00 | 0x02 | 0x00

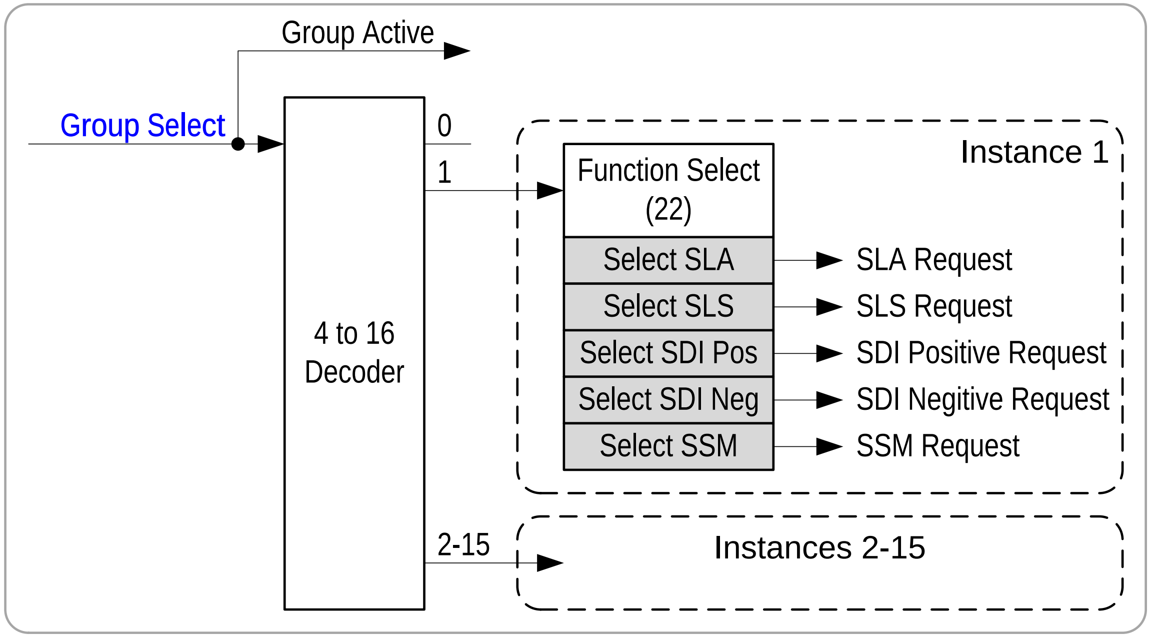
SBC Status: Release Brake | Engage Brake

