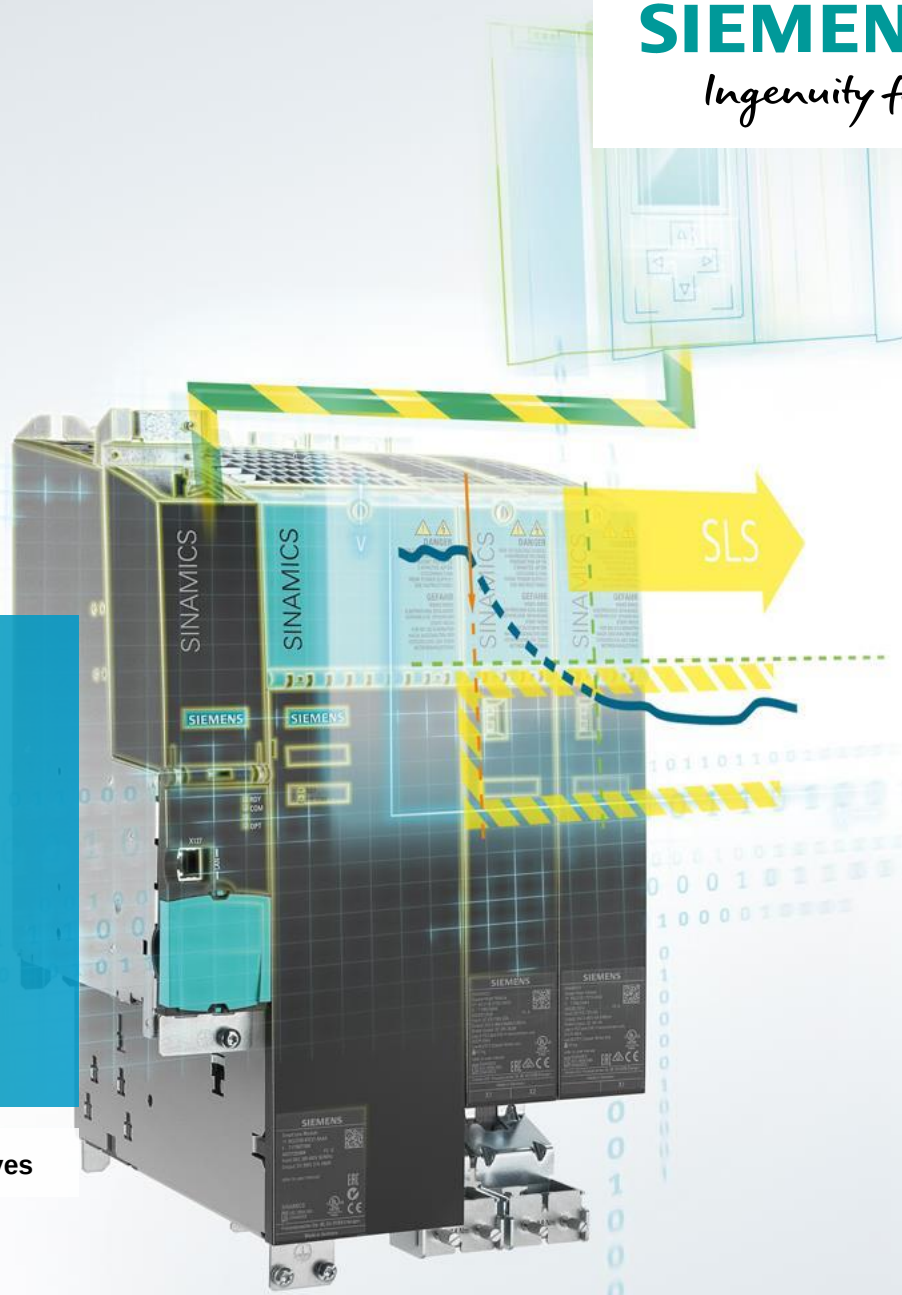
SIEMENS
Ingenuity for life

SINAMICS
Safety Integrated
Technical slides

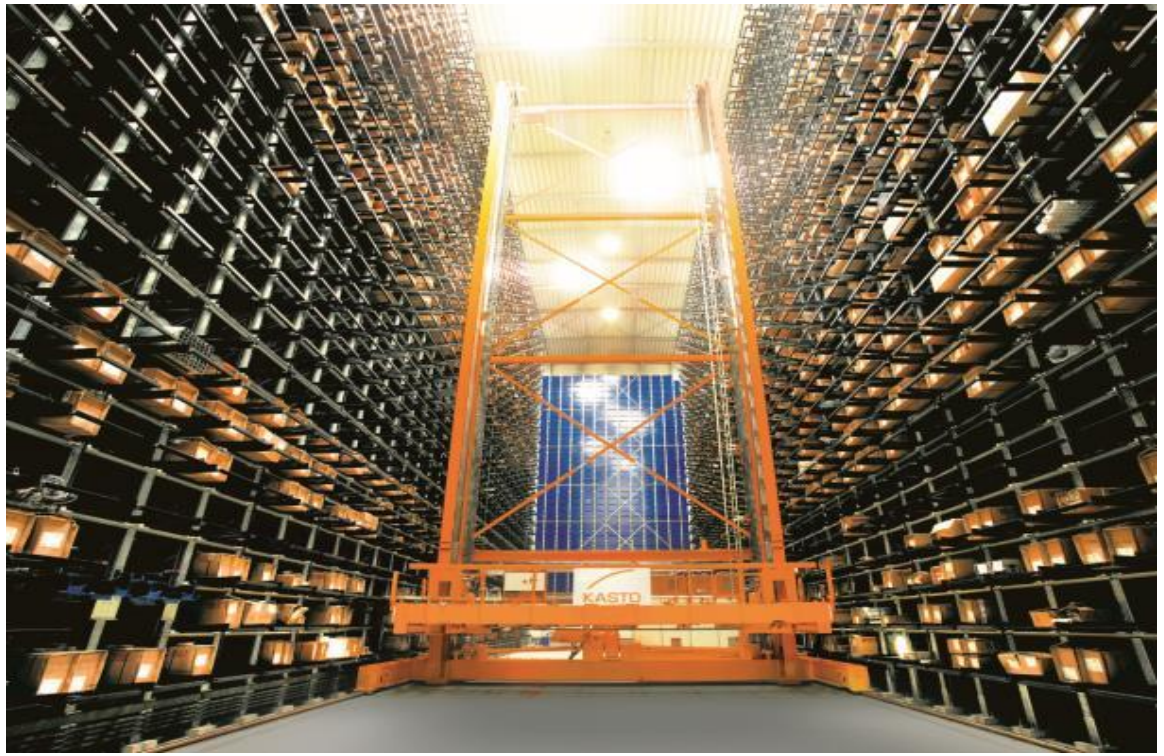


siemens.com/safety-drives

Dlaczego Safety Integrated

Dlaczego safety?

Everywhere, where...



Przewaga funkcji zintegrowanych SINAMICS Safety Integrated

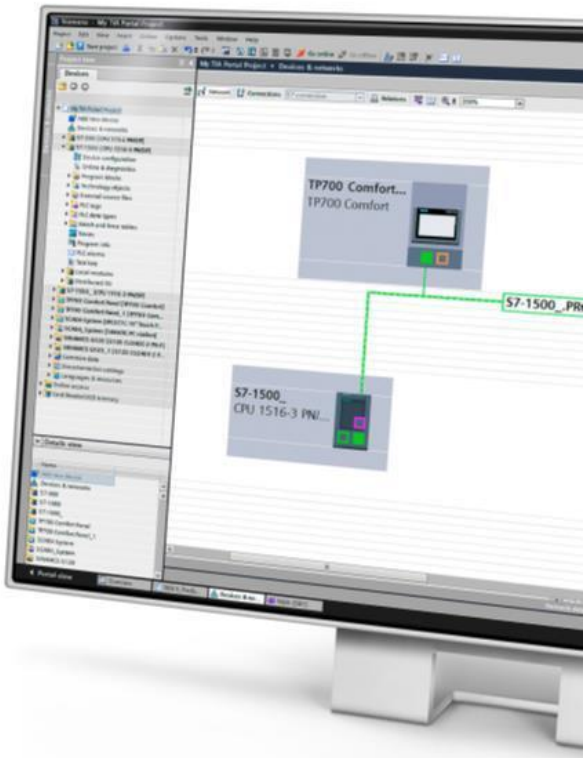
- Wysokie możliwości konfiguracyjne z krótkimi czasami reakcji
- Uproszczona weryfikacja bezpieczeństwa maszynowego zgodnie z ISO 13849 and EN 62061
- Brak dodatkowych komponentów (styki, przekaźniki bezpieczne, itp.)
- Niskie koszty kablowania
- Wysoka elastyczność: dopasowanie funkcyjne do przyjętej koncepcji sterowania
- Wysoka niezawodność: Brak styków elektromechanicznych
-

Zgodność z normami

- IEC 61508 **SIL 2**
- EN ISO 13849-1 **Cat. 3** and **PL d**

Rodzina napędów SINAMICS w TIA Portal:
Optymalny napęd dla każdej oraz wszystkich aplikacji

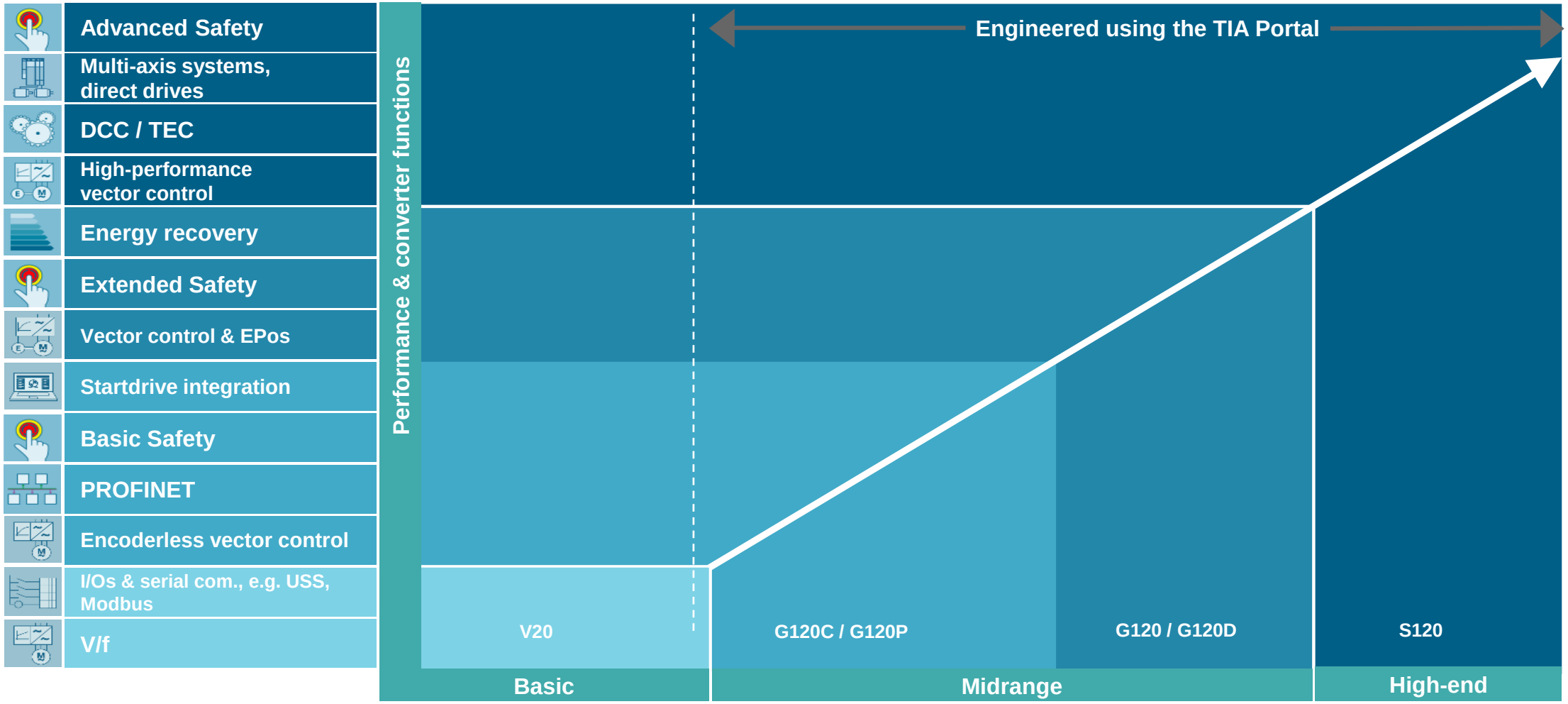
SINAMICS G120		Ogólne przeznaczenia, napędy do zabudowy oraz decentralnego sterowania IP65
SINAMICS V90		Podstawowy system servo
SINAMICS S210		System serwo z rozszerzonymi funkcjami Safety Integrated, prostym uruchomieniem, wysoką dynamiką oraz precyzją sterowania
SINAMICS S120		Wieloosiowy najbardziej zaawansowany układ napędowy: elastyczny, modułowy, szeroki zakres mocydo zastosowań w aplikacjach high-performance



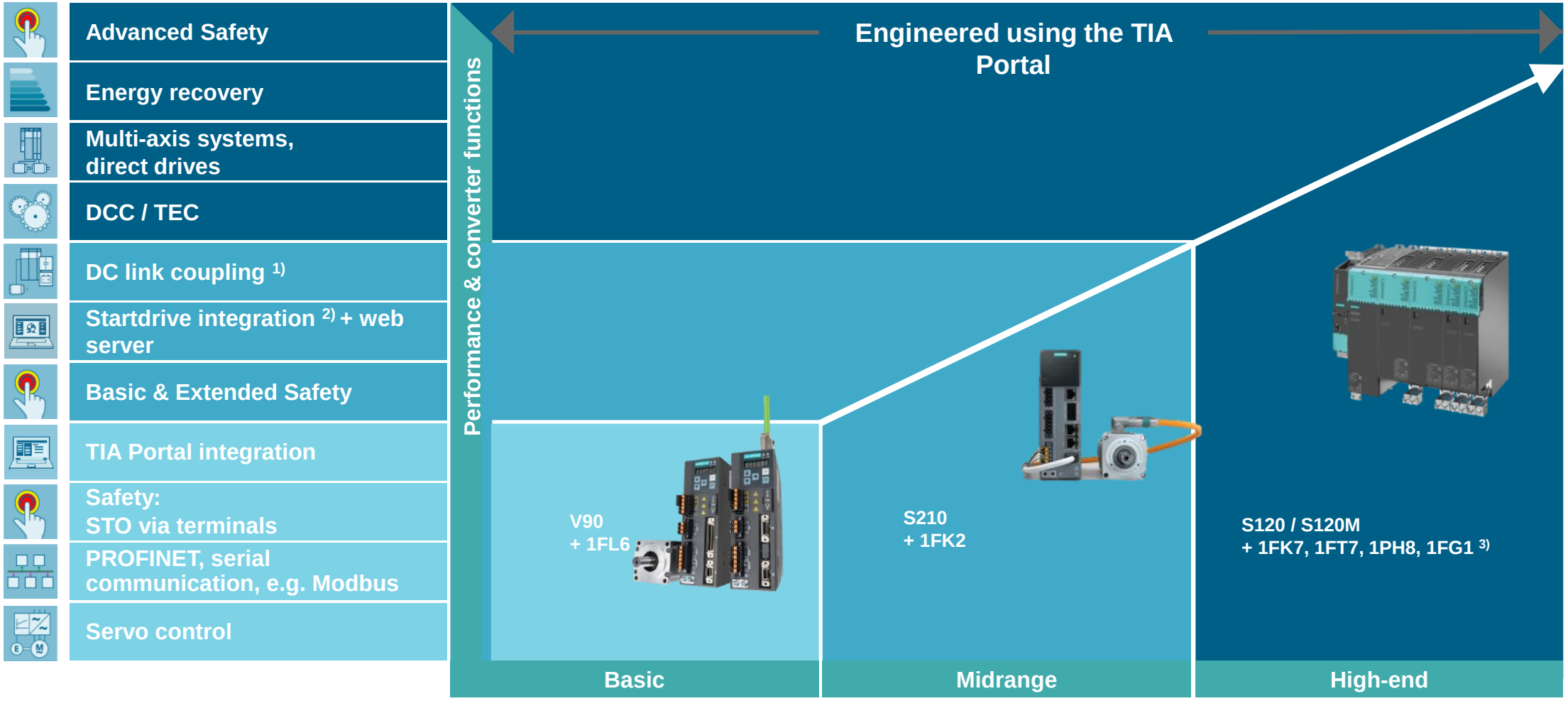
Rodzina napędów SINAMICS w TIA Portal:
Optymalny napęd dla każdej oraz wszystkich aplikacji

		Integracja i uruchomienie						Sterowanie		
		GSDML	Startdrive	HSP	Webserver	Starter	V-Assistant	SIMATIC TO	DriveLib	Standalone
SINAMICS G120		✓	✓		✓	✓		✓	✓	✓
SINAMICS V90		✓		HSP with S7-1500			✓	✓	✓	✓
SINAMICS S210		✓	V15 .1		✓			✓		
SINAMICS S120		✓	✓		✓	✓		✓	✓	✓

SINAMICS dla aplikacji standardowych
Wektor/skalar

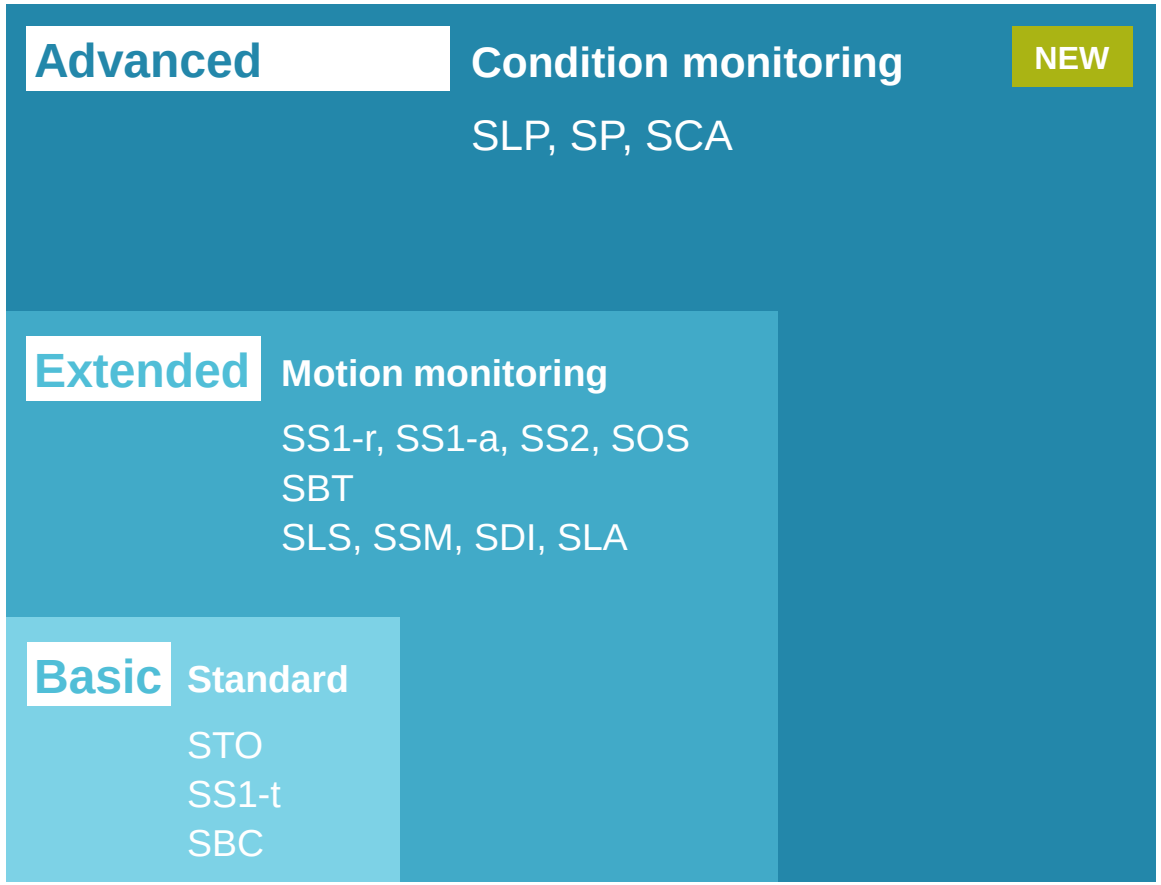


SINAMICS dla aplikacji serwo



1) Only 400V devices 2) as soon as a complete S210 product portfolio is available, E2018 3) + additional SIMOTICS

SINAMICS S120
Extended Safety FW ≥ V5.1



Safety Integrated Advanced Functions is the new license for position monitoring functions and additional functions (e.g. SLT)

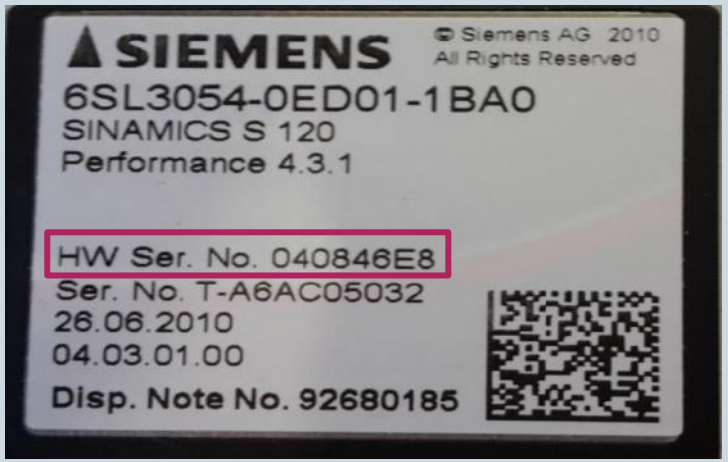
SINAMICS	
License, Extended Safety for memory card (F01)	6SL3074-0AA10-0AA0
License, Advanced Safety for memory card (A01)	6SL3074-0AA20-0AA0

SIMOTION (same concept as for SINAMICS)	
License, Extended Safety for memory card (F01)	6AU1820-2AF20-0AB0
License, Advanced Safety for memory card (L01)	6AU1820-2AG20-0AB0

SS1-t: time controlled
SS1-a: acceleration controlled
SS1-r: ramp controlled

SINAMICS S120
Karta CF – Licencje Safety

CF card



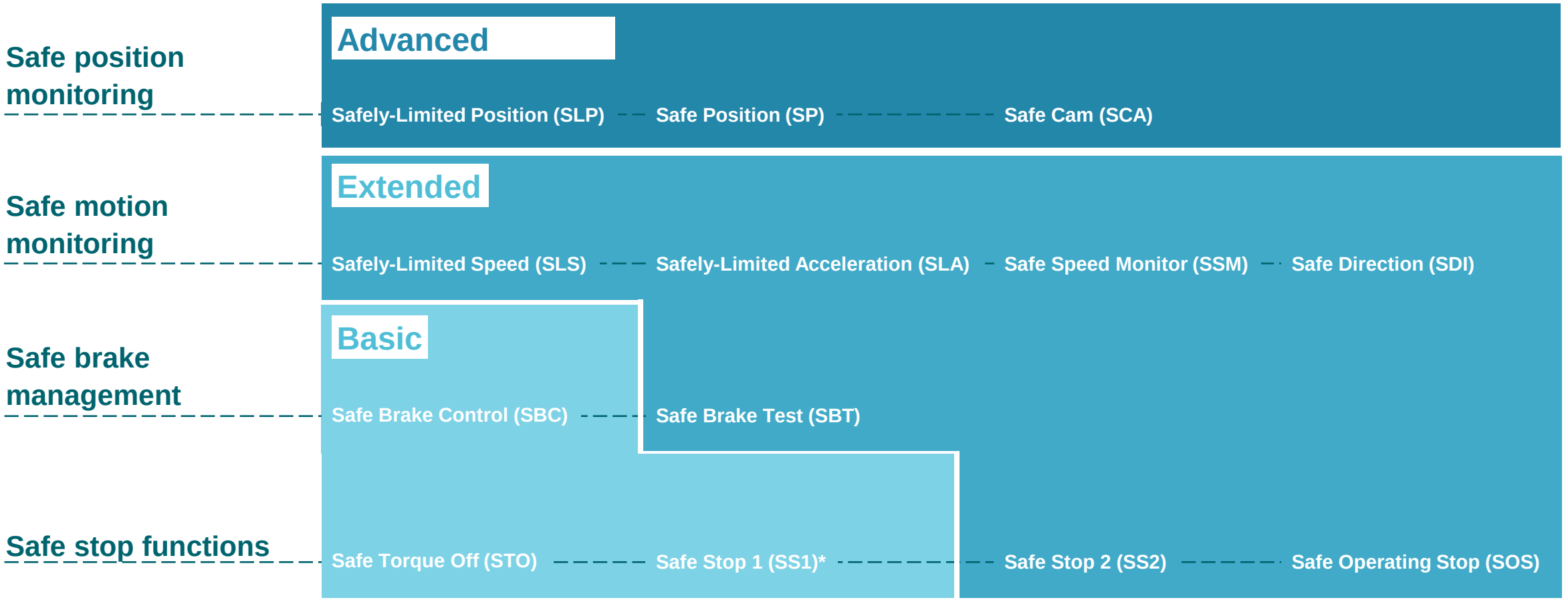
- Licenses are permanently assigned a CF card via a hardware serial number:

  ▶ **http://www.siemens.com/automation/license**

- License key is entered via the expert list of the CU (p9920)
- Due to the assignment to the specific hardware, licenses cannot be directly transferred to another CF card -> you must contact Siemens Support (hardware numbers of the old/new card, Certificate of License must be specified)

Przegląd funkcji bezpieczeństwa

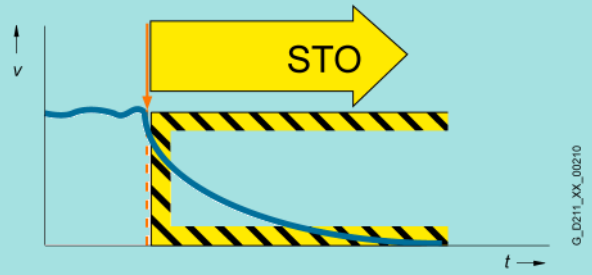
Przegląd zgodnie z EN 61800-5-2
Funkcje spełniające standardy: SIL 2, Cat. 3 oraz PL d



SBT and SP go beyond the scope laid down in standard EN 61800-5-2.
*SS1 is available from the Basic Functions; additional differentiations are possible in SS1–t; -a -r

Safe stop functions
Safe Torque Off (STO)

Function



- Prevents torque-generating energy from being supplied to the motor
- Protects against automatic restart
- Fast restart is possible as the DC link remains charged

Application

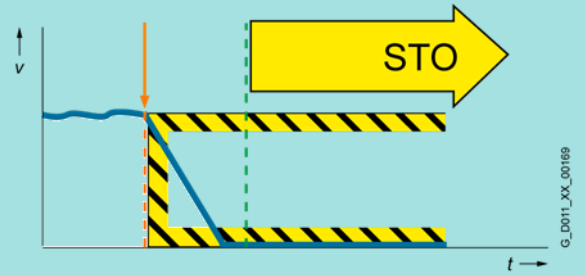
Can be used in all plants, machines and systems with moving axes, e.g. conveyor technology

