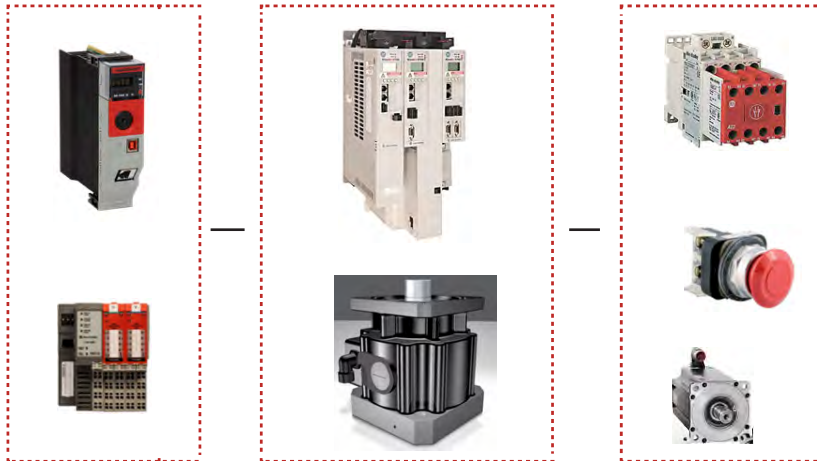


Safe Brake Control (SBC) Safety Function

Products: Kinetix 5700 ERS4 Drive, GuardLogix 5580 Controller, VPL Motor

Safety Rating: Cat. 2, PLd to ISO 13849-1: 2015



Topic	Page
Important User Information	2
General Safety Information	3
Safety Reaction Time	3
Introduction	4
Use Sample Project Files	5
Safety Function Realization: Risk Assessment	6
Safe Brake Safety Functions	6
Safety Function Requirements	6
Functional Safety Description	11
Bill of Material	22
Setup and Wiring	24
Configuration	26
Calculation of the Performance Level	44
Verification and Validation Plan	47
Appendix A – Timing and Sequencing Diagrams	48
Additional Resources	61

Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.



SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.



ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

General Safety Information

Contact Rockwell Automation to learn more about our safety risk assessment services.

IMPORTANT This application example is for advanced users and assumes that you are trained and experienced in safety system requirements.



ATTENTION: Perform a risk assessment to make sure that all task and hazard combinations have been identified and addressed. The risk assessment can require additional circuitry to help reduce the risk to a tolerable level. Safety circuits must consider safety distance calculations, which are not part of the scope of this document.

Safety Distance Calculations



ATTENTION: While safety distance or access time calculations are beyond the scope of this document, compliant safety circuits must often consider a safety distance or access time calculation.

Non-separating safeguards provide no physical barrier to help prevent access to a hazard. Publications that offer guidance for calculating compliant safety distances for safety systems that use non-separating safeguards, such as light curtains, scanners, two-hand controls, or safety mats, include the following:

- EN ISO 13855:2010 (Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body)
- EN ISO 13857:2008 (Safety of Machinery – Safety distances to help prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

Separating safeguards monitor a movable, physical barrier that guards access to a hazard. Publications that offer guidance for calculating compliant access times for safety systems that use separating safeguards, such as gates with limit switches or interlocks (including SensaGuard™ switches), include the following:

- EN ISO 14119:2013 (Safety of Machinery – Interlocking devices associated with guards – Principles for design and selection)
- EN ISO 13855:2010 (Safety of Machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body)
- EN ISO 13857:2008 (Safety of Machinery – Safety distances to help prevent hazardous zones being reached by upper and lower limbs)
- ANSI B11:19 2010 (Machines – Performance Criteria for Safeguarding)

In addition, consult relevant national or local safety standards to verify compliance.

Safety Reaction Time

The total safety reaction time is required for all examples that are used in this publication. The safety brake reaction times are added to the typical GuardLogix® reaction time, I/O delay times, and network delay calculations. The sum of all these delays determines the total safety reaction time.

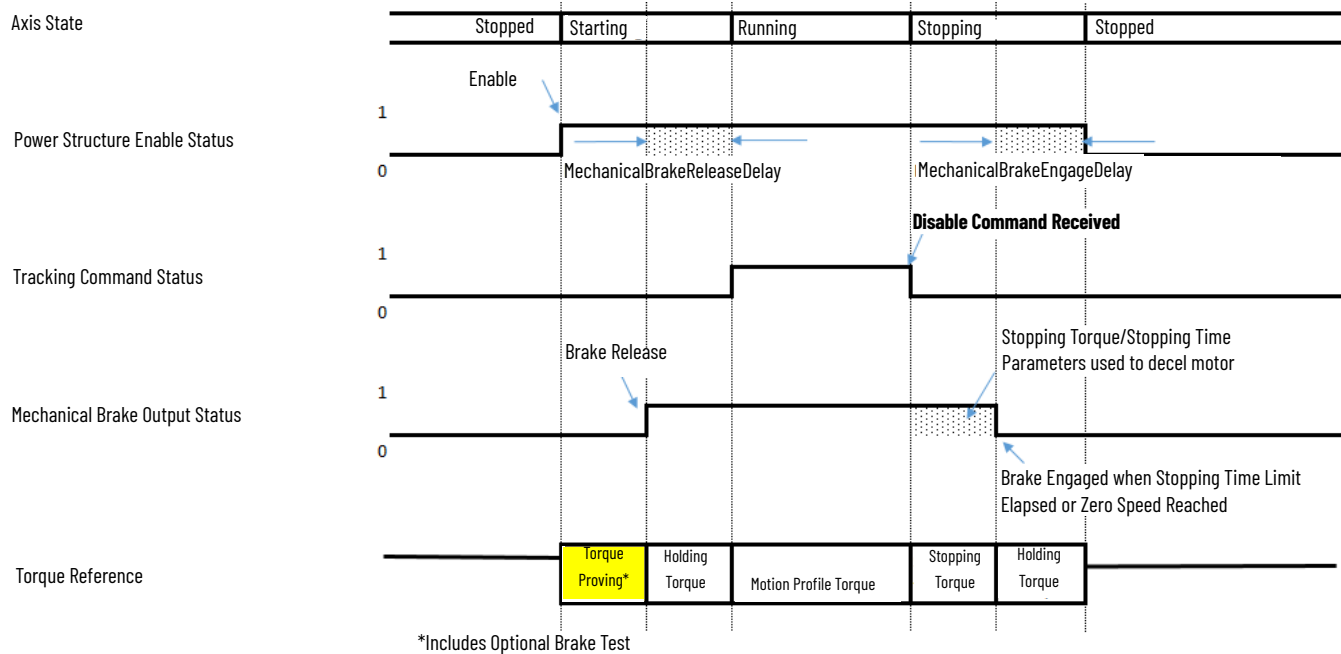
In all examples, the Motor Brake (MBRK) output is intentionally used when the safety brake is released. This publication includes an example (Disable) that intentionally uses the MBRK output to engage the safety brake. Both the E-stop and HOLD examples use the MBRK output, but as a result of an STO operation.

These delay times are used to manage the MBRK output actuation to avoid dropping a vertical load:

Mechanical Brake Engage Delay	The amount of time that the power structure of the drive remains enabled after the axis has been commanded to zero speed before disabling the power structure. The motor decelerates to a stop, the brake output actuates, and this delay provides time for the brake to engage.
Mechanical Brake Release Delay	The amount of time after the drive is enabled but before the drive is able to follow a command. During this delay, no commanded motion is permitted as the drive physically releases the brake.

This timing chart shows where the delay times are used with the MBRK output.

Disable Command and MBRK Operation



The MBRK output delay times must include the safety reaction times. The total safety reaction time includes the times for the safety brake to engage and release. The manufacturer of the safety brake that is used in this example provided the engage and release times that are shown in the following table.

Condition	Description	Time
Stopping and Engaging	Time from dropping coil power to achieving 90% of stated braking torque.	55 ms
Restarting and Releasing	Time from providing coil power to achieving 10% of stated braking torque.	80 ms

Introduction

This safety function application technique explains how to configure and program a GuardLogix 5580 controller and a Kinetix® 5700 (2198-xxxx-ERS4) inverter to control a safety brake. This publication includes safety functions that use the Safe Brake Control (SBC) instruction, and the Kinetix 5700 Safe Torque Off (STO) function to help prevent hazardous motion.

This publication describes a vertical load application with three different use case examples.

Mechanical Fastening of the Encoder

A physical connection between motor and encoder, as well as between motor and load is implied in this publication.



ATTENTION: While mechanical fastening of the encoder is beyond the scope of this publication, the physical connection between the motor and encoder, as well as between the motor and load and/or between the encoder and the load, must be evaluated in a mechanical safety assessment.

The detachment of a fastening method, which results in misrepresentation of the electrically-derived position versus mechanical position that could potentially lead to a dangerous failure, must be evaluated.

Publications that offer guidance for mechanical fastening include the following:

IEC 61800-5-3 (Adjustable speed electrical power drive systems – Safety requirements for encoders – Functional, Electrical and Environmental)



GS-IFA-M21 (IFA Whitepaper) – (Principles for the testing and certification of rotary and position measuring systems for functional safety)

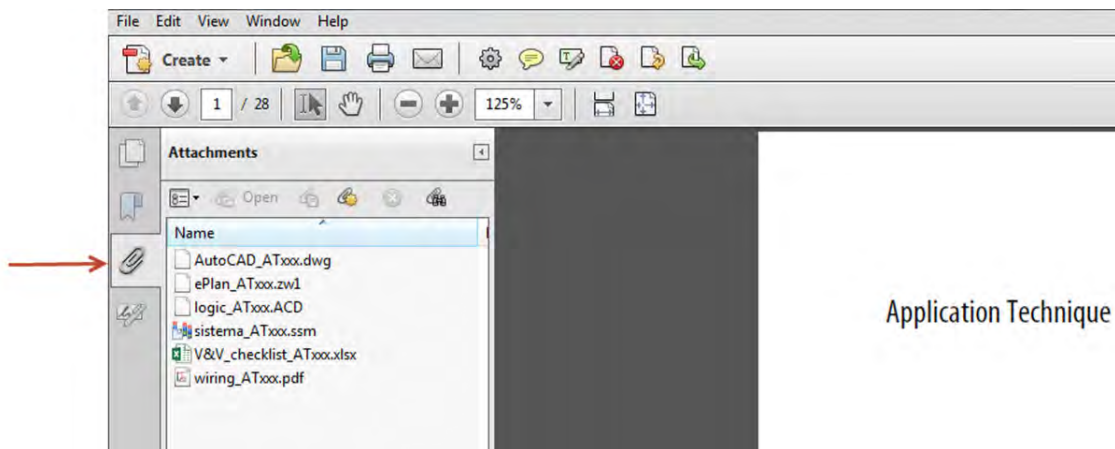
Annex A of EN ISO 13849-2 – (Validation tools for mechanical systems)

Use Sample Project Files

Sample project files (AutoCAD, EPLAN, ACD, SISTEMA, and Verification and Validation checklist) are attached to this publication to help you implement this safety function.

To access these files, follow these steps.

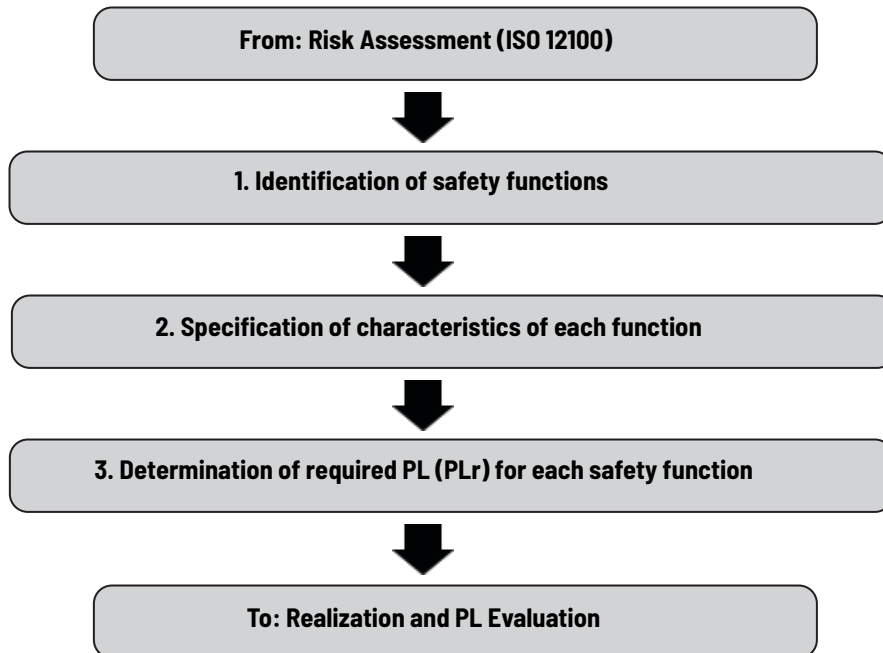
1. If you are viewing the PDF file in a browser and do not see the Attachments link , download the PDF file and open it in the Adobe Acrobat Reader application.
2. Click the Attachments link .
3. Right-click and save the desired file.



4. Open the file in the appropriate application.

Safety Function Realization: Risk Assessment

The Performance Level required (PLr) is the result of a risk assessment and refers to the amount of the risk reduction to be conducted by the safety-related parts of the control system. Part of the risk reduction process is to determine the safety functions of the machine. In this application, the Performance Level that is required by the risk assessment is category 2, Performance Level d (cat. 2, PLd), for each safety function. A safety system that achieves cat. 2, PLd, or higher, can be considered control reliable. Each safety product has its own rating and can be combined to create a safety function that meets or exceeds the PLr.



Safe Brake Safety Functions

This application technique includes two safety functions:

- Emergency stop for unintended motion.
- HOLD (normal STOP) not operating properly or Kinetix 5700 MBRK output engaged unexpectedly.

Safety Function Requirements

There can be different application uses for the safety brake. The examples in this publication use input conditions to initiate different stop conditions. With all of these examples, when the input signal is active, the stopping condition, at some point, executes the Safe Brake Control (SBC) instruction. The examples are HOLD (normal STOP), E-stop (emergency stop), and Disable. The second safety function is modeled using the worst case in the HOLD and Disable examples. Because the operation and results are the same, we use one safety function for both of these worst case examples.

The Application of a Safety Brake

When an application requires a means to engage (grab) a load so it can be safely held, a safety brake can be used on the actuator. Our examples use a STOBBER gearbox (ServoFit family) connected in-line with a STOBBER brake (ServoStop family), which is based on a mayr ROBA-TopStop safety brake that is mounted to a VPL servo motor.

It is worth noting that the STOBBER ServoStop has a custom shaft that allows the input pinion of the high speed gear to be pressed directly into this shaft. This is a Loctite and pressed fit, which reduces the chance of a coupling slipping or failing between the gearbox and brake. This fit also makes the package more compact and assures that all alignments (axially) are good.



The safety brake is designed to stop and hold a motor that is attached to a load. These loads are typically vertical but can also be horizontal. A vertical load is classified as a load that stores potential energy either by gravity or spring effect. In this type of load, the Kinetix servo motor must hold part or all of the load, even when the motor is not moving, but is still powered by the drive. A horizontal load does not store potential energy (either by spring or gravity effect) when the motor is disabled.

Vertical or horizontal loads can use a motor holding brake to keep the load stationary while the motor is disabled. Holding brakes are not designed to stop a motor, but rather to hold a motor when it is stationary and disabled.

Each safety brake manufacturer provides guidance for the maintenance of their particular safety brake. They also provide the maximum number of actuation cycles between inspections. When a safety brake stops a moving load, it counts against its maximum number of actuation cycles, after which the safety brake needs inspection for replacement or maintenance. If the load is stationary (zero speed) when the safety brake is engaged, this particular actuation instance does not count against the replacement or maintenance criteria.

A cycle in this publication refers to the actuation of the safety brake. This actuation is the engaging and releasing of the safety brake.

This publication includes the use of the Kinetix 5700 MBRK output for the engagement of the safety brake. The MBRK output is automatically controlled, which simplifies the considerations for the safety brake actuation with the state of the axis. When the Disabling input event is the Current Decel & Disable action type, the MBRK output employs timing that allows the motor to remain enabled and stationary while the safety brake is applied. This action is important to help prevent the load from dropping. Our examples monitor the MBRK function by using a safety input.

Upon the Restart or physical release of the safety brake, the MBRK output is used and the MechanicalBrakeReleaseDelay is set for the total safety reaction time to help prevent the load from dropping. The Restart cycle is used with all examples.

IMPORTANT Using a physical motor-holding brake is optional. The use of a holding brake is intended as an extra means of holding a stationary motor before the safety brake is applied so that the stopping cycle does not count against the criteria for maintenance or wear.

There can be a condition when an axis exception (Major Fault) results in a Disable & Coast action. We configure the drive to avoid this action. However, if a major fault that results in a Disable & Coast action is encountered, and if the motor-holding brake engages faster than the safety brake (the MBRK output is de-energized simultaneously for both types of brakes), use of a holding brake can minimize the risk of the load dropping.

This benefit must be weighed against the potential of the holding brake being used as a stopping brake, which it is not designed to do. The safety brake is designed to stop and hold the load. This is where the safety reaction time and Stop Action Types (found in the Kinetix 5700 Servo Drives User Manual, publication [2198-UM002](#)) are important considerations for your application.

It can be beneficial to use a holding brake in the unlikely failure of the MBRK output (for example, the output shorts to 24V DC). Because a physical holding brake is also wired to the MBRK output, the holding brake could be used to hold the stationary motor, while this condition is detected in logic (for example, miscompare safety logic). Consider that the holding brake is not a safety device and an alternative to this configuration would be to use a second safety brake on the same load.

Application Example Considerations

For all of the examples, deliberate consideration was made for the application of the safety brake when the motor is being enabled (restarting) and when the motor is being disabled. If the SBC safety instruction was solely used to stop and disable the motor, the maximum actuation limit would likely be achieved quickly and maintenance would become inefficient as the SBC alone does not consider standstill speed. Also, consider that during the restart sequence, your configuration may not have included motor brake holding times, which can potentially cause the load to drop while the motor is enabling. Additionally, we consider the normal (typical) safety brake use, as well as the non-typical brake use (for example, a failed condition). All of these considerations are used to prolong the actuation cycle limit while safely engaging the load.

For all of the examples, the Axis Safety Action for the STO function has been configured for Running Controller, which requires the GuardLogix standard program to execute the stopping actions. When the STO action in the drive is configured for Running Controller, the Guardlogix safety program controls the Module:SO.STOOutput bit. In our examples, the STO request initiates from the SBC instruction in the GuardLogix safety program.

These examples use a GuardLogix 5580 controller, but they are also applicable to the Compact GuardLogix 5380 controller.

These examples use a VPL servo motor with a factory-installed SIL 2 encoder and a factory-installed motor holding brake. The drive is configured for single feedback monitoring. This is described in the [Configuration](#) section of this publication.

If the safety connection between the GuardLogix controller and Kinetix 5700 drive is lost, the Connection Loss setting in the Kinetix 5700 drive properties determines the reaction to this fault. This is described in the safe brake examples found in the section entitled [Integrated Safety: Safe Torque Off Considerations for a Stop Category 1](#).

All examples demonstrate how to achieve the safety functions by using a Kinetix 5700 drive with Safe Monitor functions (2198-xxxx-ERS4). The bill of material uses specific part numbers for the drives, motors, safety brake, and discrete components. Consider that other catalog numbers can give you the same results.

For the Kinetix 5700 solution, the power supply is required by the system, but is not considered part of the safety system. Therefore, any of the Kinetix power supplies can be applied without affecting the safety rating of the system. There are also several choices of inverter size (amp rating) and configuration (single or dual). The inverter is part of the safety system but all Kinetix 5700 (2198-xxxx-ERS4) inverters have the same safety rating so the specific catalog number does not affect the overall rating.

The GuardLogix controller (by using the embedded EtherNet/IP port) uses safety connections to the 1734-IB8S module, the 1734-OB8S module, and the Kinetix drive over an EtherNet/IP™ network. CIP Safety™ protocol makes the network architecture a black channel, and thus not part of the safety (PL) calculation. There are also non-safety connections to the Kinetix drive and 1734-IB8 input module.

We have created a delay that is called SafeBrakeDelay in the safety task. This delay is used if additional time is required to engage a secondary mechanical braking system (for example, rotary disc brakes, or air powered brakes) when an exception, Motion Servo Off (MSF), or disable request occurs. When the MBRK output is low (0), the SafeBrakeDelay allows time for that secondary mechanism to engage and hold the load before the safety brake is applied. This is done so that the secondary braking system can attempt to bring the axis to zero speed to exclude this stopping cycle from being counted against the maximum actuation cycles of the safety brake. The secondary braking system does not include the integrated holding brakes of the motor. The integrated motor holding brakes can be used together with the safety brake.

IMPORTANT During an abnormal condition that results in a Disable & Coast stopping action, SafeBrakeDelay delays the engagement of the safety brake. The load could drop until the secondary brake engages. If the secondary brake fails to engage, the load could drop until after SafeBrakeDelay expires when the safety brake engages.

IMPORTANT It is typical for the SafeBrakeDelay time to be zero. This engages the safety brake as quickly as possible after the MBRK output transitions to low (0). If a secondary brake is not used, set this delay to zero.

EXAMPLE SafeBrakeDelay additional use case: There can be an unusual application example when a load is horizontal and not vertical, and has a large inertia. If a holding brake is not used, and a Disable & Coast action is encountered, the load coasts to a stop when a fault occurs. If a coast-to-stop can be used in the application without introducing any unacceptable risks, the SafeBrakeDelay can be used to help prevent the safety brake from stopping the moving load. In this case, the stopping cycle does not count against the maximum actuation cycles. In this scenario, the safety brake is only applied to the stationary load.

E-stop Example

In the E-stop (Emergency Stop) example, the Safe Brake Control instruction is used to engage the safety brake. The SBC instruction initiates the STO request. The Kinetix 5700 STO function is controlled in the safety task to help prevent hazardous motion after the safety brake has been engaged.

To achieve a safety integrity level of PLd, engage the load with the safety brake when the E-stop button is pressed. This example bypasses the SafeBrakeDelay. The safety brake is engaged immediately. This stop type does not attempt to decelerate and disable the motor before engaging the safety brake. The safety brake is engaged and the ability of the motor to produce torque is removed.

HOLD (normal STOP) Example

In the typical HOLD example, the Safe Stop 2 (SS2) instruction executes and the SS2 pass-through tag triggers motor deceleration by using a Motion Axis Stop (MAS) motion instruction. When the SS2 deceleration monitoring is complete, the motor remains enabled and the Safe Operating Speed (SOS) condition is active indefinitely. The SBC instruction is used to engage the safety brake. The SBC instruction initiates the STO request. The Kinetix 5700 drive with STO is controlled in the safety task to help prevent hazardous motion after the safety brake has been engaged.

The premise in this publication is that the typical HOLD (normal STOP) is not a safety function. Consider that if the HOLD does not work properly, this failure initiates a non-typical HOLD (normal STOP) action. This helps with the cat. 2 classification for the non-typical HOLD safety function (which is named: HOLD (normal STOP) not operating properly), because all typical HOLD cases can be considered tests of the non-typical HOLD safety function. Even when a typical HOLD (normal STOP) occurs, the safety brake is engaged on a stationary motor. These tests allow the single channel safety brake to be considered cat. 2. The cat. 2 classification suggests a test rate of 100 times the demand rate, and so this example assumes that there are easily over 100 normal run stops for each non-typical HOLD action.

For additional information, see the DGUV publication, [Gravity loaded axes \(Vertical axes\) Division Information Sheet](#).

In the non-typical HOLD example, to achieve a safety integrity level of PLd, the safety brake must engage (grab) the load when the typical HOLD example does not operate properly. When this occurs (for example, the SS2 instruction is faulted), this stop type does not attempt to decelerate the motor before disabling. There is no disable timing that is associated with this stop type; the drive is disabled when the MBRK output is de-energized. The SBC instruction is used to engage the safety brake. The SBC instruction initiates the STO request. The Kinetix 5700 drive with STO is controlled in the safety task to help prevent hazardous motion after the safety brake has been engaged. This achieves a performance level of PLd. The non-typical HOLD is modeled as the safety function named HOLD (normal STOP) not operating properly.

Disable Example

When using the typical Disable example, the drive receives a disable command (an example is a Motion Servo Off (MSF) instruction or exception), the motor is decelerated to zero speed, and then disabled. This action is Current Decel & Disable, which is the preferred stopping action. During the disable timing, the MBRK output is de-energized. The MBRK (Motor Brake) output is used with additional interlocks and the SBC instruction to engage the safety brake. The disable timing is such that delays can be used to keep the motor enabled so that the load does not drop while the safety brake is engaging. The SBC instruction initiates the STO request and removes the torque producing ability of the motor. The Kinetix 5700 drive with STO is controlled in the safety task to help prevent hazardous motion after the safety brake has been engaged.

In the non-typical Disable example, it is possible that the drive encounters an axis exception (Major Fault) that has a stopping action of Disable & Coast. We configure the drive to avoid this condition. This Disable & Coast action is not typical and is modeled as a worst case scenario. This stop type does not attempt to decelerate the motor before disabling. There is no disable timing that is associated with this stop type; the drive is disabled when the MBRK output is de-energized. The SafeBrakeDelay (typically zero) counts down and when it expires, the SBC instruction is used to engage the safety brake. The SBC instruction initiates the STO request and removes the torque producing ability of the motor. The Kinetix 5700 drive with STO is controlled in the safety task to help prevent hazardous motion after the safety brake has been engaged. This achieves a performance level of PLd. The non-typical Disable is modeled as the safety function named 'Kinetix 5700 MBRK output engaged unexpectedly'.