Brake Engaged: Brake Released | Brake Engaged

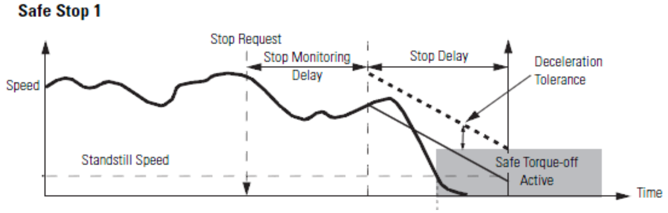
Function Reset

Group Safety Limit Function Selection

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**			

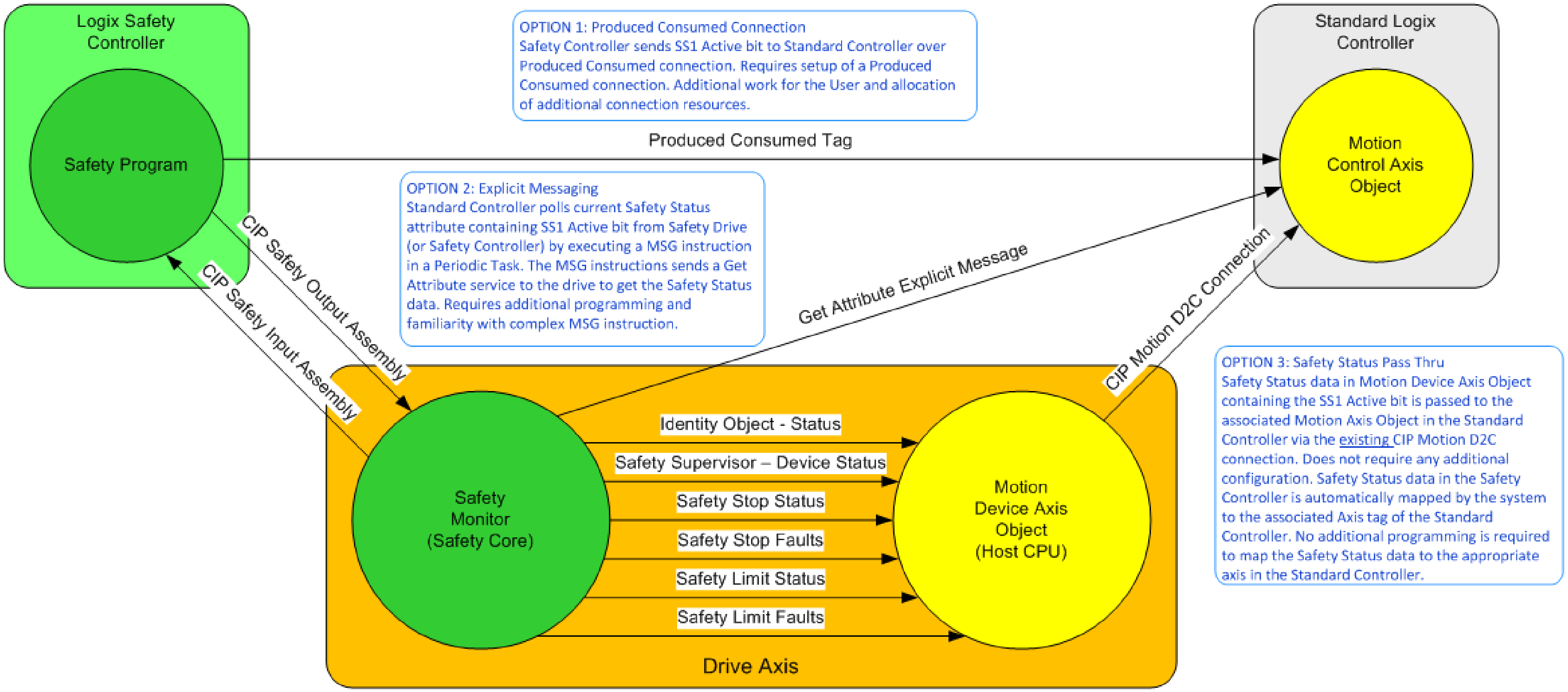


Accessing Safety Status Data



SS1 Execution by Safety Drive:
Safety Controller reads Safe Stop Input and applies to SS1 Instruction.
Safety Controller sets SS1 Request in Safety Output Assembly
Safety Controller must pass SS1 Active status bit to Standard Controller to initiate stop.

SS1 Execution by Standard Controller:
Standard Controller user task detects SS1 Active Status bit is set.
Rung logic executes Motion Axis Stop instruction on associated axis.



Logix Safety Controller

Safety Program

Standard Logix Controller

Motion Control Axis Object

OPTION 1: Produced Consumed Connection
Safety Controller sends SS1 Active bit to Standard Controller over Produced Consumed connection. Requires setup of a Produced Consumed connection. Additional work for the User and allocation of additional connection resources.

Produced Consumed Tag

OPTION 2: Explicit Messaging
Standard Controller polls current Safety Status attribute containing SS1 Active bit from Safety Drive (or Safety Controller) by executing a MSG instruction in a Periodic Task. The MSG instructions sends a Get Attribute service to the drive to get the Safety Status data. Requires additional programming and familiarity with complex MSG instruction.

CIP Safety Output Assembly

CIP Safety Input Assembly

Get Attribute Explicit Message

CIP Motion D2C Connection

OPTION 3: Safety Status Pass Thru
Safety Status data in Motion Device Axis Object containing the SS1 Active bit is passed to the associated Motion Axis Object in the Standard Controller via the existing CIP Motion D2C connection. Does not require any additional configuration. Safety Status data in the Safety Controller is automatically mapped by the system to the associated Axis tag of the Standard Controller. No additional programming is required to map the Safety Status data to the appropriate axis in the Standard Controller.

Safety Monitor (Safety Core)

Identity Object - Status

Safety Supervisor – Device Status

Safety Stop Status

Safety Stop Faults

Safety Limit Status

Safety Limit Faults

Motion Device Axis Object (Host CPU)

Drive Axis

Safety Core Passes Safety Status data to Motion Device Axis Object

Conclusion

- Drives with network safety connection support are a key component in emerging safety controller based safety architectures.
- Recently published Safety Motion Device Profile addresses critical need for a networked “*Safety Drive*”.
- 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 design challenges with respect to state behavior, commissioning, and maintenance.
- Safety Motion Device I/O assemblies and new 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.