Customer benefits

- Allows work to be safely carried out with the protective door open (restart inhibit)
- Classic Emergency Stop with electromechanical power disconnection not required
- No wearing parts as shutdown is purely electronic
- The converter remains connected to the line supply – and can still be fully diagnosed

Safe stop functions
Safe Stop 1 (SS1)

Function



- The drive is electrically braked when SS1 is initiated
- This is followed by the torque-generating energy being safely shut down (STO)

Application

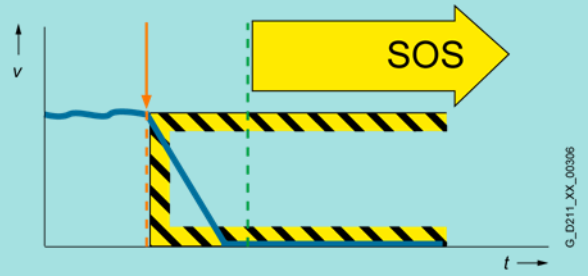
Fastest possible, safe braking of high inertia loads, e.g. saws, winders

Customer benefits

- Reduced stress on mechanical brakes as a result of the electrical braking
- Various versions (SS1-t,SS1-a,SS1-r)
- Complete drive group stopped in synchronism (SS1E)

Safe stop functions
Safe Stop 2 (SS2)

Function



- The drive is electrically braked when SS2 is initiated
- This is then followed by safe standstill monitoring (SOS)

Application

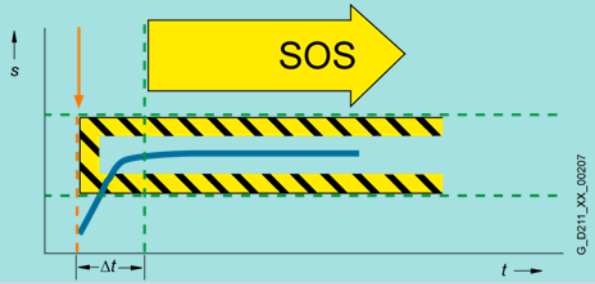
The axis is safely stopped, and the standstill position is monitored, e.g. for machine tools

Customer benefits

- Reduced stress on mechanical brakes as a result of the electrical braking
- The drive remains in closed-loop control, and can resist external forces with the maximum torque available to it

Safe stop functions
Safe Operating Stop (SOS)

Function



- Safe standstill monitoring
- The higher-level motion controller still issues the setpoint (e.g. S7-1500TF)
- The stop response SS1 (STOP B) is initiated when the standstill tolerance is exceeded

Application

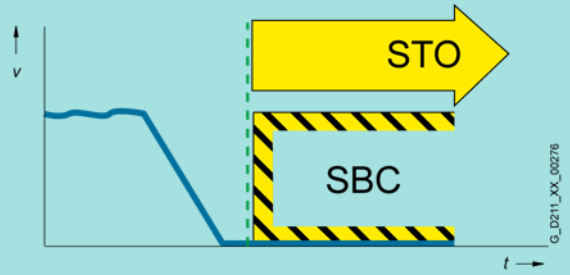
For applications where machine parts must be kept safely at standstill, and a holding torque is required – e.g. for suspended loads

Customer benefits

- The drive remains in closed-loop control, and can resist external forces with its maximum torque
- The number of cycles can be increased as the axis reference is maintained and the drive holds the current position
- A drive group can be stopped in a coordinated fashion

Safe brake management
Safe Brake Control (SBC)

Function



- Brakes that operate according to the closed-circuit principle can be safely controlled
- SBC is firmly coupled to STO

Application

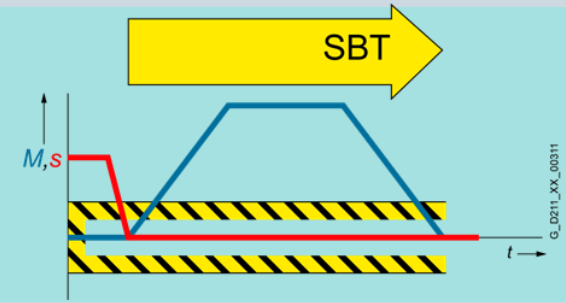
For applications where a safe position must be maintained, even when the motor is in a quiescent current state, e.g. for vertical axes

Customer benefits

- Prevents suspended loads from sagging/falling
- No external logic or additional switching elements required
- Faults in the brake control are identified

Safe brake management
Safe Brake Test (SBT)

Function



- Mechanical brakes can be functionally tested by establishing a torque against a closed brake
- Two brakes for each motor can be tested with various torques

Application

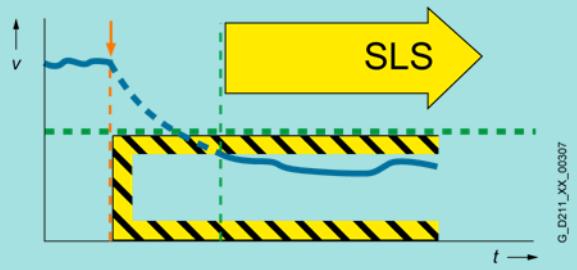
For applications where the brake is implemented in conjunction with SBC, e.g. cranes and presses

Customer benefits

- Can be used for external as well as for motor brakes
- Faults and wear in the brake mechanics can be identified
- Lower maintenance costs by automatically testing the brake
- Increased safety and availability of the machine

Safe motion monitoring
Safely-Limited Speed (SLS)

Function



- Safe speed monitoring
- Four SLS levels can be switched over
- Variable SLS limit values can be specified via PROFIsafe (S120)
- When the speed is exceeded, a parameterizable stop response can be initiated

Application

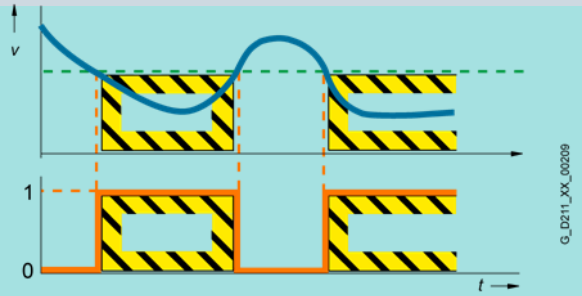
- For setting-up operation and monitoring a maximum speed
- The speed limit is continuously tracked as a function of the diameter of the material being wound

Customer benefits

- Work can be directly carried out at the machine while it is operational,
  in the setting-up mode or when carrying out maintenance work.
- The maximum speed is safely restricted to protect the operator, the machine and the workpiece itself

Safe motion monitoring
Safe Speed Monitor (SSM)

Function



Safe feedback signal as to whether the drive speed is below a parameterizable speed

Application

For releasing a protective door in a safety-relevant fashion

Customer benefits

- Release to enter a machine using safety-relevant SSM feedback signal
- No additional hardware required

Safe motion monitoring
Safe Direction (SDI)

Function

- Safe direction of rotation monitoring
- The higher-level motion controller still issues the setpoint (e.g. S7-1500TF)
- For an incorrect direction of rotation, a parameterizable stop response can be initiated

Application

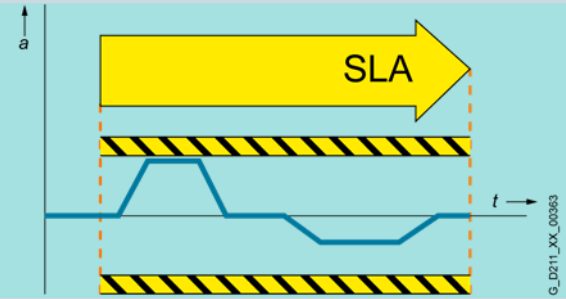
- For machines where material must be loaded or removed cyclically
- To protect against an inadmissible direction of rotation

Customer benefits

- This function increases the productivity as protective space for the operator can be enabled as soon as the operator moves the machine
- Prevents the machine from being mechanically damaged if moved in an impermissible direction

Safe motion monitoring
Safely-Limited Acceleration (SLA)

Function



- Safe acceleration monitoring
- When the acceleration is exceeded, a parameterizable stop response can be initiated

Application

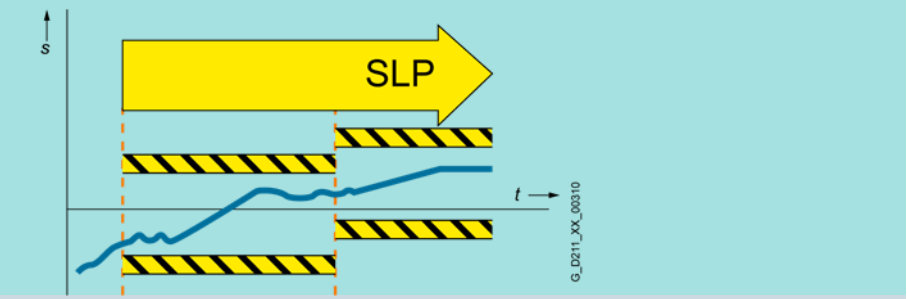
- For applications, e.g. in the setting-up mode, where a dangerous situation would occur if the motor were to accelerate uncontrollably
- SIMATIC Safe Kinematics

Customer benefits

- A maximum permissible acceleration level is monitored in the setting-up mode
- A tool center point is safely monitored for various kinematics

Safe position monitoring
Safely-Limited Position (SLP)

Function



- A position within a defined travel range is safely monitored
- A switchover can be made between two travel ranges
- A parameterizable stop response can be initiated when the travel range is exited

Application

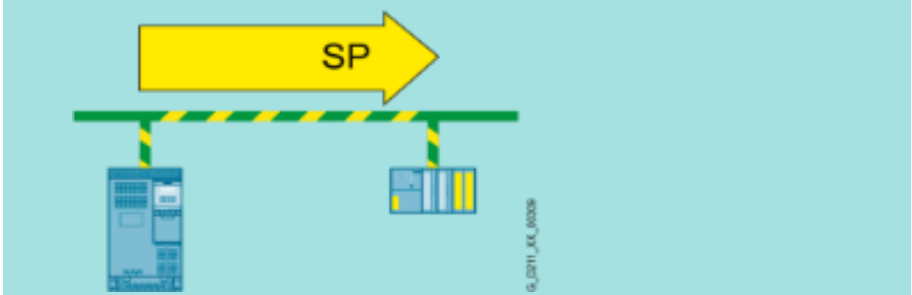
Can be used to secure travel ranges without using protective doors or protective measures – e.g. for gantry cranes and storage and retrieval machines

Customer benefits

- Safe software limit switches can be implemented
- Mechanical limit switches can be eliminated

Safe position monitoring
Safe Position (SP)

Function



Drive position actual values can be transferred via PROFIsafe in a safety-relevant fashion

Application

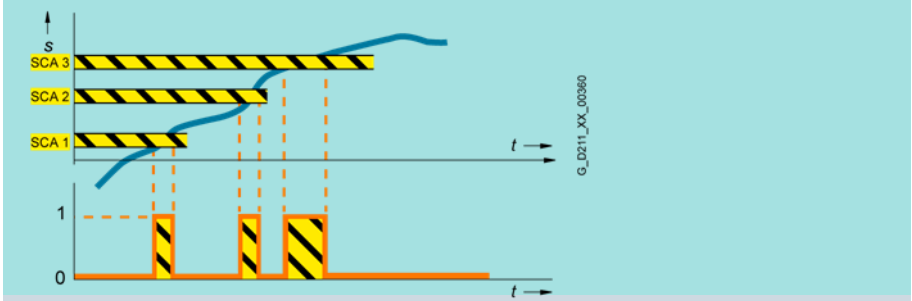
SIMATIC Safe Kinematics:
Can be used to implement zones and velocity monitoring in cartesian space

Customer benefits

- Can be flexibly used, e.g. for
  - Cam controllers
  - Safety concepts extending over several axes
  - Multi-dimensional protective areas and zone concepts
  - Different responses depending on the position of the axes
- Additional sensors and/or external encoders/transmitters can be eliminated

Safe position monitoring
Safe Cam (SCA)

Function



- Safety-related feedback signal as to whether the drive is positioned at a cam
- Up to 30 safety-relevant cams possible

Application

Monitoring for a specific position range, with corresponding application-specific response, e.g. to initiate a stop response and/or switch over to another SLS level

Customer benefits

- Safety functions are switched over in a safety-relevant fashion
- Electronic cam controllers can be implemented without requiring any additional hardware
- Implementation of safe range detection – work and protection zone demarcation

Summary

SINAMICS	STO	SS1	SS2	SOS	SBC	SBT	SLS	SLA	SSM	SDI	SLP	SP	SCA	Transfer F-DI
V90	✓													
G110M / G120C	✓													
G120 modular	✓	✓			✓ [2)]		✓		✓	✓				✓
G120D	✓	✓					✓		✓	✓				✓
S210	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
G130 / G150	✓	✓	✓ [1)]	✓ [1)]	✓ [3)]	✓ [1)]	✓ [1)]	✓ [1)]	✓ [1)]	✓ [1)]	✓	✓	✓ [1)]	
S120 / S150	✓	✓	✓	✓	✓ [3)]	✓	✓	✓	✓	✓	✓	✓	✓	✓ [4)]

[1)] Not actively marketed

[2)] Only possible with CU 250S-2 with Safe Brake Relay

[3)] For Chassis and Cabinet Modules with Safe-Brake Adapter, for Blocksize formats with Safe Brake Relay

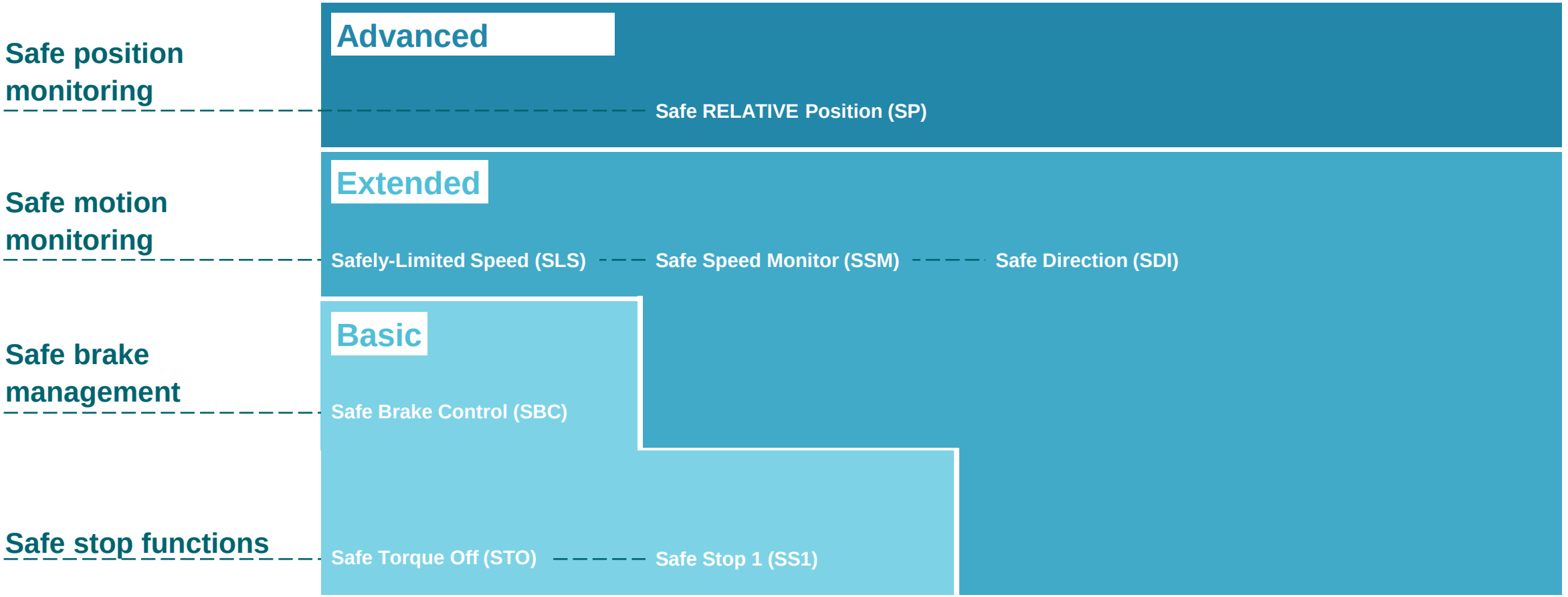
[4)] Only for CU310-2

Funkcje bezpieczeństwa z oraz bez enkodera

- Safety bez enkodera– S120
- Safety bez enkodera– G120
- Safety bez enkodera– informacje ogólne
- Safety z enkoderem

Safety bez enkodera S120

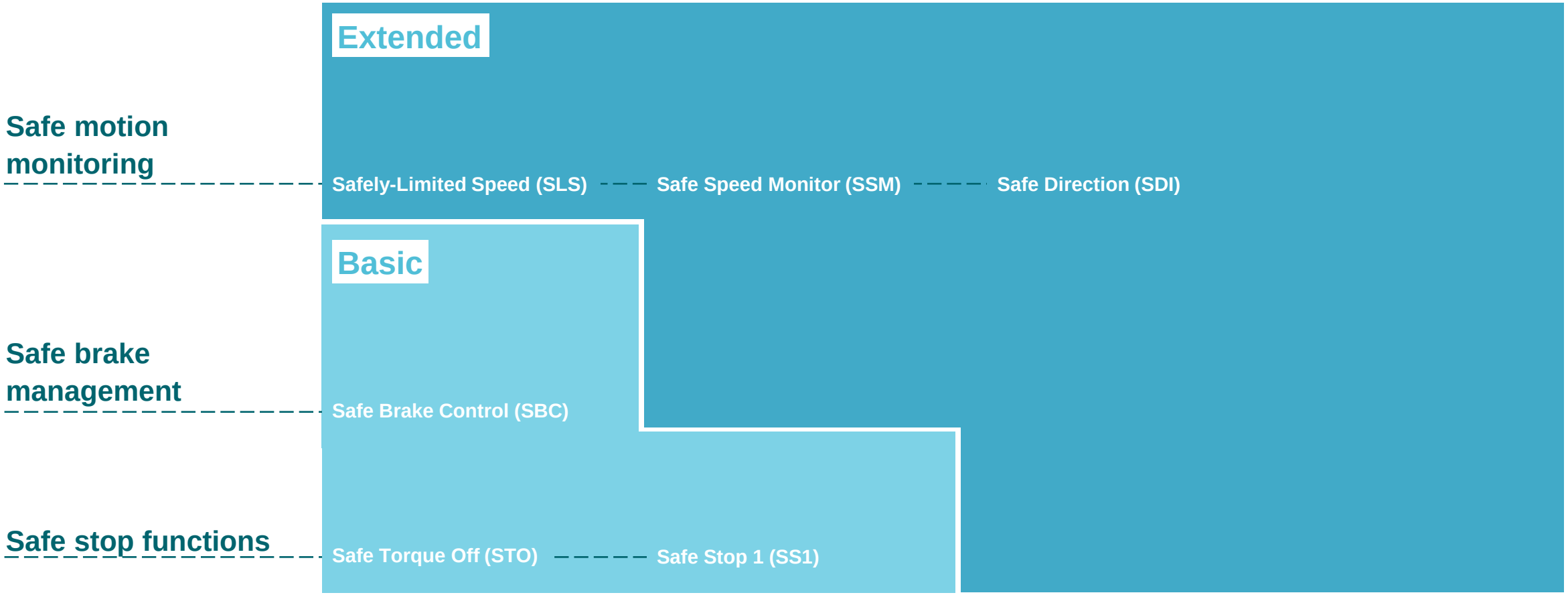
Safety functions without encoder – S120
Fulfills: SIL 2, Cat. 3 and PL d



SP goes beyond the scope listed in standard EN 61800-5-2

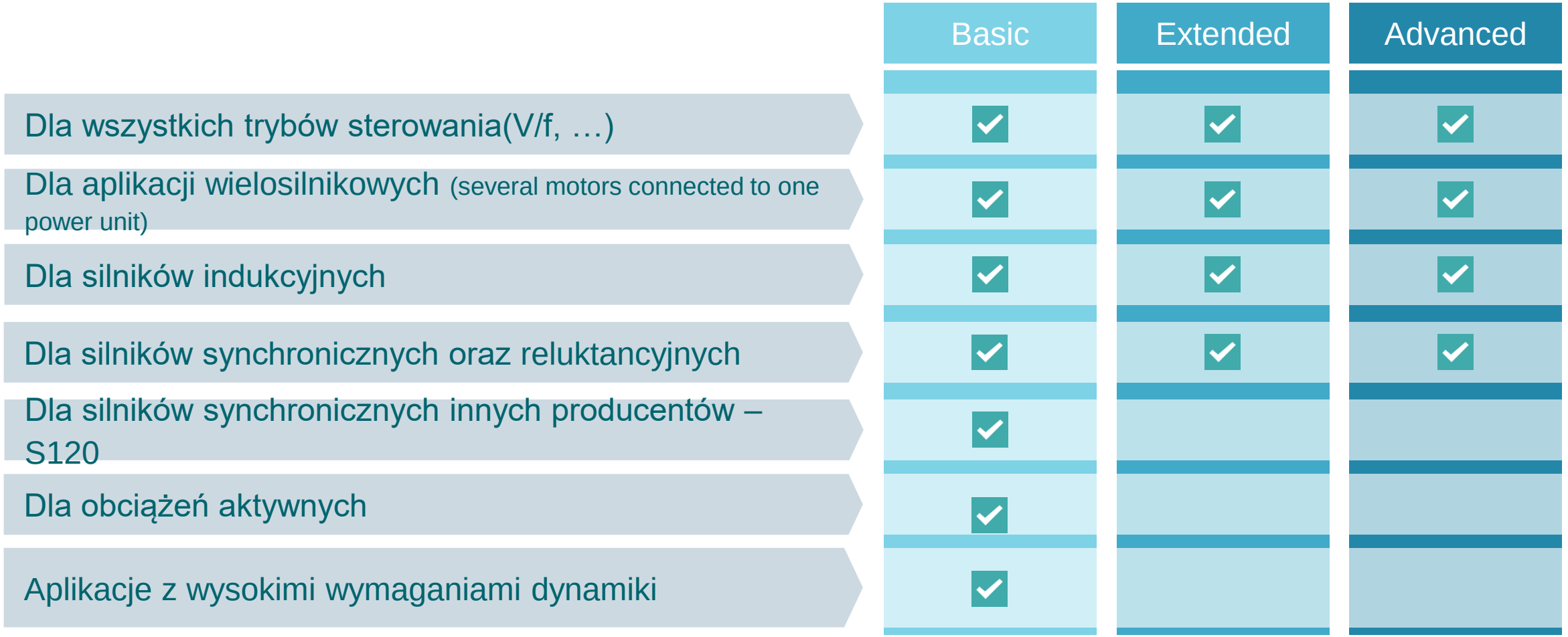
Safety bez enkodera G120

Safety functions without encoder – G120
Fulfills: SIL 2, Cat. 3 and PL d



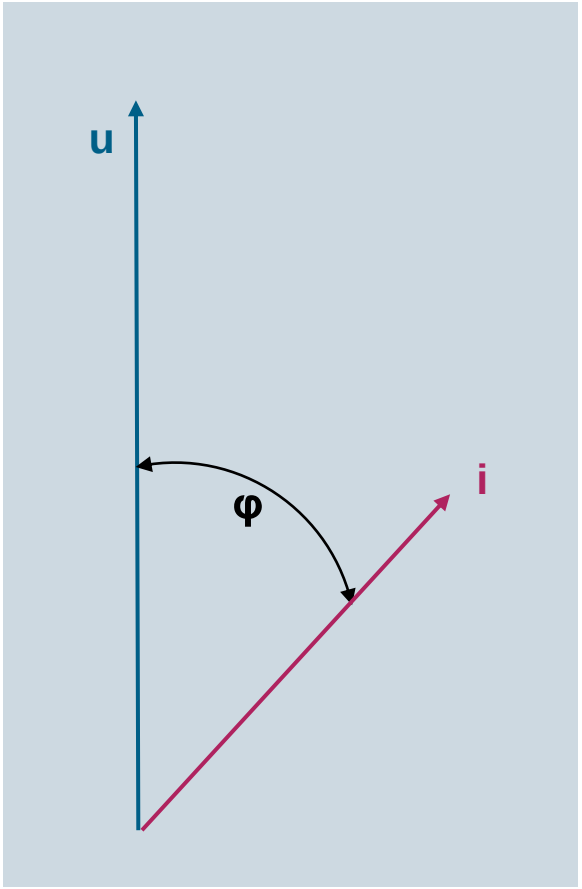
Safety bez enkodera– informacje ogólne

Informacje ogólne



[1] Only for S120

Informacje ogólne



Funkcje bezpieczeństwa bez enkodera

Działają na zasadzie estymacji – pomiar oraz obliczanie

- Prądu i
- Napiecia u
- Kąta φ

Obliczenie w sposób bezpieczny aktualnej prędkości silnika

- **Monitoring minimalnej wartości prądu**
  W trybie załączenia wartość minimalna prądu musi płynąć w torze silnikowym
- **Monitoring przyspieszenia**
  Nie jest dozwolone przekroczenie maksymalnej wartości przyspieszenia
- **Monitoring kąta**
  Rejestrowanie przesunięcia kątowego pomiędzy prądem a napięciem fazowym

Informacje ogólne

Wpływ negatywny

- Piki prądowe, nie stabilność ciągłości sygnału prądowego
- Piki napięciowe
- Zakłócenia w sygnałach pomiarowych prąd/napięcie
- Zbyt niskie wartości prądów wyjściowych bliskie 0 mA

Efekt

- Możliwość generowania błędów bezpiecznych
  (C1711, C30711, wartość błędu1040 ff)
- Powyższe nie wprowadza stanu niebezpiecznego – jednak generuje błędy co wpływa na prawidłową pracę urządzenia.

Reguła 5s

Reguła 5 sekund (Safety bez enkodera)

- Funkcja STO dla rodziny SINAMICS jest aktywowane wewnętrznie dla:
  - Blokada pulsów napędu (komenda ON) gdy aktywujemy funkcję Safety Extended / (przykładowo SLS)
  - Aktywujemy funkcję Safety Extended/Advanced i nie załączymy napędu do pracy w czasie 5 sekund (aktywacja funkcji safety przed załączeniem osi do pracy)
- Silnik jest załączany ponownie do pracy poprzez
  - Zaznaczenie oraz odznaczenie STO lub
  - Odznaczenie i ponowne zaznaczenie wybranej funkcji Extended/Advanced oraz
  - Ponowne załączenie napędu w czasie do 5 sekund
- Opis aplikacyjny

Terminal control (SIOS-ID 80561520)

Control via PROFIsafe (SIOS-ID 82526133)

Ograniczenia HW

Moduły mocy PM230

- Wspierają częściowo funkcje Safety Integrated
- STO w połączeniu z właściwą jednostką sterującą CU (przykłaowo CU240E-2)

Moduły PM240 wielkość GX

Wyłącznie **STO**, **SBC** oraz **SS1**

Ograniczenia

Praca z aplikacjami aktywnymi

- Basic Safety Functions
- Extended Safety Functions w zależności od platformy:
- G120 – nie mogą być stosowane,
- S120 – po analizie systemu napędowego dopuszcza się stosowanie,

Ograniczenia

Lotny start

A flying restart should not be executed when safety functions are active.