The safety functions in this application technique each meet or exceed the requirements for category 2, Performance Level d (cat. 2, PLd), per ISO 13849-1 and control reliable operation per ANSI B11.19.

Functional Safety Description

This section describes how to use the three examples in our vertical load application.

A starting point of these examples assumes:

- the safety brake is engaged, which means the load is being held. The safe brake feedback monitoring output is wired to the 1734-IB8S input 3, which is low (0). The safety brake's feedback is a N.O. output that we must logically invert so it works correctly with the SBC instruction. To reset the SBC instruction, both Feedback channels must be high (1).
- the STO function is active, which means the motor cannot produce torque. The Module:SO.STOOutput tag is low (0).
- the Kinetix 5700 drive is disabled so that the MBRK output is not energized. The MBRK output is wired to the 1734-IB8S input 4, which is low (0).

IMPORTANT All three examples use the SBC instruction. The SBC instruction uses a safety relay to engage and release the safety brake.

When the safety relay output transitions to low (0), the safety program uses the Safety Feedback Interface (SFX) instruction to monitor the axis velocity.

If the SFX instruction output 1 (01) is high (1), and the SFX ActualSpeed tag is less than a user-defined limit (used to indicate zero speed), this stopping cycle does not count against the safety brake maximum actuation cycles limit.

If the SFX instruction output 1 (01) is low (0), or the SFX ActualSpeed tag is greater than the user-defined limit (used to indicate zero speed), this stopping cycle counts toward the maximum actuation cycles limit. In this case, our specific safety brake can reliably manage 2000 nonzero speed cycles before maintenance or replacement is required. In the GuardLogix safety program, we increment a counter (SafeBrakecount) to register the number of nonzero speed stopping cycles that have occurred.

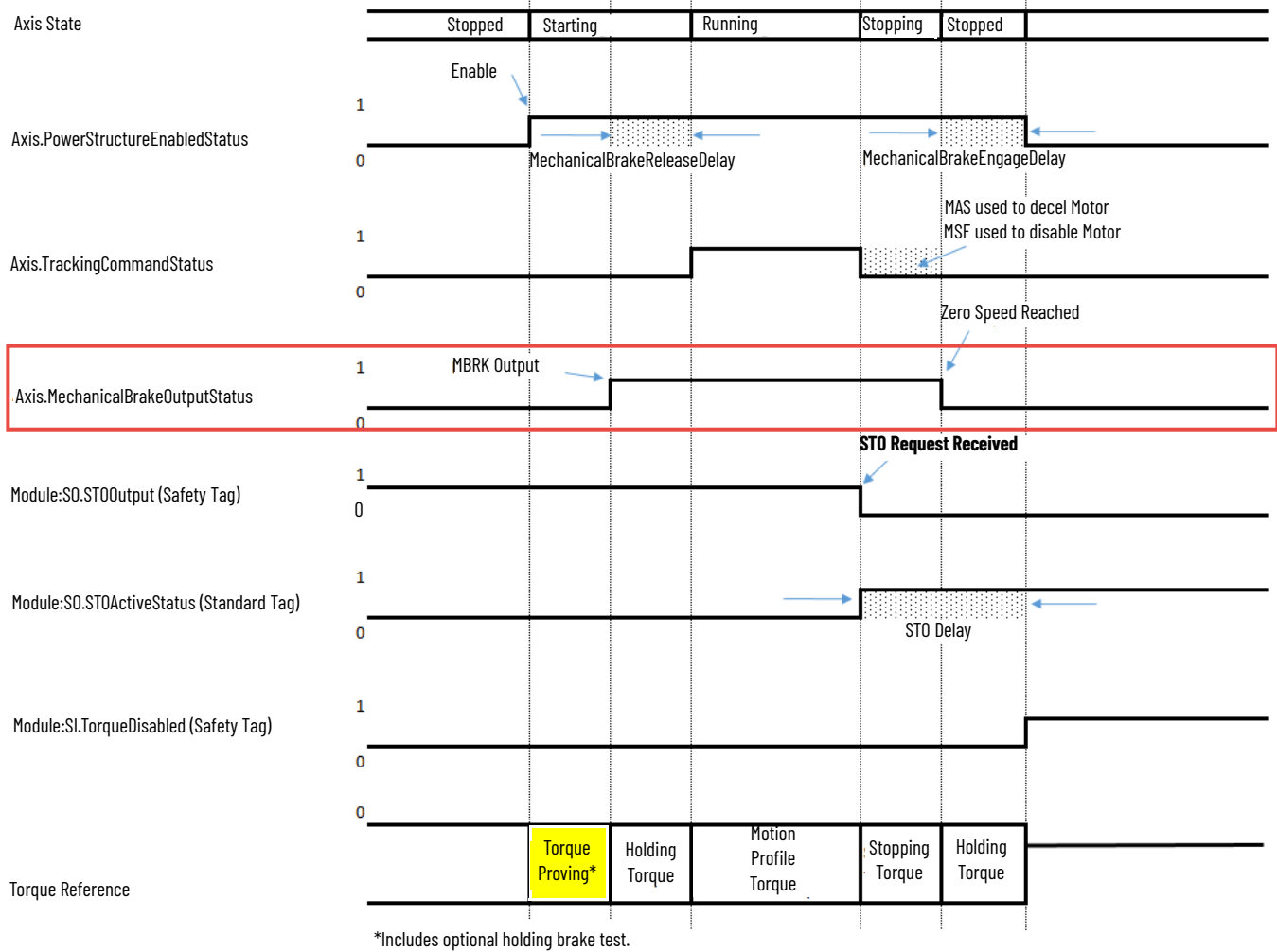
Releasing the Safety Brake

In each of the examples, the safety brake is released by following this process:

1. Use standard program logic to reset the drive or clear axis faults on the Kinetix 5700 drive.
2. Use the safety program logic to reset faults on the drive safety instructions.
3. Disable the STO function and set Module:SO.STOOutput to high (1) to restore the capability of the drive to produce motor torque.
4. Enable the drive using a Motion Servo On (MSO) instruction (executed in the standard program logic):
 - This automatically energizes the MBRK output (1734-IB8S input 4 transitions to high (1)).
 - The MBRK output has associated time delays that are used with the Kinetix 5700 drive that affect the enable timing. The Axis.MechanicalBrakeOutputStatus tag is the status of the MBRK output and can be used in a trend to monitor the status of the MBRK output. The MBRK output is wired into a safety input and is used in our safety program. Below is an example timing diagram of a controller-based STO function that uses the MBRK output and illustrates the timing for the Axis.MechanicalBrakeOutputStatus tag and the use of the Axis.PowerStructureEnabledStatus with the MBRK output. The Axis.PowerStructureEnabledStatus tag represents the overall enable status of the drive.

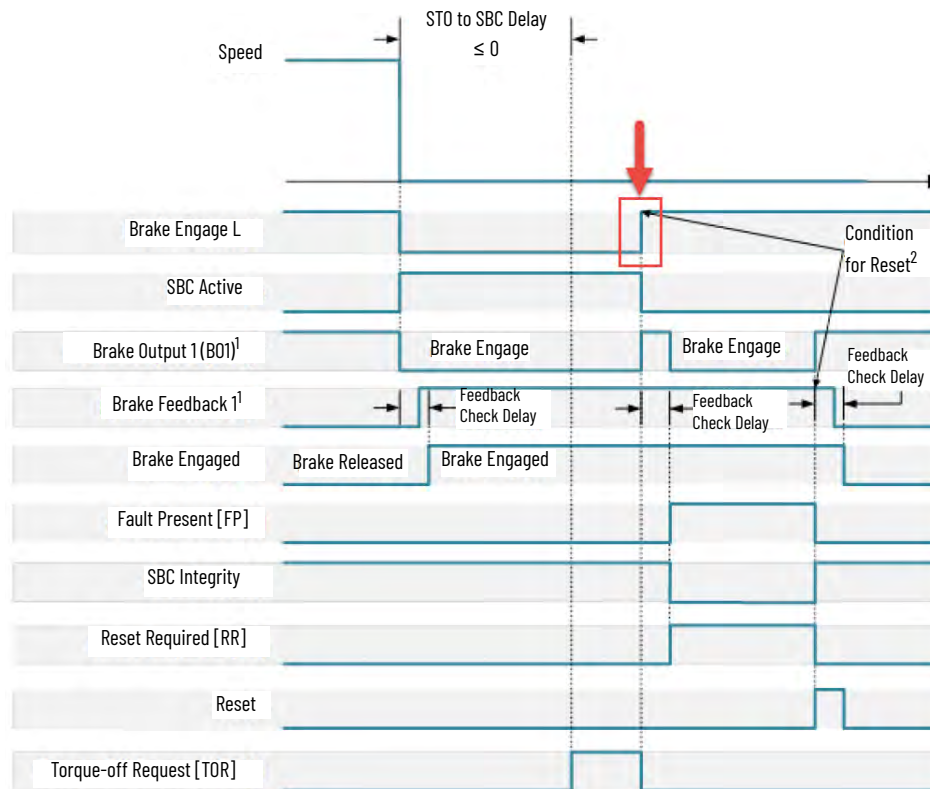
More information on the holding brake operation with the STO function can be found in Vertical Load and Holding Brake Management Application Techniques, publication [MOTION-AT003](#).

STO Request and MBRK Operation



- After MechanicalBrakeReleaseDelay expires, the Kinetix 5700 Axis State continues in the Running state.
 - Upon restart, this time can aid in enabling the motor and holding the load before the safety brake is released, for example, if a separate dedicated Release input was not used. In this example, we use the yellow console button as one permissive to release the safe brake.
 - No motion is allowed until this time expires.
 - This time includes the safety reaction time.
- When the MBRK output is energized, the yellow console button is pressed, and the SBC instruction in the safety program sets the Brake Engage L to high (1).
- The white console button is pressed to reset the SBC instruction (SBC.RR transitions to low (0)).

SBC Operation



1. Brake Output 2 (B02) and Brake Feedback 2 are not shown but function in the same manner.

2. Brake Feedback 1 and 2 must reflect the state of Brake Output 1 and 2, as set by Brake Feedback Type, in addition to Torque off Request (TOR) being OFF (0) as a condition for instruction reset.

- SBC instruction sets B01 and B02 to high (1).
- Safety relay 700CF is energized using the safety program to set output 5 of the 1734-0B8S module to high (1).
- Torque off Request (TOR) is low (0).
- Safe Brake is physically released (not holding the load).
- Safe brake feedback monitor output wired to the 1734-1B8S input 3 is low (0).
- Motor is holding the load under its own power.

Emergency Stop

This is the procedure for typical E-stop operation.

1. The E-stop can be triggered by:
 - Pressing the E-stop maintained signal. Our example uses a Bulletin 800T hardwired input. This signal is maintained throughout the E-stop operation, even if the input changes state after initial pressing.
 - Module connection fault with the safety input module.
2. When the E-stop input is detected, a DCS instruction in the safety program causes the EMERGENCYstop bit to transition to low (0).
3. An MSF Instruction is executed in the standard program to stop motor movement and disable the axis, which de-energizes the MBRK output.
4. In parallel with step 3, the Brake Engage L bit is de-activated within the SBC instruction and the request to engage the safety brake is initiated.
 - a. The SBC instruction transitions B01 and B02 outputs to low (0).
 - b. The low (0) state of the B01 and B02 signals transitions output 5 of the 1734-0B8S module to low (0). Output 5 is wired to the 700CF safety relay.
 - c. When the safety relay output transitions to low (0), 24V DC power to the safety brake coil is removed.

d. The safety brake is engaged and safety brake feedback input is used to indicate the status of the safety brake.



It is possible that the SBC actions in step 4 occur faster than the MSF actions in step 3 because these actions are parallel operations. For example, when Step 3 and 4 are initiated, if the motor is moving at high speed and the MSF instruction is executed to stop the motor, the safety brake could be applied faster than the motor could be decelerated to zero speed and therefore count against the maximum number of stopping cycles. Because this is an Emergency Stop and the motor must stop as fast as possible, the MSF action is performed to increase the chances of stopping the moving load before the safety brake is applied.



It is possible that if the safety brake engages the load while it was moving, an axis or drive fault may occur if the MSF action could not disable the motor quickly enough. If this is the case, upon restart an axis or drive fault reset would have to be executed.



ATTENTION: Consider that if the optional holding brake is not used and the MSF action occurs faster than the safety brake is engaged, the load could potentially drop, if the MechanicalBrakeEngageDelay is not set large enough to keep the drive enabled while the safety brake engages.

5. When the STO to SBC delay (negative value) expires, the SBC.TOR (Torque Off Request) transitions to high (1).
6. The SBC.TOR initiates an STO request (controller-based STO) which disables the motor after the STO Delay expires. In the E-stop example, the MSF instruction disables the motor and the STO action is an additional means of removing the torque-producing ability of the motor (safe condition).

HOLD (normal STOP)

These conditions must be met before a HOLD (normal STOP) is requested:

- The STO function is disabled, the Module:SO.STOOutput is high (1), and the drive is capable of producing torque on the motor (manipulated in safety program logic).
- The motor is enabled (this is manipulated by an MSO instruction in the standard program). The motor does not have to be in motion, but it has to be enabled. It is typical, however, for the motor to be moving.
- The MBRK output is energized. The Axis.MechanicalBrakeOutputStatus tag transitions to high (1). This implies that if a motor holding brake was used, it is released.

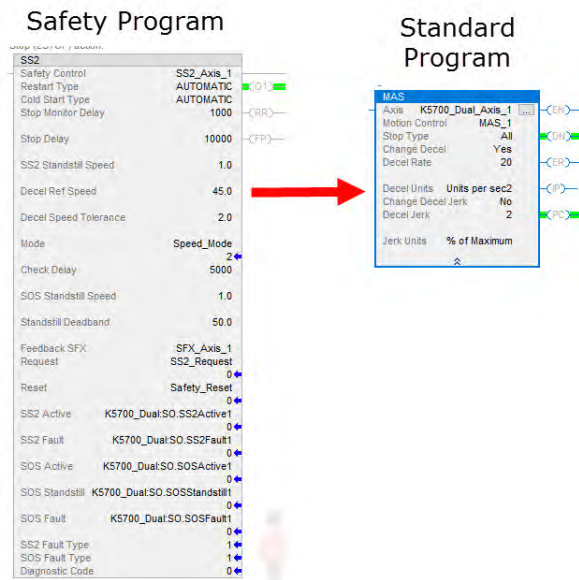
This is the process for a typical HOLD operation:

1. The HOLD (normal STOP) can be triggered by using a maintained signal. Our example uses a maintained red HMI input. This signal must be maintained throughout the HOLD operation.
2. The Guardlogix safety program initiates a Safe Stop 2 (SS2). The SS2 instruction is used to monitor the deceleration of the motor. We use the SS2 because when it is complete, it continues to monitor the motor while it is stationary and produces torque (enabled). Additionally, the SS2 instruction does not initiate an STO request. We do not want any potential to initiate an STO request when it is undesirable.



The SS1 instruction initiates an STO request when it reaches standstill speed, and automatically in some cases. When using the SS2, the motor remains stationary and produces torque (enabled) while the SBC instruction executes. The SBC initiates the STO request after it has engaged the safety brake.

- The standard program receives the SS2 pass-through signal, Axis.SS2ActiveStatus, and stops any motion using a Motion Axis Stop (MAS) instruction.

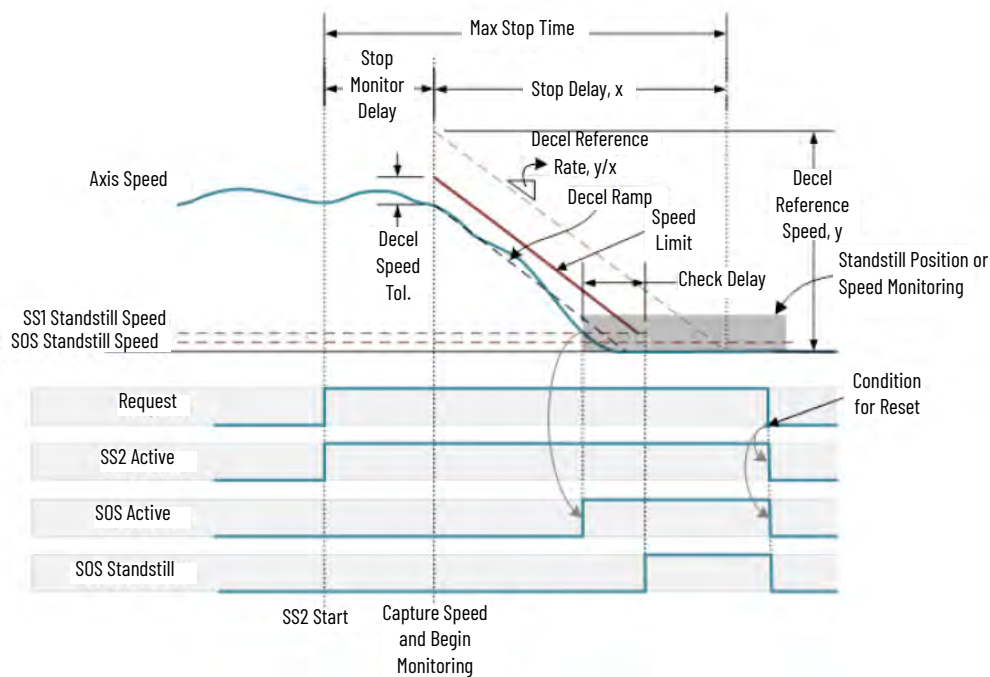


- The Stop Monitor Delay setting in the SS2 instruction is the time that elapses before deceleration monitoring begins.
 - The Check Delay setting in the SS2 instruction is the time that elapses after the standstill speed is reached, but before the SOS standstill monitoring begins. This delay can be used to verify that the motor is stationary and has settled to standstill speed.
- When the motor reaches Standstill Speed, it is possible for the motor to continue to decelerate until it reaches zero speed as a function of the MAS instruction.



The Standstill Speed output parameter in the SS2 Instruction is programmable; it can be set to trigger before a true zero speed (set in the Axis Properties) is achieved if your application requires such a condition. It is typical to set the Standstill Speed to be the same as the Zero Speed value defined in the Axis Properties of the drive.

SS2 Operation



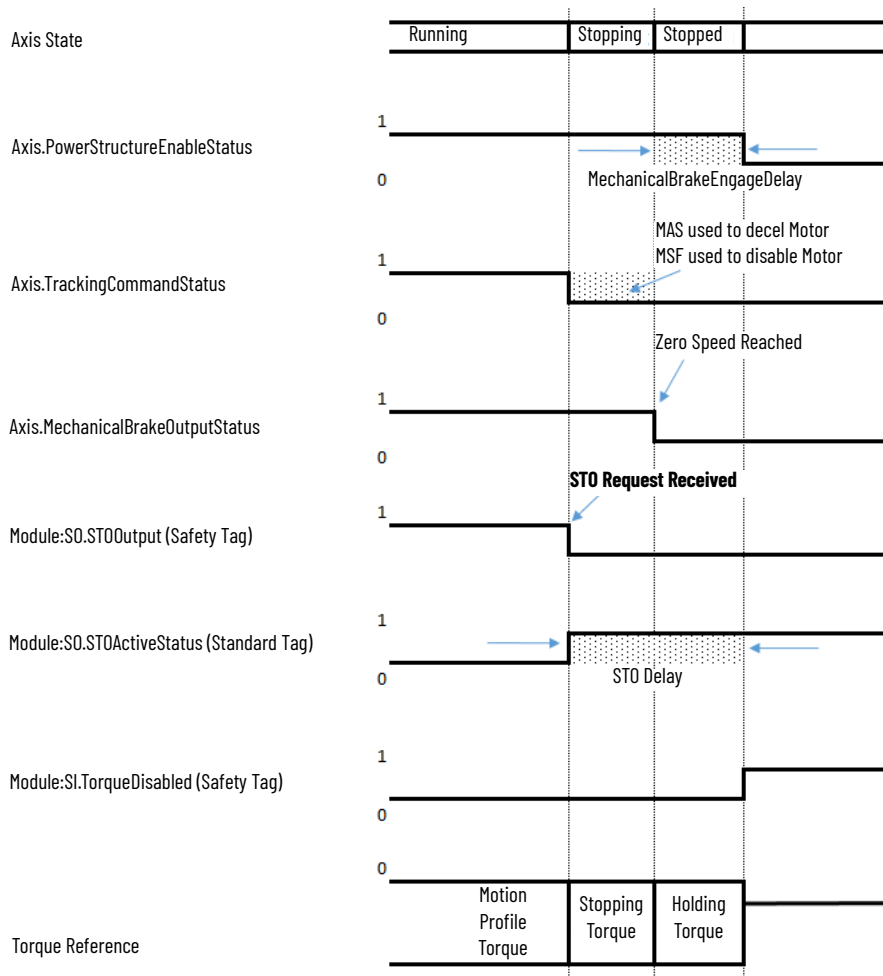
- At the Standstill Speed, the Check Delay timing begins.
- When Check Delay expires, the SOS Standstill monitoring begins.

7. Once the SOS monitoring is active, the Release_MAYR_Safety_Brake signal is low (0), the Brake Engage L is de-activated within the SBC instruction and the request to release the safety brake is initiated. In addition, the following changes occur:
 - a. The SBC instruction transitions B01 and B02 outputs to low (0).
 - b. The low (0) state of the B01 and B02 signals transitions output 5 of the 1734-OB8S module to low (0). Output 5 is wired to the 700CF safety relay.
 - c. When the safety relay output is low (0), 24V DC power to the safety brake coil is removed.
 - d. The safety brake is engaged and Safety Brake Feedback (1734-IB8S input 3) is used for feedback to indicate that the safety brake is engaged.
 - e. When the STO to SBC delay (negative value) expires, the SBC.TOR (Torque Off Request) is high (1).
 - f. The SBC TOR initiates an STO request (controller-based STO), which disables the motor after the STO Delay expires. This helps prevent the motor from remaining enabled while the safety brake is engaged.



The following timing chart shows the timing of an STO request to engage the MBRK output. In the HOLD case, after the SS2 is complete, and SOS Standstill is active, program logic directs the STO function (STO Request Received) to remove torque and the STO function (STO Request Received) removes torque from the motor without requiring any additional logic to disable it (MSF instruction). While you can use an MSF to programmatically disable the motor, the motor disable happens as a result of the STO function after the STO Delay expires. If no delay is required for the STO Signal, set this delay to zero.

STO Initiated Operation



Disable

A disable request comes from one of the following:

- a motion MSF instruction is executed.
- an exception (fault) is initiated.

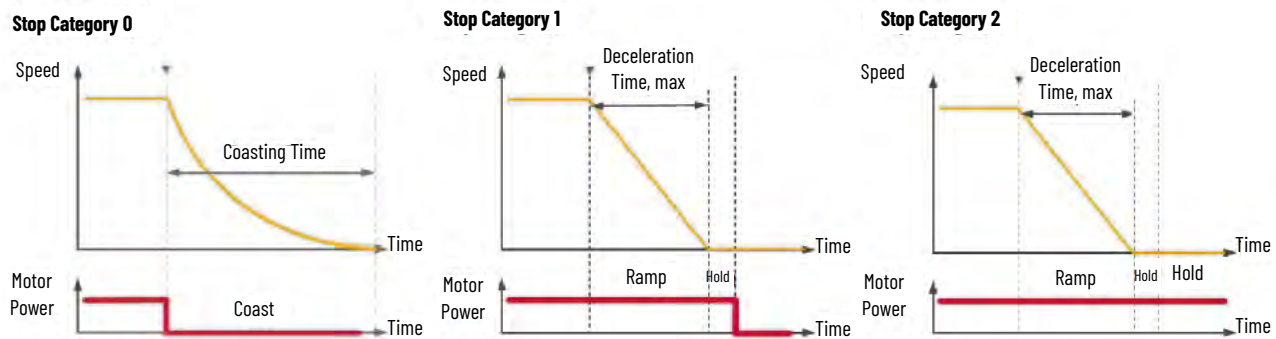
In the Disable request example, the drive uses a specific Stop Type and Action to decelerate and disable the motor. The Disable request uses the MBRK output. One of these Stop Types is used:

Stopping Categories for Vertical Applications

Stop Category Type ⁽¹⁾	Stopping Action Type (Kinetix drive configuration)	Description of Operation
Stop Category 0	Disable & Coast	The drive immediately disables the inverter power structure.
Stop Category 1	Current Decel & Disable	The motor is decelerated (trigger condition determines the rate of deceleration) to zero speed and the power structure is disabled.
Stop Category 2	Current Decel & Hold	The motor is decelerated (trigger condition determines the rate of deceleration) to zero speed and the power structure remains enabled.

⁽¹⁾ The stopping actions that are applicable to a vertical axis align with IEC-60204-1 stop categories.

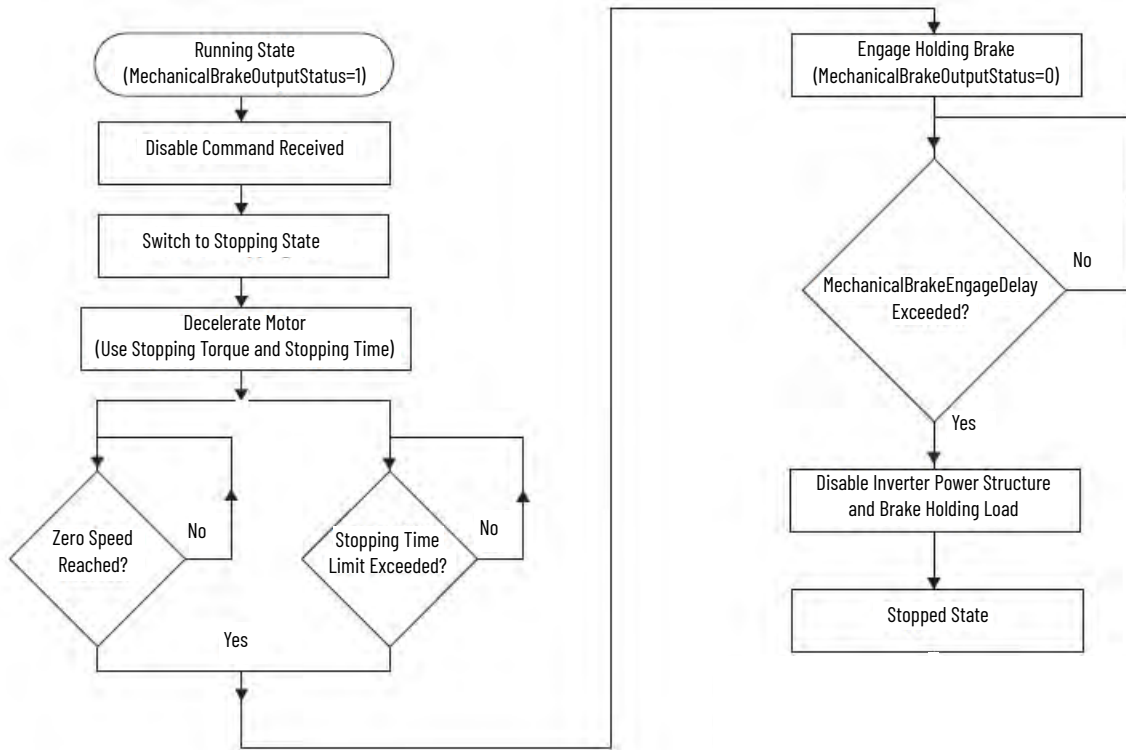
Stop Action Definitions



With any vertical application, avoid Disable & Coast and Current Decel & Hold conditions whenever possible, because with the Disable & Coast, no MBRK output timing is used and with Current Decel & Hold, the MBRK output is not used. Current Decel & Disable is the correct Stop Type to use in these examples (Hold, E-stop, and Disable).

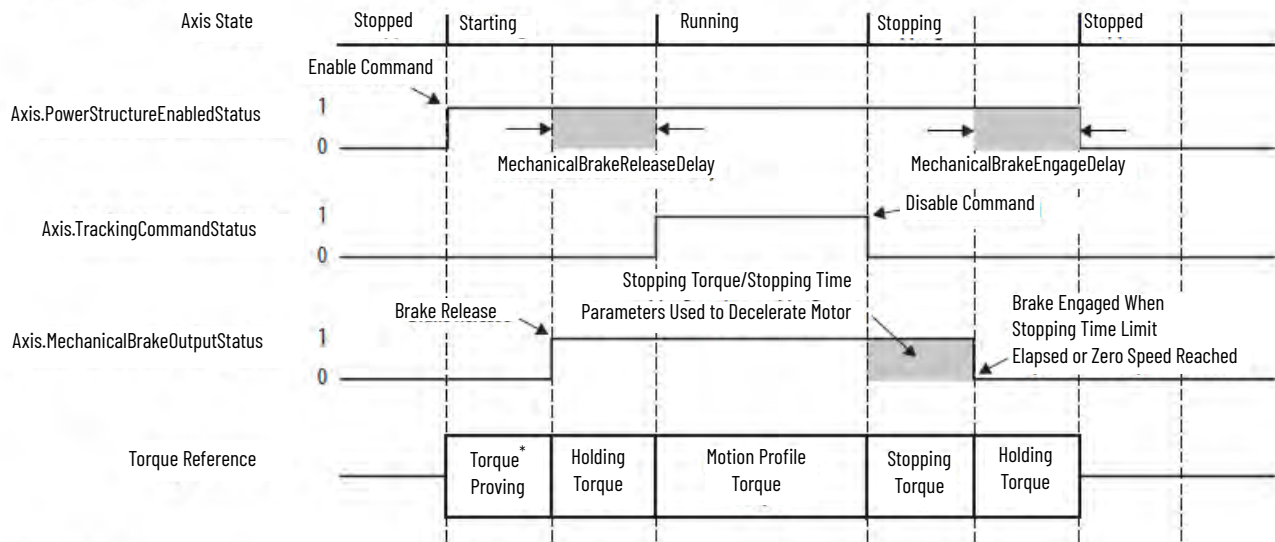
When any disable request occurs, the MBRK output is automatically controlled.

The MSF instruction, or exception (fault) when using the Current Decel & Disable action, all follow the timing that is shown below. Each Kinetix exception (fault) and its actions (when configured as the default Disable Drive¹) are found in the Kinetix 5700 Servo Drives User Manual, publication [2198-UM002](#).



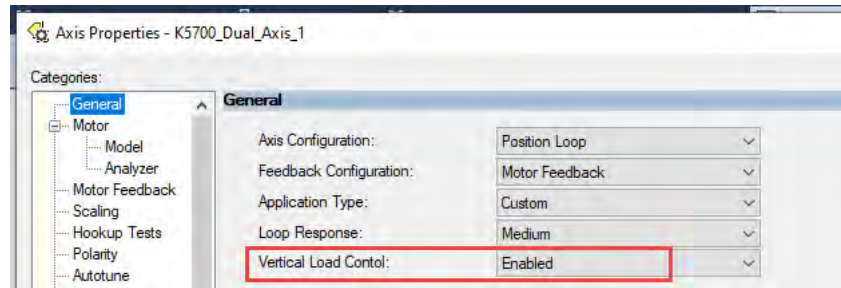
¹ Before revision 32 of Studio 5000 environment, this default was called Stop Drive.

Timing Diagram: Stop Category 1



If the Action for a fault is Disable & Coast, the MBRK output immediately transitions to low (0) when the fault occurs. The brake delay times are not used with this stop type, so the drive is immediately disabled. Once the MBRK output has transitioned to low (0), the SafeBrakeDelay (typically zero) times out, and the safety brake is engaged through the SBC instruction. The STO is initiated as a result of the SBC instruction. Because the mechanical holding brake is optional, this fault action is modeled as the worst case action and the safety brake is engaged immediately. Because we want to minimize the use of Disable & Coast faults, we use the Vertical Load Control feature.

Enabling the Vertical Load Control feature (or manually changing its associated parameters) in the Axis Properties removes uncertainty when configuring your axis for vertical load applications.



The Vertical Load Control feature changes the relevant fault actions and motor parameters so that a motor can be stopped under control while minimizing the need to engage the safety brake on a moving motor. This also contributes to minimizing the stopping cycles where the safety brake is used on a moving load.

This is the procedure that is used for the Disable example:

1. Disable command received.
2. Stopping Torque and Stopping Time are used to decelerate the motor. The Stopping Torque is applied until the motor reaches zero speed or until the configured Stopping Time expires.
3. Once the motor is decelerated, if Zero Speed is reached or the Stopping Time expires, the MBRK output transitions to low (0). This transitions input 4 of the 1734-1B8S module to low (0). The SafeBrakeDelay (typically zero) times out.
4. While the MechanicalBrakeEngageDelay is timing, an optional holding brake (if used) is applied.
5. In the safety logic program, Release_MAYR_Safety_Brake transitions to low (0), the Brake Engage L is de-activated within the SBC instruction, and the request to de-energize the safety brake is initiated.
 - a. The SBC instruction transitions the B01 and B02 outputs to low (0).
 - b. The low (0) state of the B01 and B02 signals transitions output 5 of the 1734-0B8S module to low (0). Output 5 is wired to the 700CF safety relay.
 - c. When the safety relay output transitions to low (0), 24V DC power to the safety brake coil is removed.
 - d. The safety brake is engaged and safety brake feedback (1734-1B8S input 3) is provided to indicate that the safety brake is engaged.
 - e. The MechanicalBrakeEngageDelay has expired and the drive is disabled.
 - f. When the STO to SBC delay (negative value) expires, the SBC.TOR (Torque Off Request) transitions to high (1).
 - g. The SBC.TOR initiates an STO request (controller-based STO) which prevents the drive from producing torque in the motor.

HOLD and Disable Notes

1. We have added an MBRK output comparison in the safety program to check the integrity of the MBRK output. It evaluates unlikely conditions like a short to 24V DC, wire falling off, and so on. This is done because the MBRK output does not have a feedback circuit to detect these conditions. We compare the MBRK output (1734-1B8S input 4) with the MechanicalBrakeOutputStatus tag, which is mapped into the safety program. If there is a discrepancy, we engage the E-stop condition. This time must be set to match your application. In our example, we used 1000 ms.
 - a. If a Current Decel & Disable action occurs (for example, an MSF is issued) and the MBRK safety input (1734-1B8S input 4) shorts to 24V DC, the miscompare time must be smaller than the MechanicalBrakeEngageDelay.
 - b. If a Disable & Coast action (for example, a major fault) occurs and the MBRK safety input (1734-1B8S input 4) shorts to 24V DC, a holding brake, or a second safety brake would help in preventing the load from dropping during the miscompare time period.

Integrated Safety: Safe Torque Off Considerations for a Stop Category 1

In the event of a malfunction, it is possible that the drive will use a stop category 0. When designing the machine application, timing and distance must be considered for a coast-to-stop action, and the possibility of the loss of control of a vertical load. These malfunctions include a transition (programmatic or keyswitch) from Run to Program mode, or any loss of communications that removes the STO networked tags. Use additional protective measures if this occurrence might introduce unacceptable risks to personnel.

When using the Guardlogix controller and the Kinetix 5700 (2198-xxxx-ERS4) drive, if a malfunction occurs, the motor can be controlled by deceleration, a disable action, and initiation of the STO function to remove the ability of the drive to produce torque in the motor.

These malfunctions include:

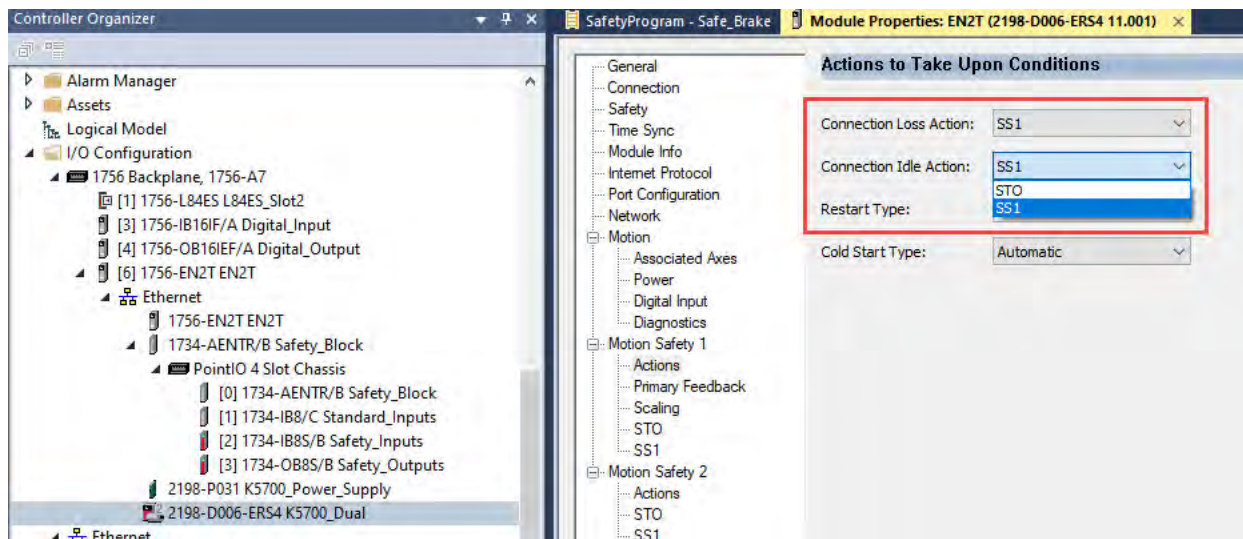
- any loss of communications that clears the STO program tags.
- transition (programmatic or keyswitch) from Run to Program mode.

Loss of Communication

In our example application, once the CTRL expires, the safety outputs transition to low (0) and the safety brake is engaged. The following information explains the operation so you understand how the drive behaves when a communication loss occurs.

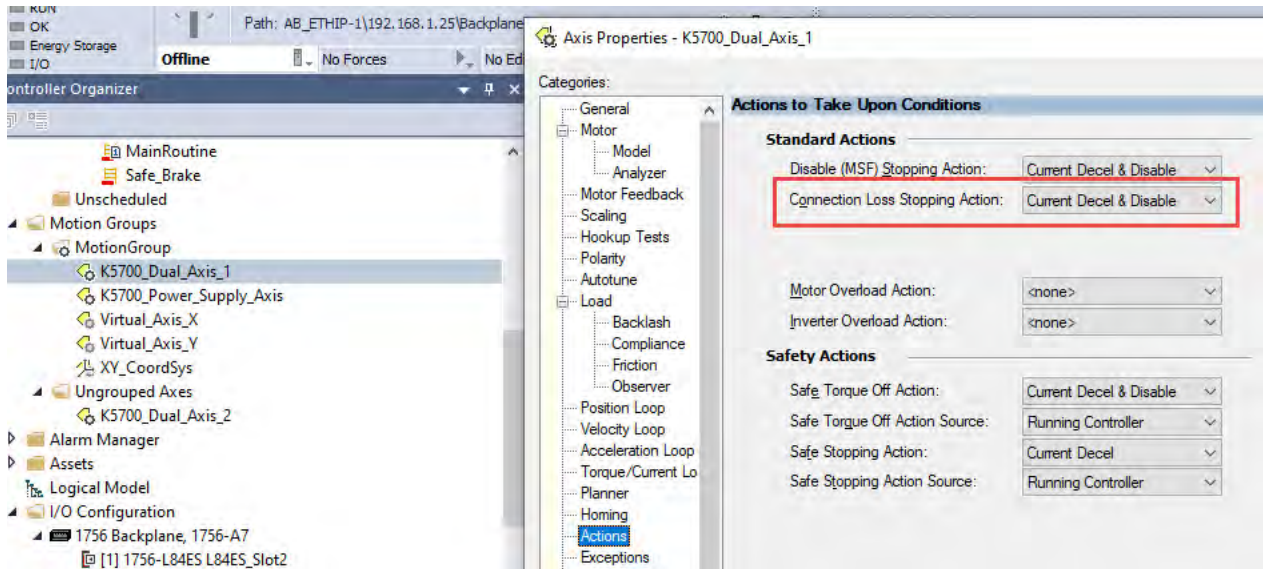
Without communication, the status of the STO output tag cannot be transmitted to the drive. If a communication loss occurs, the drive decelerates and disables the drive using the Connected Drive configuration, even if the STO action is configured as Running Controller.

The Guardlogix network safety implementation requires two connections: a safety connection and a motion connection. These connections can reside in two separate controllers. In this example, they reside in the same controller. Upon the Connection Loss (or Idle) of the safety connection, the drive can be programmed to use the pre-defined STO or SS1 actions that are found in the drive configuration. These settings are shown in the following image.



For the Connection Loss/Idle Actions, the SS1 action results in an STO operation. The SS1 brings the motor to standstill or zero speed, and then disables the motor and initiates a Connected Drive STO function. The MBRK output transitions to low (0) when the STO request becomes active. At this point, if a physical holding brake was used, it engages. If a physical holding brake is not used, a value must be entered into the STO Delay to make sure that the motor remains enabled for a period of time, so the safety brake has time to engage the load.

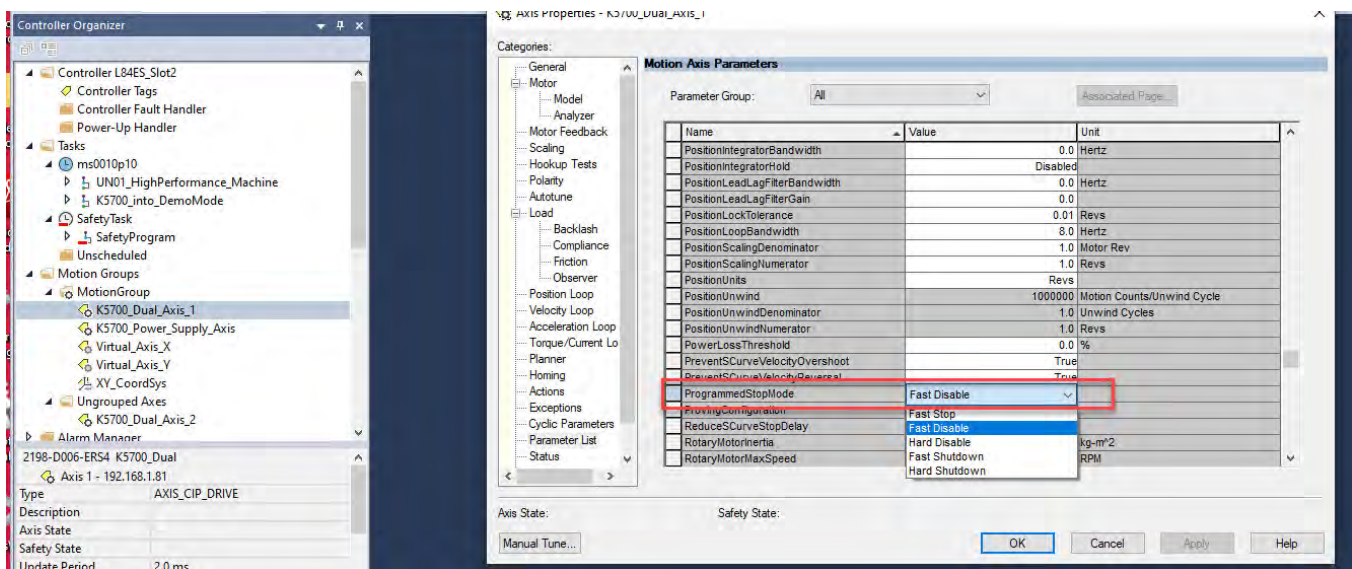
In the event of the motion connection loss, the Stopping Action can also be programmed. In this case, with Current Decel & Disable as the action, the typical Disable example is used.



Programmatic Change

In our example, safety output 5 (used to control the safety brake) transitions to low (0) when the program change occurs. This engages the safety brake immediately. The following information explains the operation so you understand how the controller and drive behave when a program change occurs outside of the safe brake control.

In the event of a transition (programmatic or via the keyswitch) from Run to Program mode, the axis behavior can also be programmed in the Axis Properties dialog box by using the stop actions that are shown in the following image.



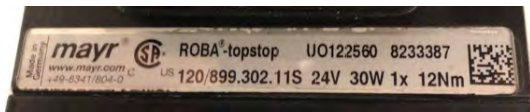
The ProgrammedStopMode descriptions are described in the table.

ProgrammedStopMode	Description
Fast Stop	When the ProgrammedStopMode attribute is configured for Fast Stop, the axis is decelerated to a stop by using the current configured value for Maximum Deceleration (from the Planner category of Axis Properties). The axis remains enabled after the axis motion has stopped.
Fast Disable	When the ProgrammedStopMode attribute is configured for Fast Disable, the axis is decelerated to a stop by using the value for Maximum Deceleration (in the Planner Category of Axis Properties). Once the motor has decelerated to a stop, the axis is disabled, and the holding brake output is set. The MechanicalBrakeEngageDelay is observed in this mode.
Hard Disable	When configured for Hard Disable, the axis uses Stopping Torque to decelerate the motor to a stop. Once the motor has decelerated to a stop, the axis is disabled, and the holding brake output is set. The MechanicalBrakeEngageDelay is observed in this mode.
Fast Shutdown	When configured for Fast Shutdown, the axis is decelerated similar to Fast Stop, but once the axis motion is stopped, the axis is placed in the Shutdown state, the axis is disabled, and the holding brake output is set. Recovering from the Shutdown state requires execution of one of the axis or group Shutdown Reset instructions (MASR or MGSR). The MechanicalBrakeEngageDelay is not observed in this mode.
Hard Shutdown	When configured for Hard Shutdown, the axis is immediately placed in the Shutdown state, the axis is disabled, and the holding brake output is set. If the axis was moving, unless the drive is configured to provide some form of dynamic braking, the result is a Disable & Coast stop action (not recommended for vertical axes). The MechanicalBrakeEngageDelay is not observed in this mode. Recovering from the Shutdown state requires execution of one of the axis or group Shutdown Reset instructions (MASR or MGSR).

Choose the mode to fit your application. We used Fast Disable in our example. This type disables the motor, and as part of the Program mode change, the outputs transition to low (0) and the safety brake is applied. Consider that the safety module outputs (1734-0B8S) will likely de-energize faster than the ProgrammedStopMode Action and engage the safety brake faster than the motor has a chance to decelerate and disable. It is relevant to understand possible actions that take place while the controller is undergoing a mode change, even if that action (ProgrammedStopMode) does not complete because the outputs are transitioned to low (0).

Bill of Material

This application technique uses these products.

Cat. No.	Description	Quantity
800T-FXM6A7	30.5 mm (1.20 in.) Type 4/13 3 Pos. push button, non-illuminated, mushroom Hd (push-pull), red, OUT/CNTR/IN-Mom/Maint/Maint, 1 NCLB-1 NC (E-stop function)	1
800FC-5Z	800FC pendant station enclosure, 5-hole	1
800FP-E3PX10	800F push button, plastic, extended, green, no legend, standard pack, screw contact block, 1 normally open	1
800FP-E5PX10	800F push button, plastic, extended, yellow, no legend, standard pack, screw contact block, 1 normally open	1
800FP-E1PX10	800F push button, plastic, extended, white, no legend, standard pack, screw contact block, 1 normally open	1
800FP-SM22PX10	800F two-position selector switch, plastic, maintained, black, standard knob, standard orientation, 1 normally open contact block, standard pack	1
800FP-SR22PX10	800F two-position selector switch, plastic, spring return from right, black, standard knob, standard orientation, 1 normally open contact block, standard pack	1
VPL-B1654D-QK14AA	VPL Motor (SIL 2 capable)	1
K513AGxxxxMB30	STOBER ServoFit gearbox with integrated ServoStop safe brake based on mayr ROBA-topstop listed below: mayr ROBA-topstop 	1
700S-CF620QJBC	Safety control relay, 8-pole, 3 normally open/1 normally closed base, 1 normally open/3 normally closed auxiliary, bifurcated contact, 24V DC (with electric coil)	1
2198-P031	Kinetix 5700 DC bus supply	1
2198-D006-ERS4	Kinetix 5700 dual axis inverter	1
1734-AENTR	24V DC Ethernet/IP adapter, 2-port	1

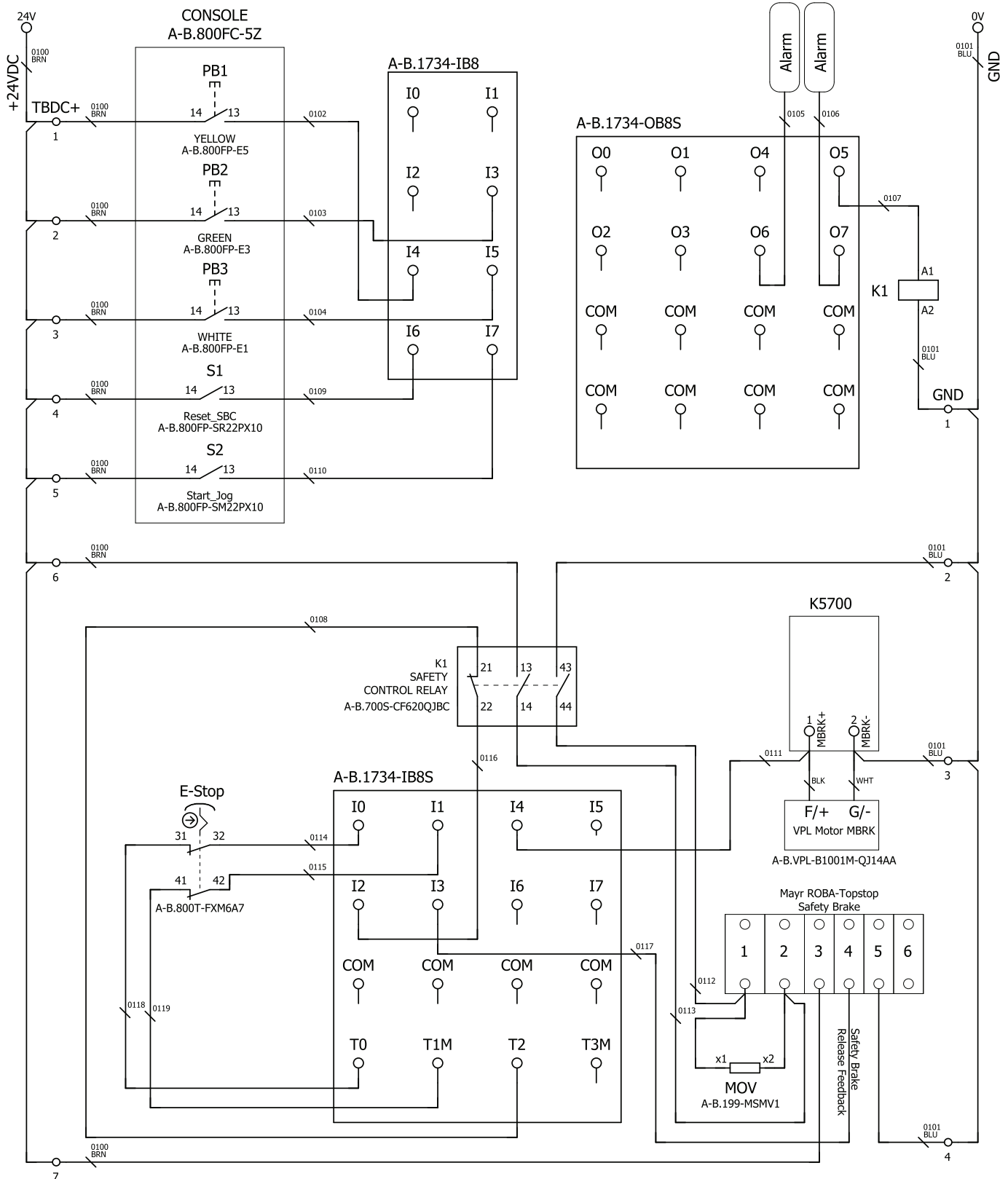
Cat. No.	Description	Quantity
1734-TB	Module base with removable IEC screw terminals	5
1734-IB8S	POINT Guard I/O™ safety 8 point 24V DC sinking input module	1
1734-IB8	POINT I/O™ 8 point 24V DC sinking input module	1
1734-OB8S	POINT Guard I/O safety 8 point 24V DC sourcing output module	1

Choose either the GuardLogix 5580 hardware list or the Compact GuardLogix 5380 hardware list.