Tip If a flying restart is required: Before the flying restart, deactivate the Safety Integrated Functions (with the exception of SSM) – and after the flying restart has been completed, reactivate them.

Note Carefully check as to whether it is permissible to deactivate the safety functions during the flying restart!

Ograniczenie prądu

When the power unit current limiting responds, it must be expected that the encoderless safety-relevant actual value sensing develops a fault condition and an associated stop response.

Note When engineering the drive and when parameterizing the current or torque limits, it should be carefully ensured that the power unit current limiting does not respond.

Ograniczenia

Hamowanie DC

This function involves braking using a DC current. This can result in the encoderless safety-relevant actual value sensing developing a fault condition and issuing an associated stop response.

Tip If it is crucial that a DC brake is used: Before activating the DC brake, deactivate the Safety Integrated Functions (with the exception of SSM) – and then reactivate them.

Note Carefully check as to whether it is permissible to deactivate the safety functions while braking!

Identyfikacja silnika

When using the measurement functions (stationary and rotating measurement) to determine the motor data, it must be expected that the encoderless, safety-relevant actual value sensing issues a fault message.

Note The motor data identification routine should always be carried out before commissioning the Safety Integrated Functions.

Ograniczenia

DDS

- For safety functions without encoder, the motor and drive data set switchover can always be used. For several motor data sets, it must be ensured that all motors have the same number of pole pairs.
- Switching over between induction and synchronous motors is locked (i.e. not possible)

Generator rampy

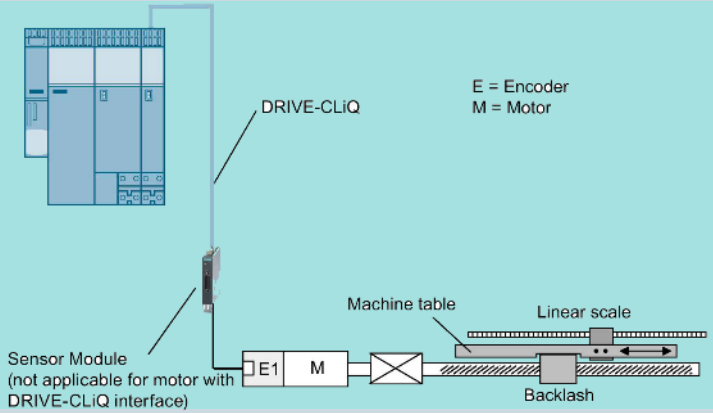
Only one acceleration ramp and braking ramp are permissible within one second.

Note Adjust the controller settings and profile so that no overshoot can occur in the speed characteristic.

Safety z enkoderem

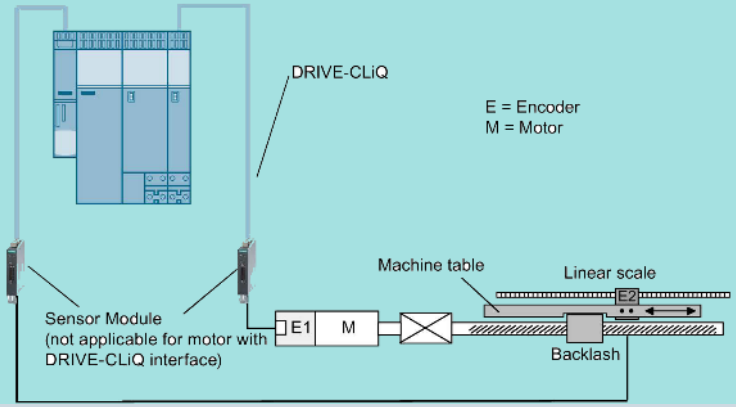
Dozwolone systemy pomiarowe

System jednoenkodrowy



Enkoder silnikowy

System 2 enkoderowy



Enkoder silnikowy oraz enkoder zewnętrzny

Wymagania

System 1 enkoderowy

- **Enkoder sin/cos** $1V_{pp}$
- Czysty sygnał **analogowy** (detekcja zamrożenia ścieżek A/B)
- **Integracja w** S120 poprzez:
  - DRIVE-CLiQ
  - SMC20
  - SME20/25
  - SME120/125
  - SMC40

System 2 enkoderowy

- **2 enkodery sin/cos** $1V_{pp}$
- **2 enkodery HTL lub TTL**
- **Integracja w** S120 poprzez:
  - SMC30
  - Wbudowane przyłącza CU310-2
  - CUA32
- Kombinacja enkoderów sin/cos oraz HTL lub TTL możliwa

Sterowanie funkcjami safety

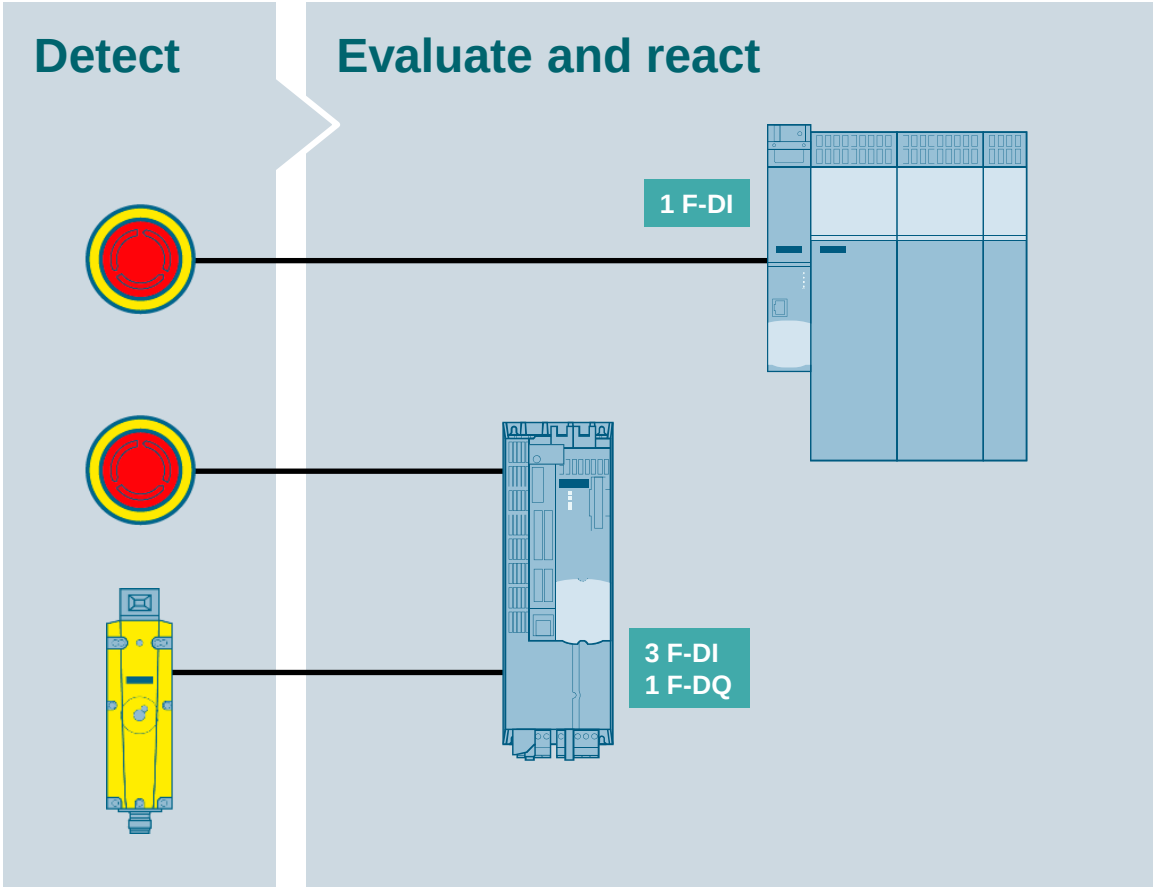
- S120
- S210
- G120
- PROFIsafe

S120

S120


Basic
Extended
Advanced
Wbudowane IO
Tylko CU310-2
Tylko CU310-2
PROFIsafe
TM54F
Tak, poza SLA
Tak, poza SCA
Zawsze aktywne/
bez wyboru
SLS, SDI

S120
Wbudowane IO



Wbudowane wejścia bezpieczne dla …

CU310-2: 3 F-DI / 1 F-DQ

CU320-2: 1 F-DI dla Basic Functions
1 kanał: wejście Control Unit
2 kanał: terminal EP modułu mocy/silnikowego

Cechy

- Zastosowanie przy konwencjonalnym wykonaniu aplikacji
- Dla małych instalacji
- Zdefiniowany sposób wykonania połączeń po stronie napędu

Przykład realizacji połączeń (SIOS-ID 39700013)

S120
TM54F

Onboard terminal for…

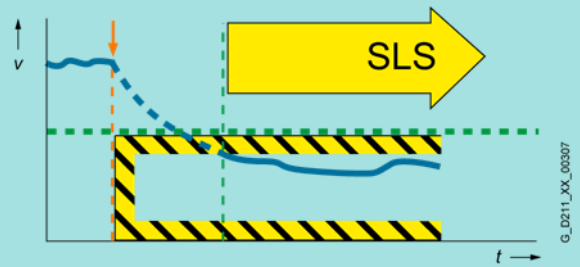
- Rozszerzenie IO bezpiecznych dla platformy S120:
- 10 F-DI and 4 F-DQ
- F-DI są parametryzowane jako NC/NC lub NC/NO
- Komunikacja z CU320-2 poprzez DRIVE-CLiQ
- Zasilanie z dynamiczną odpowiedzią

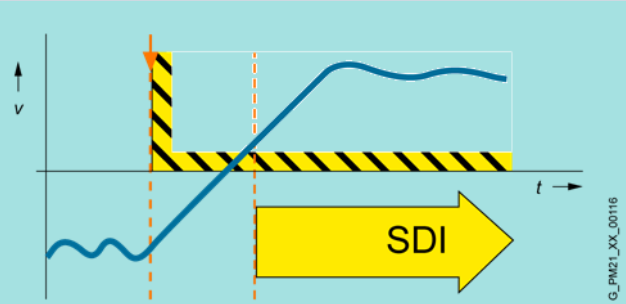
→ Pozwala na bezpieczne testowanie podłączonych sygnałów
(test stop F-DI oraz F-DQ)

▶ Connection examples (SIOS-ID 39700013)

S120
Bez aktywacji – wybrane ciągle

Permanentnie aktywne





Sterowanie poprzez F-DI oraz PROFISAFE nie jest wymagane

Cechy

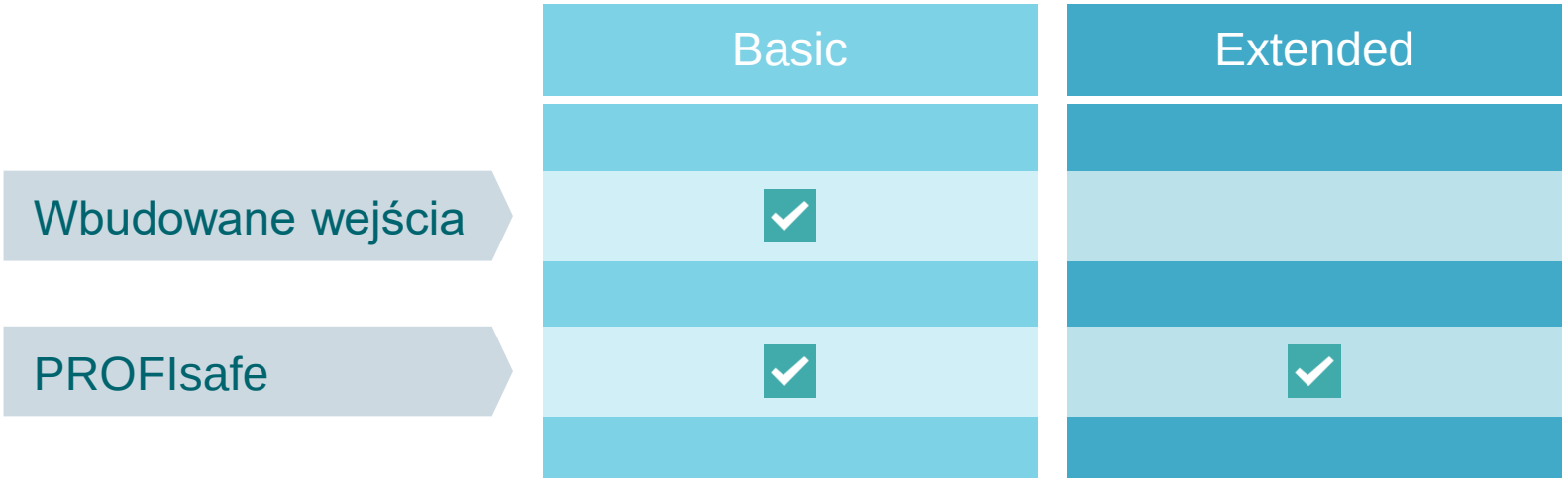
- Swobodnie parametryzowana reakcja zatrzymania na przekroczenie ustawionego limitu
- Dedykowane dla bezpieczeństwa z oraz bez enkodera

Przykłady zastosowań

- Monitoring maksymalnej prędkości
- Zwolnienie tylko jednego kierunku ruchu

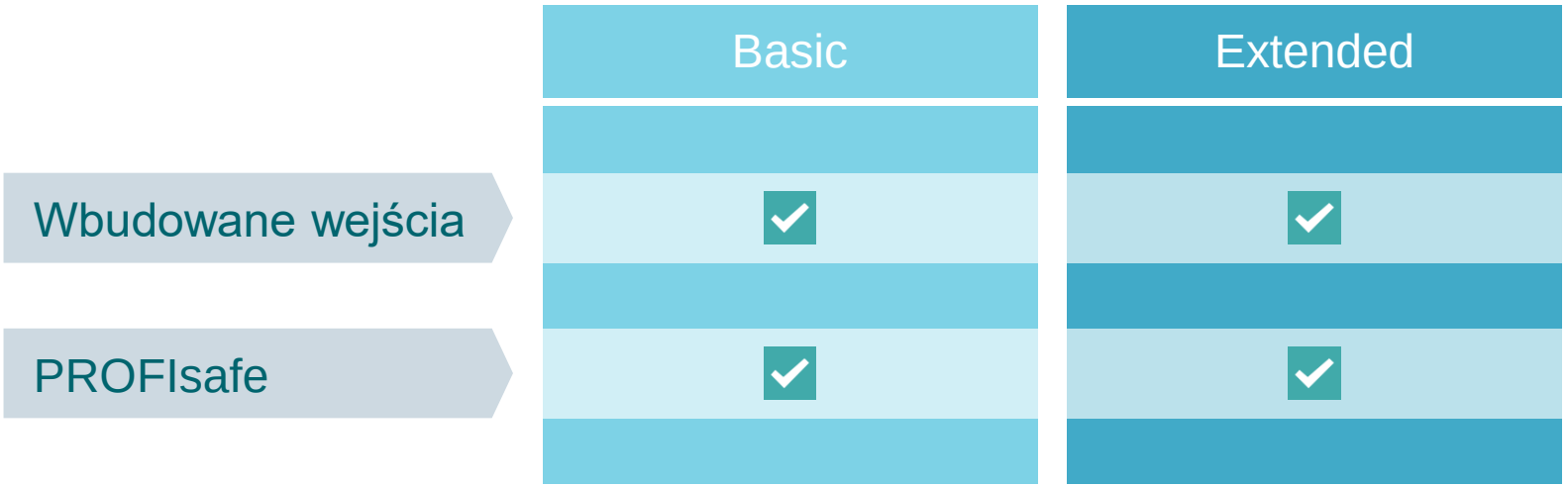
S210

S210



G120

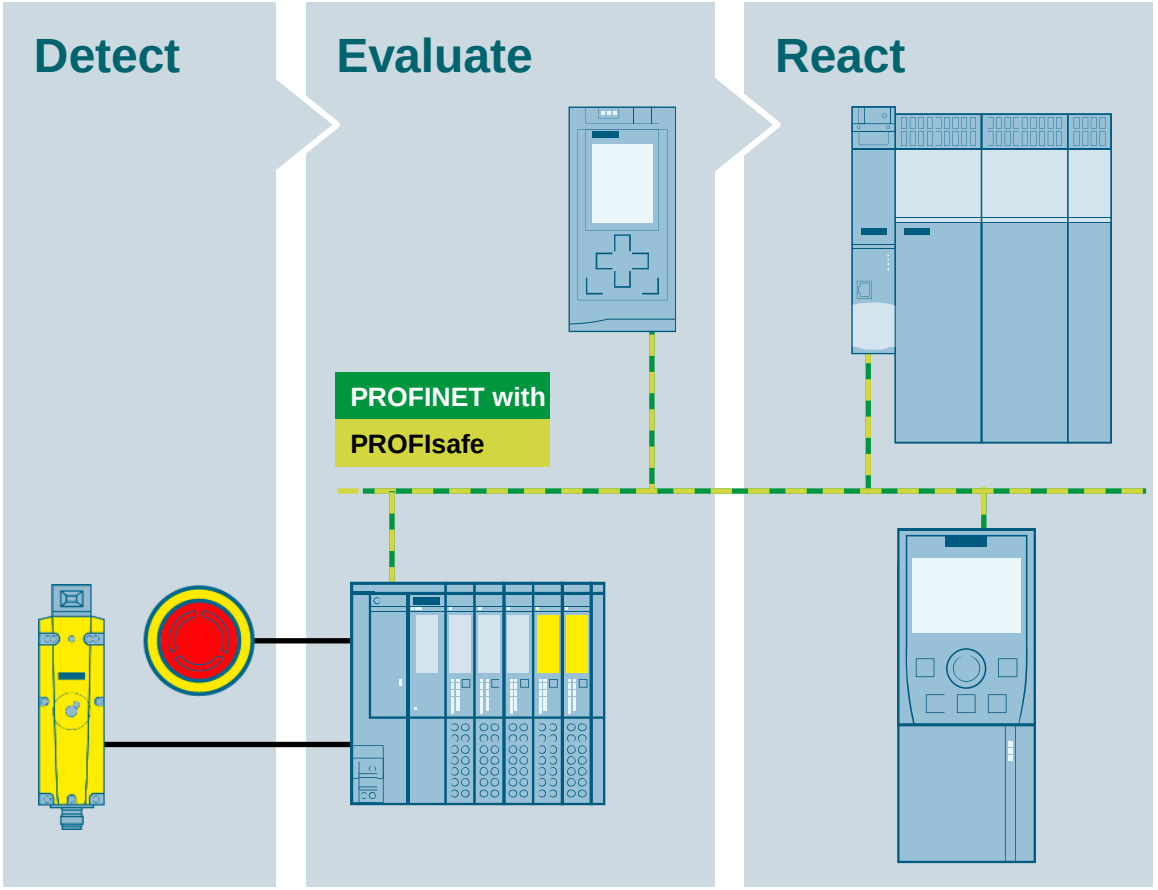
G120



W zależności od typu przekształtnika, jednostki sterującej, modułu mocy istnieje wiele restrykcji oraz opcji do sterowania funkcjami bezpieczeństwa.

Sterowanie poprzez PROFIsafe

PROFIsafe



Cechy

- Sekwencja sterowania realizowana po stronie F-PLC
- Komunikacja PROFIBUS/PROFINET
- Prosta integracja napędów w aplikacji – brak dodatkowego kablowania.

PROFIsafe
Telegram 30

PROFIsafe control word (S_STW1 in telegram 30)							
Byte 1							
7	6	5	4	3	2	1	0
Internal Event Ack	-	-	SLS	-	-	SS1	STO

Byte 0							
7	6	5	4	3	2	1	0
Internal Event Ack	-	-	SLS	-	-	SS1	STO

PROFIsafe status word (S_ZSW1 in telegram 30)							
Byte 1							
7	6	5	4	3	2	1	0
Internal event	-	-	SLS active	-	-	SS1 active	STO active

Byte 0							
7	6	5	4	3	2	1	0
Internal event	-	-	SLS active	-	-	SS1 active	STO active

2 bajty
kanał nadawania i odbioru

- S_STW1
  (safety control word 1)
- S_ZSW1
  (safety status word 1)

PROFIsafe
Telegramy bezpieczne

Telegram depending on the safety function	STO	SS1	SS2	SOS	SBC	SBT	SLS	SSM	SDI	SLP	SP	SLA	SCA	Transfer F-DI
30	✓	✓	✓	✓	Acts simultaneously with STO	Does not have to be controlled in a safety-relevant fashion	✓	✓	✓	✓		✓		
31	✓	✓	✓	✓			✓	✓	✓	✓		✓		✓
900	✓	✓					✓	✓	✓			✓		✓
901	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓		✓
902	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓		✓
903	✓	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓

PROFIsafe
Biblioteka LDrvSafe

Cechy

- Failsafe SIMATIC S7 library
  ▶ SIOS-ID:109485794

- Wsparcie programowe dla implementacji funkcji zintegrowanego bezpieczeństwa w środowisku TIA

Wymagania

- Hardware:
  S7-1200F/S7-1500F TIA Portal
- Software:
  SIMATIC STEP 7 Safety Advanced

Certified by the German Trade Association (subgroups wood and metal) (DGUV)
up to **SIL2** (DIN EN 62061) / **PL d**, **Cat. 3** (EN ISO 13849-1)

PROFIsafe
LDrvSafe

PROFIsafe control

S7-1200F / S7-1500F ✓

- Control words for all PROFIsafe telegrams
- Status words for all PROFIsafe telegrams

Winders

S7-300F / S7-1200F / S7-1500F ✓

- Failsafe sensing of the diameter
- Tracking the Safely-Limited Speed (SLS) limit as a function of the sensed diameter

Additional blocks

S7-1200F / S7-1500F ✓

- Safety Info Channel / Safety Control Channel
- Failsafe referencing for safety functions SP, SLP and SCA
- Acknowledging a hardware replacement after safety-relevant hardware has been replaced (e.g. Sensor Module)

PROFIsafe
LDrvSafe

- Osobne bloki dla słów sterującego roa statusowego dla telegramów PROFIsafe (30, 31, 900, 901, 902, 903)
- Dezaktywacja funkcji (sygnał wysoki) jako domyślny
- Struktura telegramu PROFIsafe mapowana do data type (F-UDT)
- Nie jest wymagana znajomość struktury telegramu w celu obsługi funkcji

Interaction between Safety Integrated and TO

Failsafe kwitowanie błędów

Bezpieczne kwitowanie błędów

Power ON

Wyłączenie/włączenie jednostki sterującej

Wbudowane F-DI

Poprzez zdefiniowane F-DI

PROFIsafe

Bit 7 pierwszego słowa sterującego PROFIsafe

Rozszerzone kwitowanie alarmu

Bezpieczne kwitowanie poprzez załączenie/wyłączenie STO – następnie wykonanie standardowego kwitowania

TM54F

Zdefiniowane F-DI modułu TM54F

Test stop

Podstawy

Cechy

- Zgodność z wymaganiami definiowanymi przez normy ISO 13849-1 oraz IEC 61508 (detekcja błędu w każdym wcześniejszym stanie)
- Test wewnętrznej ścieżki wyłączenia oraz funkcjonowania w celu zapewnienia prawidłowego działania
- Wykonanie przynajmniej raz w roku; częstotliwość realizacji testu uwarunkowana analizą ryzyka

Wymagania

- STO w trybie inicjalizacji; nie może być aktywne w momencie aktywacji test stop
- Dla modułów mocy PM, aktywacja w trybie postojowym - standstill

Przykładowe uwarunkowania czasowe aktywacji funkcji test stop

- Kiedy występują przestoje nieprodukcyjne
- Z zdefiniowanym rytmie czasowym – po każdej zmianie
- W trybie automatycznym, zależnym od czasu i okoliczności (w chwili otwierania drzwi ochronnych)

Test stop dla Basic Functions

Parametryzacja czasu aktywacji test stop

Przynajmniej raz w roku

Sterowanie funkcją test stop

- Aktywacja STO, SS1 lub
- Załączenie zasilania ON

Po przekroczeniu zdefiniowanego czasu

- Alarm na wyjściu "Motion monitoring functions must be tested"
- Funkcja test stop musi zostać ponownie wykonana

Test stop dla Extended i Advanced Functions

Parametryzacja czasu aktywacji test stop

Przynajmniej raz w roku

Sterowanie funkcją test stop

- Manualne: program, obsługa, ...
  - Wejście cyfrowe
  - Magistrala komunikacyjna
  - SCC (Safety Control Channel)
- Automatyczne: w chwili podania komendy załącz (tylko SINAMICS S120 oraz S210)

Po przekroczeniu zdefiniowanego czasu

- Alarm na wyjściu "Motion monitoring functions must be tested"
- Funkcja test stop musi zostać ponownie wykonana

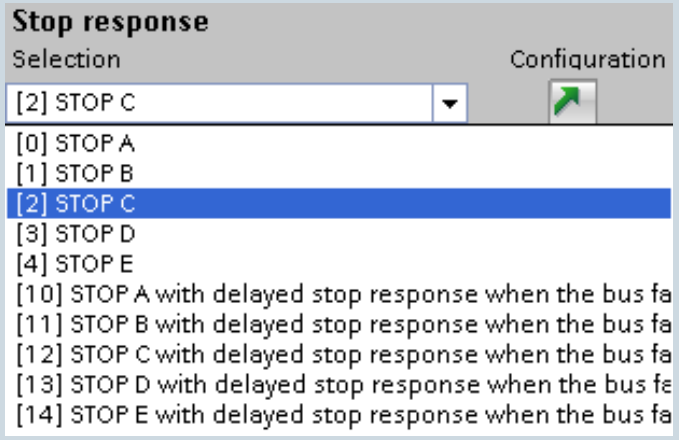
Szczegółowe informacje

- Stop response when a limit value is violated
- Safe Stop 1 (SS1)
- Safe Stop 2 (SS2)
- Safe Operating Stop (SOS)
- Safe Brake Control (SBC)
- Safe Brake Test (SBT)
- Safely-Limited Speed (SLS)
- Safe Speed Monitor (SSM)
- Safe Direction (SDI)
- Safe Position (SP)
- Safely-Limited Position (SLP)
- Safe Cam (SCA)
- Safe Referencing
- Safely-Limited Acceleration (SLA)

Stop response when a limit value is violated

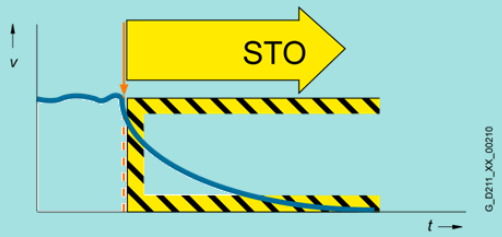
Stop response when a limit value is violated

Selecting the stop response



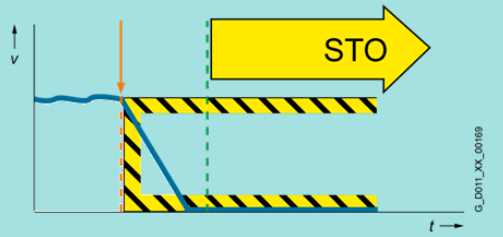
- STOP A to E
- STOP A to E – with delayed stop response when the bus fails