Controller	Cat. No.	Description	Quantity
GuardLogix 5580	1756-L81ES 1756-L82ES 1756-L83ES 1756-L84ES	Safety Controller, 3 MBRK standard memory, 1.5 MBRK safety memory Safety Controller, 5 MBRK standard memory, 2.5 MBRK safety memory Safety Controller, 10 MBRK standard memory, 5 MBRK safety memory Safety Controller, 20 MBRK standard memory, 6 MBRK safety memory	1
	1756-PA72	Power supply, 120/240V AC input, 3.5 A @ 24V DC	1
	1756-A4	Four-slot ControlLogix® chassis	1
Compact GuardLogix 5380	5069-L306ERMS2 5069-L310ERMS2 5069-L320ERMS2 5069-L330ERMS2 5069-L340ERMS2 5069-L350ERMS2 5069-L380ERMS2 5069-L3100ERMS2	Safety Controller, 0.6 MBRK standard memory, 0.3 MBRK safety memory, 2 axis Safety Controller, 1.0 MBRK standard memory, 0.5 MBRK safety memory, 4 axis Safety Controller, 2.0 MBRK standard memory, 1.0 MBRK safety memory, 8 axis Safety Controller, 3.0 MBRK standard memory, 1.5 MBRK safety memory, 16 axis Safety Controller, 4.0 MBRK standard memory, 2.0 MBRK safety memory, 20 axis Safety Controller, 5.0 MBRK standard memory, 2.5 MBRK safety memory, 24 axis Safety Controller, 8.0 MBRK standard memory, 4.0 MBRK safety memory, 28 axis Safety Controller, 10.0 MBRK standard memory, 5.0 MBRK safety memory, 32 axis	1
	1769-PA4	CompactLogix™ power supply, 120/240V AC	1
	5069-ECR	Right end cap and terminator	1

Setup and Wiring

For detailed information on how to install and wire the products in this application technique, refer to the publications that are listed in the [Additional Resources](#).



System Overview

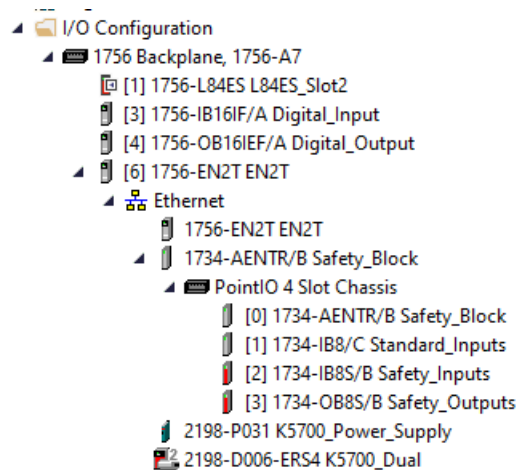
The examples in this publication use the SBC instruction. An STO is initiated as a result of the SBC instruction completing. The sequence for SBC engagement is different for each example. The HOLD example uses the SS2 instruction and then the SBC instruction. The E-stop example uses the SBC instruction only. The Disable example uses the MBRK output and then the SBC instruction.

In our examples, the following conditions apply:

- HOLD (normal STOP) using the Safe Stop 2 (SS2) is triggered with an HMI-maintained button (HMI_RedButton_safety).
- Disable is initiated by an MSF instruction, or by exception (fault).
- E-stop (EmergencyStop) is triggered with an 800T push button using two test inputs that are wired to the 1734-IB8S safety input module. Inputs zero (0) and one (1) are used.
- The MBRK output from the Kinetix 5700 drive is wired using one input on the 1734-IB8S safety input module. Input 4 is used.
 - The MBRK output is also wired to the servo motor holding brake (if one is used).
- The safety brake release monitoring output, which is used to provide a feedback status of the safety brake state, is wired to the 1734-IB8S safety input module, Input 3 is used.
 - The SBC instruction uses the safety brake N.O. contact as Feedback Signal 1. The SBC instruction requires the Feedback Signal to be high when the instruction output is not true. This safety brake contact must be inverted. The inversion of this signal is done in the safety program logic.
- 24V DC supply terminals (+/-) are wired into the N.O. terminals of the 700CF safety relay in series, and when the circuit is complete, energize the safety brake coil that is used to release the safety brake.
- 700CF auxiliary contact is wired using one input on the 1734-IB8S safety input module. Input 2 is used.
 - The SBC instruction uses the 700CF N.C. aux contact as Feedback Signal 2. The SBC instruction requires the state to be high when the instruction output is not true. This signal does not need to be inverted.
- The status of the B01 and B02 outputs is used to energize the 700CF relay coil and allow the safe brake coil to be energized. Output 5 is wired from the 1734-OB8S safety output module to energize the 700CF relay coil.
- One of the safety requirements for the safety brake is to generate an alarm if the safety brake does not operate correctly. To meet this requirement, the SBC fault status is used to energize these outputs in the safety logic. There are two alarm outputs that are used: outputs 6 and 7 from the 1734-OB8S safety output module.

Network Architecture

For an electrical schematic in AutoCAD or EPLAN format, see the attached files.



Configuration

The GuardLogix controller is configured by using the Studio 5000 Logix Designer® application, version 31 or later. You must create a project and add the GuardLogix controller, Kinetix 5700 (2198-DXXX-ERS4) drive, and appropriate safety and standard I/O modules. The integrated Ethernet/IP port on the GuardLogix controller is used, so there is no Ethernet bridge required. A detailed description of each step is beyond the scope of this publication. Knowledge of the Logix Designer application is assumed.

The Kinetix 5700 drive uses firmware revision 11 or later.

For a Studio 5000 Logix Designer project file that you can import into your own project, see the attached ACD files (logic_AT178_1.ACD is for Logix Designer version 31). The attached ACD file includes a GuardLogix 5580 controller, but if you choose a Compact GuardLogix 5380 controller, you can change the controller in the Logix Designer application program.

Minimum Logix Designer Application Version	Product
31	GuardLogix 5580 controller
31	Compact GuardLogix 5380 controller

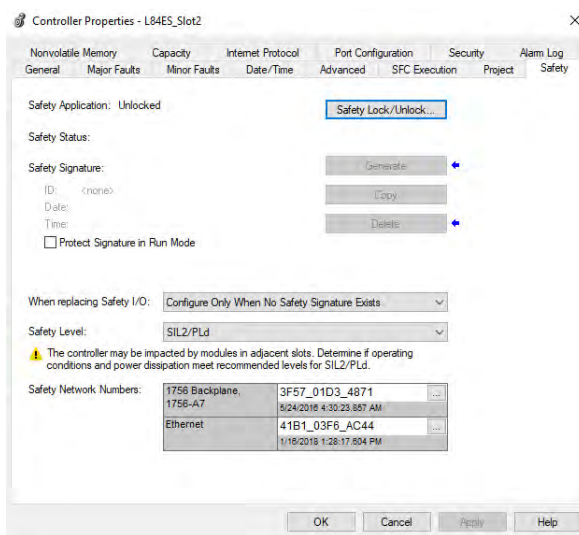
Only the GuardLogix 5580 and Kinetix 5700 configuration options that are related to our examples are shown.

Create a Project with a GuardLogix Controller and a Kinetix 5700 Drive

If you are not using the attached ACD file, follow these steps to create a project.

GuardLogix Controller Properties

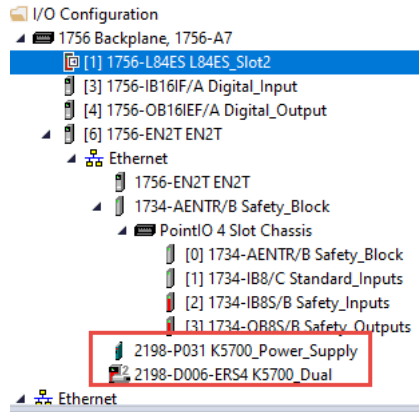
1. Create a GuardLogix project at revision 31 or later for SBC and SS2 instruction support.
2. On the controller Safety tab, select SIL2/PLd Safety Level.



This example has a PL requirement of PLd. The Primary only (no 1756-L8SP partner) GuardLogix 5580 controller is capable of PLd.

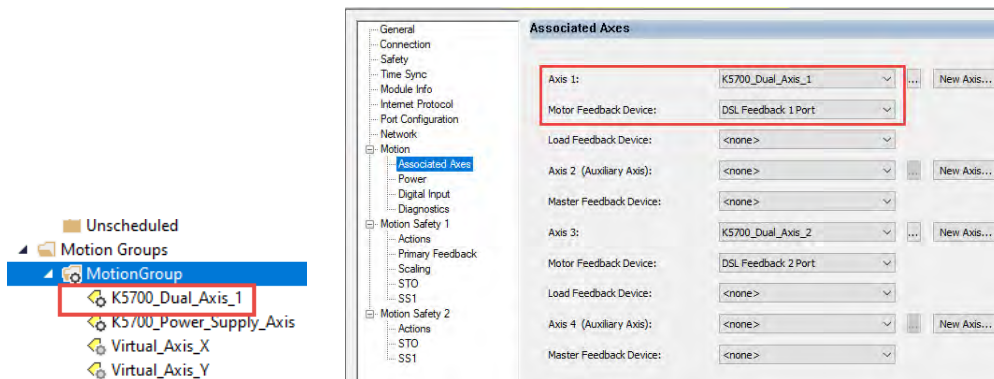
Advanced Safety Drive Configuration

1. Add the Kinetix drive hardware to the I/O configuration.



Include the Kinetix 5700 power supply (2198-P031) and the Kinetix 5700 drive axis module (2198-D006-ERS4).

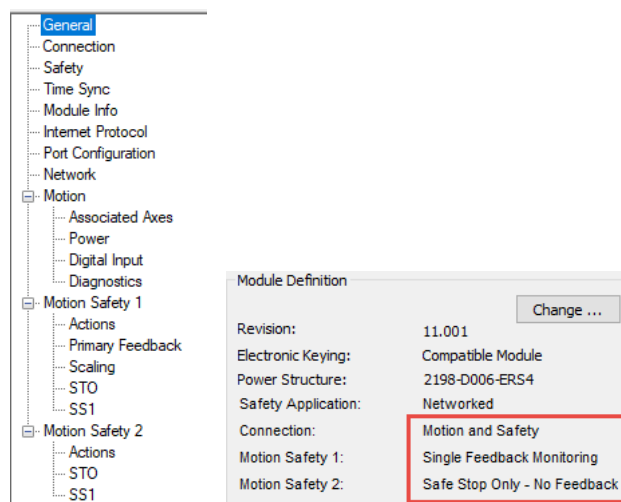
2. For integrated motion applications, create your motion group and axis.



Associate the axis to the drive hardware.

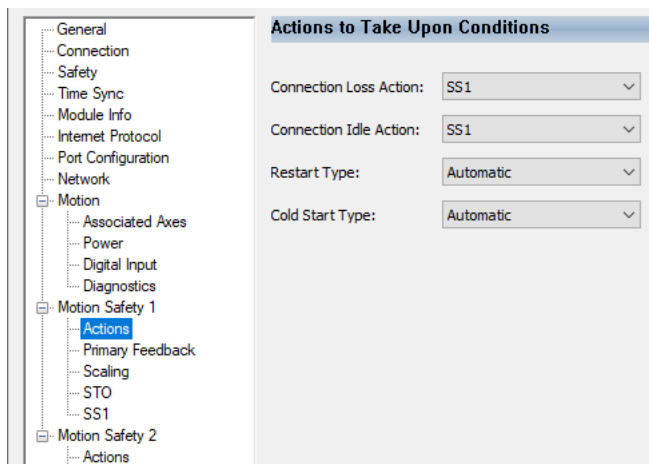
3. Configure the general safety properties of the drive as shown in the following table.

	Kinetix 5700 Drive
Safety Application	Networked
Connection	Motion and Safety
Motion Safety/Safety Instance	Single Feedback Monitoring



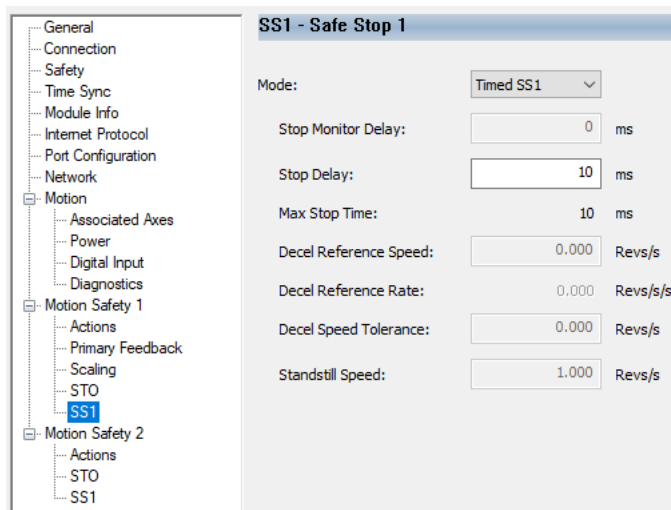
Secondary feedback is not required to achieve PLd for the safety function being used in this example. This configuration is found in the drive properties.

4. Configure the drive safety actions as shown in the graphic.



This configuration is found in the drive properties.

5. Configure SS1 settings per the safety assessment.



In this example, we configured the mode as Timed SS1 with a Stop Delay of 10 ms.

6. Configure the safety Primary Feedback based on the drive hardware and feedback resolution selected.

Primary Feedback

Device: Velocity Average Time: ms

Catalog Number: Standstill Speed: Rev/s

Type:

Units:

Resolution Units: Cycles/Rev

Cycle Resolution: Cycles/Rev

Cycle Interpolation: Counts/Cycle

Effective Resolution: Counts/Rev

Polarity:

SIL Capability:

The encoder within the VPL motor over the Digital Servo Link (configured in the Axis Properties) has an Effective Resolution equal to the Cycle Resolution. The effective resolution varies depending on the feedback device used.

7. Configure the Primary Feedback Scaling.

Scaling

Feedback Resolution: Counts/Rev

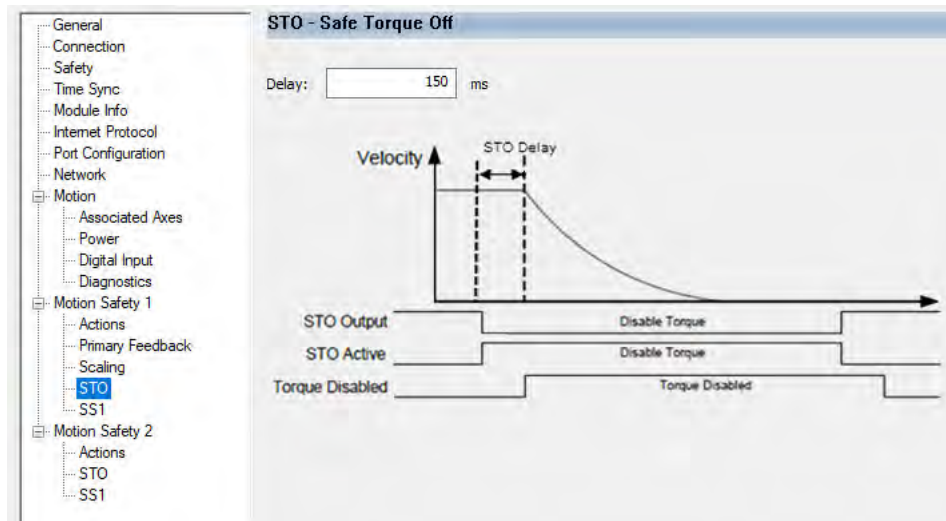
Position Units:

Time Units:

Position Scaling: Counts/1.0 Revs

Drive-based actions use the scaling in this window. This scaling is not used in these examples because the SFX instruction converts counts within the instruction itself.

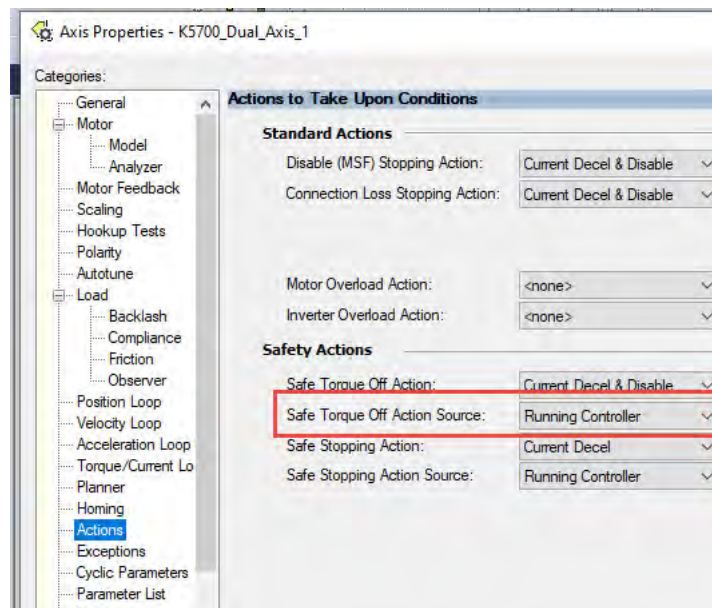
8. Configure the STO Delay time.



While the drive is enabled and the STO is requested, the STO Delay is used. The MBRK timing is used in this case. In our examples, the STO Delay must be nonzero with the value being set to allow enough time for the safety brake to engage. While this delay is active, the motor still produces torque. Our example shows 150 ms for the STO Delay. Set this value based on your application requirements. If the drive is disabled (by MSF action or by exception), and then an STO is initiated, the STO Delay is not used. This is important to understand, and it is why we cannot simply use the STO Delay to decelerate and disable the motor.

Axis 1 Configuration

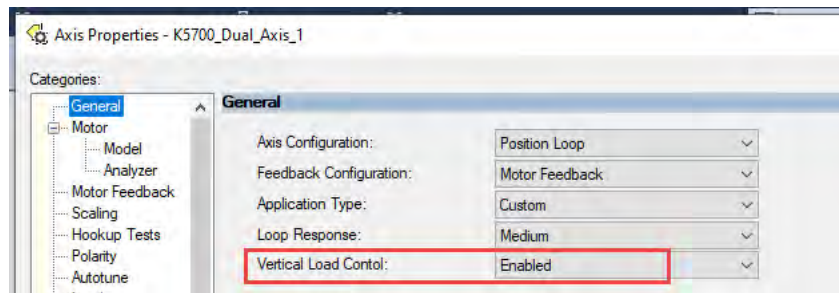
1. Configure the STO action source as Running Controller.



For Integrated Motion applications, this is done in the Actions category of the Axis Properties dialog box. In our examples, the STO is controlled from the safety program. The Safe Stopping Action Source is also configured as Running Controller.

IMPORTANT With this configuration, all conditions that require the drive to stop or enter an STO state, except for communication faults, must be managed in the controller.

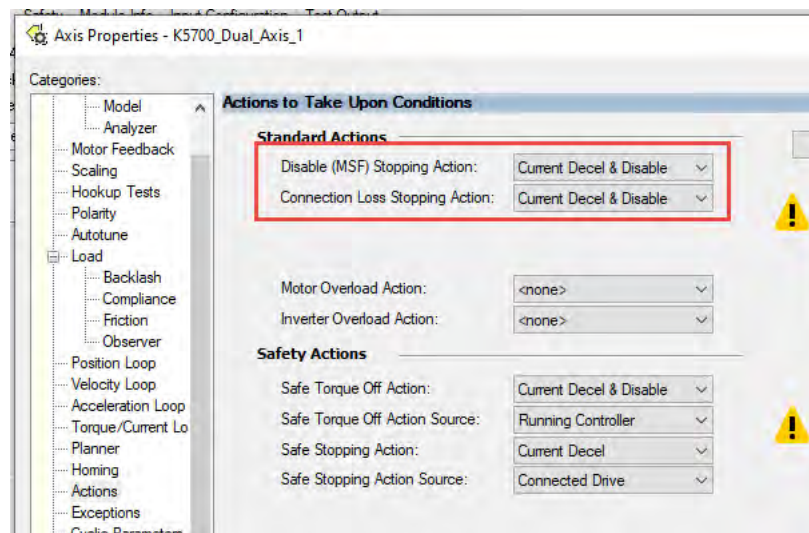
- On the General tab, enable the Vertical Load Control feature.



The Vertical Load Control feature changes the relevant fault actions so that a moving motor under control can be stopped without engaging the safety brake on a moving load (as often as possible). This contributes to minimizing the stopping cycles in which the safety brake is used on a moving load. For a description of the parameters that are automatically adjusted for a vertical load when this feature is enabled, see Vertical Load and Holding Brake Management Application Techniques, publication [MOTION-AT003](#). You can also choose not to use the Vertical Load Control feature and manually change the values to best suit your application.

There are also some Fault Actions default configurations that are changed to Current Decel & Disable. Additionally, the Torque Prove function and brake tests are enabled with this feature. It is possible that these values may need to be modified for your application. For detailed explanations of these parameters and how they are determined, see Vertical Load and Holding Brake Management Application Techniques, publication [MOTION-AT003](#).

- On the Actions tab, set the Disable (MSF) Stopping Action and Connection Loss Stopping Action to Current Decel & Disable.



When this is set, the motor is decelerated and disabled when an MSF action or a Motion Connection fault has occurred. Recall that we want to avoid the Disable & Coast and Current Decel & Hold settings.

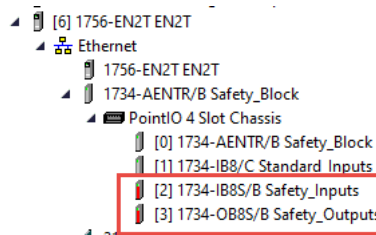
4. On the Parameter List page, verify that the parameters are set as shown in the following table.

Parameter Name	Value
CoastingTimeLimit	Zero (0)
MechanicalBrakeControl	Automatic
MechanicalBrakeEngageDelay	>0 (consider safety reaction times as described in Safety Reaction Time on page 3.)
MechanicalBrakeReleaseDelay	>0 (consider safety reaction times as described in Safety Reaction Time on page 3.)
StoppingTorque	>0 (ideally set for application limited torque required to stop the motor and load)
StoppingTimeLimit	>0 (ideally set for allowable time to decelerate the motor and load)
ZeroSpeed	>0 (set to indicate a zero speed condition on the motor)

IMPORTANT The values in the table are set when the Vertical Load Control feature is Enabled. Make sure that they are set to match your application.

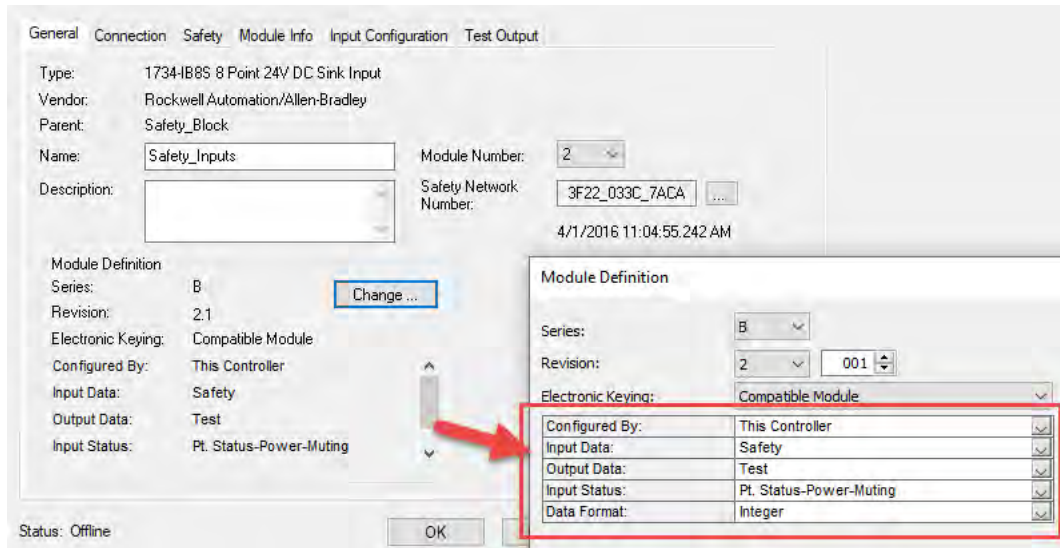
POINT Guard I/O Module Configuration

1. Add POINT Guard I/O modules.



Two modules are required for this application; a safety 1734-IB8S input module and a safety 1734-OB8S output module. In our examples, we use a standard input module (1734-IB8) for the console inputs.

2. In the Module Definition section of the General tab, do the following:
 - a. Configure the 1734-IB8S Input Status for Pt. Status-Power-Muting to generate an individual point status tag for each channel.
 - b. Configure the Output Data for Test.



3. Configure the Input Configuration tab as shown in the graphic.

Point	Point Operation		Point Mode	Test Source	Input Delay Time (ms)	
	Type	Discrepancy Time (ms)			Off->On	On->Off
0	Single	0	Safety Pulse Test	0	0	0
1	Single	0	Safety Pulse Test	1	0	0
2	Single	0	Safety Pulse Test	2	0	0
3	Single	0	Safety	None	0	0
4	Single	0	Safety	None	0	0
5	Single	0	Safety	None	0	0
6	Single	0	Safety	None	0	0
7	Single	0	Safety	None	0	0

Point	Point Mode
0	Pulse Test
1	Pulse Test
2	Pulse Test
3	Pulse Test

Input Error Latch Time: 1000 ms

The 1734-IB8S Input Configuration tab represents the wiring that is used in this example (E-stop inputs points 0 and 1, 700CF status input 2, Safe Brake feedback monitor input 3).

- On the Test Output tab, configure all four test outputs for Pulse Test in this application.
- In the Module Definition section of the General tab, configure the 1734-OB8S Input Status for Pt. Status to generate an individual point status tag for each channel.

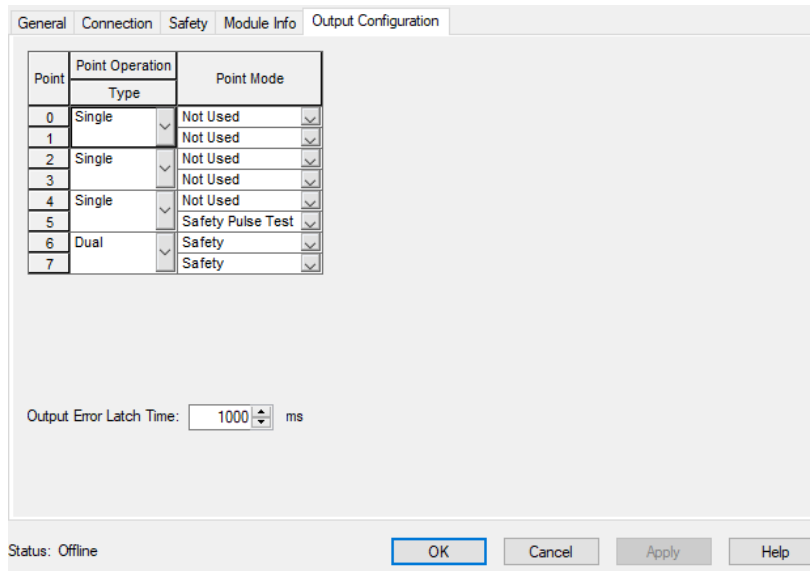
General Connection Safety Module Info Output Configuration

Type: 1734-OB8S 8 Point 24V DC Source Output
 Vendor: Rockwell Automation/Allen-Bradley
 Parent: Safety_Block
 Name: Safety_Outputs
 Description:
 Module Number: 3
 Safety Network Number: 3F22_033C_7ACA
 4/1/2016 11:04:55.242 AM

Module Definition

Series: B
 Revision: 2
 Electronic Keying: Compatible Module
 Configured By: This Controller
 Input Data: None
 Output Data: Safety
 Input Status: Pt. Status
 Data Format: Integer

- On the Output Configuration tab of the module definition, configure the 1734-0B8S Point Operation Type for points 5, 6, and 7 as Single and the Point Mode as Safety.

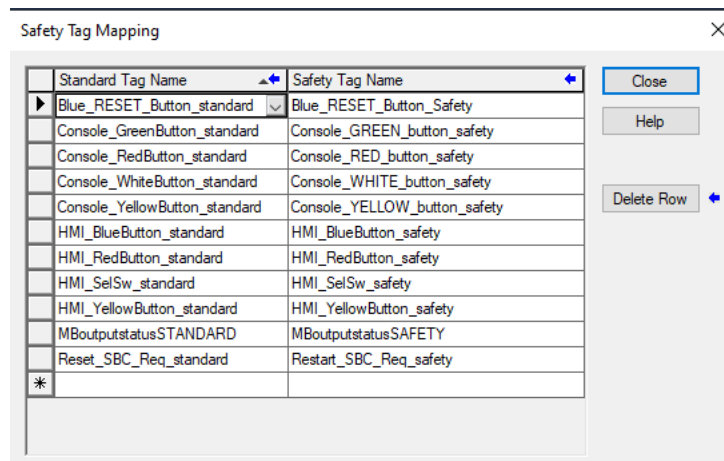


In this application, safety outputs are used for the 700CF relay coil and for the alarm outputs.

Safety Tag Mapping

These tags are the tags in the mapping tool. They are required because the MechanicalBrakeOutputStatus, the red HMI, Blue_Reset, and console buttons are wired into a standard input module and used in the standard task. To use these tags in the safety task, they must be explicitly copied to a safety tag by using the Safety Tag Mapping tool.

The mapped tags are shown in the graphic.



Programming

For controller logic that you can download to your controller, see the attached ACD files. Logic_AT178_1.ACD is for Logix Designer version 31 of the Logix Designer Application.

Our example test bed uses a hardwired console unit. There are three hardwired buttons and two hardwired selector switches. Each button on the console is wired to our standard inputs (mapped to safety inputs). The console button operation is described below. Reset_SBC is a two-position return switch and Jog_Motor is a two-position selector switch. Reset_SBC is a single input used in our example to initiate a reset of the SBC instruction when the SBC.RR is high (1). The Restart_SBC_Request sequence energizes the STOutput bit in safety program logic. We

need this sequence because the SBC instruction requires the BrakeEngageL bit to be high (1) when a reset is requested. We achieve this by energizing the STOOutput bit, pressing the Green_Console_Button (MS0), and pressing the Yellow_Console_Button. When a reset is required, the White_Console_Button must also be pressed.

In this publication, the GuardLogix safety program uses Drive Safety instructions to:

- Initiate and monitor the motor deceleration by using the Safe Speed 2 (SS2) instruction.
- Provide actual motor speed (via the SFX instruction) for SS2 monitoring and evaluating nonzero motor speed conditions.
- Engage and release the safety brake by using the Safe Brake Control (SBC) instruction.

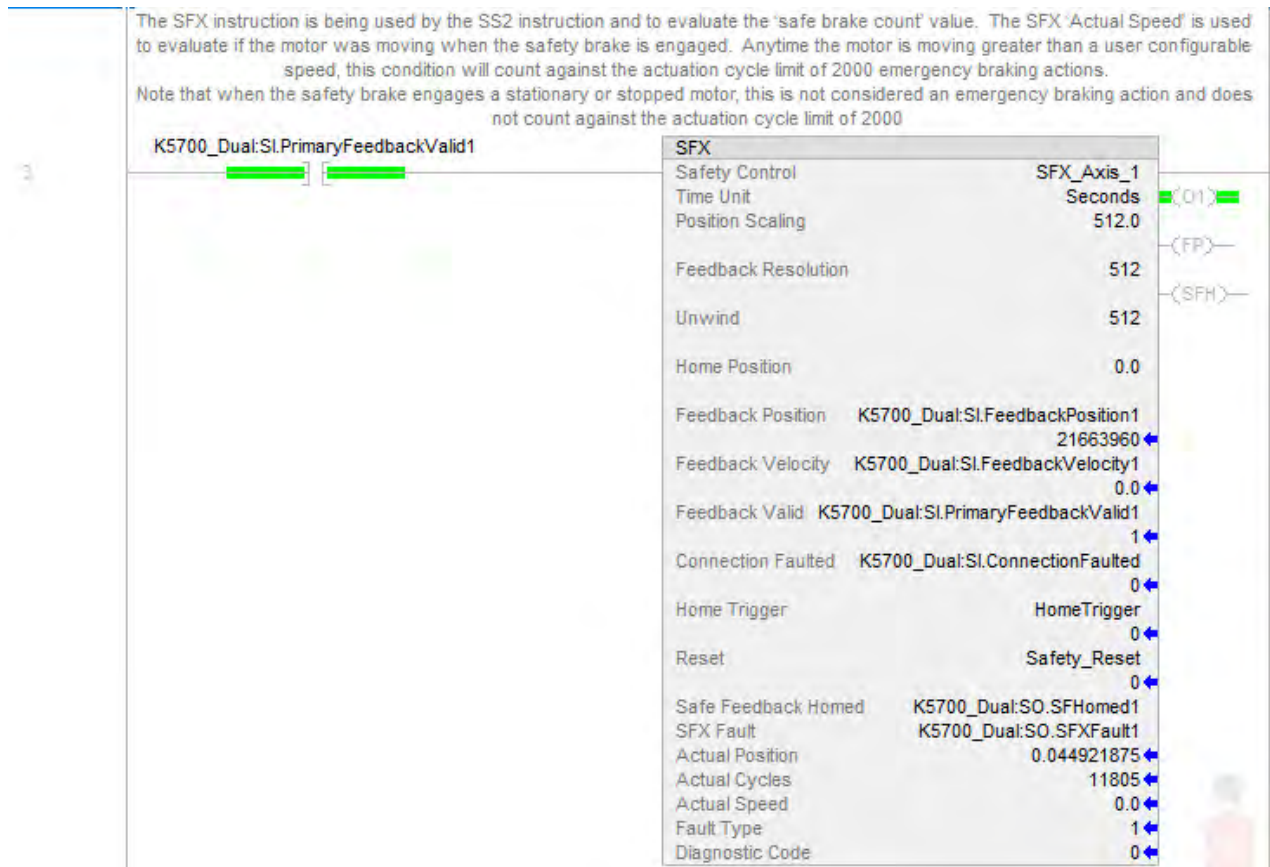
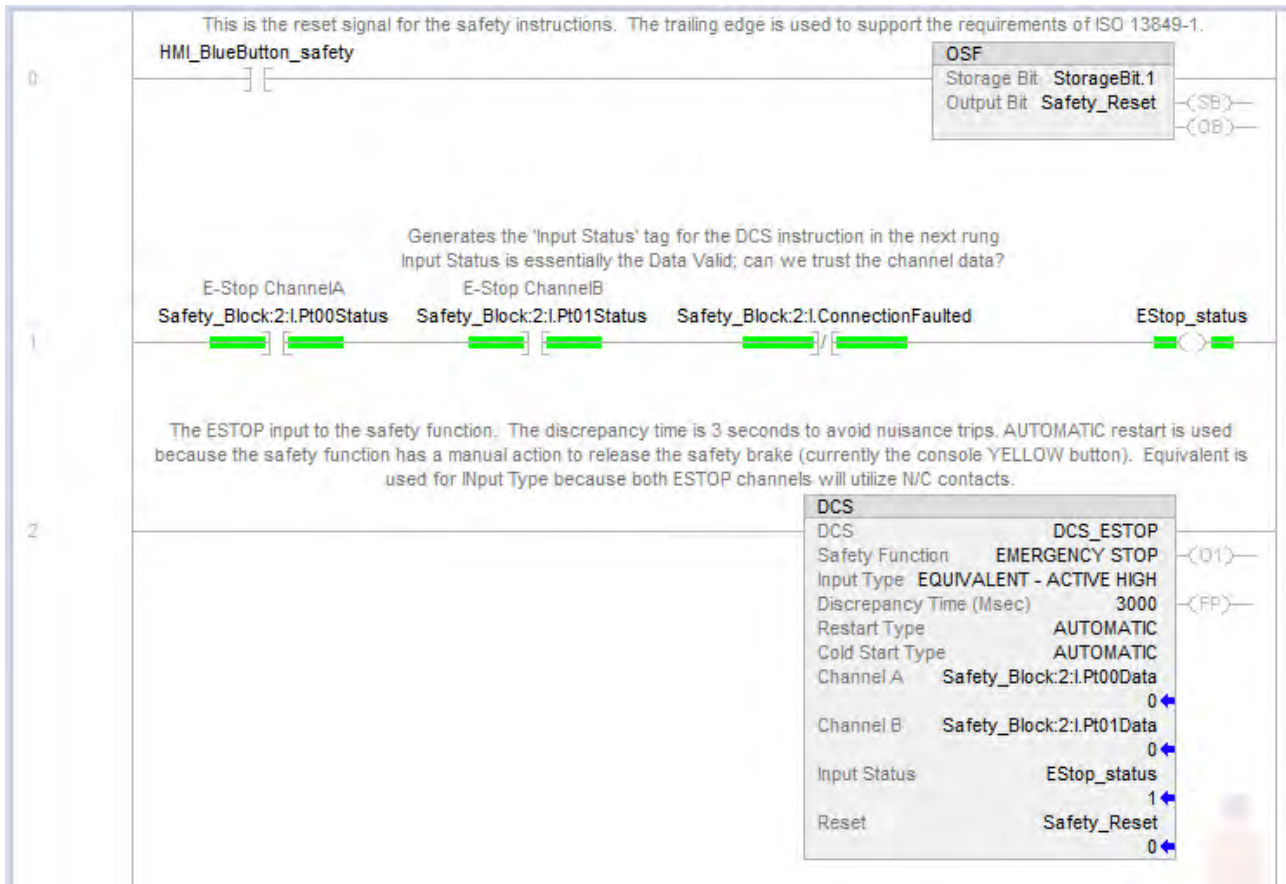
STO is controlled in the safety task to help prevent hazardous motion.

See [Safety Logic Programming](#) and [Motion \(Standard\) Programming](#) in the following sections.

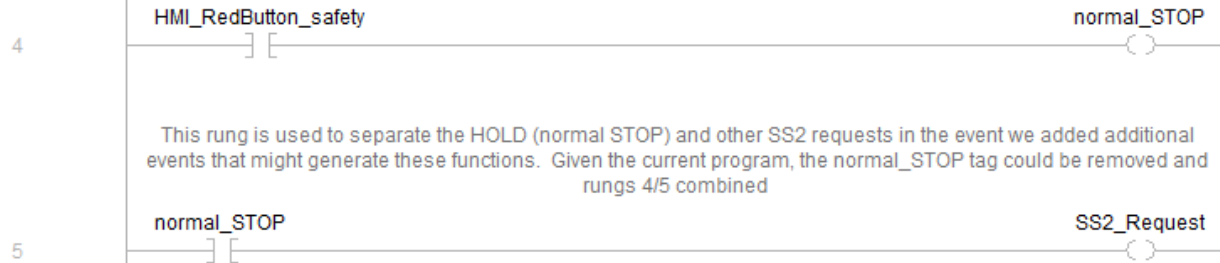
Falling Edge Reset

ISO 13849-1 stipulates that instruction reset functions must occur on falling edge signals. To comply with this requirement, a One Shot Falling (OSF) instruction is used on the reset rung. Then, the OSF instruction Output Bit tag is used as the reset bit.

Safety Logic Programming



A HOLD (normal STOP) is triggered using the HMI_REDbutton maintained signal. This signal needs to be maintained throughout the HOLD (normal STOP) cycle. While this is currently a manual action, there is no reason it could not be handled automatically. The current premise is that a typical HOLD (normal STOP) is not a safety function. Note that if the HOLD (normal STOP) does not work properly, then a 'non-typical' HOLD (normal STOP) action is generated. This helps with the CAT2 declaration for the non-typical HOLD(normal STOP), because all the typical HOLD (normal STOP) cycles can be considered tests of the 'HOLD (normal STOP) not operating properly' safety function. Because even when a typical HOLD (normal STOP) occurs, the safety brake is engaged, but it is engaged on a stationary axis. These 'tests' allow the single channel safety brake to be considered CAT2. CAT2 suggests a test rate of 100x the demand rate, and so this example assumes that there will easily be over 100 typical HOLD (normal STOP) operations for each emergency braking action (non-typical HOLD).



6

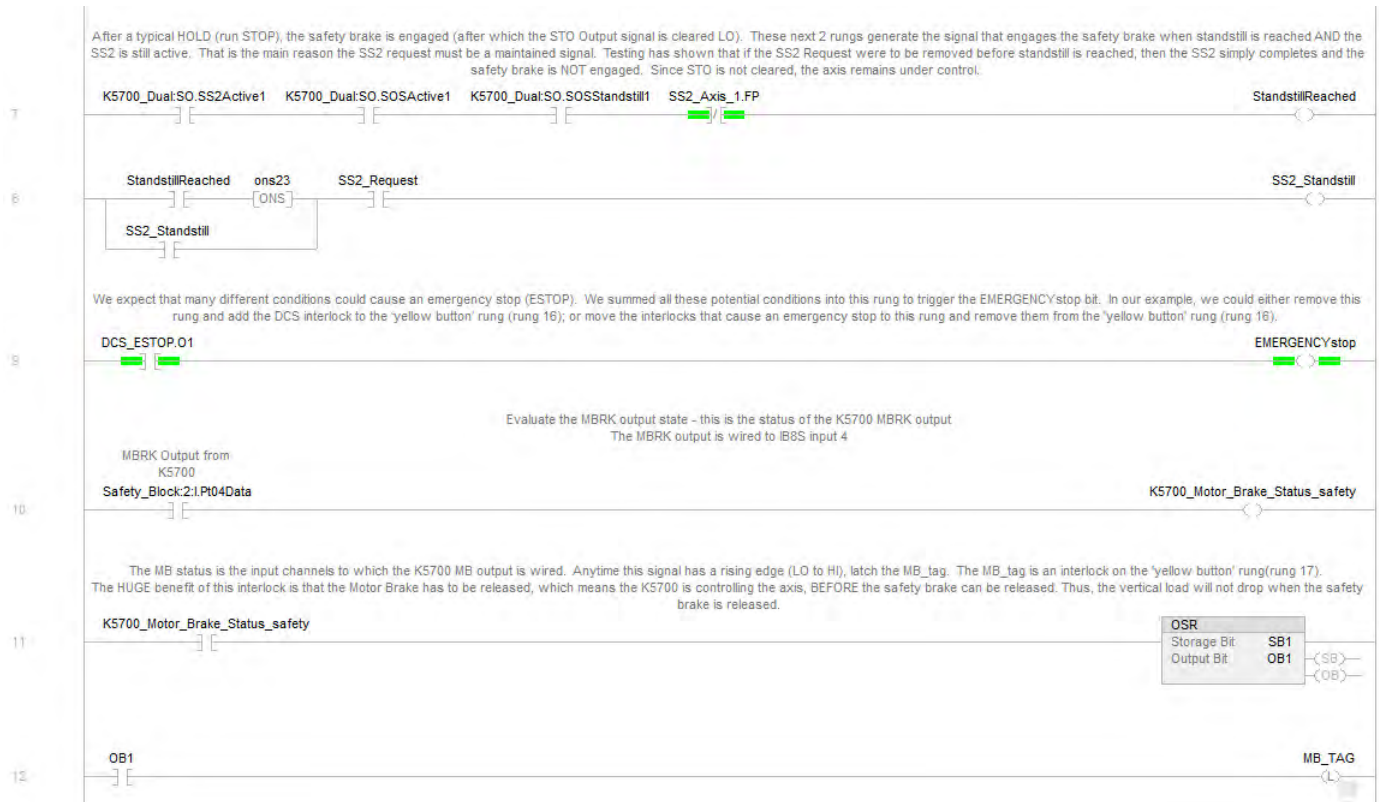
To generate a HOLD (normal STOP), an SS2 instruction is used. The reason an SS2 is used is that it's the best way to avoid any STO signal removal from the K5700 drive BEFORE the Safety Brake is engaged. If the STO signal were removed from a vertical load BEFORE the Safety Brake engages, there is a possibility that the vertical load could drop. Note that the SS1 instruction is designed to clear the STO signal (STOOutput=LO) when the standstill speed is reached. The SS2 instruction does not automatically control the STO signal.

The total delays of 1 second for Stop Monitor Delay and 5 seconds for Check Delay can certainly be reduced in the application logic. They are set purposely large to make it easier to test the safety function and ensure its correct operation.

Note that if the SS2 does not operate properly, the SS2 Fault tag will be set HI; which will cause the drive to fault with a fault action of Disable & Coast which will also clear the MB output LO. This is considered a non-typical HOLD (normal STOP).

SS2		
Safety Control	SS2_Axis_1	
Restart Type	AUTOMATIC	(O1)
Cold Start Type	AUTOMATIC	
Stop Monitor Delay	1000	(RR)
Stop Delay	10000	(FP)
SS2 Standstill Speed	1.0	
Decel Ref Speed	45.0	
Decel Speed Tolerance	2.0	
Mode	Speed_Mode	
	2	
Check Delay	5000	
SOS Standstill Speed	1.0	
Standstill Deadband	50.0	
Feedback SFX	SFX_Axis_1	
Request	SS2_Request	
	0	
Reset	Safety_Reset	
	0	
SS2 Active	K5700_Dual:SO.SS2Active1	
	0	
SS2 Fault	K5700_Dual:SO.SS2Fault1	
	0	
SOS Active	K5700_Dual:SO.SOSActive1	
	0	
SOS Standstill	K5700_Dual:SO.SOSStandstill1	
	0	
SOS Fault	K5700_Dual:SO.SOSFault1	
	0	
SS2 Fault Type		1
SOS Fault Type		1
Diagnostic Code		0

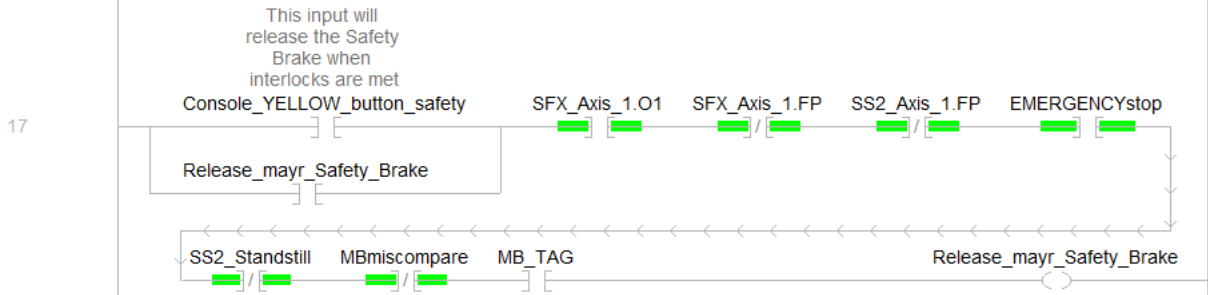




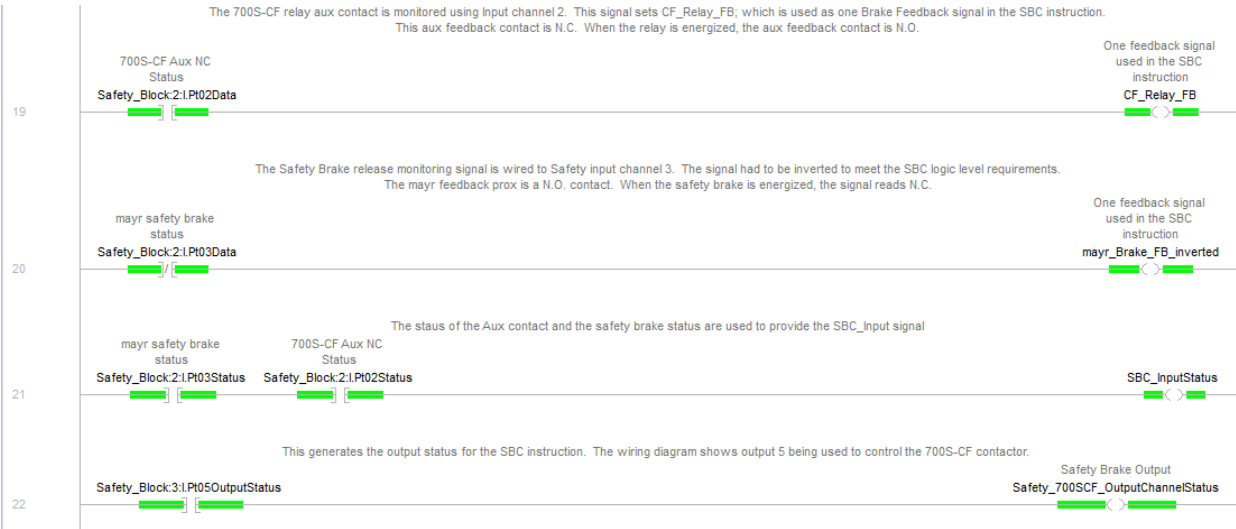
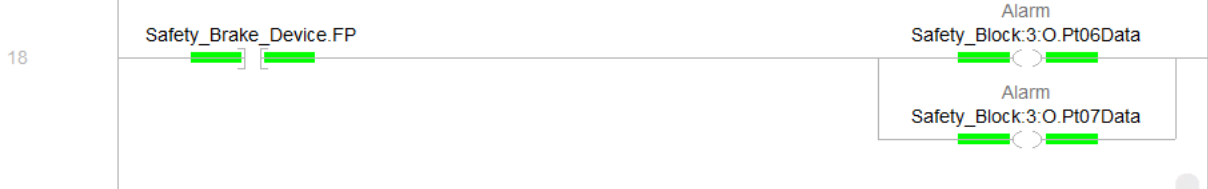
This is the interlock rung to control the Safety Brake. 'Release_MAYR_Safety_Brake' is used with the 'Brake Engage L' tag of the SBC instruction. When this bit is HI, the safety brake will be released. When this bit is LO, the safety brake will be engaged.