STOP A



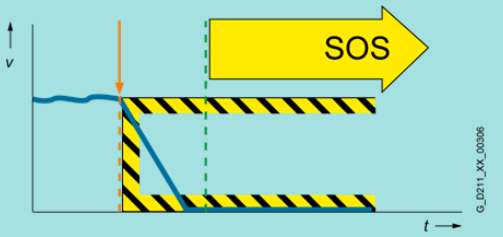
Corresponds to the selection of STO

STOP B



- Corresponds to the selection of SS1
- The parameterization of SS1-t, SS1-a, SS1-r or SS1E applies

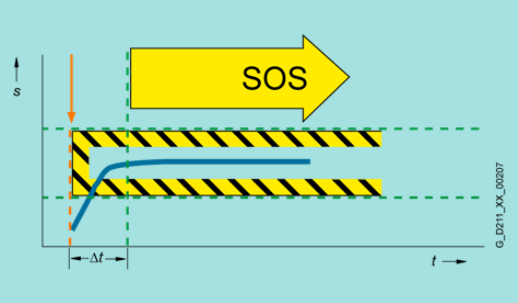
STOP C



Corresponds to the selection of SS2

Stop response when a limit value is violated

STOP D



Corresponds to the selection of SOS

STOP E

- Corresponds to the selection of SOS with separate delay time (p9554)
- Initiates drive function ESR (extended stop and retraction)
  = the drive independently retracts the axis, in the case of a fault, e.g. when a communication error occurs

With delayed stop response when the bus fails

Delays the stop response after a bus failure (STOP A or STOP B) by a maximum of 800 ms (p9697)

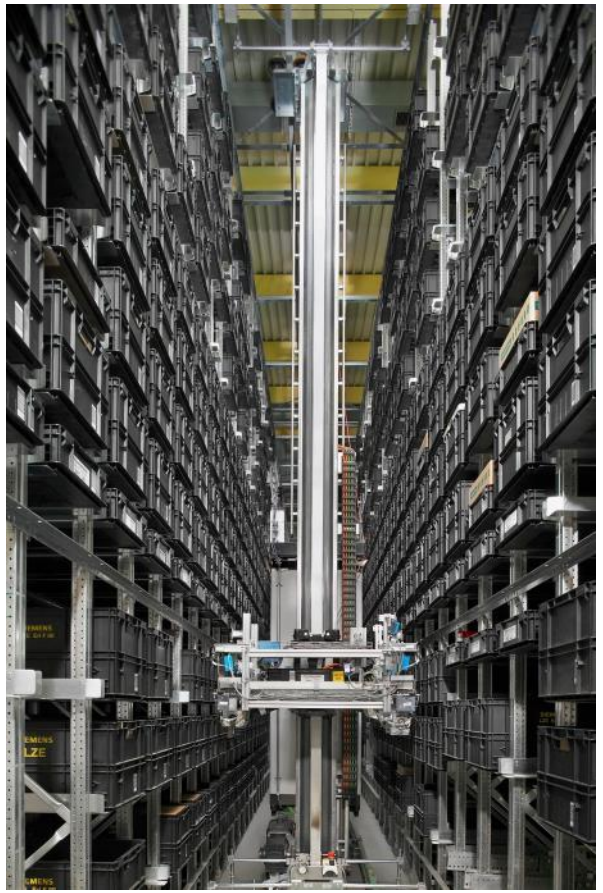
➔ Time window so that STOP E can be effective

Example

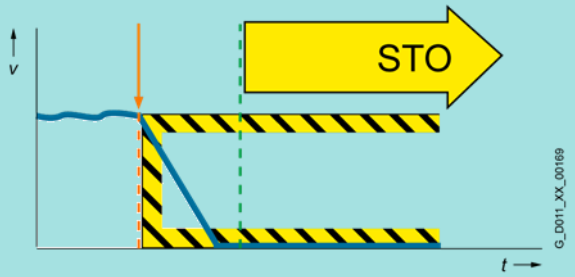
Communication is interrupted while a workpiece is being milled. The milling tool must be retracted from the workpiece so that the workpiece is not damaged.

Safe Stop 1 (SS1)

Safe Stop 1 (SS1) Overview



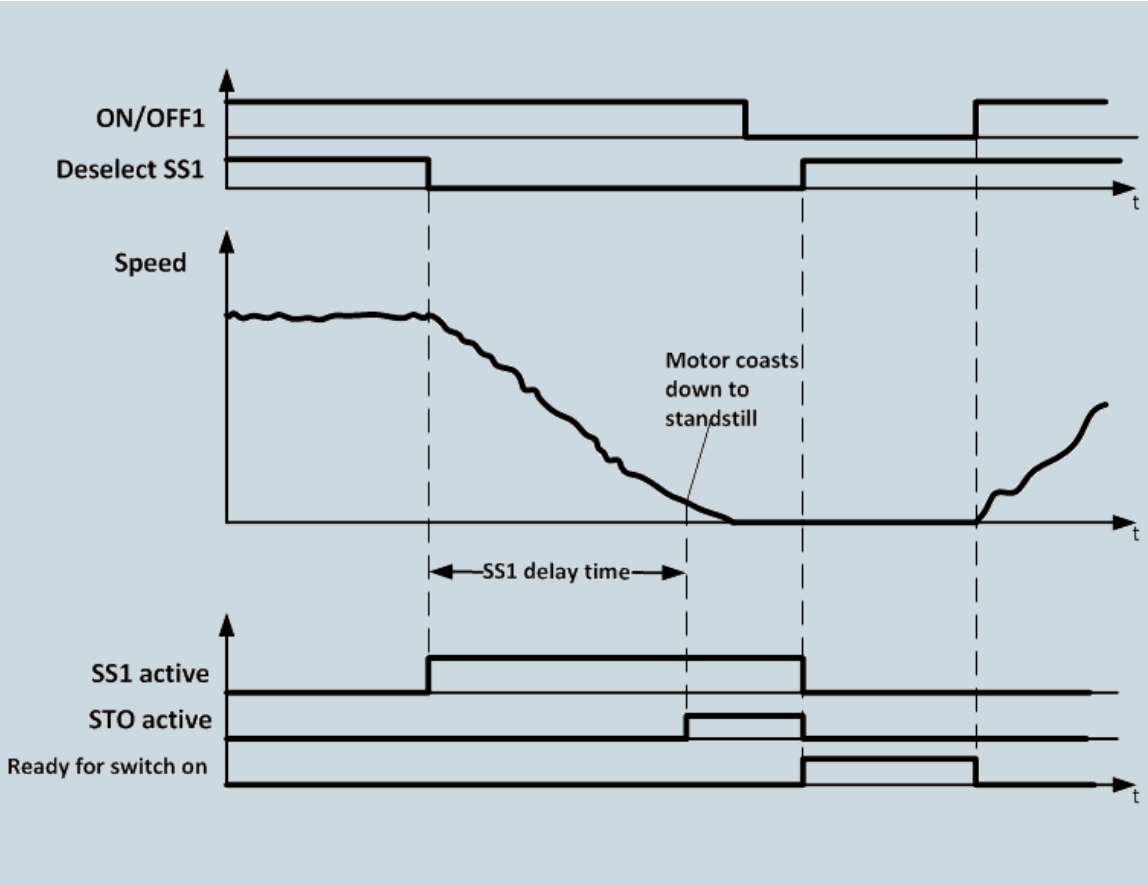
Example



Using an Emergency Stop, the storage and retrieval machine is braked before the pulses are canceled, the mechanical brakes and buffer at the end of the aisle are not used – therefore reducing wear.

- Controlled stopping of large masses and moments of inertia
- Four different versions, depending on the requirement
  - SS1-t
  - SS1E
  - SS1-a
  - SS1-r

Safe Stop 1 (SS1)
With time monitoring (SS1-t)



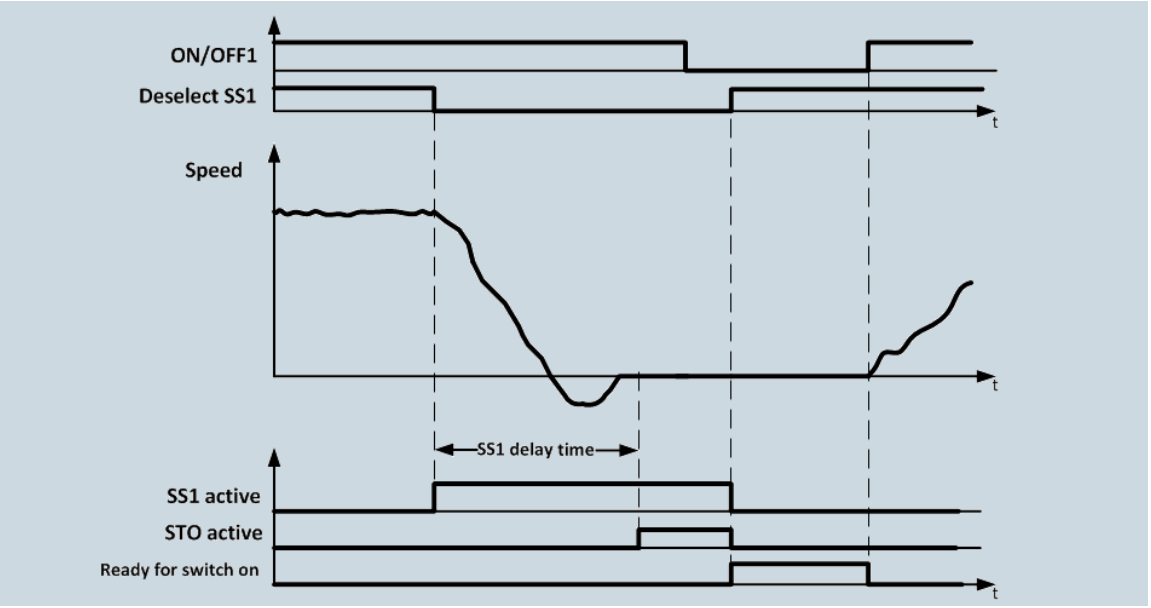
Timing

- Select SS1-t
- The SS1 delay time starts
- The drive independently brakes along the OFF3 ramp in the closed-loop speed controlled mode
- After the SS1 delay time expires:
  - → STO is activated

Features

- The braking ramp is not monitored (it is only controlled from a time perspective)
- Available from Basic Functions

Safe Stop 1 (SS1)
With external stop (SS1E)



SS1E only for S120 and S210

Alternative solution based on an engineered application: time-delayed STO

Timing

- Select SS1E
- The SS1 delay time starts
- The drive does not independently brake
  - → Stopping is initiated with the appropriate setpoint from the control system
- After the SS1 delay time expires:
  - → STO is activated

Features

- The braking ramp is not monitored (it is only controlled from a time perspective)
- Available from Basic Functions

Safe Stop 1 (SS1)
With external stop (SS1E)

SS1E in conjunction with higher-level controllers

Identify that SS1E was selected:

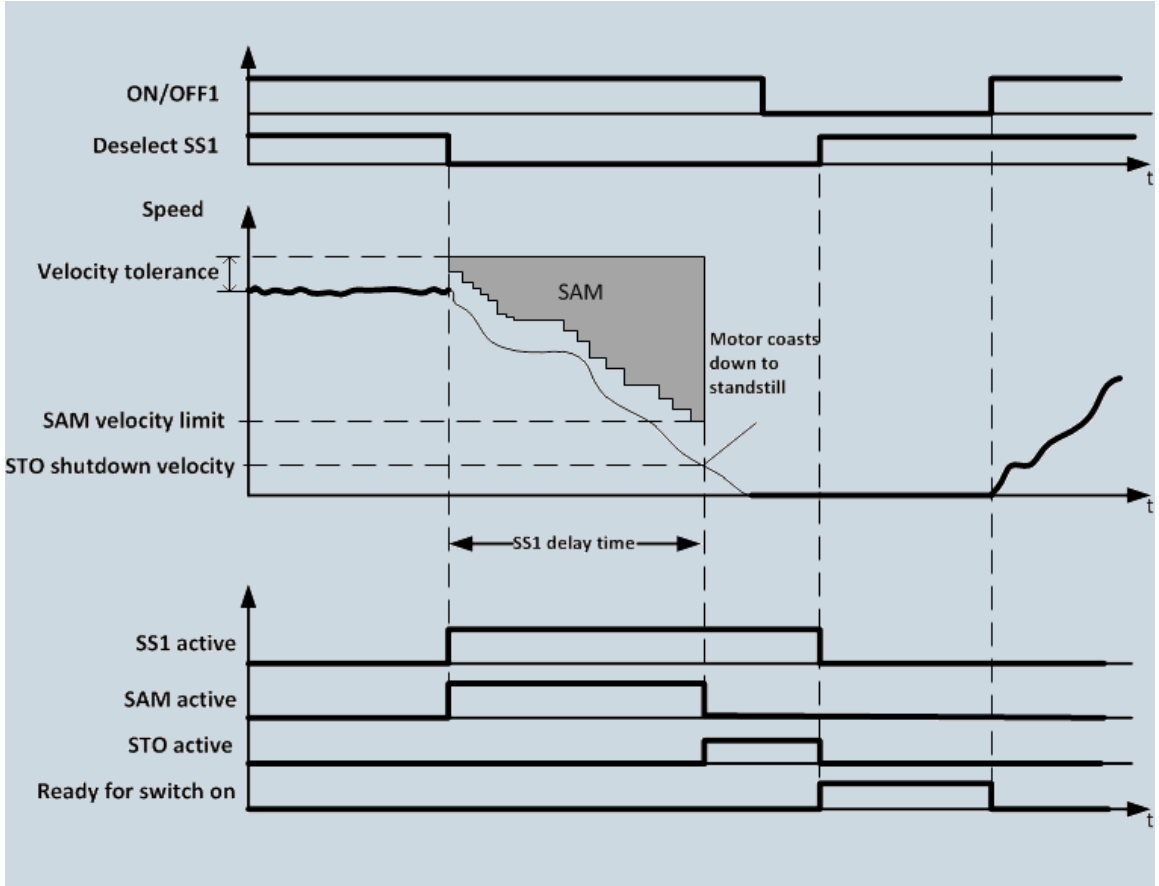
- Evaluate the PROFIsafe telegram or
- Evaluate the Safety Info Channel

Advantages

- The complete drive group can be stopped in synchronism within the SS1 delay time
- Suitable for coupled axes – e.g. for winders, handling systems, packing systems

→ e.g. the material being wound is not broken

Safe Stop 1 (SS1)
With acceleration monitoring SAM (SS1-a)



Timing

- Select SS1-a
- The SS1 delay time starts
- The drive independently brakes along the OFF3 ramp in the closed-loop speed controlled mode
- Braking is monitored to ensure that the drive does not accelerate (SAM)
- STO is activated:
  - After the SS1 delay time expires
  - After the shutdown velocity has been fallen below
  - When acceleration monitoring responds (SAM)

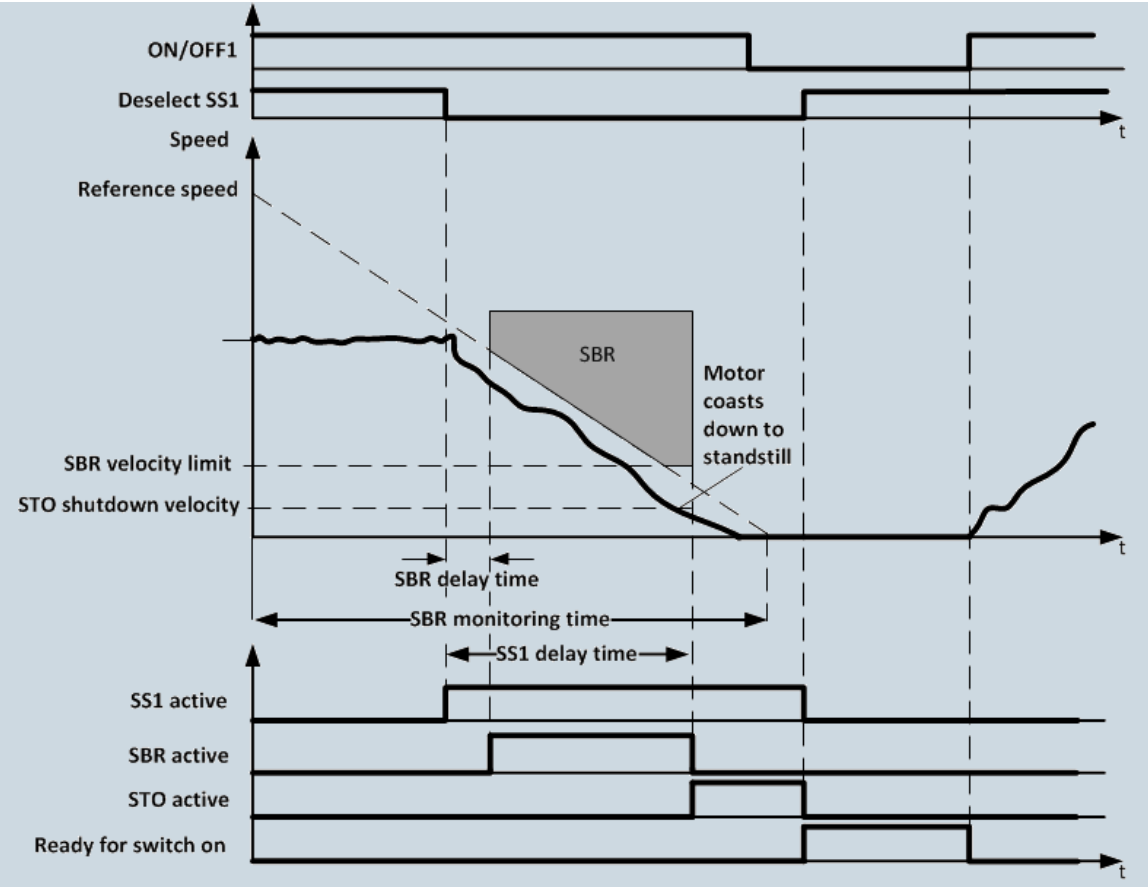
Safe Stop 1 (SS1)
With acceleration monitoring SAM (SS1-a)

Features

- Braking is monitored along the OFF3 ramp to ensure that the drive does not accelerate
- Available from Extended Functions
- The speed limit is continuously tracked with an adjustable tolerance
- Acceleration monitoring SAM is deactivated once a parameterizable speed limit has been fallen below
- When acceleration monitoring responds (violated):

  → STOP A

Safe Stop 1 (SS1)
With brake ramp monitoring SBR (SS1-r)



Timing

- Select SS1-r
- The SS1 delay time starts
- The drive independently brakes along the OFF3 ramp in the closed-loop speed controlled mode
- Braking is monitored with definable brake ramp monitoring (SBR)
- STO is activated:
  - After the SS1 delay time expires:
  - After the shutdown velocity has been fallen below
  - When acceleration monitoring responds (SBR)

Tip Braking ramp monitoring (SBR) should be parameterized in parallel to the OFF3 ramp!

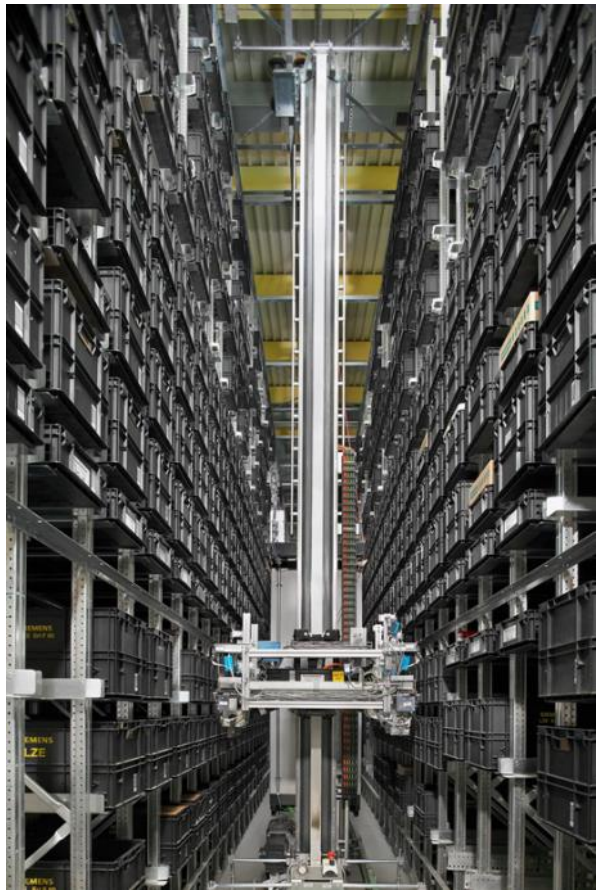
Safe Stop 1 (SS1)
With brake ramp monitoring SBR (SS1-r)

Features of the brake ramp monitoring SBR

- Braking is monitored along the OFF3 ramp using the brake ramp monitoring function
- Available from Extended Functions
- After selecting SS1
  - → Start the SBR delay time (together with the SS1 delay time)
- Define the gradient of the brake ramp monitoring based on speed and time
- Brake ramp monitoring SBR is deactivated when a parameterizable speed limit is fallen below
- When the brake ramp monitoring responds (violated):
  - → STOP A

Safe Stop 2 (SS2)

Safe Stop 2 (SS2) Overview



Timing

- Select SS2
- The SS2 delay time starts
- The drive independently brakes along the OFF3 ramp in the closed-loop speed controlled mode
- After the SS2 delay time expires:

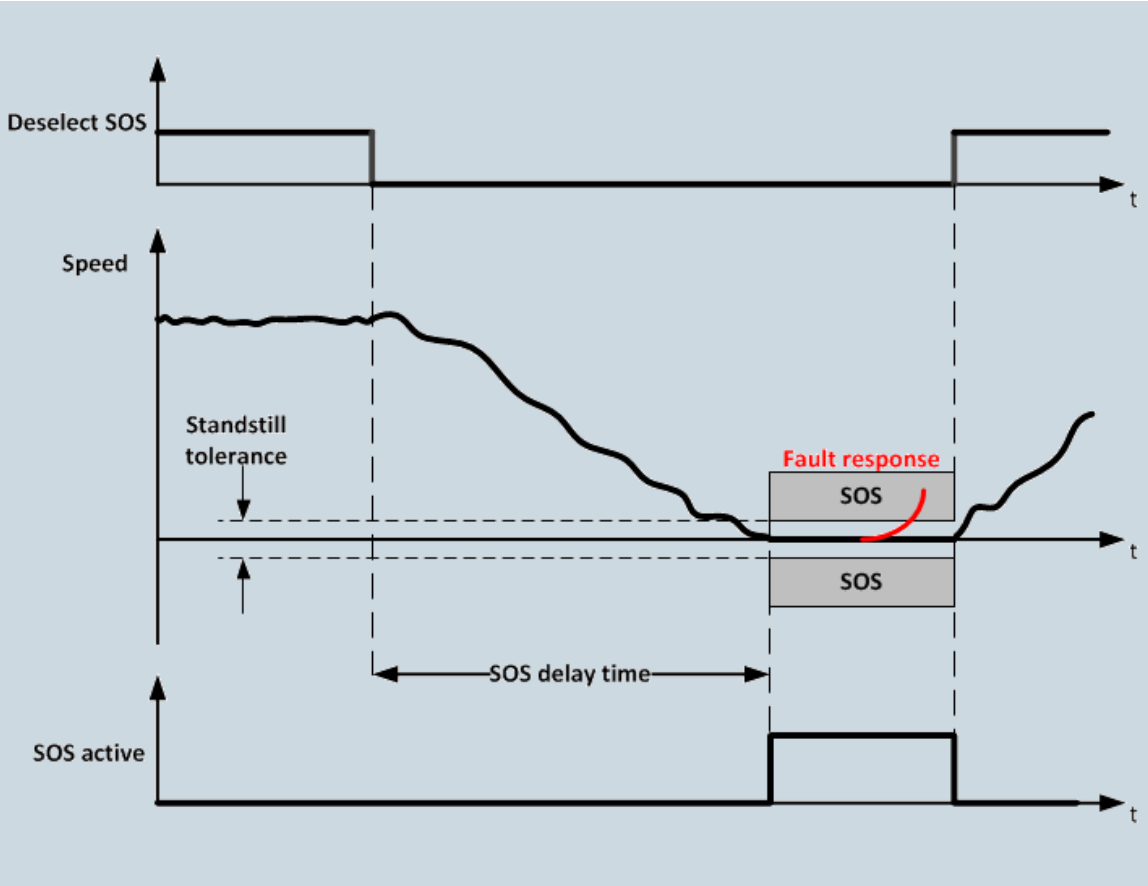
  → SOS is activated

Features

- Available from Extended Functions
- Different versions of the SS2 function are available, identical to SS1: SS1-t, SS1E, SS1-a, SS1-r

Safe Operating Stop (SOS)

Safe Operating Stop (SOS)
Overview



Timing

- Select SOS
- The SOS delay time starts
- Stopping is initiated with the appropriate setpoint from the control system
- After the SOS delay time expires:
  - The motor is safely monitored at its standstill position
  - Current still flows through the motor so that it is actively held at standstill
- Deselect SOS

➔ The axis can be immediately traversed again

Safe Operating Stop (SOS)
Special features

- The drive does not independently brake (contrary to SS1 and SS2)
  - → The control system remains responsible for issuing the setpoint
  - → Response to selecting SOS in the user program:
    The drive is braked down to standstill within the SOS delay time
- SOS delay time:
  - → This must be dimensioned so that within this time the drive can be braked down to standstill from every speed that occurs in the process.
- When the standstill tolerance is violated:
  - → STOP B

Safe Brake Control (SBC)

Safe Brake Control (SBC) Overview

Booksize

Brake connection on Motor Modules

24V DC / 2A

Blocksize

Safe Brake Relay

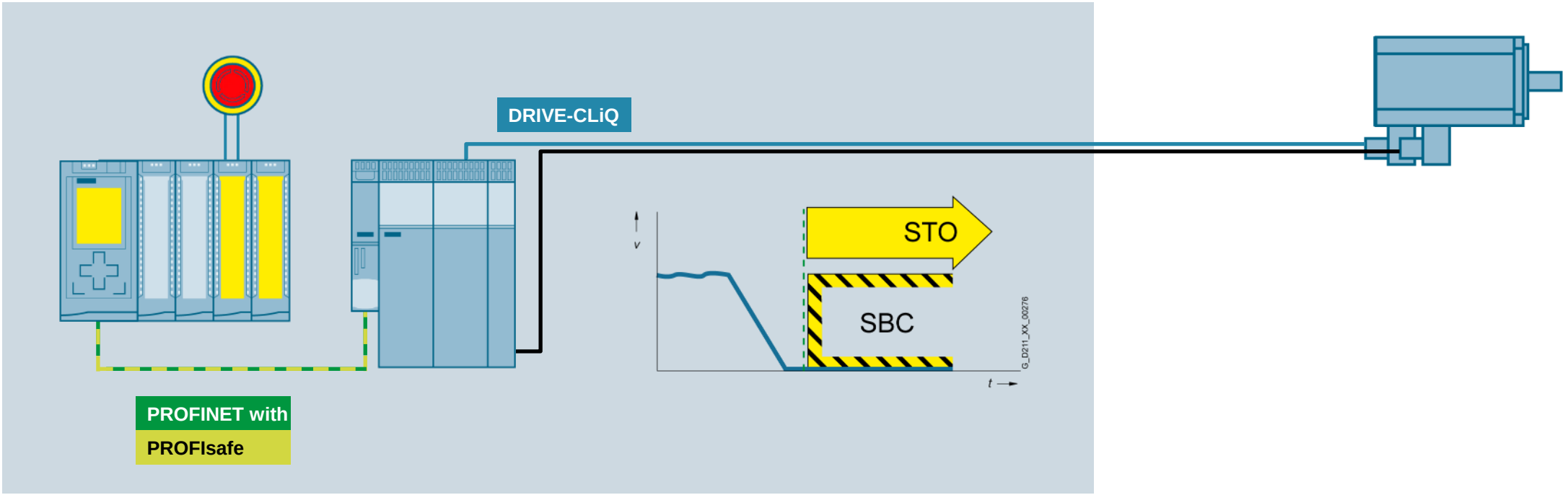
24V DC / 2,5A

Chassis / Cabinet

Safe Brake Adapter

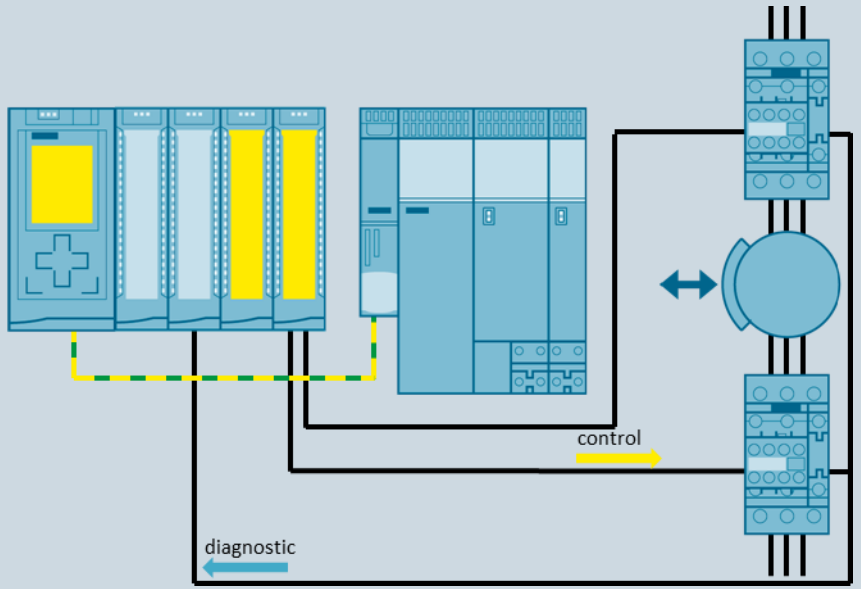
230V AC / 2A

Safe Brake Control (SBC)
Controlling the brake via SINAMICS



Up to PL b (Cat. b) or PL c (Cat. 1, if brake = "well-tried component")

Safe Brake Control (SBC)
Controlling the brake via F-PLC and interface (coupling) relay



Pro

- Independent of the voltage/current requirement of the brake
- More than one brake can be safely controlled
- Seamlessly consistent solution with respect to the SIMATIC portfolio

Contra

- Not a solution integrated in the drive
- No seamless diagnostics
- The standard brake signal is transferred from SINAMICS to the F-PLC
  - → Longer signal propagation time until the brake closes
  - → The load can briefly sag/drop

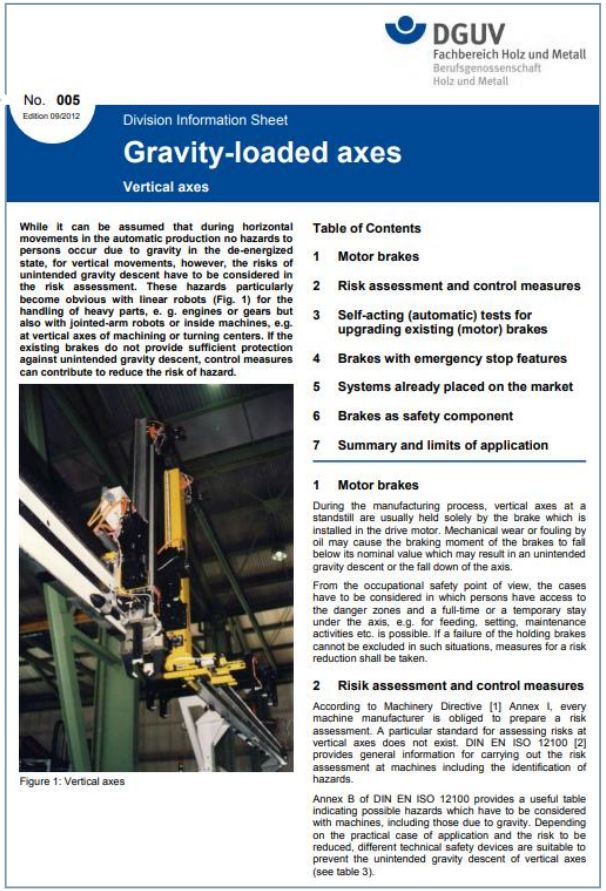
Safe Brake Test (SBT)

Safe Brake Test (SBT) Overview

Fault scenario, bus failure

- Analysis of vertical axes under practical perspectives
- Overview of various use cases with different requirements
- Cyclic brake test as requirement

  Safe Brake Test (SBT)



DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft Holz und Metall

No. 005
Edition 09/2012

Division Information Sheet

Gravity-loaded axes

Vertical axes

While it can be assumed that during horizontal movements in the automatic production no hazards to persons occur due to gravity in the de-energized state, for vertical movements, however, the risks of unintended gravity descent have to be considered in the risk assessment. These hazards particularly become obvious with linear robots (Fig. 1) for the handling of heavy parts, e. g. engines or gears but also with jointed-arm robots or inside machines, e.g. at vertical axes of machining or turning centers. If the existing brakes do not provide sufficient protection against unintended gravity descent, control measures can contribute to reduce the risk of hazard.

Table of Contents

1 Motor brakes

During the manufacturing process, vertical axes at a standstill are usually held solely by the brake which is installed in the drive motor. Mechanical wear or fouling by oil may cause the braking moment of the brakes to fall below its nominal value which may result in an unintended gravity descent or the fall down of the axis.

From the occupational safety point of view, the cases have to be considered in which persons have access to the danger zones and a full-time or a temporary stay under the axis, e.g. for feeding, setting, maintenance activities etc. is possible. If a failure of the holding brakes cannot be excluded in such situations, measures for a risk reduction shall be taken.

2 Risik assessment and control measures

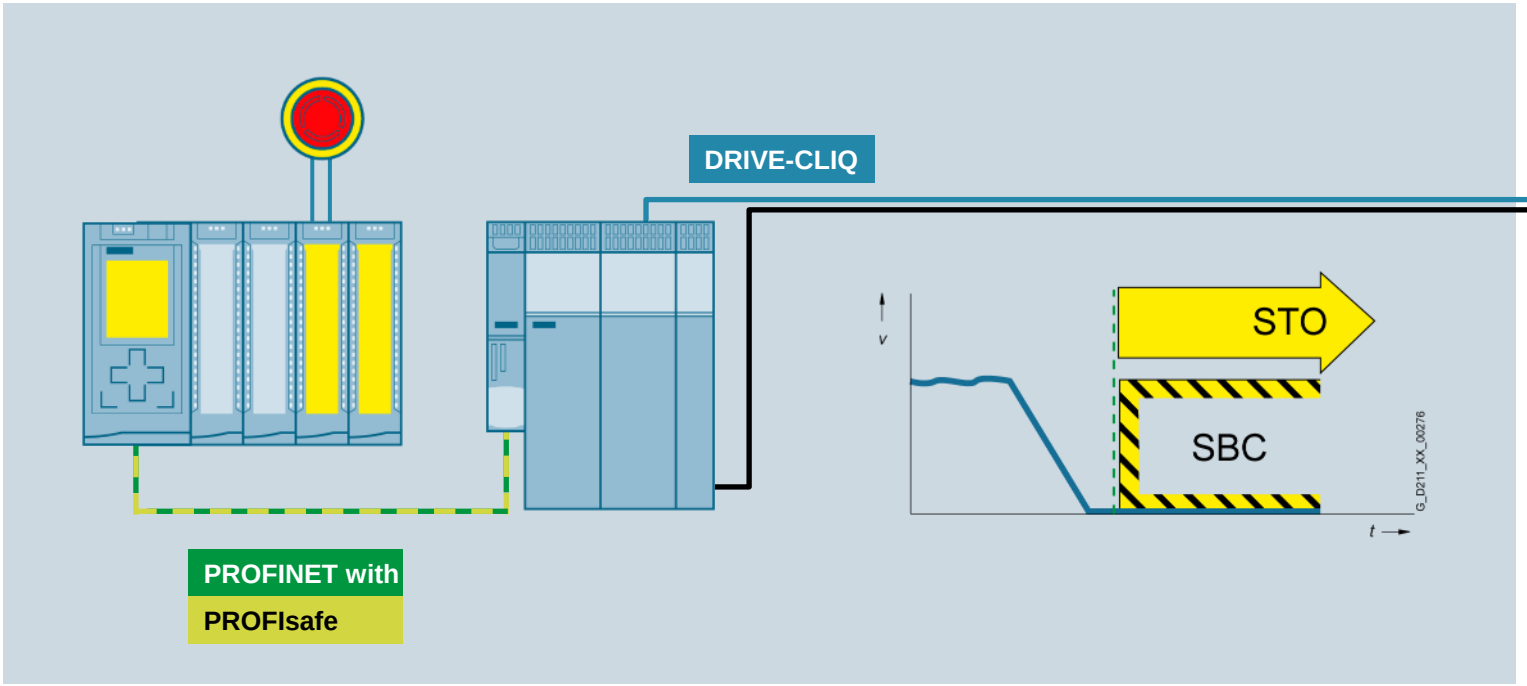
According to Machinery Directive [1] Annex I, every machine manufacturer is obliged to prepare a risk assessment. A particular standard for assessing risks at vertical axes does not exist. DIN EN ISO 12100 [2] provides general information for carrying out the risk assessment at machines including the identification of hazards.

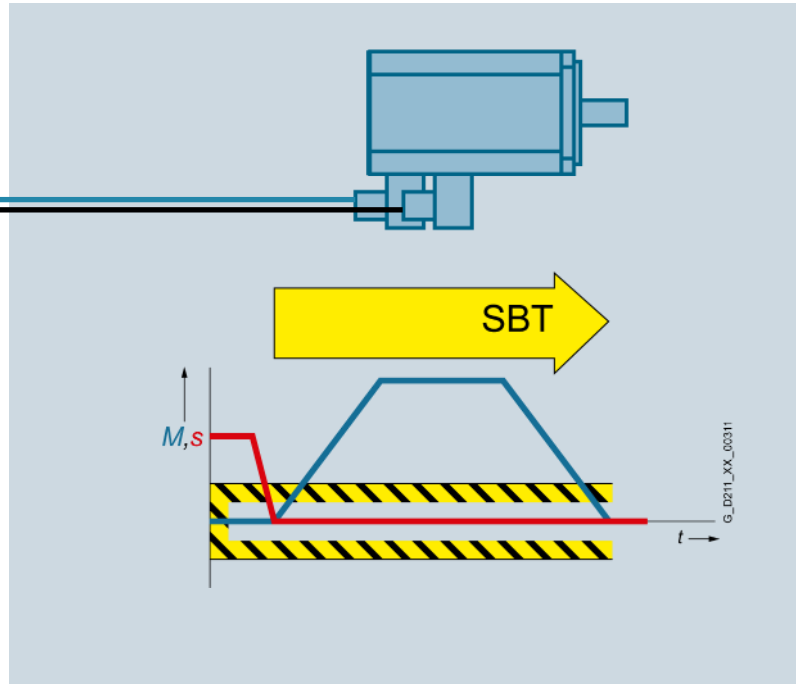
Annex B of DIN EN ISO 12100 provides a useful table indicating possible hazards which have to be considered with machines, including those due to gravity. Depending on the practical case of application and the risk to be reduced, different technical safety devices are suitable to prevent the unintended gravity descent of vertical axes (see table 3).

Information sheet of the DGUV (German Statutory Accident Insurance) in the wood and metal subsegments

https://www.dguv.de/medien/fb-holzundmetall/publikationen-dokumente/infoblaetter/infobl_englisch/005_vertical-axes.pdf

Safe Brake Test (SBT)
Brake control with SBC and SBT





Up to PL d (Cat. 2)

Safe Brake Test (SBT)
Functionality

SBT is not a safety function

SBT is a diagnostics function that is compliant with the requirements relating to Category 2 according to EN ISO 13849-1.

Features

- Available for SINAMICS S120/S150 and G130/G150
- Linear and rotary axes
- Suitable for motor holding brakes and external brakes
  - 1 motor holding brake / 2 external brakes
  - Mixed configurations possible
  - A total of 2 brakes
- 2 test sequences per brake
- Automatic detection and consideration of static suspended loads

Certificate (SIOS-ID 109479632)

Safe Brake Test (SBT)
Requirements

Preconditions

- Closed-loop speed control with encoder
- Safety-capable encoder system (sin/cos encoder or 2 HTL/TTL encoders)

For motor holding brake additionally apply:

- SBC is activated
- Brake configuration: Brake same as sequence control

Safe Brake Test (SBT) Control

Test stop

Only for motor holding brakes with one sequence

BiCo interconnection

6 parameters available

- Select the brake test
- Start the test sequence
- …

Safety Info Channel (SIC) / Safety Control Channel (SCC)

- Information about controlling SBT is provided in SIC/SCC
- SIC/SCC is mapped in PROFIdrive telegram 701

Configuration example SIC/SCC (SIOS-ID 76457011)

Safe Brake Test (SBT)
Control from a higher-level controller

SIMATIC

Library including SBT

- SIMATIC S7-F/P Press Safety Blocks (SIOS-ID 48299432)
- Failsafe blocks for storage and retrieval machines (SIOS-ID 101167223)

SIMOTION

Available system functions

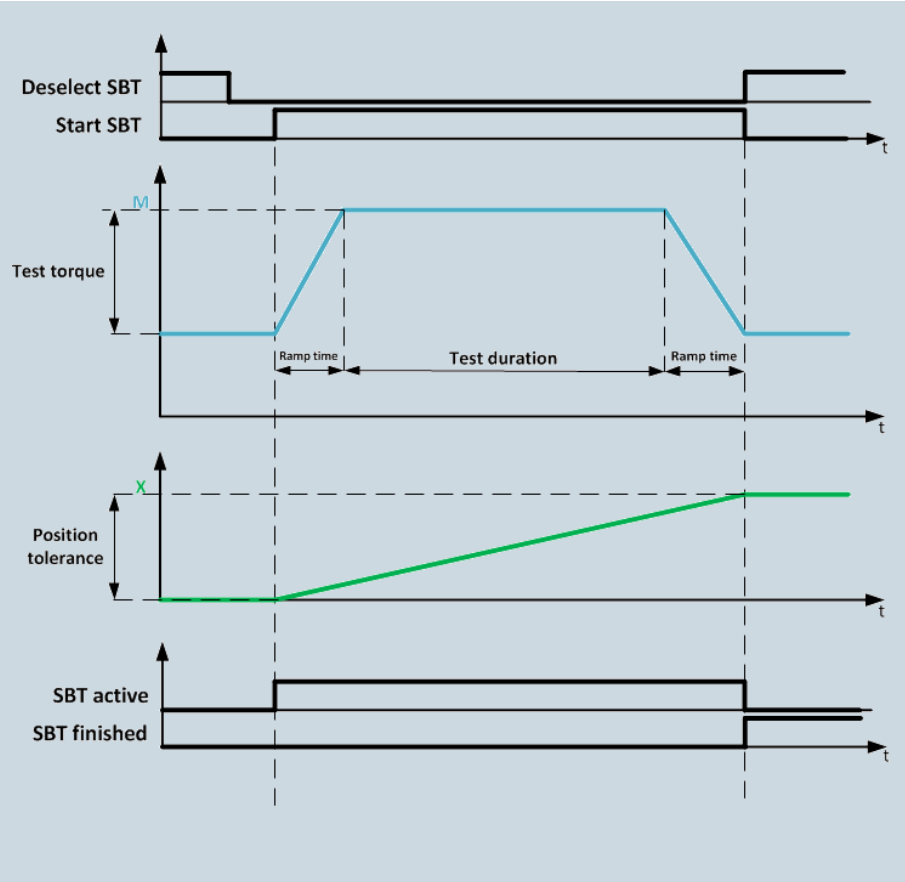
_*executeAxisSafetySbt*: Executing an SBT cycle on an axis

_*setAxisSafetySbtExtBrakeState*: Feedback from an external brake (via SCC)

SINUMERIK

- Block to control SBT (SIOS-ID 109477754)

Safe Brake Test (SBT)
Explanation of the function using a motor holding brake



1 Set the pulse enable and open the brake

2 Select SBT

- The static load torque is automatically determined
- Test torque = parameterized torque ± determined static load torque

3 Start SBT

- The brake is automatically closed
- The test torque is established along a parameterizable ramp
- The actual speed is monitored < 10 % of n_{Max}
- The actual torque is monitored < ±20 % of the test torque
- The position is monitored < parameterized tolerance
- The test torque is reduced to zero
- The brakes are automatically opened

4 SBT exited

Safe Brake Test (SBT)
Practical experience

Problem

The actual speed deviates by ≥ 10% of the parameterized maximum speed

➔ Fault message A01784 (bit6) is initiated

Reason

Gearbox backlash between the motor encoder and external brake is too high

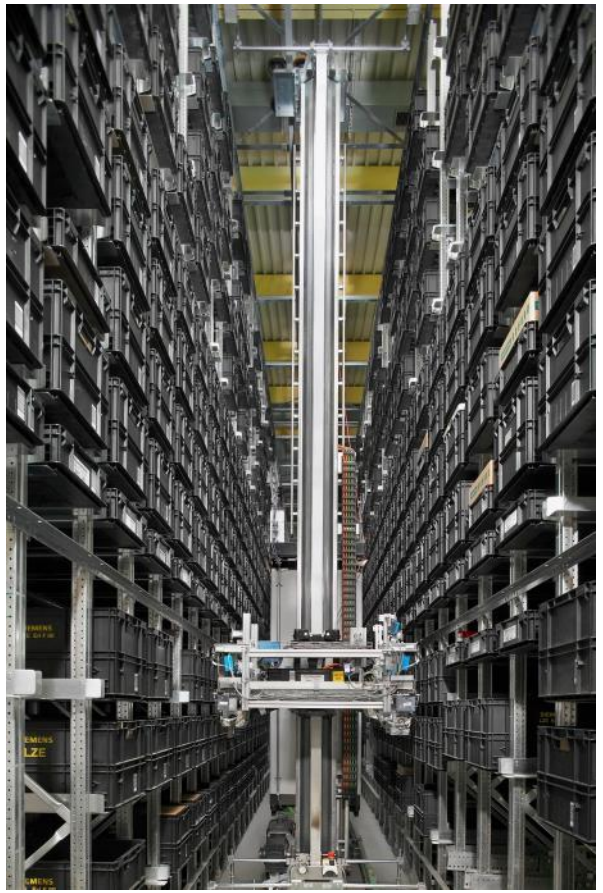
➔ The motor encoder detects motion for tooth flank changes in the gearbox

Remedy

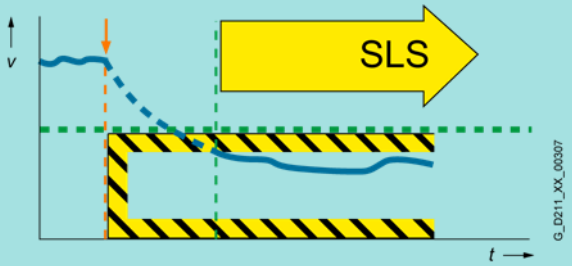
- Increase the time to establish/reduce the test torque
- Set a higher maximum speed
- Reduce the dynamic response of the control loop

Safely-Limited Speed (SLS)

Safely-Limited Speed (SLS) Overview



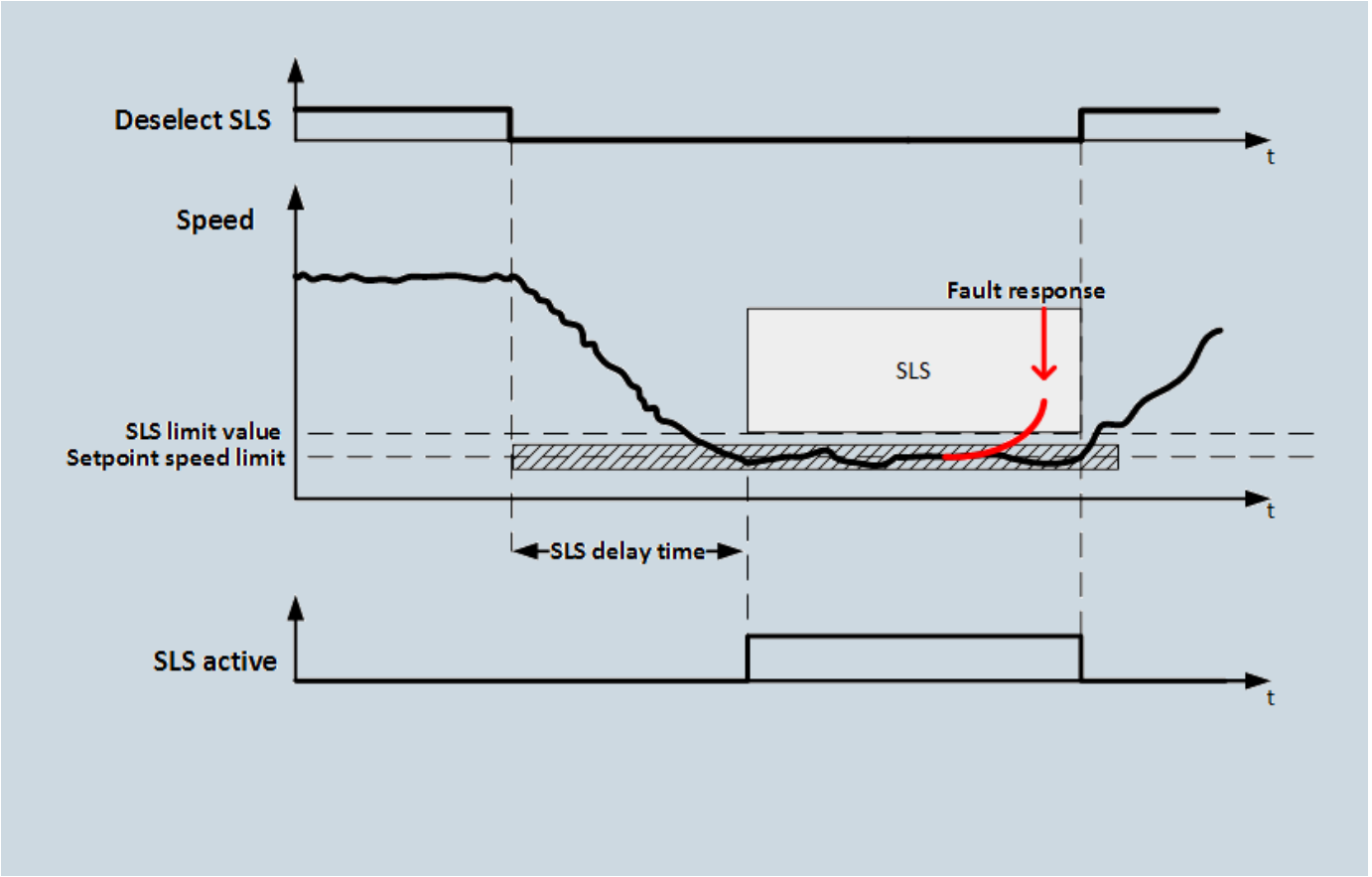
Example



The speed of the storage and retrieval machine is safely monitored when requesting that the protective door is released.