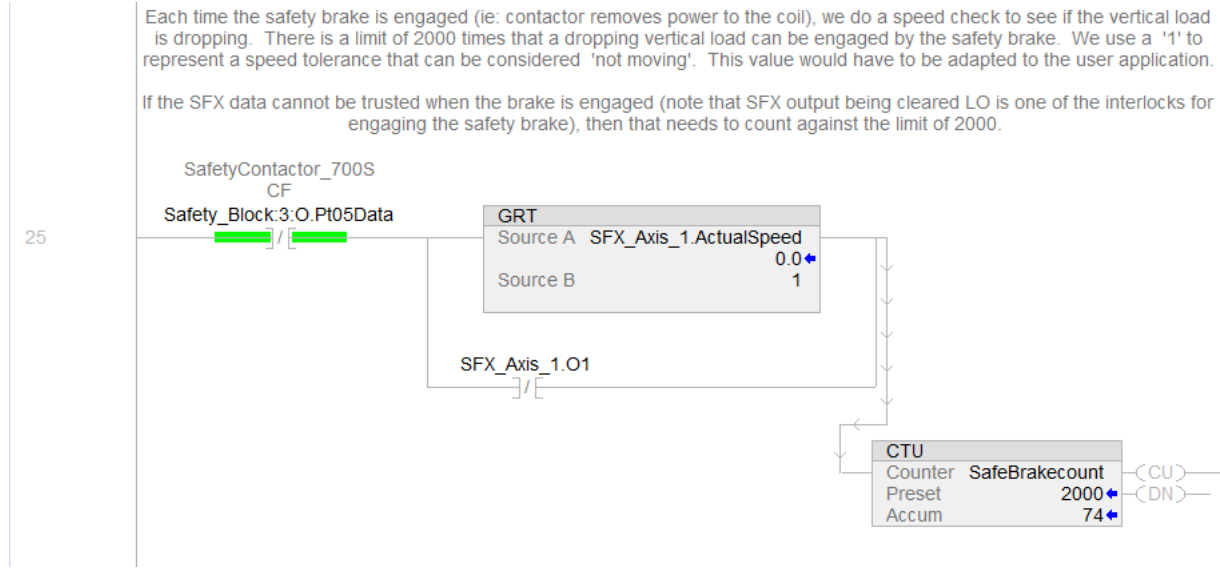
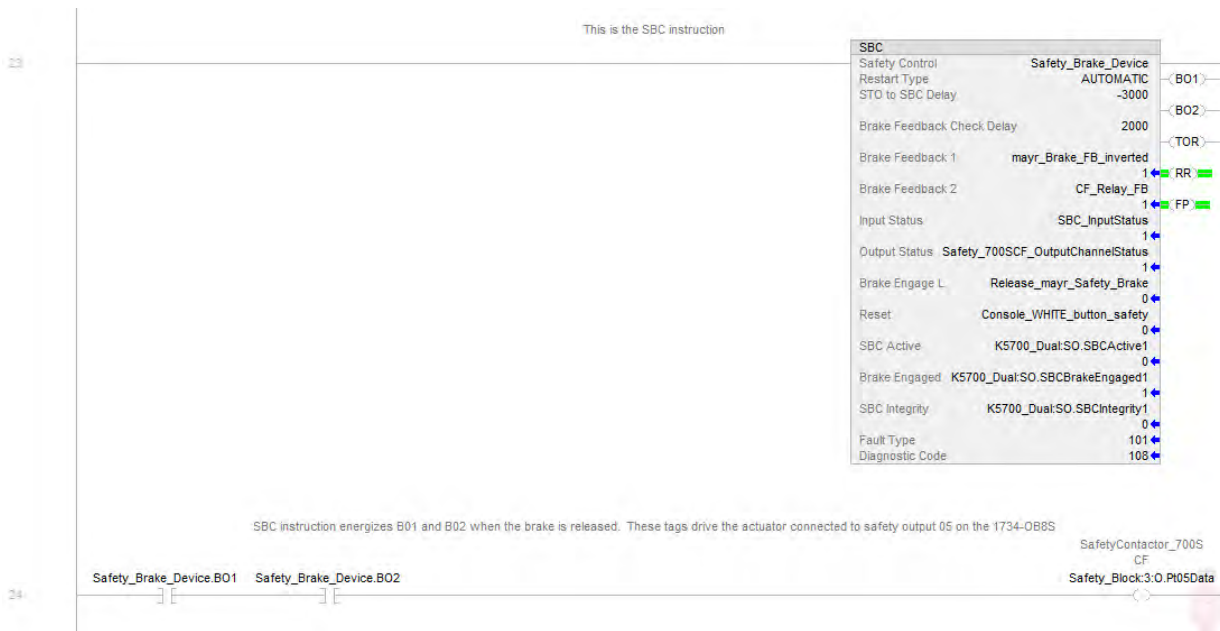
To release the safety brake, the SFX instruction must be OK, the SBC instruction can have no faults, The Emergency Stop Button DCS must be released and the DCS output HI, a typical HOLD (normal STOP) cannot be taking place, the Motor Brake signal must compare between K5700 and the safety input channel it is wired to (IB8S Input 4), and most importantly, the motor brake has to be released first to ensure the axis is under control before releasing the safety brake.

If any of these interlocks drop out, the safety brake will be engaged. The Emergency Stop pressed. Standstill is reached during a typical HOLD (normal STOP). There is a miscompare of the MB signal. The motor brake has been engaged for any reason (perhaps wire falling off) and the safe brake delay timer has expired.



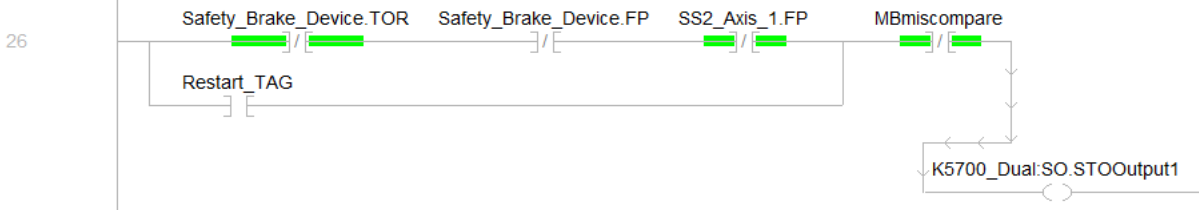
One of the safety requirements for the safety brake is to generate an alarm if the safety brake does not operate correctly. To meet this requirement, the .FP tag is used when the SBC instruction has a fault present





This rung controls the K5700 STO signal. The STO Output has to be set (STOOutput1=HI) for the drive to provide torque to the motor.
 For vertical loads, the SBC instruction uses a negative delay time. At the start of this time, the safe brake is engaged and at the end of this time the STO signal is cleared LO. This ensures that STO is not removed (which can drop the vertical load) before the safety brake has a chance to engage.
 The K5700 drive requires the STO Output signal to be HI in order to energize (release) the MBRK (Motor Brake) Output (via an MSO instruction), which is one of the interlocks to release the safety brake. The manual signal (Restart TAG) is required to set the STO Output so that the drive can be enabled. During the drive enabling process, the MBRK (Motor Brake) Output is energized, which allows the safety brake to be released. The Restart_TAG is controlled below, notice that since the Restart_TAG is used only to energize the SBC from this .TOR state, we want the Restart_TAG to be cleared LO once that the enable is applied within a certain time period - in case the standard input Restart_SBC_Req_safety is not cleared LO by the operator or there is a problem with it. One of the requirements of the SBC to be reset is that the 'Brake Engage L' be HI before the SBC can be reset, the STO in addition with the energized motor will allow the SBC to restart.

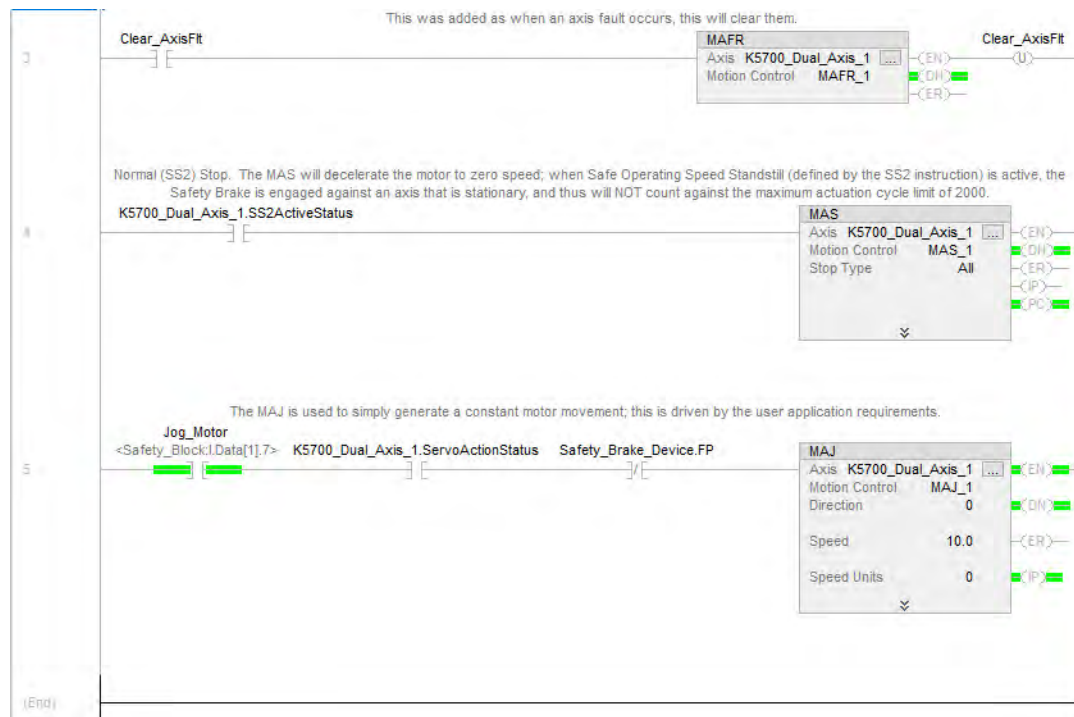
The MBmiscompare interlock was added to prevent the system from restarting with the following fault: If the motor brake wire (IB8S safety input wired to the MB output) falls off (or shorts to common) while the MechanicalBrakeOutputStatus is ON, or HI in the drive's firmware, this fault is not detected. MBmiscompare detects this fault only after the motor brake is set. Conversely, if the motor brake wire is supposed to be LO, but is stuck HI while the MechanicalBrakeOutputStatus is LO in the drive's firmware, this fault is not detected. MBmiscompare detects this fault only after the motor brake is released. In both cases the fault is generated only when the timer expires. The MBmiscompare signal is interlocked with enable STO output AFTER the MBmiscompare timer expires, preventing a restart.

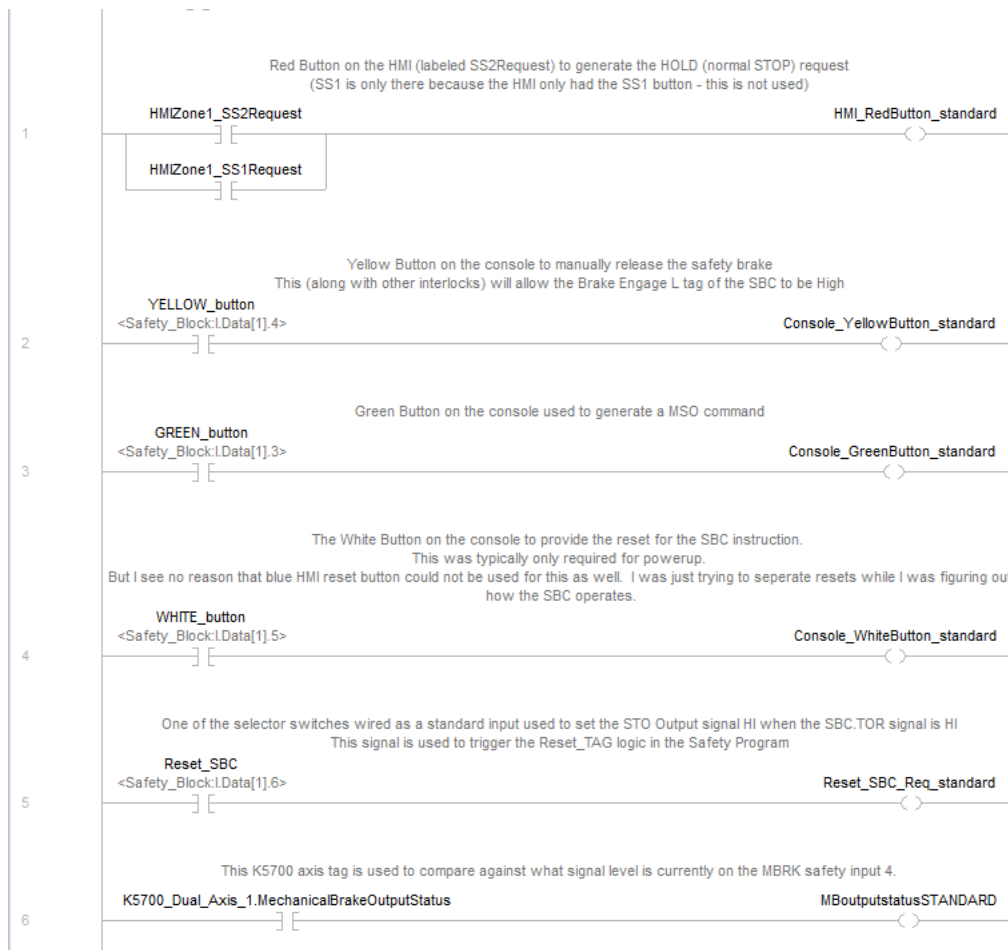


As described in the above rung, this sequence of rungs is used as a means to 'reset' the SBC instruction from a .TOR state. The MBRK output is required to be ON (HI) in order to release the safety brake. Because of this, we need to enable the axis before we can release the safety brake. This sequence will look evaluate the Restart_SBC_Req_safety input and will enable the STO output for the specified time (10sec in this example) just so the Green and Yellow Console buttons can be used to reset the SBC instruction.
 If the Green and Yellow Console buttons are not executed in the specified time interval, the STO Output is removed and the process has to be repeated.
 Once the SBC is reset (SBC.TOR = LO), the input (Restart_SBC_Req_safety) should be turned OFF.



Motion (Standard) Programming





For information about timing and sequencing for this safety function, see [Appendix A – Timing and Sequencing Diagrams on page 48](#).

Calculation of the Performance Level

When properly implemented, this safety function can achieve a safety rating of category 2, Performance Level d (cat. 2, PLd), according to ISO 13849-1: 2015, as calculated by using the SISTEMA software PL calculation tool.

IMPORTANT To calculate the PL of your entire safety function, you must include the specific subsystems that you chose. Depending on the devices you choose, the overall safety rating of your system will be different.

The SISTEMA file that is referenced in this safety function application technique is attached to this publication.

The GuardLogix 5580 controller subsystem uses 6.4% of PLe bandwidth (less than 1% of PLd bandwidth). The Compact GuardLogix 5380 controller subsystem uses 7.2% of PLe bandwidth (less than 1% of PLd bandwidth).

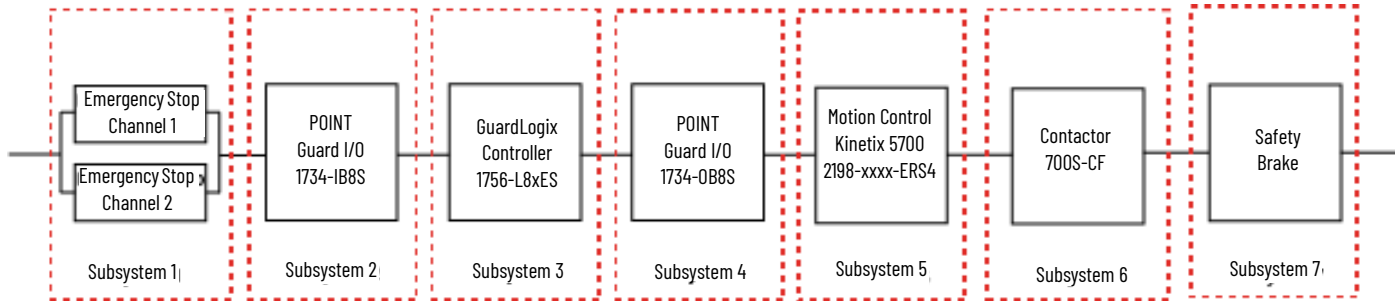
Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	MTTFD [a]	Category	Requirements of the category
✓ SB	GuardLogix 5580 Primary Controller Only	d	d	6.4E-9	not relevant	not relevant	3	fulfilled
✓ SB	Compact GuardLogix 5380 Controller	d	d	7.2E-9	not relevant	not relevant	3	fulfilled

Assuming the following subsystem choices, the overall performance level that is achieved for each safety function is shown in the graphic.

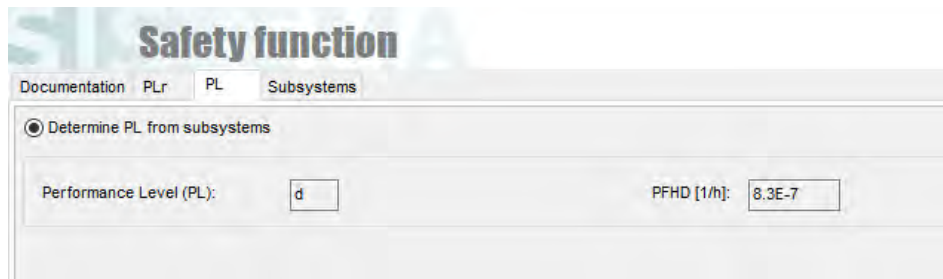
mayr Safe Brake Control - ESTOP safety function

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category	Use case
✓SB	Emergency Stop Pushbutton	e	n.a.	9.1E-10	80 (fulfilled)	99 (High)	2,500 (High)	4	fulfilled	[Unintended Motion]
✓SB	POINT Guard I/O: 1734-IB8S Series B	e	n.a.	1.2E-10	not relevant	not relevant	not relevant	4	fulfilled	[Dual Channel] - - -
✓SB	Safety PLC: GuardLogix 1756-L8xES	d	n.a.	7.1E-9	not relevant	not relevant	not relevant	3	fulfilled	[Standard Use Case]
✓SB	POINT Guard I/O: 1734-OB8S Series B	d	n.a.	4.6E-9	not relevant	not relevant	not relevant	2	fulfilled	[Single Channel] - - -
✓SB	Motion Control: Kinetix 5700 ERS4 Servo Drive	d	n.a.	3.8E-9	not relevant	not relevant	not relevant	3	fulfilled	[Standard Use Case]
✓SB	Contactors	d	n.a.	2.3E-7	100 (fulfilled)	99 (High)	100 (High)	2	fulfilled	[700S-CF contactor is used to remove...]
✓SB	Safety Brake	d	n.a.	5.8E-7	80 (fulfilled)	60 (Low)	100 (High)	2	fulfilled	[MAYR Safety Brake ROBA topstop 89...]

This safety function can be modeled as follows:



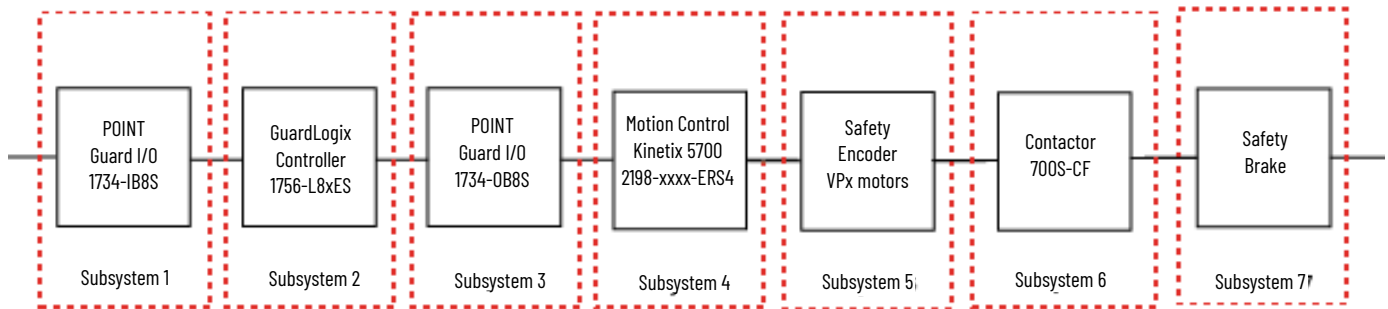
IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is 8.3E-07. The PL for the complete safety function is PLd.



mayr Safe Brake Control - Normal Stop Not Operating Properly or K5700 Motor Brake Engaged Unexpectedly

Status	Name	PL	PL-Software	PFHD [1/h]	CCF score	DCavg [%]	MTTFD [a]	Category	Requirements of the category	Use case
✓SB	POINT Guard I/O: 1734-IB8S Series B	e	n.a.	1.2E-10	not relevant	not relevant	not relevant	4	fulfilled	[Dual Channel] - - -
✓SB	Safety PLC: GuardLogix 1756-L8xES	d	n.a.	7.1E-9	not relevant	not relevant	not relevant	3	fulfilled	[Standard Use Case]
✓SB	POINT Guard I/O: 1734-OB8S Series B	d	n.a.	4.6E-9	not relevant	not relevant	not relevant	2	fulfilled	[Single Channel] - - -
✓SB	Motion Control: Kinetix 5700 ERS4 Servo Drive with Single Encoder	d	n.a.	3.8E-9	not relevant	not relevant	not relevant	3	fulfilled	[Standard Use Case]
✓SB	Safety Encoder: VPx motors, VPL-xxxxxx-Wx1xAx, Frames 63-75	d	n.a.	4E-8	not relevant	not relevant	not relevant	3	fulfilled	[Standard Use Case]
✓SB	Contactors	d	n.a.	2.3E-7	100 (fulfilled)	99 (High)	100 (High)	2	fulfilled	[700S-CF contactor is used to remove...]
✓SB	Safety Brake	d	n.a.	5.8E-7	80 (fulfilled)	60 (Low)	100 (High)	2	fulfilled	[MAYR Safety Brake ROBA topstop 89...]

This safety function can be modeled as follows:



IMPORTANT The PFH for this complete safety function, with the sensor, logic, and actuator subsystems, is $8.7E-07$. The PL for the complete safety function is PLd.



Functional Safety Data Required for Determining the Performance Level of Electromechanical Devices

Because these E-stops and actuators are electromechanical devices, the functional safety data that is required for the Performance Level calculation includes the following:

- Mean Time to Failure, dangerous (MTTFd)
- Diagnostic Coverage (DCavg)
- Common Cause Failure (CCF)

The functional safety evaluations of the electromechanical devices include the following:

- How frequently they are operated
- Whether they are effectively monitored for faults
- Whether they are properly specified and installed

SISTEMA calculates the MTTFd by using B10d data that are provided for the contactors along with the estimated frequency of use, entered during the creation of the SISTEMA project.

The DCavg (99%) for the E-stop is selected from the Input Device table of ISO 13849-1 Annex E, Cross Monitoring.

The CCF value is generated by using the scoring process that is outlined in Annex F of ISO 13849-1. The complete CCF scoring process must be performed when actually implementing an application. A minimum score of 65 must be achieved.

FAULT EXCLUSION: When an application includes two-channel, single-actuator mechanical safeguarding devices such as interlocks or mechanical emergency stop devices such as E-stops or cable pull switches, fault exclusion for single-actuator failure must be taken into account and, when required, applied when determining the Performance Level.

Exclusion of the possible fault of the single actuator failing to switch the two channels properly is not allowed. Therefore, single types of electromechanical devices are limited to a maximum Performance Level of d. The Performance Level required (PLr) in safety function application techniques is PLd. Redundancy of safeguarding switches is required to achieve Performance Level e.

If the maximum number of operations of an electromechanical emergency stop device is in accordance with IEC 60947- 5-5, regarding the mechanical aspects of the device, exclusion of the possible fault of the single actuator of that device failing to switch the two channels properly is allowed per EN ISO 13849-2, Annex D, Table D8. Therefore, single types of devices, properly applied, are not limited and can achieve Performance Level e.

The emergency stop function is a complementary protective measure, which is intended to be used with other safeguarding measures and protective devices to sufficiently reduce risk. The design of the emergency stop functions shall not impair the effectiveness of other safety functions or protective devices in the system. The actual number of operations (NOP) is used for the purposes of the MTTFd calculation in this publication.

Verification and Validation Plan

Verification and validation play important roles in the avoidance of faults throughout the safety system design and development process. ISO 13849-2 sets the requirements for verification and validation. The standard calls for a documented plan to confirm that all safety functional requirements have been met.

Verification is an analysis of the resulting safety control system. The Performance Level (PL) of the safety control system is calculated to confirm that the system meets the required Performance Level (PLr) specified. The SISTEMA software is typically used to perform the calculations and assist with satisfying the requirements of ISO 13849-1.

Validation is a functional test of the safety control system to demonstrate that the system meets the specified requirements of the safety function. The safety control system is tested to confirm that all safety-related outputs respond appropriately to their corresponding safety-related inputs. The functional test includes normal operating conditions and potential fault injection of failure modes. A checklist is typically used to document the validation of the safety control system.

Before validating the GuardLogix safety system, confirm that the safety system and safety application program have been designed in accordance with the controller safety reference manuals that are listed in the [Additional Resources](#), and the GuardLogix Application Instruction Safety Reference Manual, publication [1756-RM095](#).

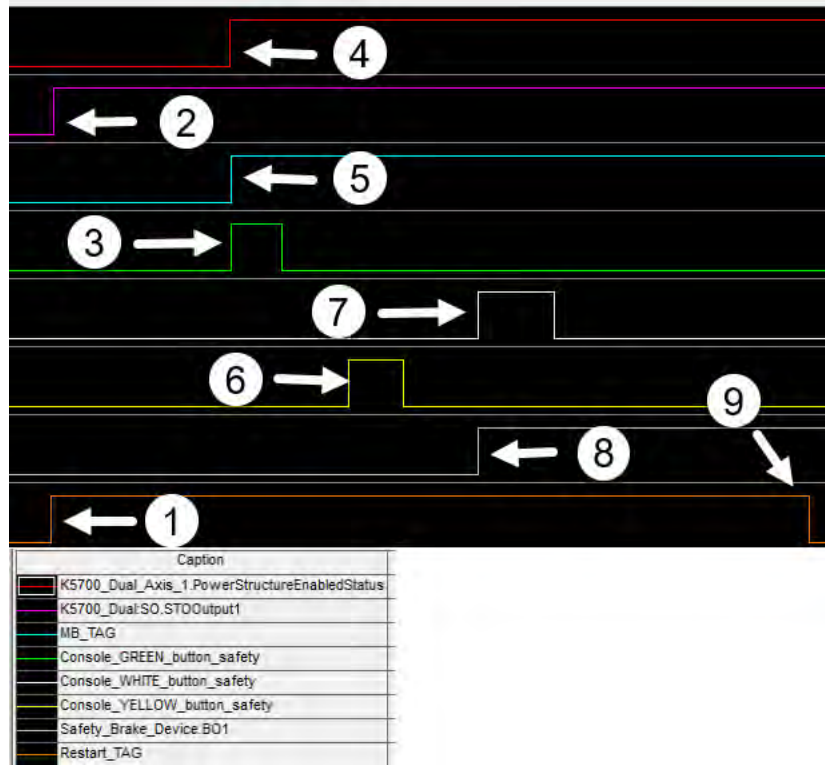
For a validation checklist, see the attached spreadsheet.

Appendix A – Timing and Sequencing Diagrams

The following sections provide details about proper timing and sequencing for your safety function.

Restart Sequence

This is the sequence for a restart. This sequence is used after power is applied to the machine. This sequence can be requested after the controller and the drives have powered up.

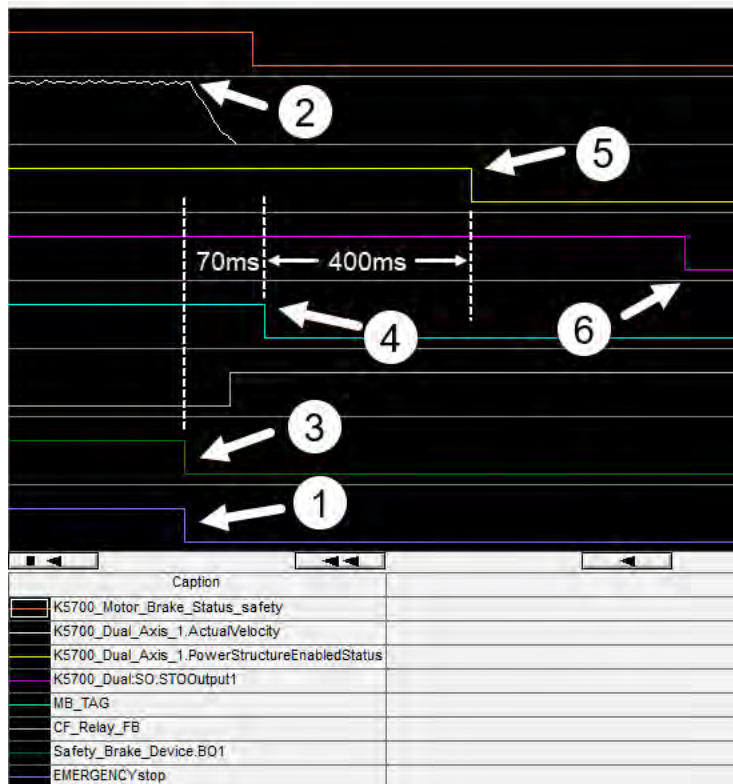


The pre-condition to this sequence is that there are no safety or axis faults.

1. The Restart_TAG is high (1).
2. The STO_Output is high (1).
3. Press the Green_Console_Button (low (0) to high (1)).
4. The motor is Enabling.
5. The MB_TAG is high (1) (in this case, the MBRK Output is high (1)).
6. Press the Yellow_Console_Button (low (0) to high (1)) - a permissive to allow the SBC to release the brake.
7. Press the White_Console_Button (low (0) to high (1)) - resets the SBC instruction and releases the safety brake.
8. The SBC.B01 (B02 is implied) transitions to high (1) indicating the safety brake is releasing.
9. The Restart_TAG is low (0).

E-Stop Request

This sequence is for an E-stop request.

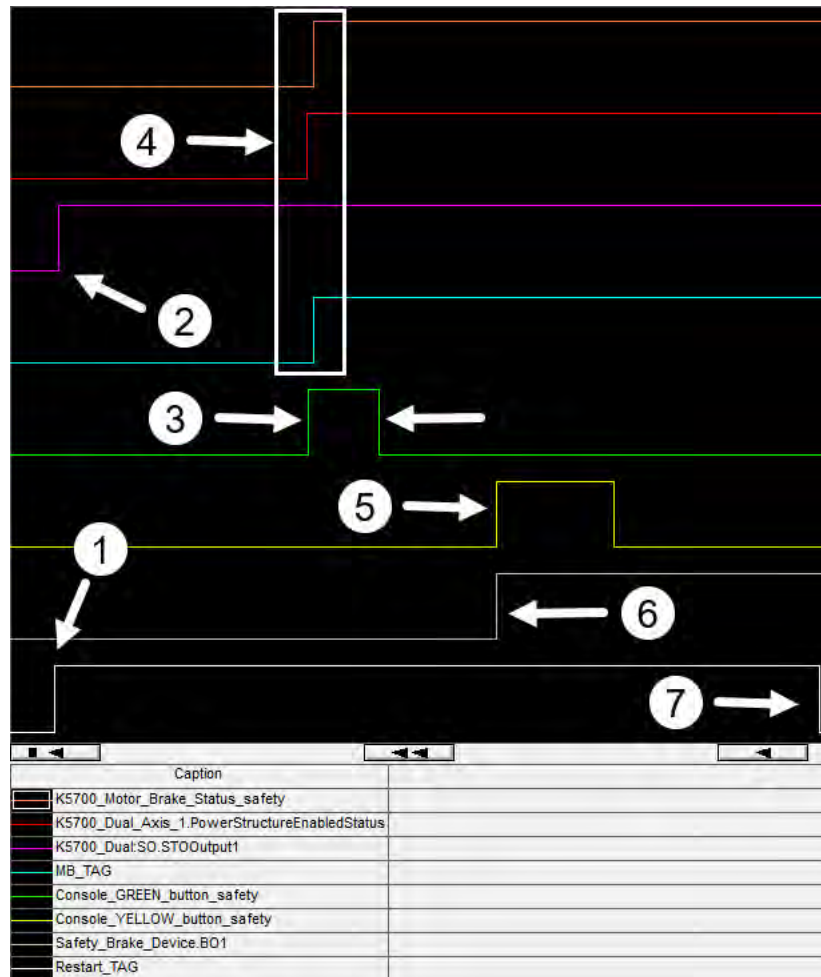


The pre-condition to this sequence is that the motor is enabled, and the safety brake is released. The motor is jogging (MAJ).

1. The E-Stop Safety Input is activated (EMERGENCYstop).
2. The MSF action occurs when the E-Stop Safety Input is activated (Current Decel & Disable).
3. The SBC.B01 output is low (0) (B01/B02 outputs low (0)) indicating the safety brake is engaging.
4. We show 70 ms for the Deceleration to occur. In reality, this may not happen because the Safety Brake B01/B02 has been set to engage the load in Step 3. The MB_Tag is low (0) once zero speed is achieved. This deceleration detail is provided to demonstrate the drive behavior. Normally, when SBC.B01/B02 is low (0), the safety brake is used to stop the motor. If the motor was stopped using the safety brake before the motor reaches zero speed, this case counts against the maximum actuation cycles value. One reason we use the MSF instruction in the E-Stop case is if we are close to, or at zero speed, we could decelerate the motor to zero speed before the safety brake engages. In this case, the E-Stop would not count against the maximum actuation cycles value. You can see in the trend, the CF_Relay_FB (grey pen) shows the 700S relay feedback status. It transitions from low (0) to high (1) close to zero speed, so it does take some amount of time to engage the safety brake.
5. The servo power is removed from the motor when MechanicalBrakeEngageDelay expires (400 ms in this example).
6. The STO_Output is removed after the STO->SBC Delay Expires.

E-Stop Reset

This is the sequence to reset the E-stop.

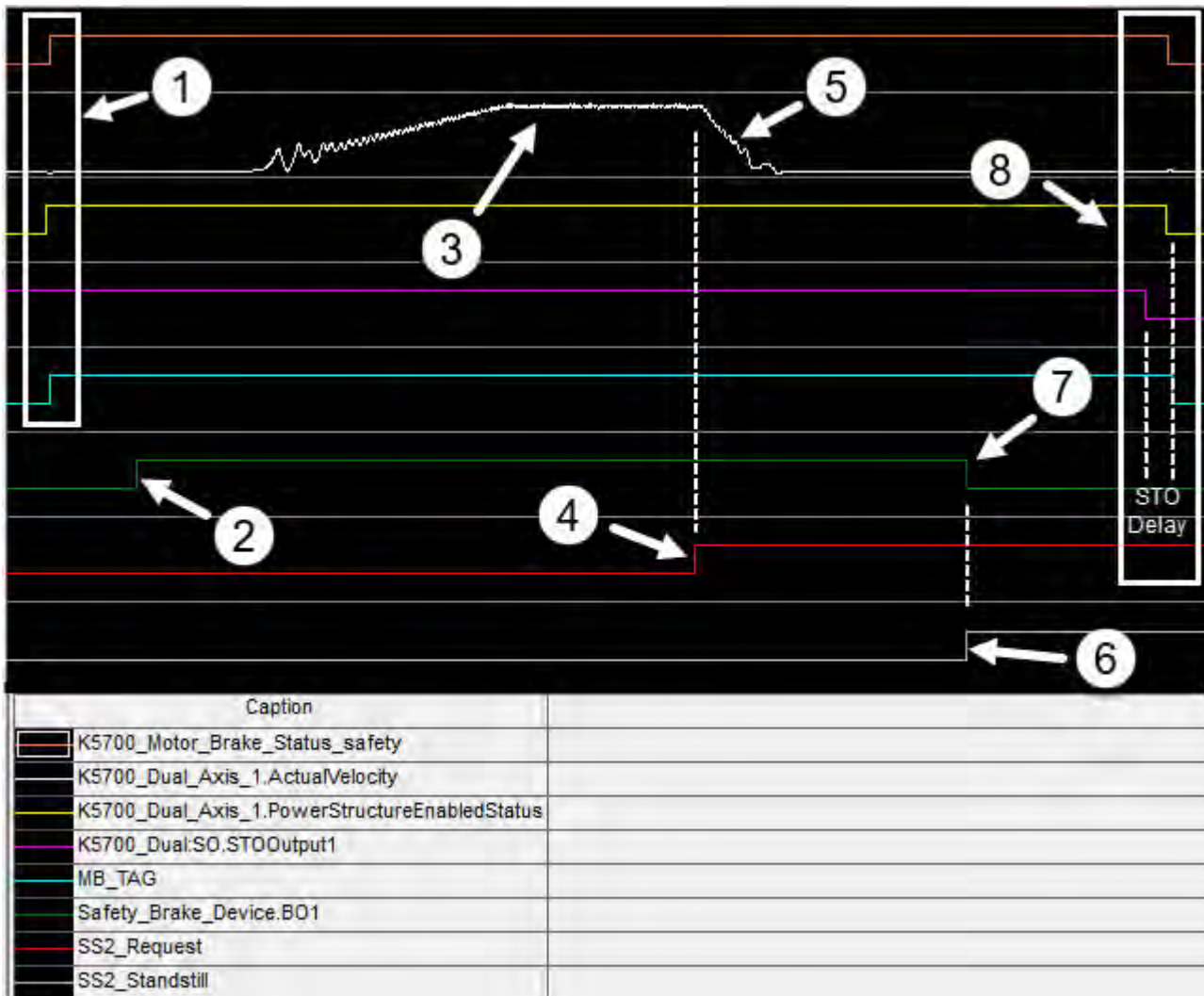


The pre-condition to this sequence is that there are no safety faults. If there are safety faults, use the safety task programming to clear them.

1. The Restart_Tag is high (1).
2. The STO_Output is high (1).
3. Press the Green_Console_Button (low (0) to high (1)).
4. The motor is Enabling and the Holding Brake is released. Notice that the tags used for indicating an enable condition are out of timing sequence. This is due to the tag update in the safety task. The enable timing is shown in the timing diagrams throughout this publication. This trend only shows the safety task tags.
5. Press the Yellow (0)_Console_Button (low (0) to high (1)).
6. The Safety Brake is Released (SBC.B01 is high (1) - B02 is implied. Only 8 pens are available in a trend).
7. The Restart_TAG is low (0).

Typical HOLD (Normal STOP) Request

This sequence shows the Typical HOLD. Recall the Typical HOLD uses the SS2 and SBC and completes with an STO operation.

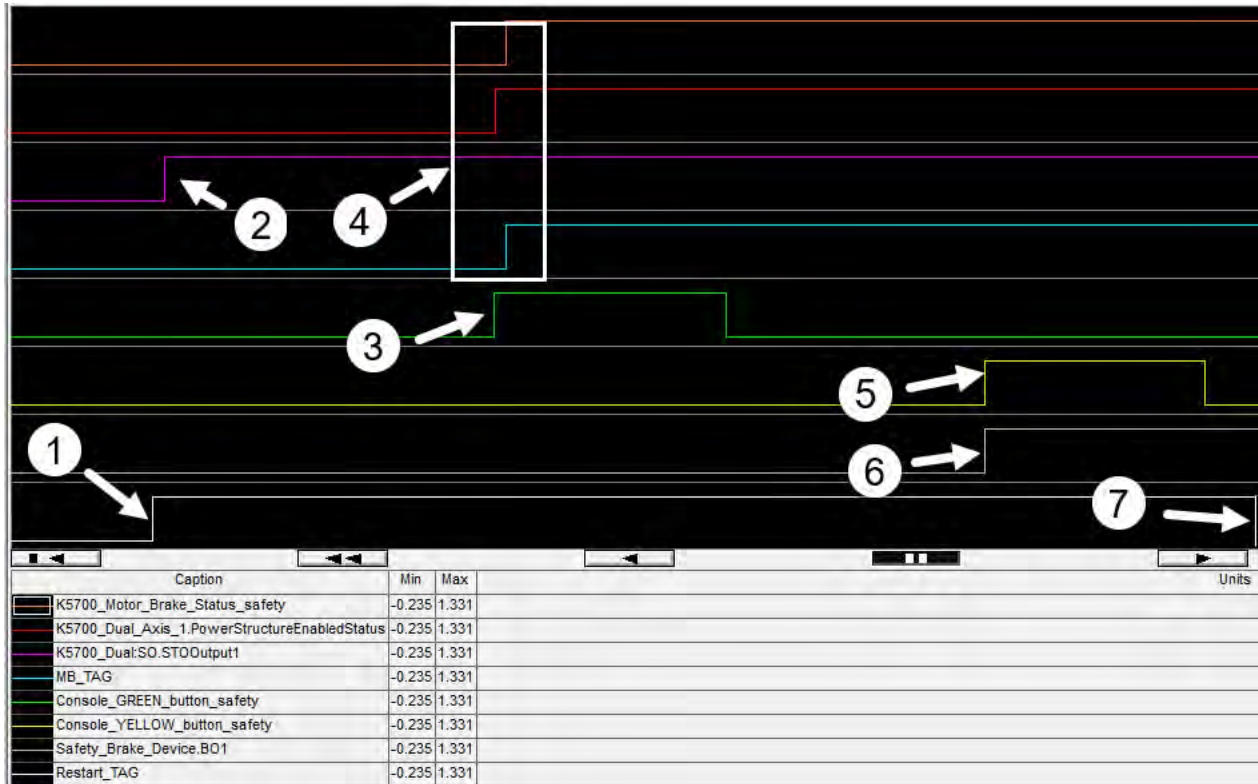


The pre-condition to this sequence is that the Green_Console_Button is pressed (MSO). The sequence begins at that point.

1. The motor is Enabling and the Holding Brake is released. Notice that the tags used for indicating an enable condition are out of the timing sequence. This is due to the tag update in the safety task. The enable timing is shown in the timing diagrams throughout this publication. This trend only shows the safety task tags.
2. Press the Yellow_Console_Button and SBC.B01 transitions to high (1), indicating the safety brake is releasing.
3. Motion Starts (MAJ) using the Jog Selector Input Switch.
4. The SS2_Request (HMI_RedButton) is high (1).
5. The motor is Stopped (using the MAS instruction that is monitored in the SS2 instruction).
6. After the Stop Monitor Delay and Check Delay expires, the SS2_Standstill is evaluated (Standstill is high (1)).
7. The SBC Output is low (0) (B01/B02 outputs are low (0)) and the safety brake is engaging.
8. When the STO->SBC Delay expires, the STO Output is low (0) and the motor is disabled (notice there is a STO Delay). The STO Delay is configured in the drive properties and keeps the motor power on after the STO transitions to low (0). The STO Delay is identified in the trend to explain why the motor power remains enabled after the STO Output transitioned low (0). The example of an SBC fault in this appendix shows how the STO Delay can be useful.

Typical/Non-Typical HOLD (Normal Stop) Reset

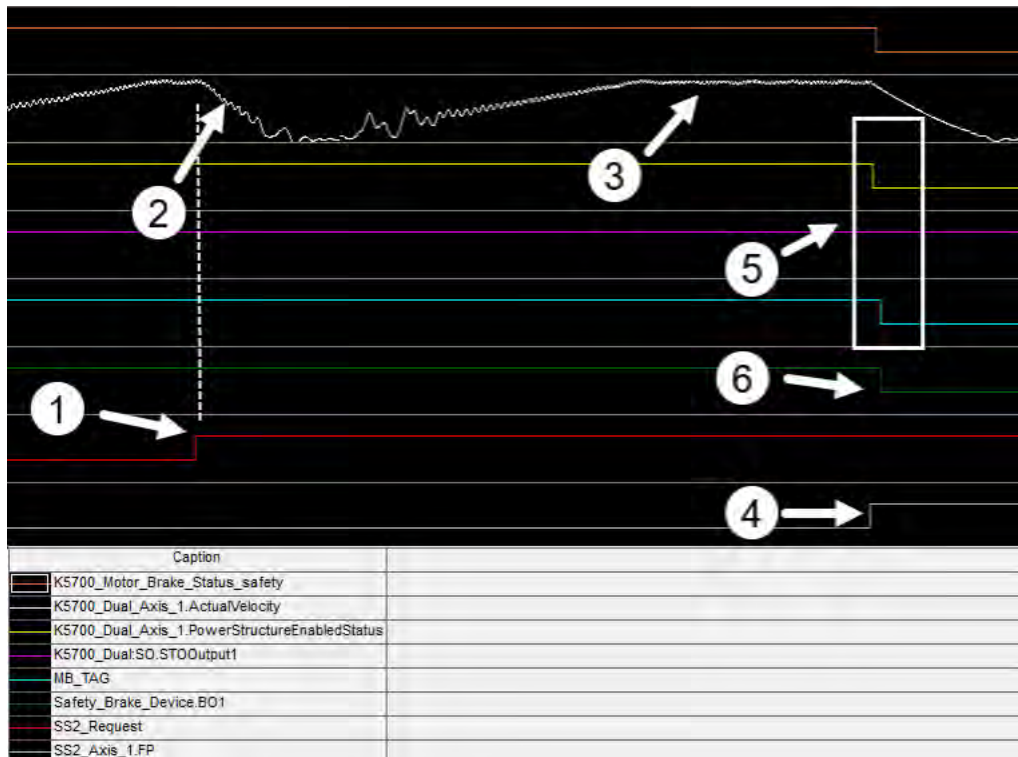
This is the reset for the Typical HOLD operation.



1. The Restart_TAG is high (1).
2. The STO_Output transitions from low (0) to high (1).
3. Press the Green_Console_Button (low (0) to high (1)).
4. The motor is Enabling and the Holding Brake is released. Notice that the tags used for indicating the enable condition do not follow the timing sequence specified throughout this document. This is due to the tag update in the safety task. This trend only shows the safety task tags.
5. Press the Yellow_Console_Button (low (0) to high (1)).
6. The safety brake is Released (SBC.B01 is high (1)).
7. The Restart_TAG is low (0).

Non-Typical HOLD Request

This condition was simulated by creating an SS2 fault.

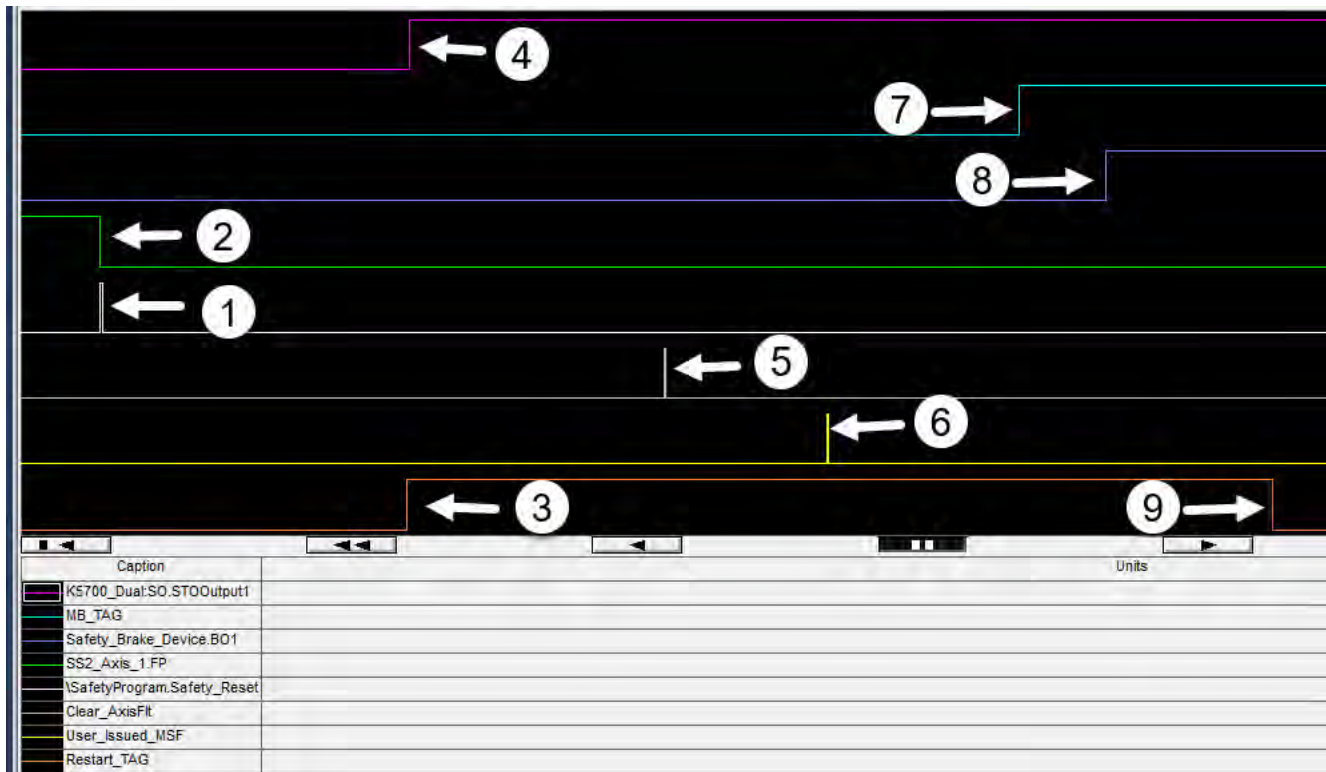


The pre-condition to this sequence is that the motor is enabled and the safety brake is released. The motor is jogging (MAJ).