- The speed is monitored in the positive and negative directions of rotation
- The system can switch between four speed limit values during the runtime
- One speed limit value that can be changed during the runtime via PROFIsafe

Safely-Limited Speed (SLS)



Timing

- Select SLS
- The SLS delay time starts
- The drive does not independently brake
  - Speed setpoint issued by the control system is below the selected SLS limit value
- After the SLS delay time expires:
  - SLS is activated

Safely-Limited Speed (SLS)

Features of Safely-Limited Speed (SLS)

- Available from Extended Functions
- Parameterizable stop response when the SLS limit value is exceeded

  → STOP A-E

Switching over between SLS levels

- To the lower limit value: After the SLS delay time expires, the selected level becomes active
- To the higher limit value: Selected level becomes immediately active

Safely-Limited Speed (SLS)
Setpoint speed limiting SINAMICS G

Setpoint speed limiting SINAMICS G

The speed is automatically limited via a ramp-function generator of the SINAMICS G when SLS is selected

Default: 80% of the selected SLS limit value

➔ Only makes sense for applications without a higher-level motion controller (e.g. T-CPU, SIMOTION) – or when using speed axes

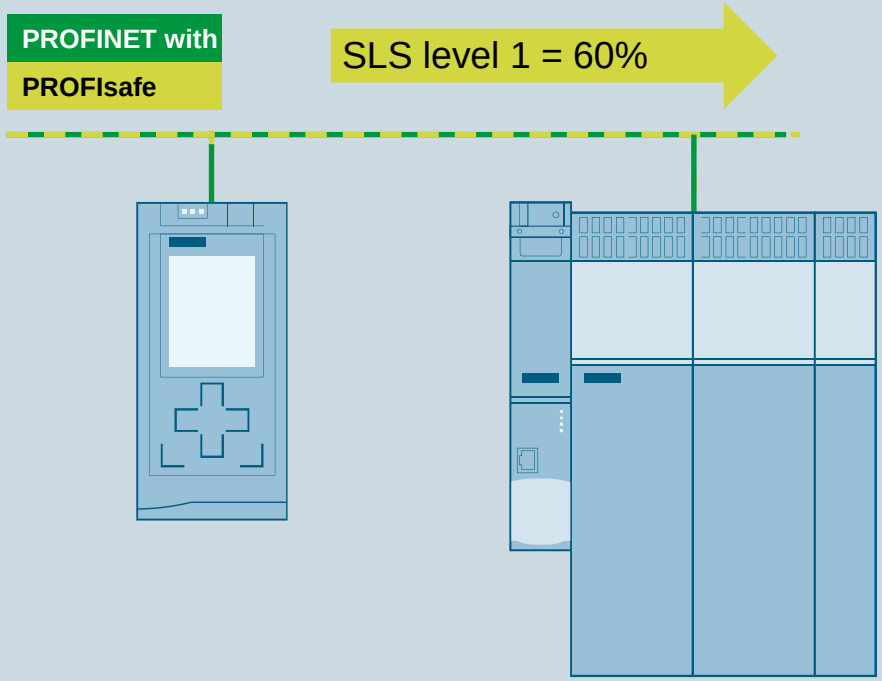
For applications with higher-level motion controller:

- The interconnection via ramp-function generator must be withdrawn
- The SLS selection is evaluated (e.g. via the Safety Info Channel), and the motion controller issues a speed setpoint below the selected SLS limit value

Safely-Limited Speed (SLS)
Differences - G120, S120 and S210

	G120	S120	S210
Number of settable limit values	Up to 4	Up to 32,770	Up to 32,770
Selection of limit values	PROFIsafe / F-DI	PROFIsafe / F-DI	PROFIsafe
Dynamic adaptation of SLS limits		✓ Level 1	✓ Level 1
SLS without selection		✓	

Safely-Limited Speed (SLS)
Variable SLS limit – only for SINAMICS S120 and S210



Special feature

Dynamic adaptation of SLS level 1 via PROFIsafe between 0.01 % and 100 %

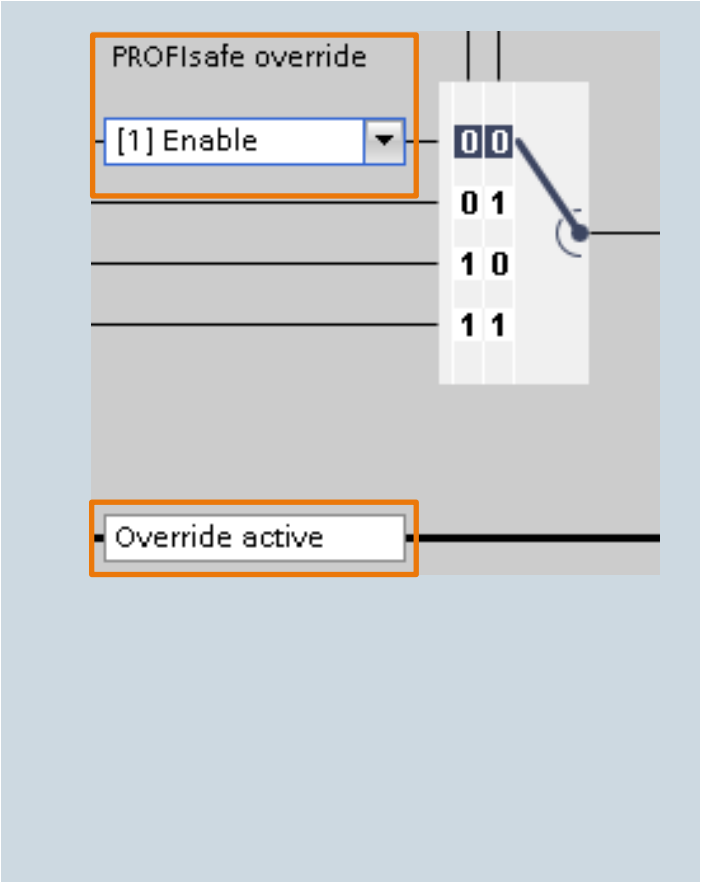
Advantage

Valid speed/velocity limit can be flexibly set without any restrictions to 4 limit value levels, e.g. dependent on the operator, workpiece, position, etc.

Applications

- Storage and retrieval machines, tracking the SLS limit close to end positions/end stops
- Lathes (different tools), winders, ...

Safely-Limited Speed (SLS)
Variable SLS limit – only for SINAMICS S120 and S210

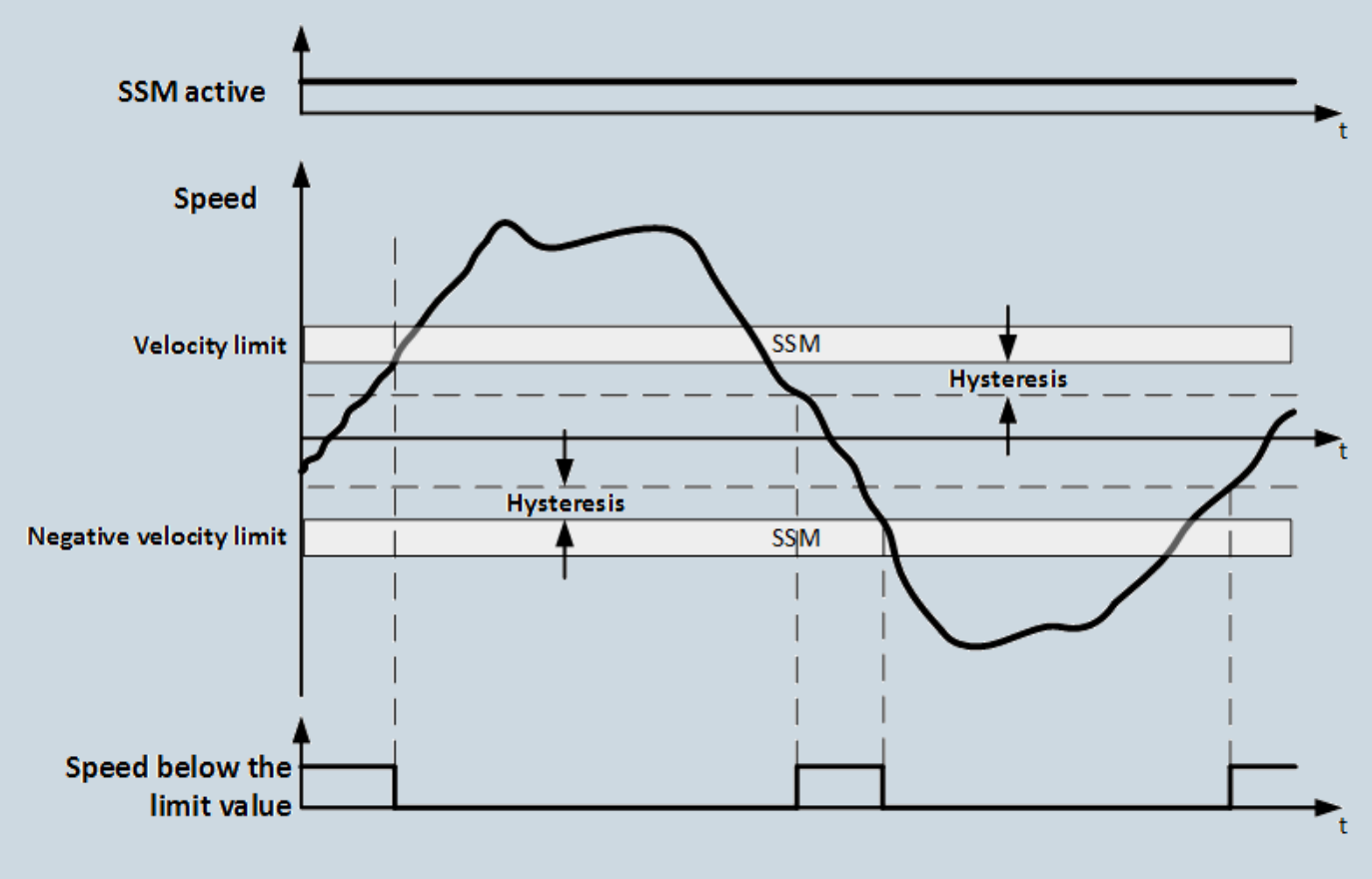


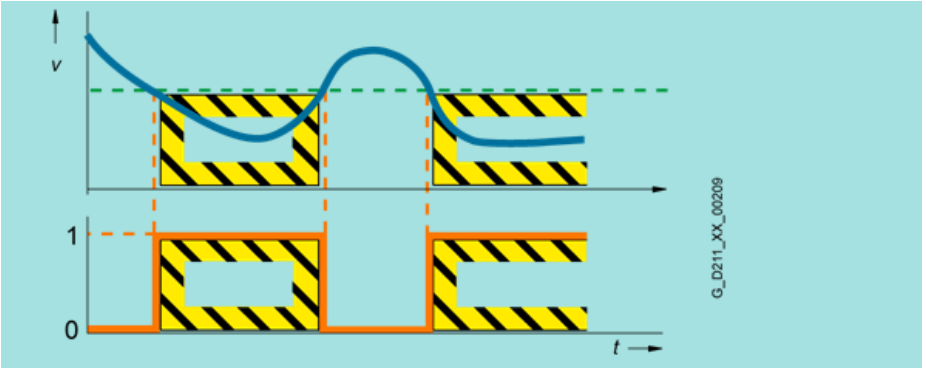
Features

- Available for safety with and without encoder
- Supported with PROFIsafe telegrams 901, 902 and 903
- Value range: 1 to 32767 (0.01 % to 100 % of SLS level 1)
- Invalid values initiate the parameterized stop response for SLS level 1
- SLS levels 2-4 can still be selected

Safe Speed Monitor (SSM)

Safe Speed Monitor (SSM)



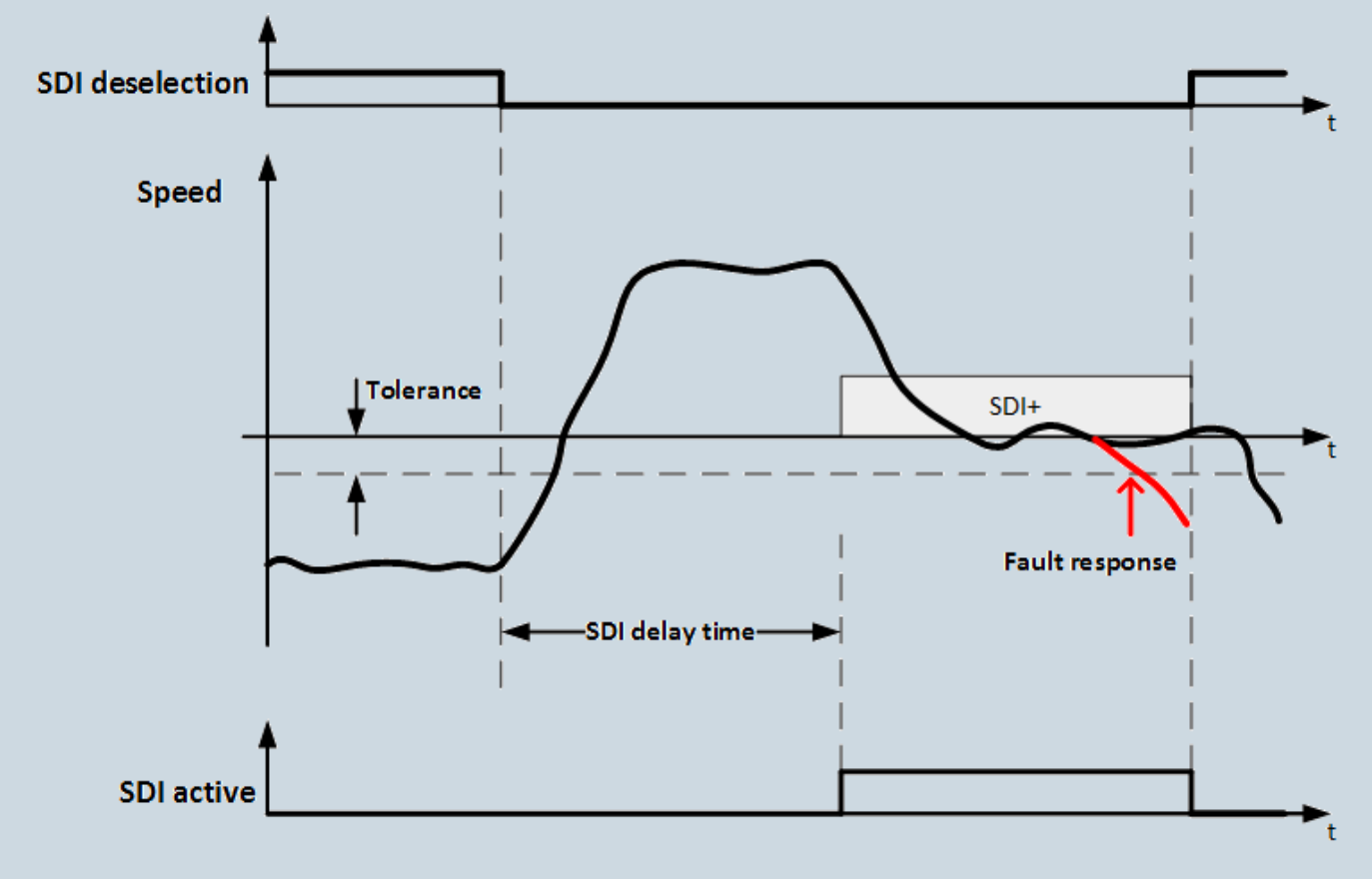


SSM provides a **safe feedback** signal which indicates whether the speed of a drive is below a parameterized value.

This feedback can be used, for example, to release a protective door.

Safe Direction (SDI)

Safe Direction (SDI)

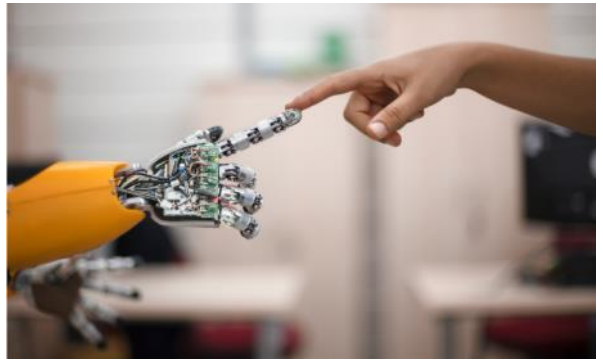


Timing

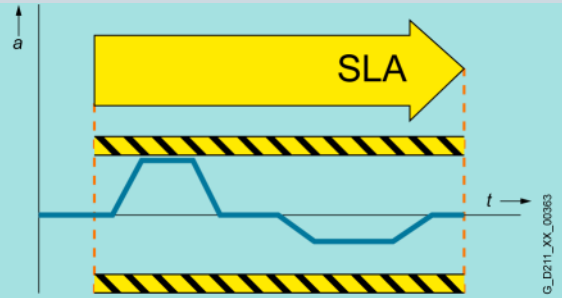
- Select SDI (positive or negative)
- The SDI delay time starts
- Direction of rotation issued by the control system
- After the SDI delay time expires:
  - → Safe monitoring of the selected direction of rotation of the motor with parameterizable tolerance
- Deselect SDI
  - → Motor can immediately be moved again in both directions of rotation
- Parameterizable stop response (A-E) when turning the motor in the direction of rotation not enabled

Safely-Limited Acceleration (SLA)

Safely-Limited Acceleration (SLA)
General information about the safety function



Example

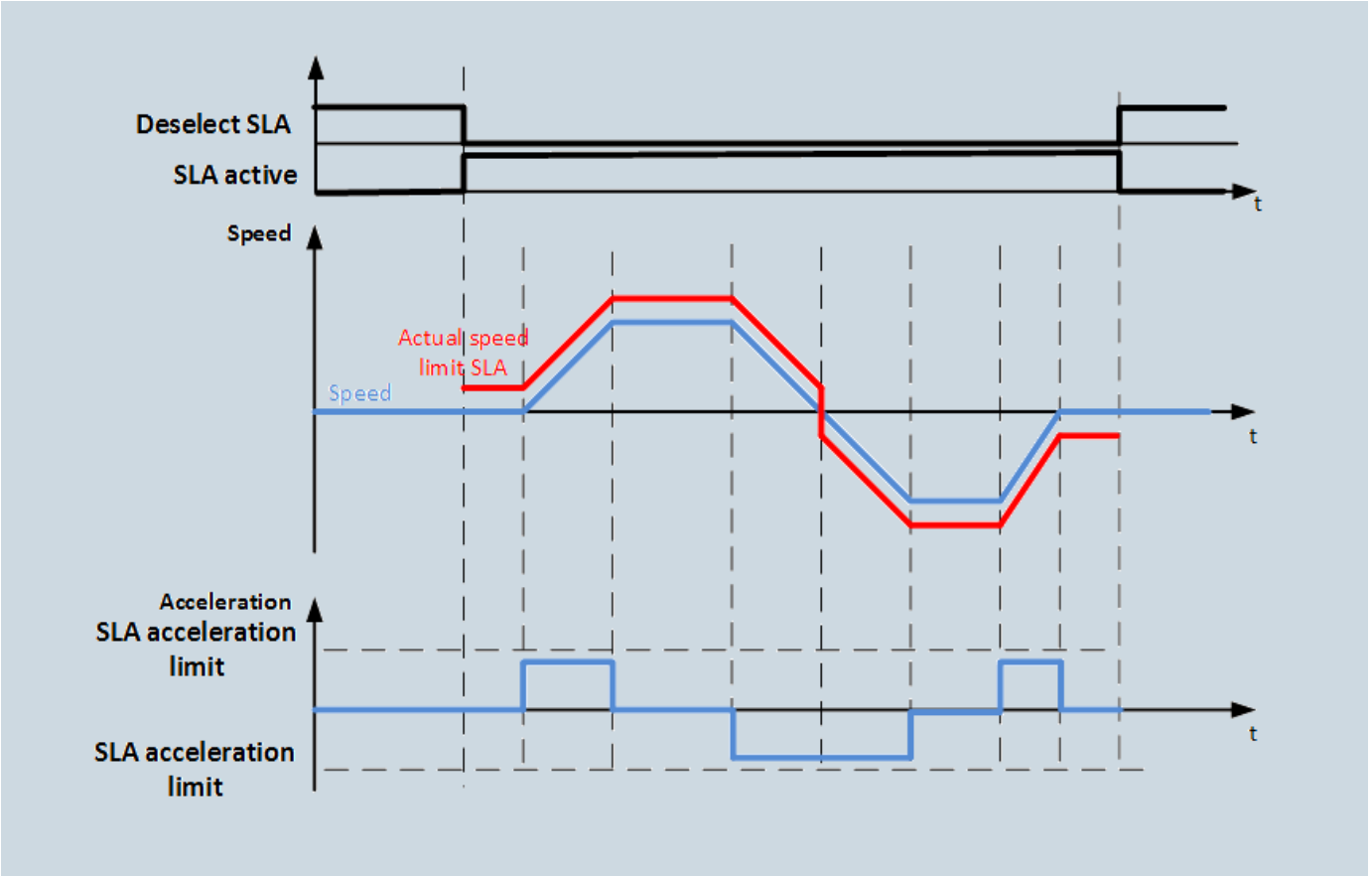


SLA identifies when a kinematic axis accelerates in an uncontrollable fashion, and initiates a stop response at an early stage.

- Acceleration monitoring
  (is only active when accelerating, but not when braking!)
- Can only be used in a 1-encoder safety system
- There is no delay time between selecting and activating SLA
- Parameterizable stop response when the SLA limit value is exceeded

→ STOP A-E

Safely-Limited Acceleration (SLA)



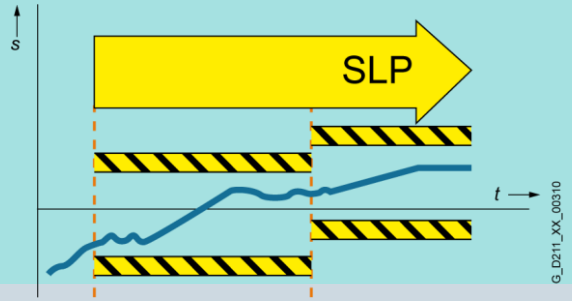
Timing

- Select SLA
- The selected SLA limits (positive and negative) are directly monitored
- The configured stop response (A-E) is initiated when the limit values are exceeded

Safely-Limited Position (SLP)

Safely-Limited Position (SLP)
Overview

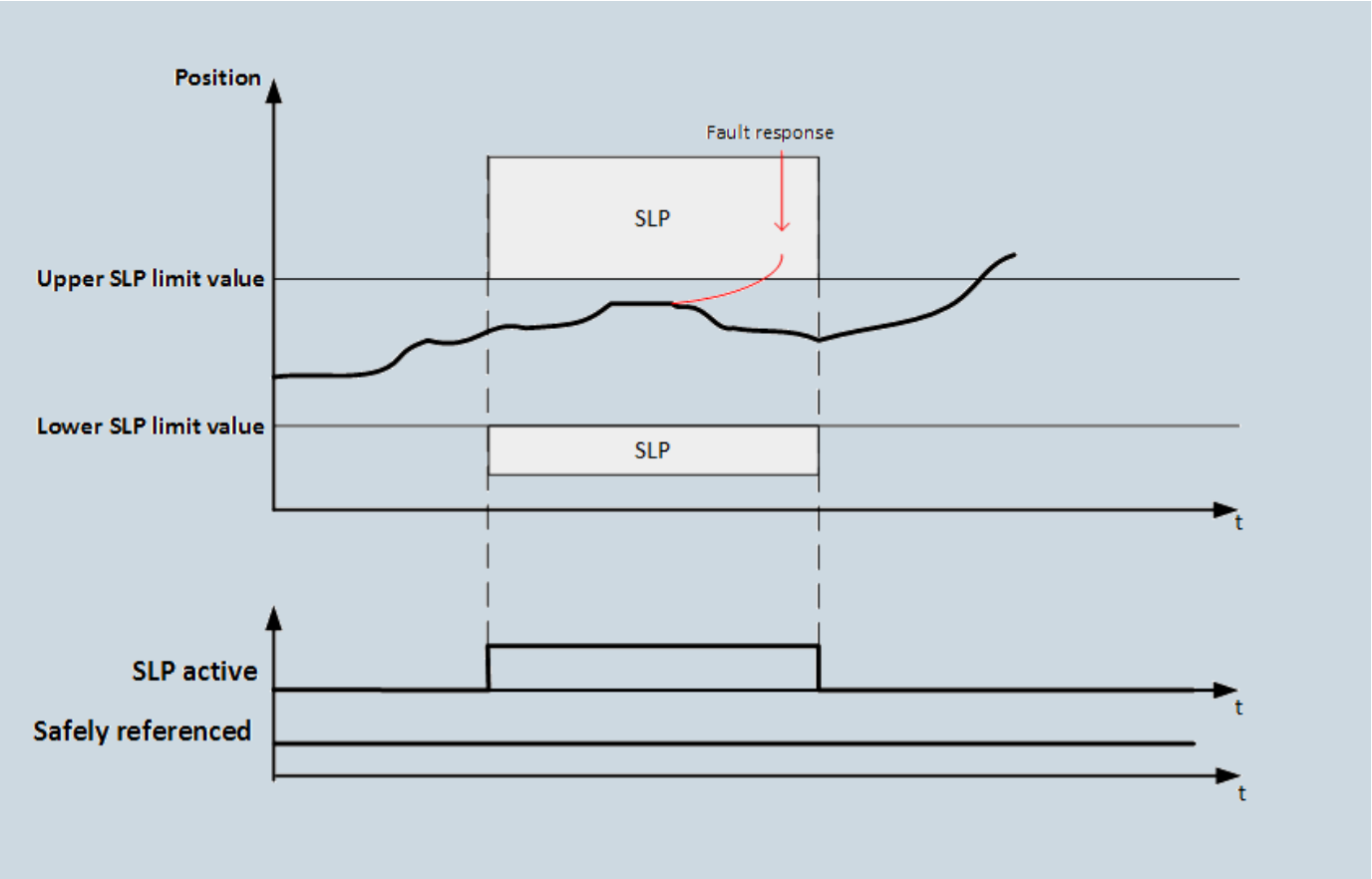
Example



It is only permissible that a crane travels within a safely defined range of positions.

- Monitoring a range of positions
- Two position ranges can be switched between during the runtime

Safely-Limited Position (SLP)



Timing

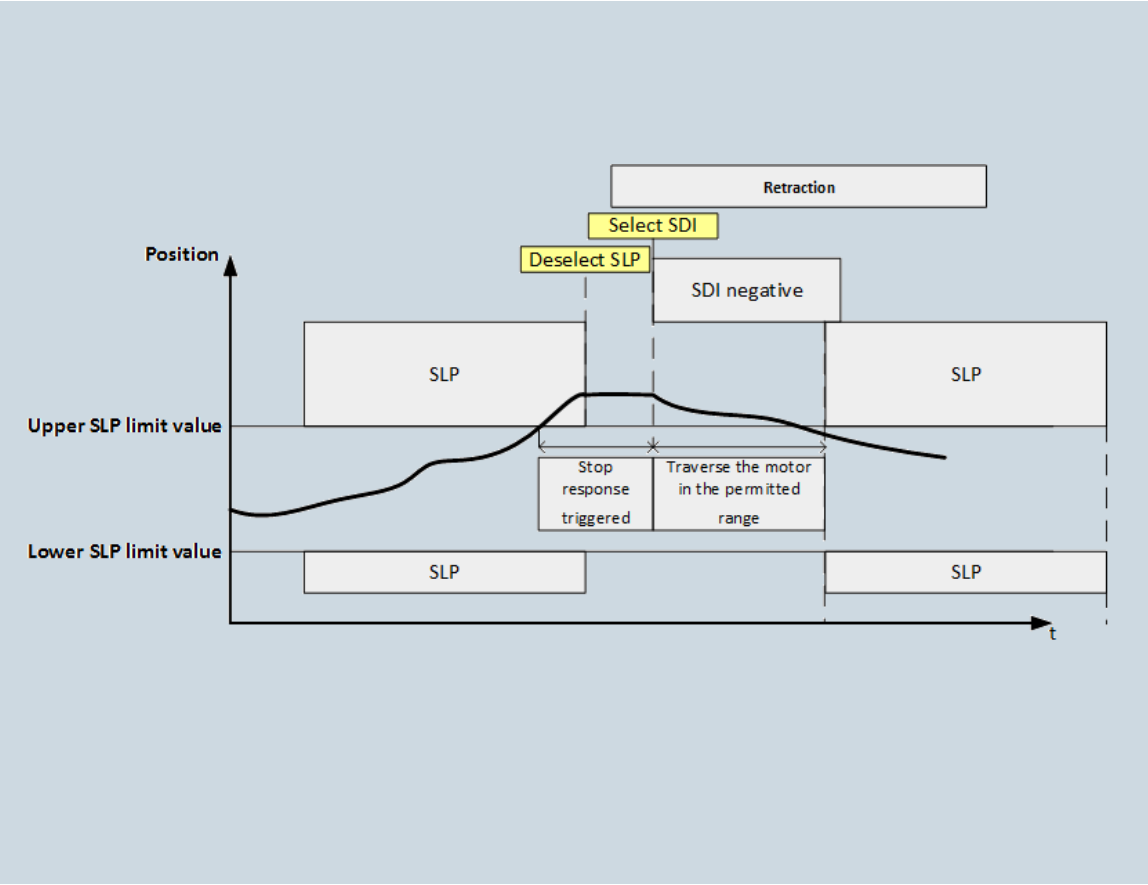
- Select SLP
- The SLP delay time starts
- The drive does not automatically travel into the selected position range
  - → The control system issues the position setpoint in the selected SLP position range
- After the SLP delay time expires:
  - → SLP is activated

Safely-Limited Position (SLP)

Features of Safely-Limited Position (SLP)

- Available from Advanced Functions
- Precondition: Drive safely referenced
- Parameterizable stop response when the SLP position range is exited
  - → STOP A-E
  - → The axis must be retracted to the permissible position range → Retract

Safely-Limited Position (SLP)
Retraction using PROFIsafe



Step sequence

If the safety functions are controlled via PROFIsafe, then the following step sequence must be created in the user program on the F-CPU:

- Select SDI+ when the lower SLP limit is violated
  Select SDI- when the upper limit is violated
- Deselect SLP
- Safe acknowledgment of safety messages
- Return to the permissible range
- Select SLP
- Deselect SDI

Safely-Limited Position (SLP)
Retract with F-DI (TM54F or Onboard F-DI CU310-2)

Retract routine sequence

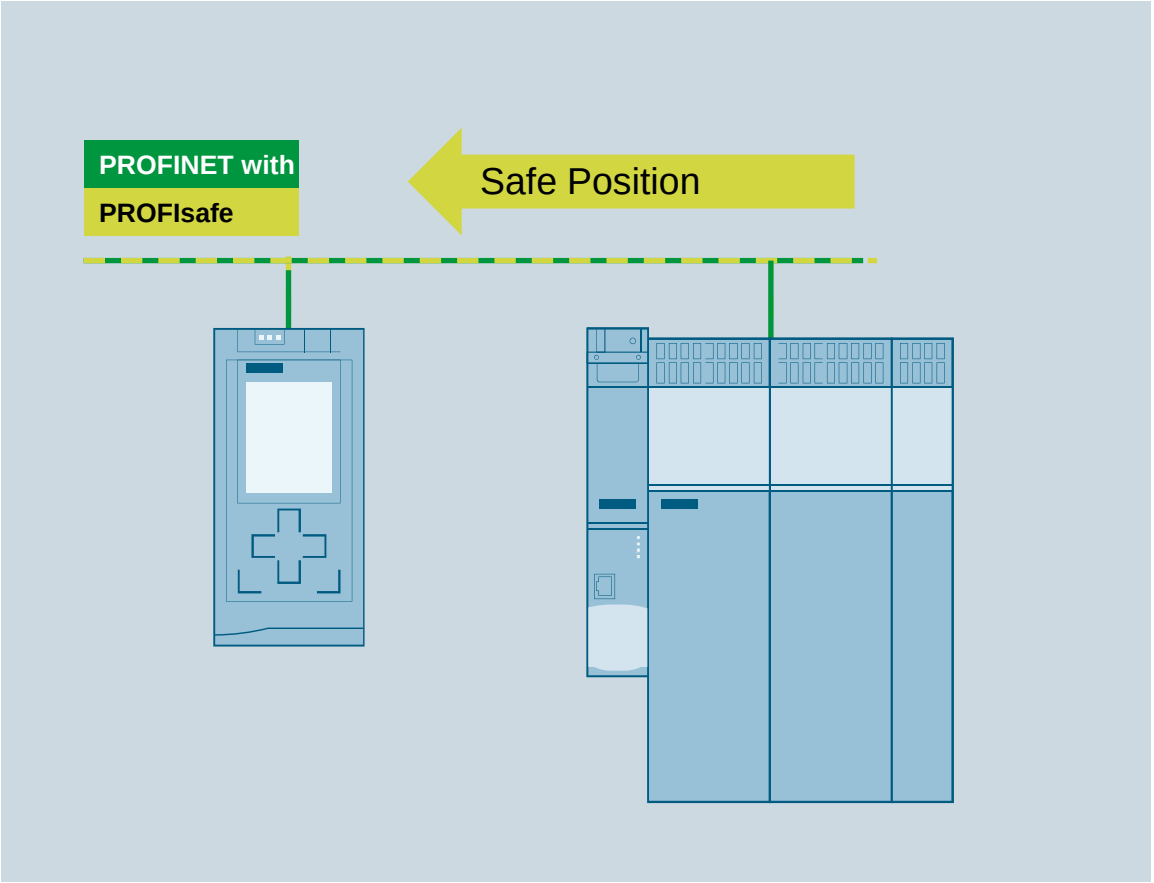
- Selected retract for all drives with active SLP, and where the position range has been violated
  - → Select SDI+ or SDI-
  - → Deselect SLP
- Safely acknowledge safety messages
- Traverse the drive into the permissible range
- Deselect retract
  - → Select SLP
  - → Deselect SDI+ or SDI-

For TM54F and CU310-2, retraction is saved as selectable function (p10009).

This function is selected via F-DI.

Safe Position (SP)

Safe Position (SP)
Overview



Features

The safety-relevant position of a motor is transferred via PROFIsafe telegrams 901 and 902

Safe absolute position (only with encoder)

- Safe position value is valid
- Safe referencing required

Safe relative position (with and without encoder)

- Safe position value is valid
- Safe referencing not required
- **Only application case:**
  Calculating a safe velocity/speed in the F-PLC

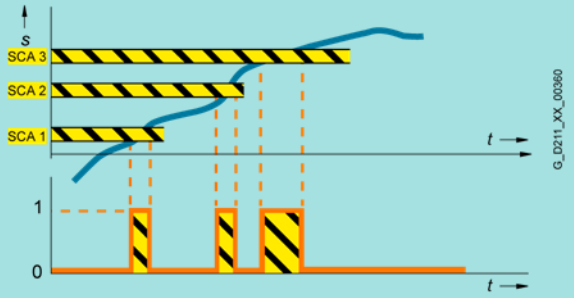
Safe Position (SP)
Difference, telegram 901 vs. 902

	901	902
Scaling factor SF	Yes	No
Resolution	Dependent on SF	µm & m°
Maximum value range	32767 mm for SF = 1000 32767 µm for SF = 1	737,280,000
Transfer variable	16 bit	32 bit
Response when the value range is exceeded	Fault message and stop response	Overflow without stop response

Safe Cam (SCA)

Safe Cam (SCA)
General information about the safety function

Example



Different responses can be initiated, depending on the position range (cam) and feedback signal from the protective door.

- Up to 30 position ranges (cam pairs) can be transferred via PROFIsafe telegram 903
- A hysteresis is taken into account
- Prerequisites:
  - Safe position value is valid
  - Drive safely referenced

  → The evaluation is made in the safety user program of the F-PLC

Safe referencing

Safe referencing
Overview

Safe referencing means

Defining a safe absolute position

Safe referencing is necessary for

Safety functions SLP, SP (absolute position) and SCA

Differentiation between

Initial referencing and **subsequent** referencing

Safe referencing
Details, initial referencing

Initial referencing with motion controller (e.g. SIMOTION, T-CPU, …) is required

when commissioning the system for the first time – or if subsequent referencing was not successful

Sequence

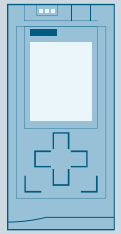
- Carry out standard referencing using the motion controller
- Transfer the reference position to the SINAMICS (p9572), e.g. using an acyclic write task (it is not permissible that the drive moves!)
- Confirm the transferred reference position (p9573 = 89)
- User agreement: Declare the reference position as valid (p9726 = p9740 = AChex within 4 seconds)

User agreement **within** 4 seconds	Drive **safely** referenced
User agreement **not** within 4 seconds	Fault C01711/30711 with fault value 1002 Drive **not** safely referenced

Safe referencing
Schematic, initial referencing

Controller

e.g. T-CPU, SIMOTION

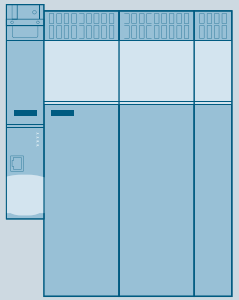


Reference position:
249°

Transfer the reference position to SINAMICS and acknowledge

User agreement

SINAMICS

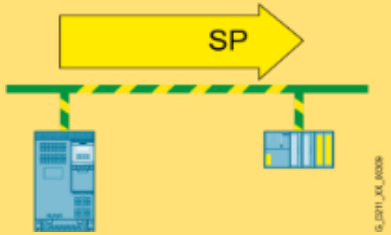


Reference position:
0°

Reference position:
249°

Referenced

Safely referenced at position:
249°



Safe referencing
Details, subsequent referencing

Subsequent referencing with motion controller (e.g. SIMOTION, T-CPU, …) is required

after switching on the Control Unit and after deparking the axis

Sequence

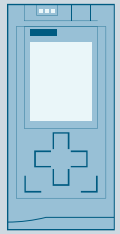
- Transfer the actual standard absolute position of the motion controller to SINAMICS (p9572), e.g. using an acyclic write task
- Confirm the transferred position (p9573)
- The firmware compares the actual standard absolute position with the last safe position before switching off the CU

Deviation **less than or equal to** the parameterizable tolerance (p9544)	Drive **safely** referenced
Deviation **greater than** the parameterizable tolerance (p9544)	Fault C01711/30711 with fault value 1003 Drive **not** safely referenced → initial ref.

Safe referencing
Schematic, subsequent referencing

Controller

e.g. T-CPU, SIMOTION

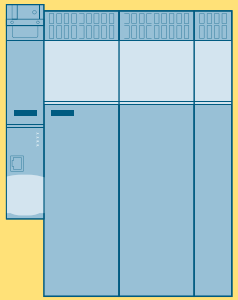


Actual position after switching on:

250°

Transfer the actual position to SINAMICS and acknowledge

SINAMICS



Last safe position before switch-off:

249°

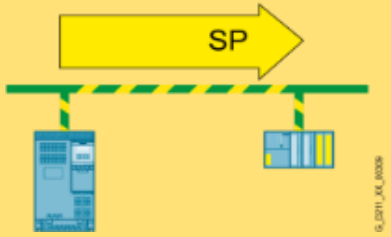
Comparison:

Within tolerance?

Yes

Safely referenced at position:

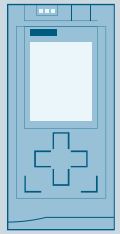
250°



Safe referencing
Schematic, subsequent referencing

Controller

e.g. T-CPU, SIMOTION

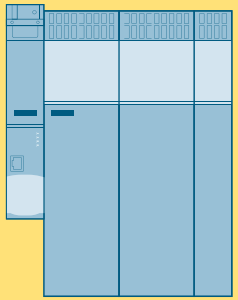


Actual position after switching on:

145°

Transfer the actual position to SINAMICS and acknowledge

SINAMICS



Last safe position before switch-off:

249°

Comparison:

Within tolerance?

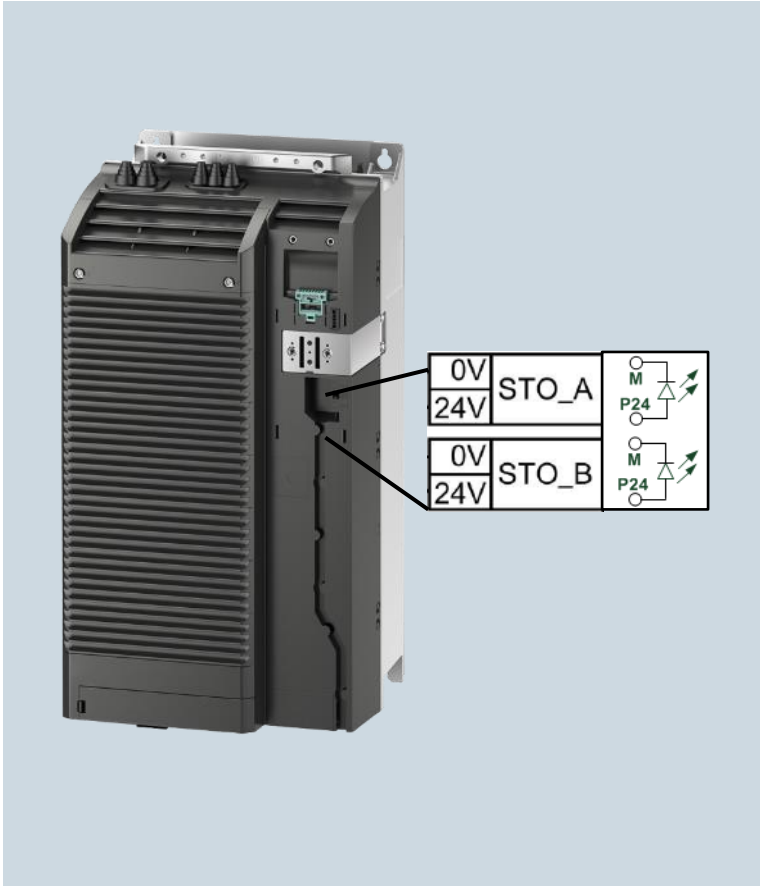
No

Not safely referenced!

Initial referencing required!

STO via terminals at the PM240-2 FSD - FSF

STO terminals at the PM240-2 FSD-FSF
Attributes



- Control with CU240E-2 and CU250S-2
  - ➔ Comply with the requirements according to Category 3 and PLe to ISO 13849 as well as SIL 3 to IEC 61508
  - ➔ Local Emergency Stop concepts can be simply implemented
- Can be used in parallel to the safety functions on the Control Unit
- 4ms hardware filter
  - ➔ Test pulses can be tolerated at the STO terminals

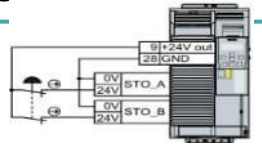
Preconditions for the subsequent connection examples

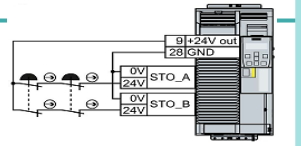
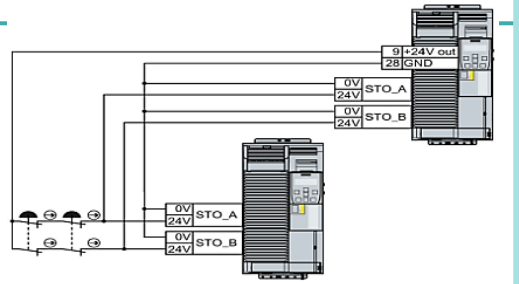
Cables are routed so that they are cross-circuit and short-circuit proof

▶ **Certificate**

STO terminals at the PM240-2 FSD-FSF
Connection examples for STO

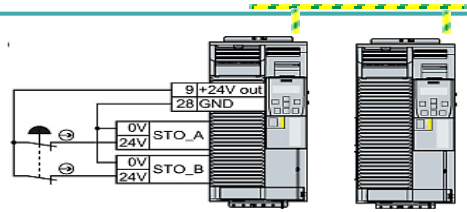
Connection examples for protective devices that cannot be passed around or behind according to EN ISO 13855		CU240E-2[1], CU250S-2[1]		CU230P-2, CU240B-2 CU305, CU310, CU320	
	HW-STO required in:	**SIL 2 / PL d**	**SIL 3 / PL e**	**SIL 2 / PL d**	**SIL 3 / PL e**

Connecting an Emergency Stop command device		• Integration in the Basic Functions with
		  • Discrepancy monitoring
		  • Forced checking procedure (test stop)
		  • Selection/deselection SBC (SIL2) with STO
		  • Signal "STO_active" (SIL2 / PLd) using F-DQ and PROFIsafe
		• SIL 2 / PLd: Test stop once per year
		• SIL 3 / PLe: Test stop every 3 months
		
		➔ Complete safety function for local Emergency Stop Concept
				Not supported	

Series circuit of several Emergency Stop command devices connected to one converter					
Parallel control of several converters with one Emergency Stop command device					

[1] CU240-2 standard and failsafe as well as CU250S-2 with/without safety license from V4.7 SP3

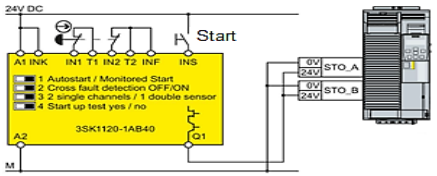
STO terminals at the PM240-2 FSD-FSF
Connection examples for STO

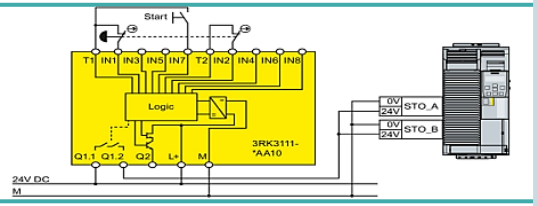
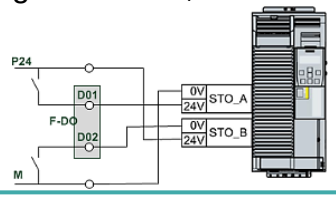
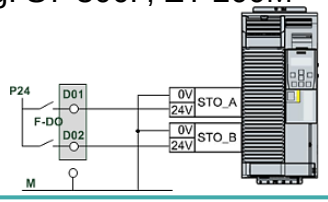
Connection examples for protective devices that cannot be passed around or behind according to EN ISO 13855		CU240E-2[1], CU250S-2[1]		CU230P-2, CU240B-2 CU305, CU310, CU320	
	HW-STO required in:	SIL 2 / PL d	SIL 3 / PL e	SIL 2 / PL d	SIL 3 / PL e
STO transfer via PROFIsafe		By evaluating "STO active“, STO can be controlled (in SIL2 / PLd) on other CUs via the F-PLC	Not supported	Not supported	

[1] CU240-2 standard and failsafe as well as CU250S-2 with/without safety license from V4.7 SP3

STO terminals at the PM240-2 FSD-FSF
Connection examples for STO

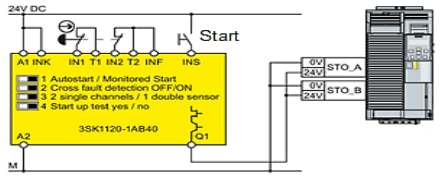
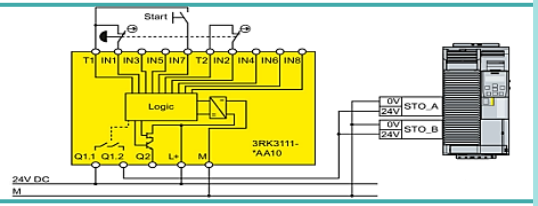
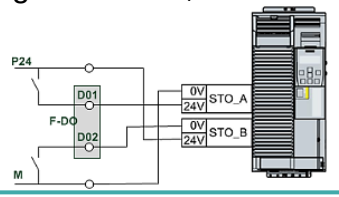
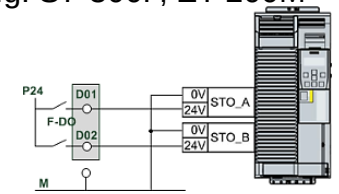
Connection examples for protective devices that can be passed around or behind according to EN ISO 13855	CU240E-2[1], CU250S-2[1]	
HW-STO required in:	**SIL 2 / PL d**	**SIL 3 / PL e**

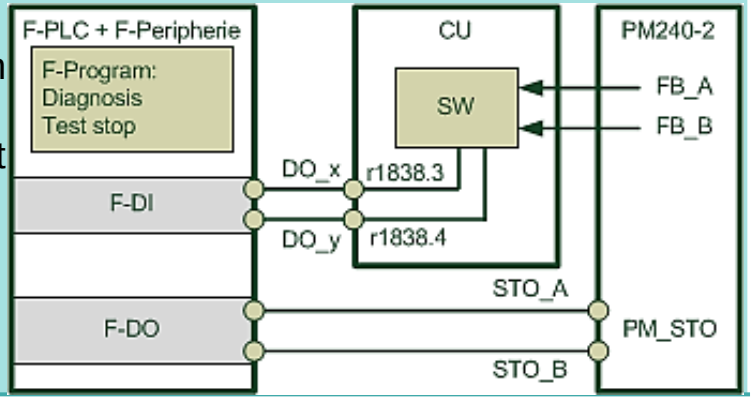
SIRIUS 3SK2 	• Same properties as for the connection examples for protective devices that cannot be passed around or behind
	
	• In addition:
	Manual reset function according to ISO 13849-1 required, e.g. with:
	  • SIRIUS 3SK2
	  • MSS 3RK3
	  • SIMATIC S7	

SIRIUS 3RK3 		
SIMATIC S7 P/M switching e.g. S7-1200F, ET 200SP 		
P/P switching e.g. S7-300F, ET 200M 		

[1] CU240-2 standard and failsafe as well as CU250S-2 with/without safety license from V4.7 SP3

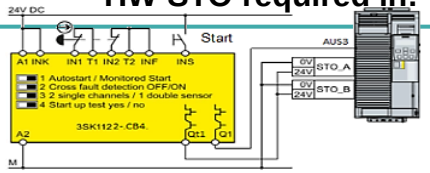
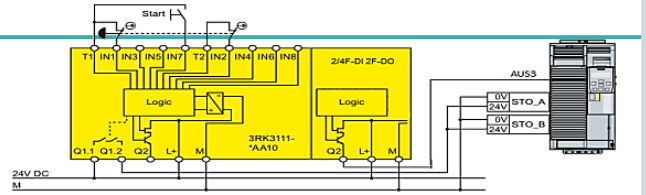
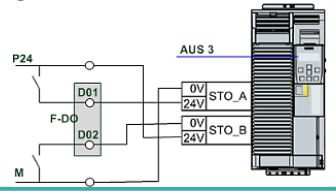
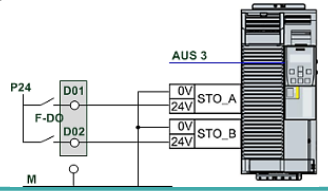
STO terminals at the PM240-2 FSD-FSF
Connection examples for STO

Connection examples for protective devices that can be passed around or behind according to EN ISO 13855	CU230P-2[2], CU240B-2[2] CU305[3], CU310-2[4], CU320-2 with CUA32[4]
HW-STO required in:	**SIL 2 / PL d** — **SIL 3 / PL e**
SIRIUS 3SK2 	• No discrepancy monitoring by the CU ➔ External discrepancy monitoring, e.g. using: • SIRIUS 3SK2 2 channel dyn. feedback circuit • MSS 3RK3: 2 channel dyn. feedback circuit • SIMATIC: F program (e.g. FDBACK) • No timer up to executing the test stop ➔ A timer function is implemented in the PLC user program • SIL 2 / PL d: Test stop once per year • SIL 3 / PL e: Test stop every 3 month • Provision of the feedback signal cont of the internal PM240-2 relay via BiCo at the DQ of the CU
SIRIUS 3RK3 	
SIMATIC S7 P/M switching e.g. S7-1200F, ET 200SP  P/P switching e.g. S7-300F, ET 200M 	



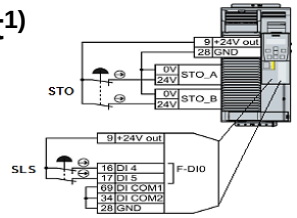
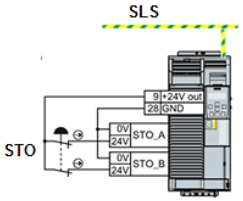
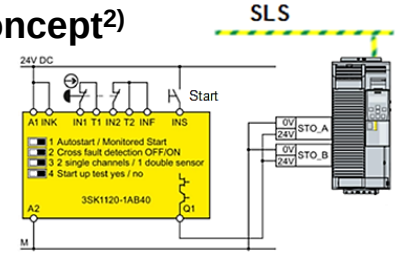
[2] From V4.7 SP3 [3] From V4.4 SP3 [4] From V4.8

STO terminals at the PM240-2 FSD-FSF
Connection examples for SS1

Connection examples for protective devices that can be passed around or behind and protective devices that cannot be passed around or behind	CU240E-2[1], CU250S-2[1]		CU230P-2[2], CU240B-2[2] CU305[3], CU310-2[4], CU320-2 with CUA32[4]	
HW-STO required in:	**SIL 2 / PL d**	**SIL 3 / PL e**	**SIL 2 / PL d**	**SIL 3 / PL e**
SIRIUS 3SK1 	• Same properties as for the connection examples for protective devices that can be passed around or behind for STO • In addition: Controlling the OFF3 ramp of the SINAMICS via standard terminals and delayed control of STO			
SIRIUS 3RK3 				
SIMATIC S7 P/M switching e.g. S7-1200F, ET 200SP  P/P switching e.g. S7-300F, ET 200M 				

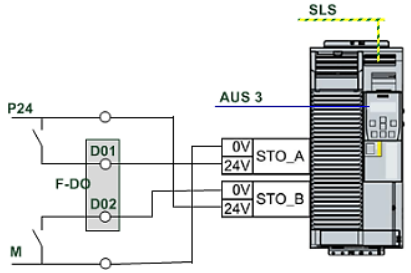
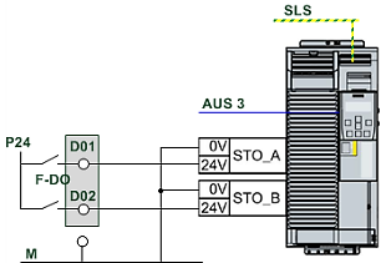
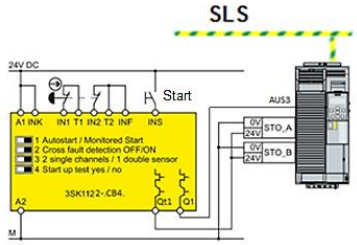
[1] CU240-2 standard and failsafe as well as CU250S-2 with/without safety license from V4.7 SP3
[2] From V4.7 SP3 [3] From V4.4 SP3 [4] From V4.8

STO terminals at the PM240-2 FSD-FSF + F-DI on the CU
Connection examples for STO and SLS

Connection examples	Control Unit	CU240E-2[3], CU250S-2[3]		CU230P-2, CU240B-2 CU305, CU310, CU320	
	HW-STO required in:	SIL 2 / PL d	SIL 3 / PL e	SIL 2 / PL d	SIL 3 / PL e
Local Emergency Stop concept[1] and SLS via local connection command device		Makes sense for stand-alone solutions (without automation)	Makes sense if STO is required in SIL3 / PLe (SLS in SIL2 / PLd)	Not supported	
Local Emergency Stop concept[1] and SLS via PROFIsafe		Wiring is not practical ➔ Implement control completely via PROFIsafe	Makes sense if STO is required in SIL3 / PLe (SLS in SIL2 / PLd)		
Local Emergency Stop concept[2] and SLS via PROFIsafe			Makes sense if STO is required in SIL3 / PLe Manual reset function required for protective devices that can be passed around or behind		

[1] For protective devices that cannot be passed around or behind according to EN ISO 13855
[2] For protective devices that can be passed around or behind according to EN ISO 13855
[3] CU240-2 standard and failsafe as well as CU250S-2 with/without safety license from V4.7 SP3

STO terminals at the PM240-2 FSD-FSF + F-DI on the CU
Connection examples for SS1 and SLS

Connection examples for protective devices that can be passed around or behind and protective devices that cannot be passed around or behind	CU240E-2[1], CU250S-2[1]		CU230P-2, CU240B-2 CU305, CU310, CU320	
HW-STO required in:	**SIL 2 / PL d**	**SIL 3 / PL e**	**SIL 2 / PL d**	**SIL 3 / PL e**
Local Emergency Stop concept via SIMATIC I/O and SLS via PROFIsafe P/M switching e.g. S7-1200F, ET 200SP  P/P switching e.g. S7-300F, ET 200M  	Same properties as for the connection examples for STO and SLS		Not supported	
Local Emergency Stop concept and SLS via PROFIsafe  				