1. The SS2_Regeust (HMI_RedButton) is high (1).
2. The motor is Stopped (using the MAS instruction and monitored by the SS2 instruction).
3. During the Stop Monitor Delay and Check Delay, we jog the motor again. When Standstill is expected, we are in motion, so this faults the SS2 instruction.
4. The SS2 instruction is faulted and the SS2.FP goes high (1).
5. The Disable & Coast action is used. The motor is disabled immediately. This shows the motor coasting to zero speed. This would not happen as the Safety Brake would engage the load at Step 6 and stop the motion. This is shown so you can see that this case counts against the maximum actuation cycles value (the motor speed was non-zero when the safety brake was applied).
6. The SBC Output is low (0) (BO1/BO2 outputs are low (0)) and when the STO->SBC Delay expires, the STO Output is low (0), so the motor cannot produce torque.
7. The STO_Output transitions to low (0) after STO->SBC Delay Expires.

Non-typical HOLD Reset

This sequence shows fault recovery from an SS2 fault. Notice that in this recovery, we do not have to use the White_Console_Button because the SBC instruction is not faulted.



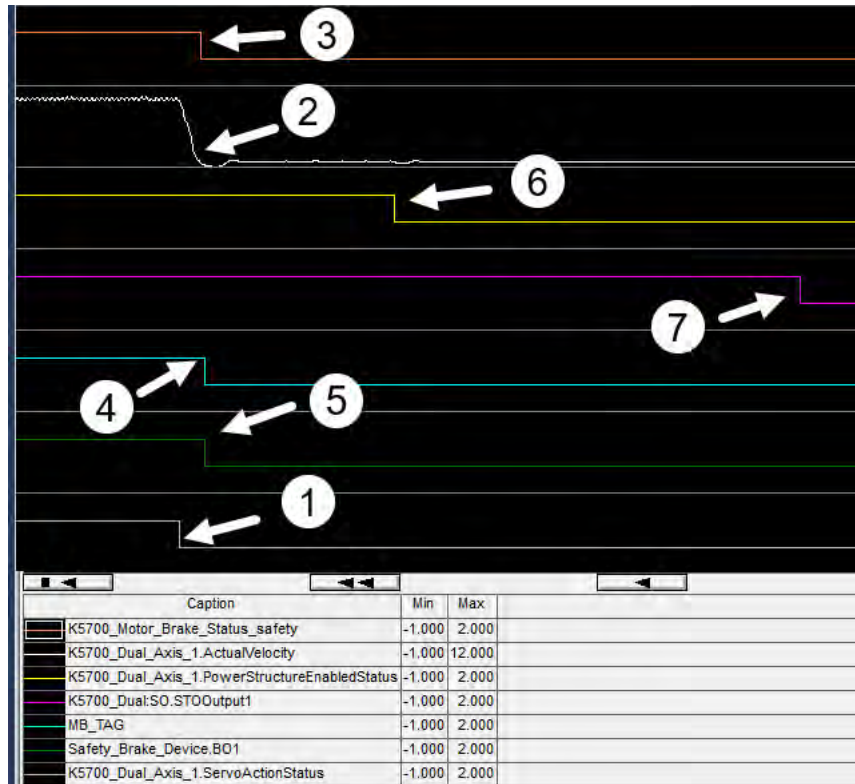
1. The Reset_Safety (Blue HMI Button) is high (1). This resets the SS2 fault in the safety task.
2. The SS2_Axis1.FP transitions to low (0).
3. The Restart_TAG is high (1) (Toggle Reset_SBC standard Input).
4. The STO_Output is high (1).
5. Clear Axis Faults (MAFR) - this is required as the standard program is faulted. This MAFR can also be done before the Restart_TAG is high (1), step 3.
6. Execute an MSF (User_Issued_MSF). This Motion Servo Off is required as part of the reset process.
7. Press the Green_Console_Button (low (0) to high (1)). The motor is enabled and the holding brake is released. The MB_TAG is high (1).
8. Press the Yellow_Console_Button (low (0) to high (1)). The safety brake is Released (SBC.B01 is high (1) - B02 is implied. Only 8 pens are available in a trend).
9. The Restart_TAG is low (0).

Typical Disable Request

This sequence is the Typical Disable. There is no SafeBrakeDelay (used for a secondary brake system) in this example. The motor is being disabled by a command; this means the BrakeEngageDelay is used, but the STO Delay is not used. The SBC instruction is triggered by the MBRK output.



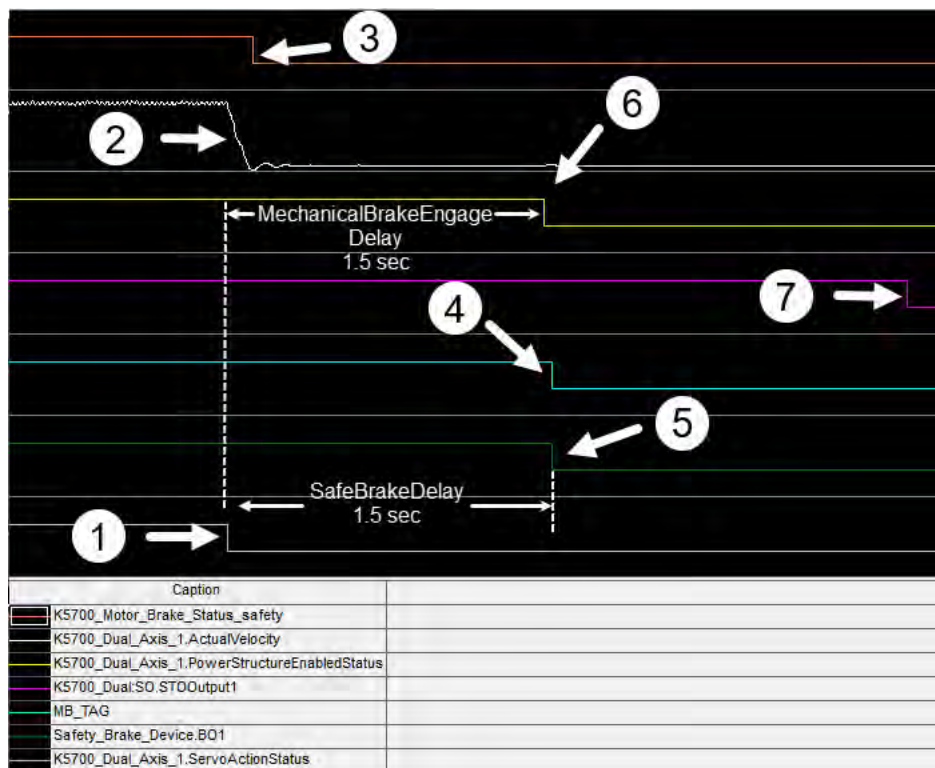
If the motor was enabled when the STO is removed, the STO_Delay is used.



1. The Disable command is received and the ServoActionStatus transitions from high (1) to low (0).
2. The Stopping Action (Current Decel & Disable) is used to decelerate and disable the motor, and the motor reaches zero speed, as defined in the Axis Properties dialog box.
3. At zero speed, the MBRK Output is low (0).
4. The MB_Tag is low (0).
5. The SBC.BO1 Output is low (0) (B01/B02 outputs low (0)). The safety brake is engaging.
6. The motor remains enabled for MechanicalBrakeEngageDelay. This helps to ensure that the safety brake has time to engage physically.
7. The STO Output is low (0) after the STO -> SBC Delay expires.

Typical Disable Request (SafeBrakeDelay used)

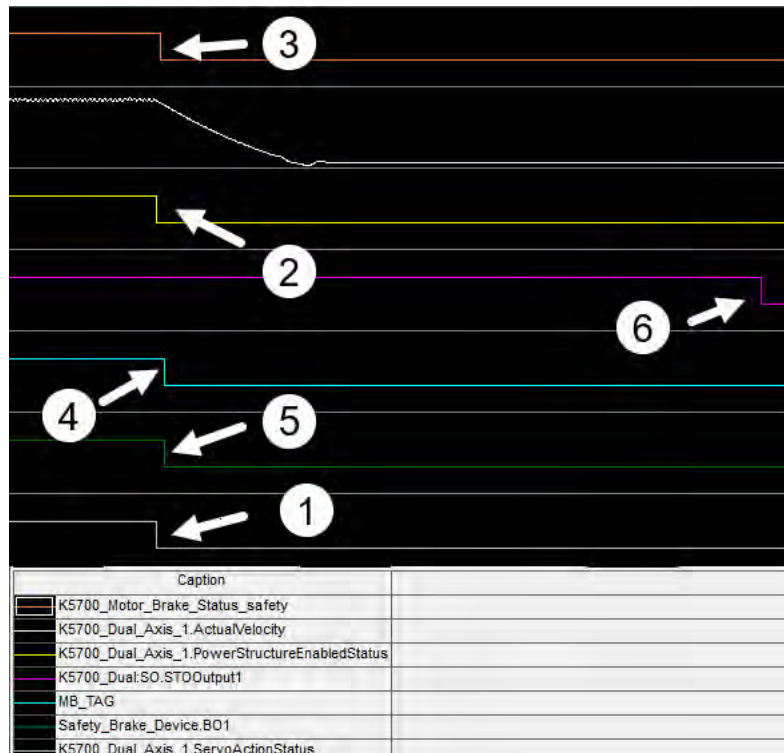
This sequence is the Typical Disable and the SafeBrakeDelay is used. The MechanicalBrakeEngageDelay is set for 1.5 s, so you can clearly see how it keeps the motor enabled while the secondary brake is engaging. In this example, if a secondary braking system was used, these two delays should be set to the same values so that the motor remains enabled while the secondary braking system is engaging. The SBC instruction is triggered by the MBRK output.



1. The Disable command is received and the ServoActionStatus transitions from high (1) to low (0).
2. The Current Decel & Disable used to decelerate and disable the motor.
3. The MBRK Output is low (0). The orange pen is the safety mapped value of the MBRK Output.
4. The motor remains enabled for the MechanicalBrakeEngageDelay (1.5 s). This helps to ensure that the safety brake has time to engage physically. The motor disables after the delay expires, and the MB_Tag is low (0).
5. The safety brake is not engaged until the SafeBrakeDelay expires. Then the SBC.B01 output is low (0) (B01/B02 outputs low (0)) and the safety brake is engaging.
6. The motor is disabled at the same point as step 4.
7. The STO output is low (0) after the STO -> SBC Delay expires.

Non-Typical Disable Request

This sequence is the Non-Typical Disable. In this example, the Disable & Coast action is used. This can be because of a Major Fault. This is modeled as the worst-case example. The safety brake engagement occurs when the MBRK output is low (0) so the time to engage the safety brake is important in this example, because the load could drop proportionally to the amount of time it takes to engage the safety brake. The SBC instruction is triggered by the MBRK output.



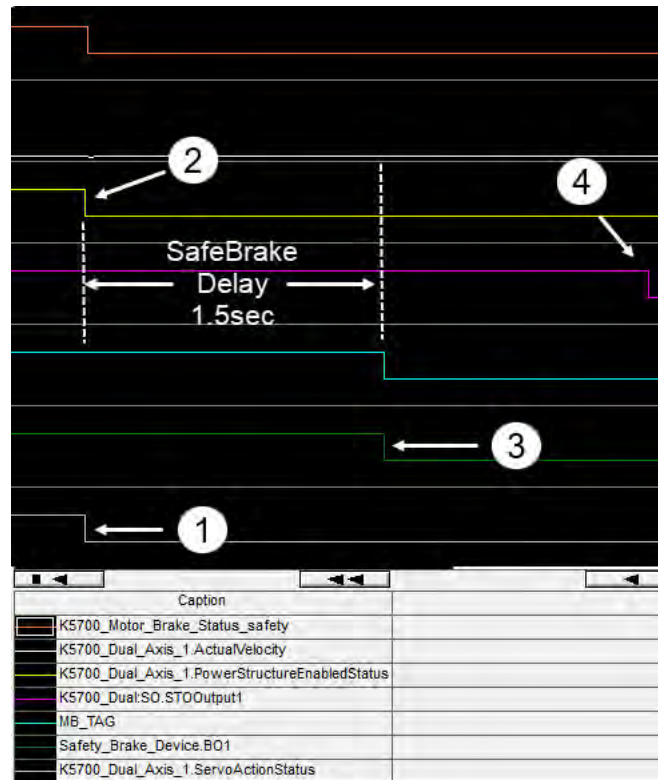
1. The Disable command is received and the ServoActionStatus transitions from high (1) to low (0).
2. The Disable & Coast Action is used, and the motor is disabled immediately. This shows the motor coasting to zero speed. This would not happen, as the Safety Brake would engage the load at Step 5 and stop the motion. This is shown so you can see that this case counts against the maximum actuation cycles value because the motor speed was non-zero when the safety brake was applied.
3. The MBRK output is low (0).
4. The MB_Tag is low (0).
5. The SBC.B01 output is low (0) (B01/B02 outputs are low (0)). The safety brake is engaging.
6. The STO output is low (0) after the STO -> SBC Delay expires.

Non-Typical Disable (SafeBrakeDelay used)

IMPORTANT The SafeBrakeDelay delays the engagement of the safety brake.

Consider that during a Non-Typical Disable that results in a Disable & Coast action (for example, a Major Fault), the secondary brake engagement (or even if the secondary brake would fail) could potentially result in a load that drops until the secondary brake engages or drops until the safety brake is engaged (that is, when the SafeBrakeDelay expires). The SBC instruction is triggered by the MBRK output.

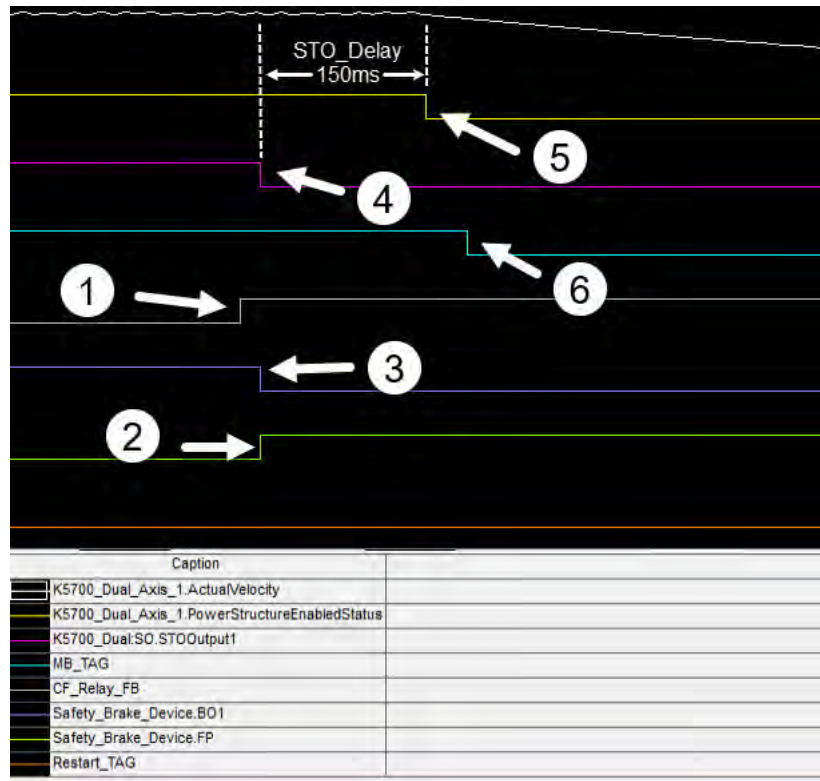
IMPORTANT While there are useful cases for the SafeBrakeDelay to be non-zero, if using the SafeBrakeDelay and delaying the safety brake engagement creates an unacceptable risk, the SafeBrakeDelay should not be used. In that case, SafeBrakeDelay should be zero.



1. The Disable & Coast condition is high (1).
2. The motor power is removed, because this is a Disable & Coast condition.
3. The SBC.B01 output is low (0) (B01/B02 outputs are low (0)) and the safety brake engages. This is the point at which the secondary braking system is engaged; however, the load could drop based on the amount of time it takes to engage the secondary braking system.
4. The STO output is low (0) after the STO -> SBC Delay expires.

Safe Brake Control - Instruction Fault Present

This example shows the timing of a Fault Present (SBC.FP) in the Safe Brake Control Instruction. Because the instruction uses the STO to disable the motor, the STO Delay is used (the motor is still enabled when the STO is requested).



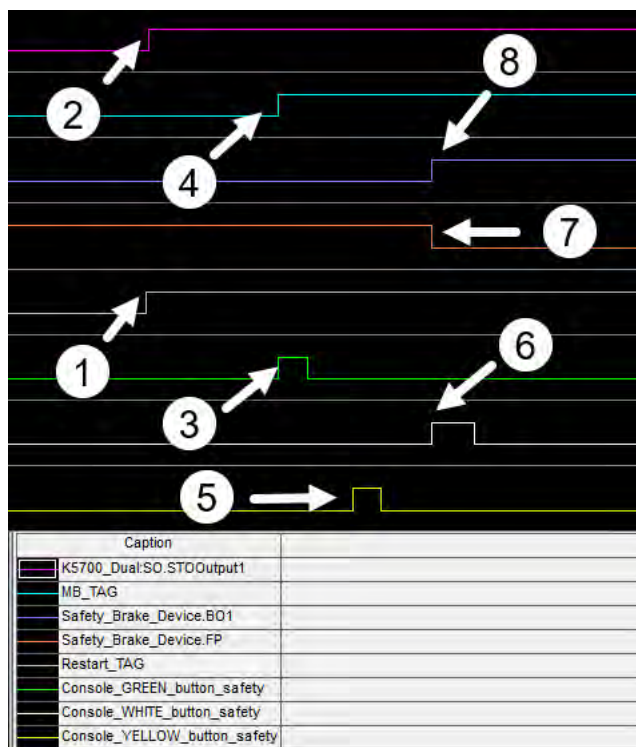
1. The SBC instruction faults because the CF_Relay_FB is shorted to 24V DC.
2. The SBC.FP is high (1).
3. The SBC.B01 (and B02) outputs are low (0). The safety brake is engaging. The Disable & Coast Action is used. This example shows the motor coasting to zero speed (white pen). This would not happen as the safety brake would engage the load at Step 3 and stop the motion. This is shown so you can see that this case counts against the maximum actuation cycles value because the motor speed was non-zero when the safety brake was applied.
4. The STO output is low (0).
5. When the STO_Delay expires, the motor is disabled.
6. The MB_TAG is low (0).

STO_Delay

Notice that in this case, the safety brake would engage the load before the motor is disabled. The purpose of showing the STO_Delay is that this delay can be useful depending on the time it takes to engage the safety brake. If this example were at zero speed, you could use this delay to leave the motor enabled until enough time has passed for the safety brake to physically engage. This case does not count against the maximum actuation cycles value because the motor speed was zero when the safety brake was applied.

Safe Brake Control - Fault Reset

This sequence is used to reset a fault on the Safe Brake Control.



1. The Restart_TAG is high (1) (Toggle Reset_SBC standard Input).
2. The STO_Output is high (1).
3. Press the Green_Console_Button (low (0) to high (1)). The motor is enabled.
4. The holding brake is released (MB_TAG is high (1)).
5. Press the Yellow_Console_Button (low (0) to high (1)). This makes the SBC.Brake Engage L transition from low (0) to high (1) and is required to Reset the SBC instruction.
6. Press the White_Console_Button (low (0) to high (1)).
7. The fault on the SBC instruction is cleared (high (1) to low (0)).
8. The SBC.BO1/BO2 are set high (1) on the SBC instruction.

Additional Resources

These publications contain additional information concerning related products from Rockwell Automation.

Resource	Description
GuardLogix 5580 and Compact GuardLogix 5380 Controller Systems Safety Reference Manual, publication 1756-RM012	Describes the GuardLogix 5580 and Compact GuardLogix 5380 controller system. Provides instructions on how to develop, operate, or maintain a controller-based safety system that uses the Studio 5000 Logix Designer application.
ControlLogix and GuardLogix 5580 Controllers User Manual, publication 1756-UM543	Provides information on how to install, configure, and program the GuardLogix 5580 controllers in the Logix Designer application.
CompactLogix and Compact GuardLogix Controllers User Manual, publication 5069-UM001	Provides information on how to install, configure, and program the Compact GuardLogix 5380 controllers in the Logix Designer application.
GuardLogix Application Instruction Safety Reference Manual, publication 1756-RM095	Describes the Rockwell Automation GuardLogix Safety Application Instruction Set. Also provides instructions on how to design, program, or troubleshoot safety applications that use GuardLogix controllers.
Kinetix 5700 Safe Monitor Functions Safety Reference Manual, publication 2198-RM001	Explains how the Kinetix 5700 drives can be used in up to Safety Integrity Level (SIL 3), Performance Level (PLe) applications. Describes the safety requirements, including PFH values and application verification information. Also provides information on how to configure and troubleshoot the Kinetix 5700 drives with safe-stopping and safe-monitoring functions.
Kinetix 5700 Servo Drives User Manual, publication 2198-UM002	Provides instructions on how to install, mount, and wire Kinetix 5700 power supplies, single-axis inverters, dual-axis inverters, and accessory modules. Also includes system configuration with the Studio 5000 Logix Designer application, and instructions on how to mount and wire the input for an iTRAK® power supply.
Vertical Load and Holding Brake Management Application Technique, publication MOTION-AT003	Provides an in-depth discussion on how to apply Kinetix drives in vertical load applications and how the servo motor holding-brake option can be used to help prevent a load from dropping. Features Kinetix motion control applications with Kinetix integrated motion on EtherNet/IP™ servo drives (Kinetix 5500, Kinetix 5700, Kinetix 6500, and Kinetix 350) and Kinetix VP and MP-Series™ servo motors.
Operating Instructions STOBBER motor adapter with brake MB, publication 44186_en_08_BAL_MB (STOBBER 441846/rev8/07-2018)	Provides instructions on how to operate the mayr brake.
Gravity-Loaded axes (Vertical Axes), DGUV website, https://www.dguv.de/medien/fb-holzundmetall/publikationen-dokumente/infoblaetter/infobl_englisch/005_vertical-axes.pdf	Describes measures for the improvement of occupational safety at vertical axes that are primarily suitable for application at systems that are intended to be put on the market.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, rok.auto/certifications .	Provides declarations of conformity, certificates, and other certification details.
Safety Automation Builder and SISTEMA Library website, rok.auto/sistema	Download Safety Automation Builder® to help simplify machine safety design and validation, and reduce time and costs. Integration with our risk assessment software provides you with consistent, reliable, and documented management of the Functional Safety Lifecycle. The SISTEMA tool, also available for download from the Safety Automation Builder page, automates calculation of the attained Performance Level from the safety-related parts of a machine's control system to (EN) ISO 13849-1.

You can view or download publications at rok.auto/literature.

Rockwell Automation Support

Use these resources to access support information.

Technical Support Center	Find help with how-to videos, FAQs, chat, user forums, and product notification updates.	rok.auto/support
Knowledgebase	Access Knowledgebase articles.	rok.auto/knowledgebase
Local Technical Support Phone Numbers	Locate the telephone number for your country.	rok.auto/phonesupport
Literature Library	Find installation instructions, manuals, brochures, and technical data publications.	rok.auto/literature
Product Compatibility and Download Center (PCDC)	Get help determining how products interact, check features and capabilities, and find associated firmware.	rok.auto/pcdc

Documentation Feedback

Your comments help us serve your documentation needs better. If you have any suggestions on how to improve our content, complete the form at rok.auto/docfeedback.

Safety Function Capabilities

Visit rok.auto/safety for more information on our Safety System Development Tools, including [Safety Functions](#).





Allen-Bradley, CompactLogix, ControlLogix, expanding human possibility, GuardLogix, iTRAK, Kinetix, MP-Series, POINT Guard I/O, POINT I/O, Rockwell Automation, Safety Automation Builder, SensaGuard, and Studio 5000 Logix Designer are trademarks of Rockwell Automation, Inc.

CIP Safety and EtherNet/IP are trademarks of ODVA, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Automation maintains current product environmental information on its website at rok.auto/pec.

Rockwell Otomasyon Ticaret A.Ş. Kar Plaza İş Merkezi E Blok Kat:6 34752, İçerenköy, İstanbul, Tel: +90 (216) 5698400 EEE Yönetmeliğine Uygundur

Connect with us.    

rockwellautomation.com ————— expanding **human possibility**[™]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SAFETY-AT178C-EN-P - February 2021

Supersedes Publication SAFETY-AT178B-EN-P - November 2020

Copyright © 2021 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.