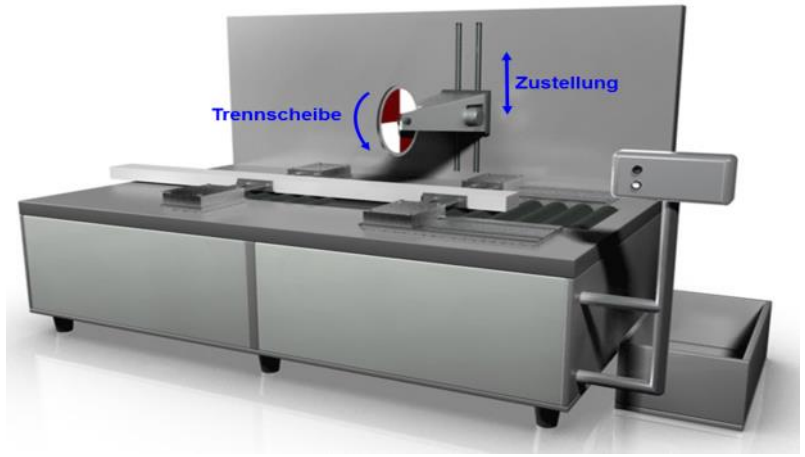
[1] CU240-2 standard and failsafe as well as CU250S-2 with/without safety license from V4.7 SP3

Validating safety functions

- Fundamentals
- Acceptance test for Safety Integrated

Fundamentals

Fundamentals
3 process steps



The Machinery Directive navigates the way to obtain a safe machine in three distinct process steps:

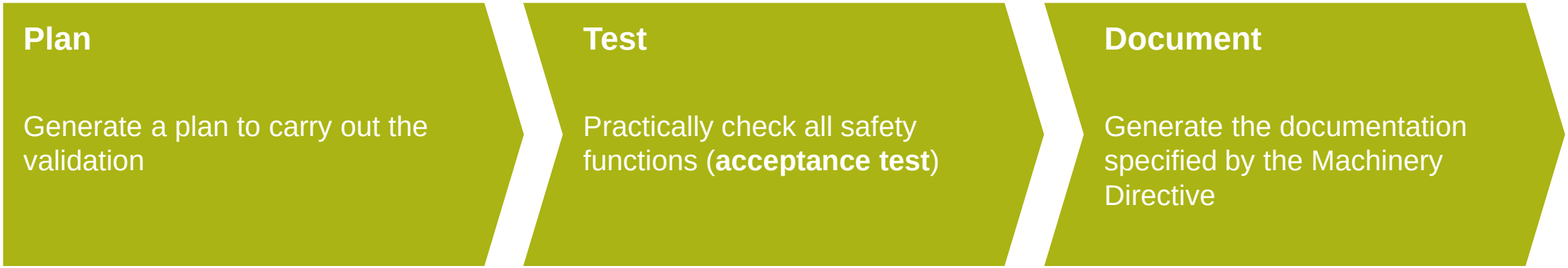
Risk assessment → **Risk minimization** → **Verification**

Fundamentals
Verification in detail

The manufacturer must carry out the following steps in detail for the verification:

Fundamentals
Validation in detail

Conformity with the Machinery Directive is verified through successful validation



- Check and document measures to minimize risk across all product fabrication phases
- Phased verification during the product fabrication process within the scope of the V model according to ISO 13849-1
- Renewed verification with (partial) acceptance test when changes are made to the machine

Acceptance test for Safety Integrated

Acceptance test for Safety Integrated
Overview

Benefits

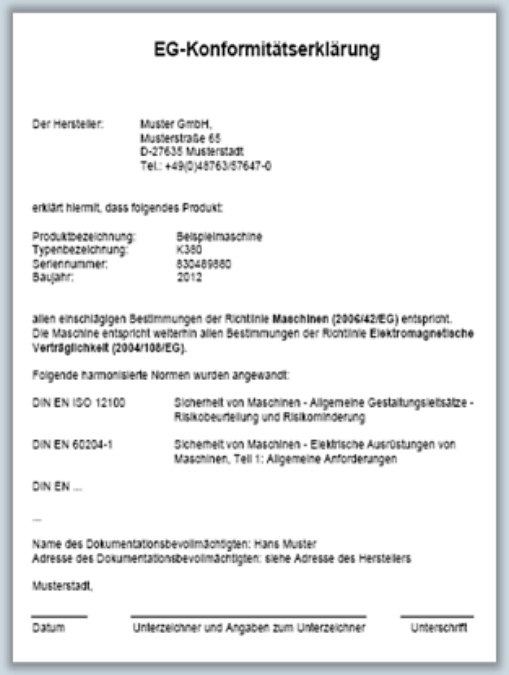
- A check is made that the safety functions have been correctly parameterized
- The configured safety functions are subject to a plausibility check based on
  - Measuring response times
  - Monitoring stop responses when limit values are violated

    → Detecting potential configuring errors
- Documenting the parameterized safety functions

The acceptance test and its documentation are important elements for the CE marking!

Acceptance test for Safety Integrated
EC Declaration of Conformity and CE marking

EC Declaration of Conformity



EG-Konformitätserklärung

Der Hersteller: Muster GmbH,
Musterstraße 65
D-27635 Musterstadt
Tel.: +49(0)48763/67647-0

erklärt hiermit, dass folgendes Produkt:

Produktbezeichnung: Beispielmaschine
Typenbezeichnung: K360
Seriennummer: 83048980
Baujahr: 2012

allen einschlägigen Bestimmungen der Richtlinie **Maschinen (2006/42/EG)** entspricht.
Die Maschine entspricht weiterhin allen Bestimmungen der Richtlinie **Elektromagnetische Verträglichkeit (2004/108/EG)**.

Folgende harmonisierte Normen wurden angewandt:

DIN EN ISO 12100 Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung

DIN EN 60204-1 Sicherheit von Maschinen - Elektrische Ausrüstungen von Maschinen, Teil 1: Allgemeine Anforderungen

DIN EN ...

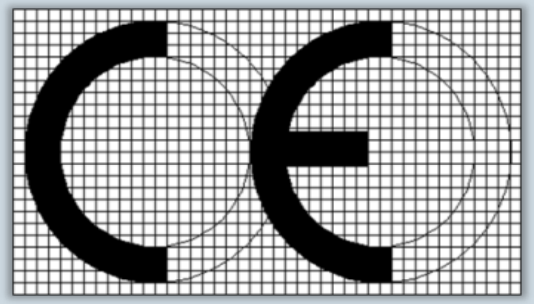
...

Name des Dokumentationsbevollmächtigten: Hans Muster
Adresse des Dokumentationsbevollmächtigten: siehe Adresse des Herstellers

Musterstadt,

Datum | Unterzeichner und Angaben zum Unterzeichner | Unterschrift

CE marking



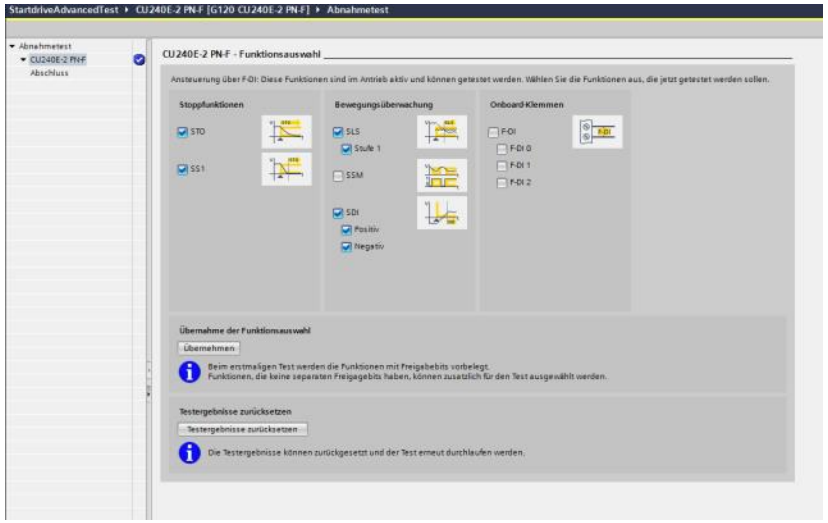
The manufacturer:

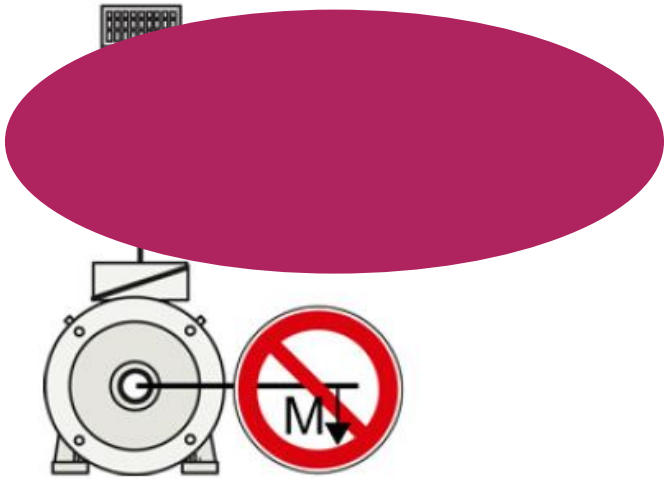
- Confirms that the Machinery Directive is complied with based on a Declaration of Conformity
- Confirms that all of the relevant directives have been complied with based on the CE marking
- In the case of damage, can verify that the machine is in conformance with the applicable directives

The path to a safe machine is completed with the EC Declaration of Conformity and the CE marking.

Acceptance test for Safety Integrated Possibilities

Manual	Safety acceptance test from Startdrive V15.1	Customer-specific
Step-by-step description	Safety Integrated acceptance test • Navigation using the acceptance test wizard • Generation of an acceptance test report • Available for SINAMICS G, S120 and S210	The customer draws up acceptance instructions and documents these according to EN ISO 13849-1 and EN ISO 13849-2.



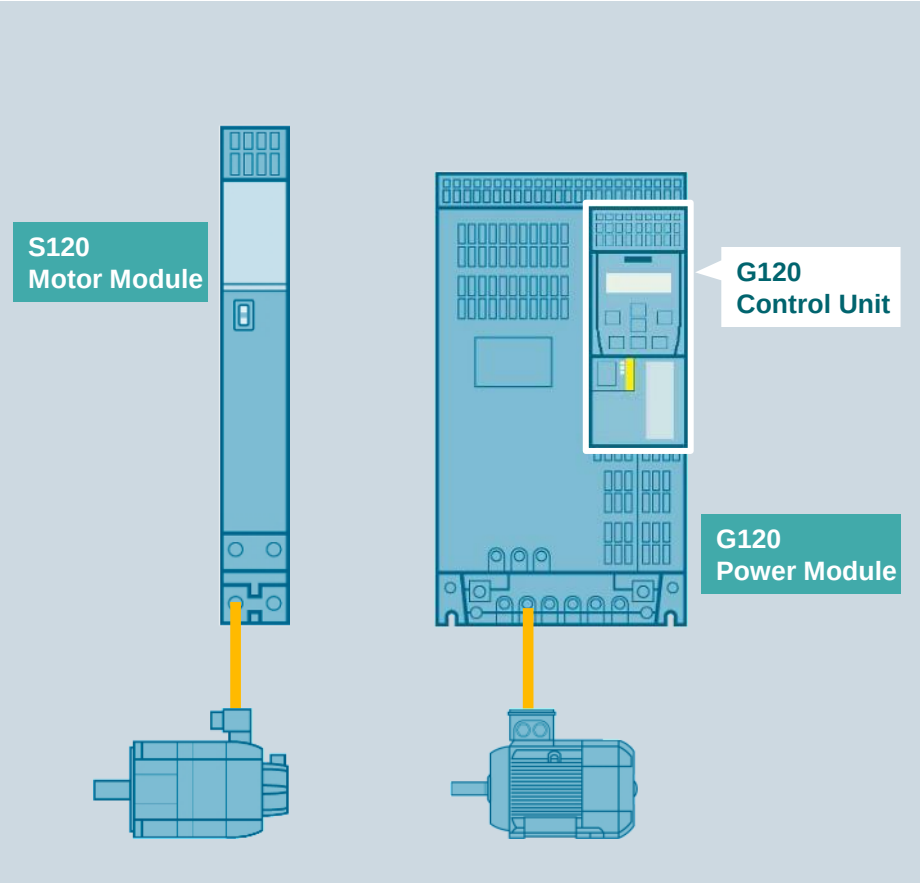


Replacing components

- Checksums
- Replacing components – S120
- Replacing components – G120

Checksums

Checksums
Safety Basic, Extended and Advanced Functions



Channel 1

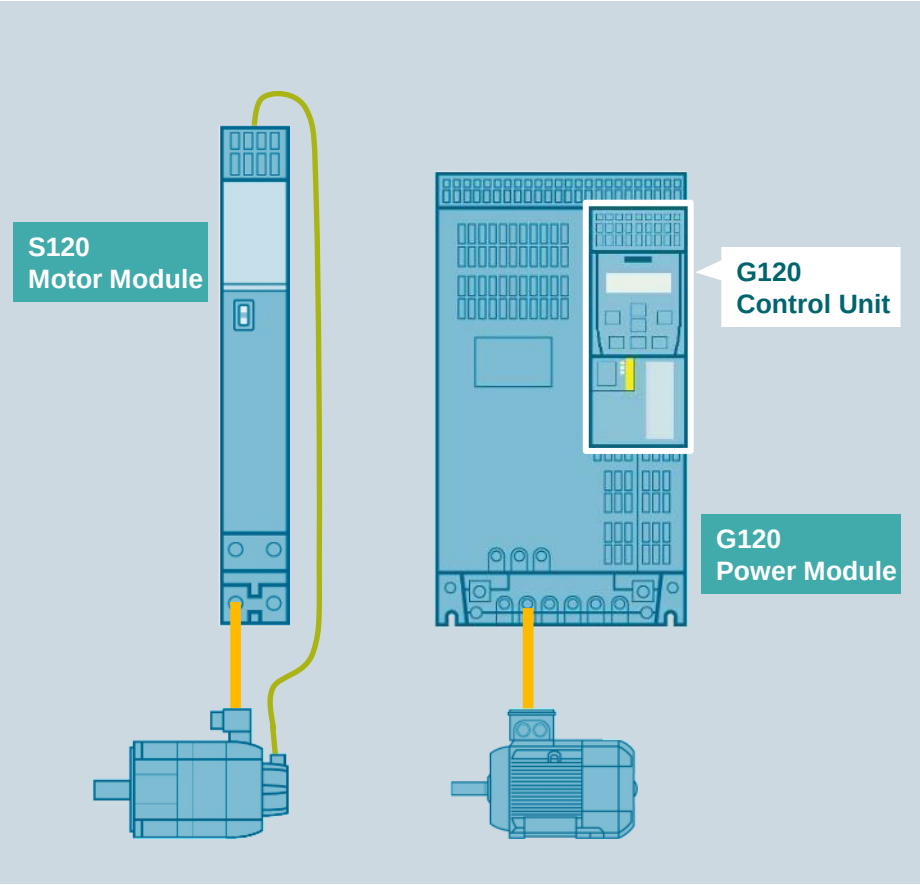
p9799: Reference checksum SI parameters

Channel 2

p9899: Reference checksum SI parameters

→ Checksum change as soon as a safety parameter of the Basic Functions is changed

Checksums
Safety Extended and Advanced Functions



Channel 1

p9729[0]: Reference checksum SI parameters for motion monitoring

→ Checksum change as soon as a safety parameter that is not referred to encoder data Extended/Advanced Functions changes

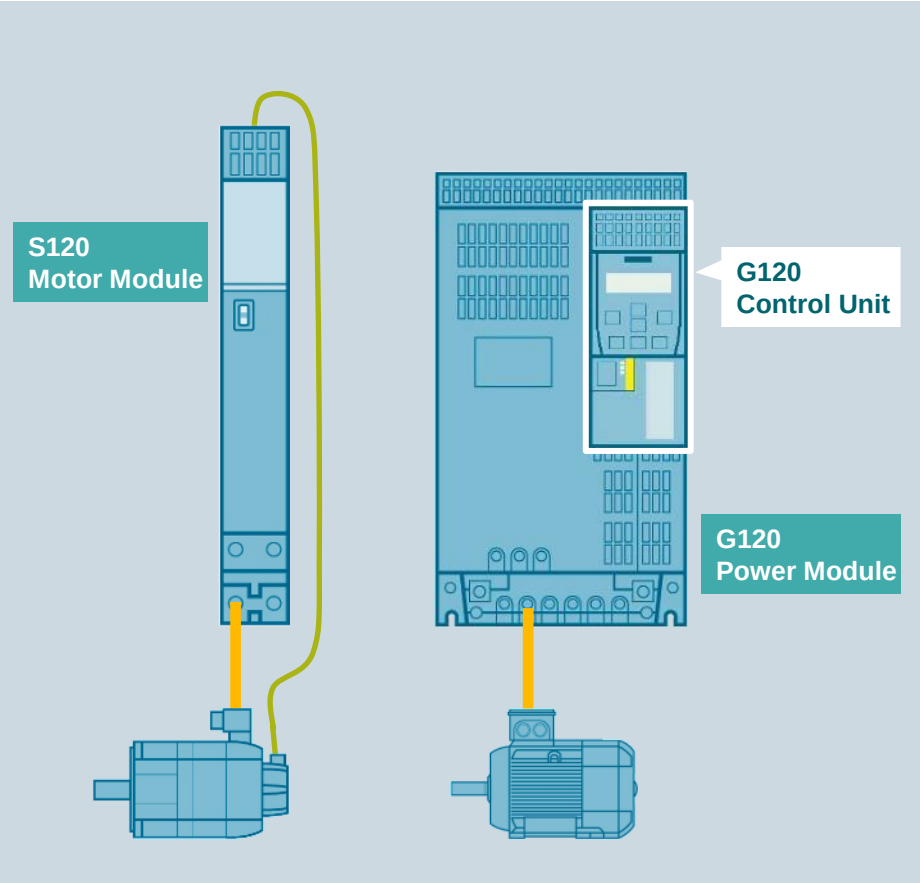
p9729[1]: Reference checksum SI parameters for actual values

→ Checksum change as soon as encoder parameters change (e.g. encoder pulse number or fine resolution) – or mechanical settings (e.g. gearbox or spindle pitch)

p9729[2]: Reference checksum SI parameters for hardware

→ Checksum change as soon as a Sensor Module, evaluated by Safety Integrated, is replaced

Checksums
Safety Extended and Advanced Functions



Channel 2

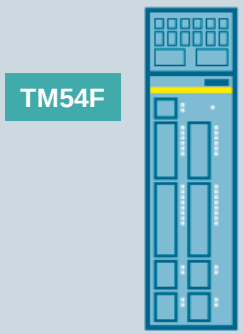
p9399[0]: Reference checksum SI parameters for motion monitoring

→ Checksum change as soon as a safety parameter of Extended/Advanced Functions changes

p9399[1]: Reference checksum SI parameters with reference to hardware

→ Checksum change when replacing safety-relevant hardware

Checksums
TM54F



For master and slave module

p10005[0]:
Reference checksum, hardware-independent TM54F parameters

➔ Checksum change as soon as a safety parameter of the TM54F changes

p10005[1]:
Reference checksum, hardware-dependent TM54F parameters

➔ Checksum change if a Motor Module, controlled via the TM54F is replaced

Checksums
Safety logbook

S120 Control Unit

G120 Control Unit

The safety logbook is used to identify changes to safety parameters and the hardware.

Parameters

r9781[0]: Functional checksum

→ Change as soon as the safety parameter of a drive – assigned to the Control Unit or the TM54F – changes

r9781[1]: Hardware-dependent checksum

→ Change as soon as a Sensor Module evaluated by Safety Integrated or a Motor Module used with TM54F is replaced

r9782[0]: Time stamp for the functional checksum

r9782[1]: Time stamp for the hardware-dependent checksum

Replacing components – S120

Replacing components – S120
Components that can be replaced

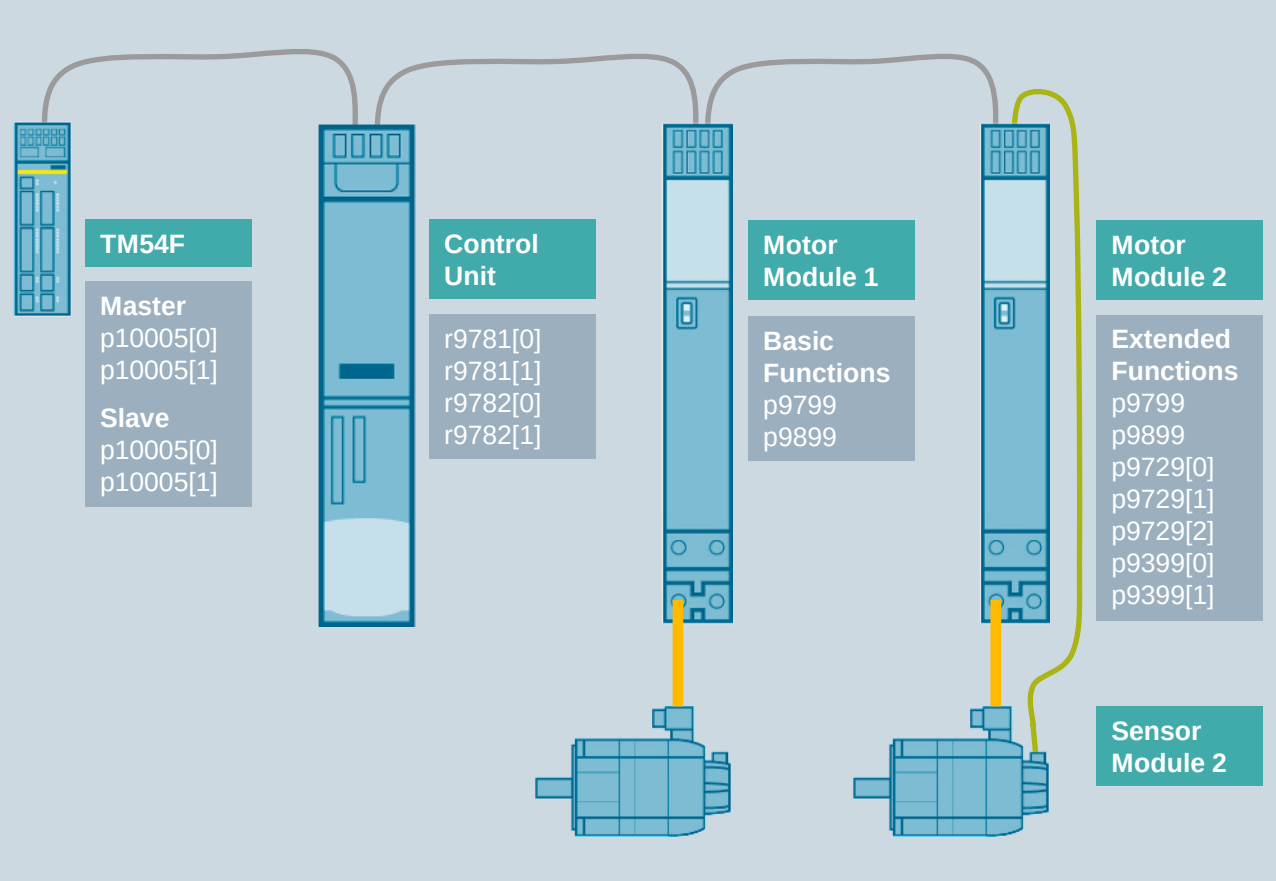
Control Unit

Motor Modules

Encoder evaluation

TM54F

Replacing components – S120
Checksums of the safety functions

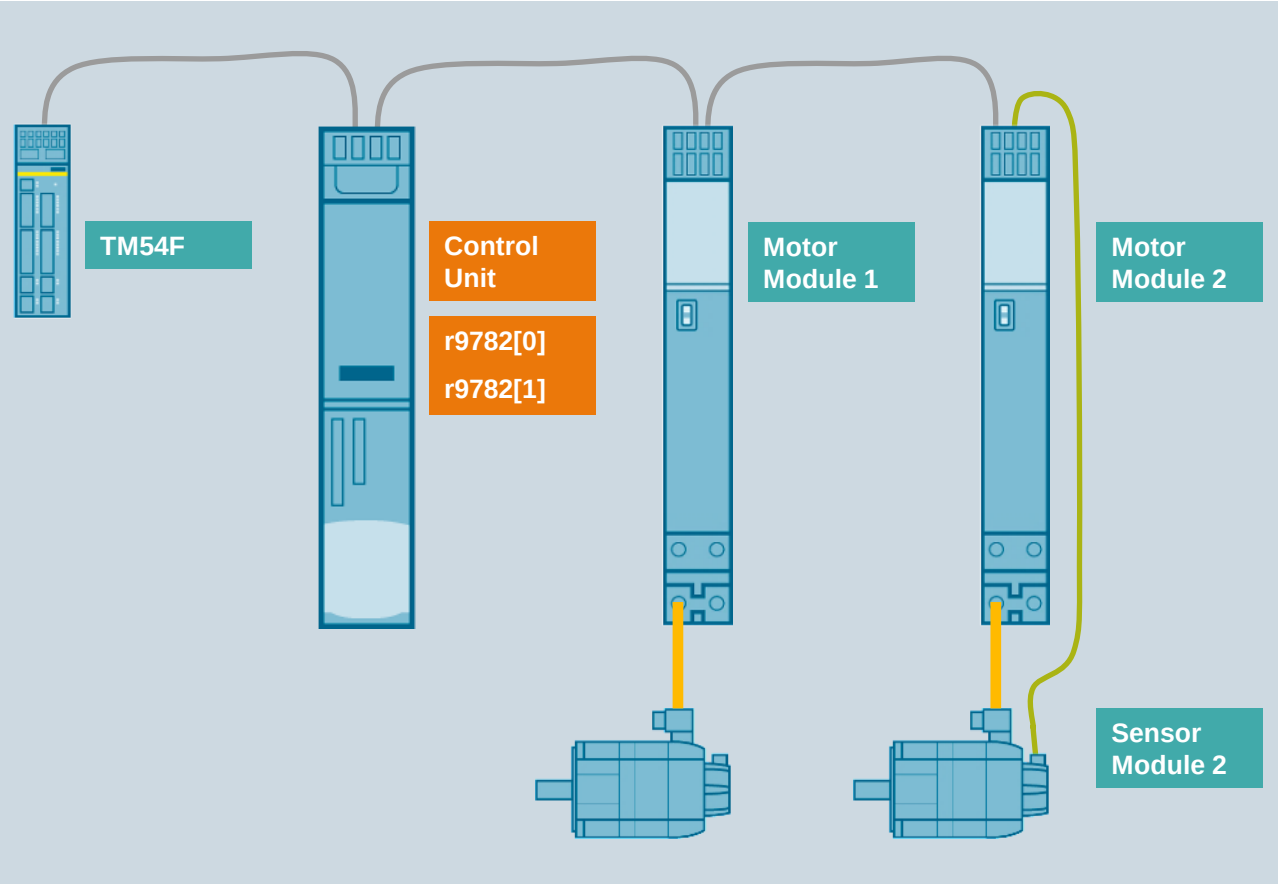


Example

The Basic Functions at Motor Module 1 are controlled via terminal – and the Extended/Advanced functions at Motor Module 2 are controlled via TM54F.

The relevant checksums are shown in the diagram at the left.

Replacing components – S120
Checksums of the safety functions



Action

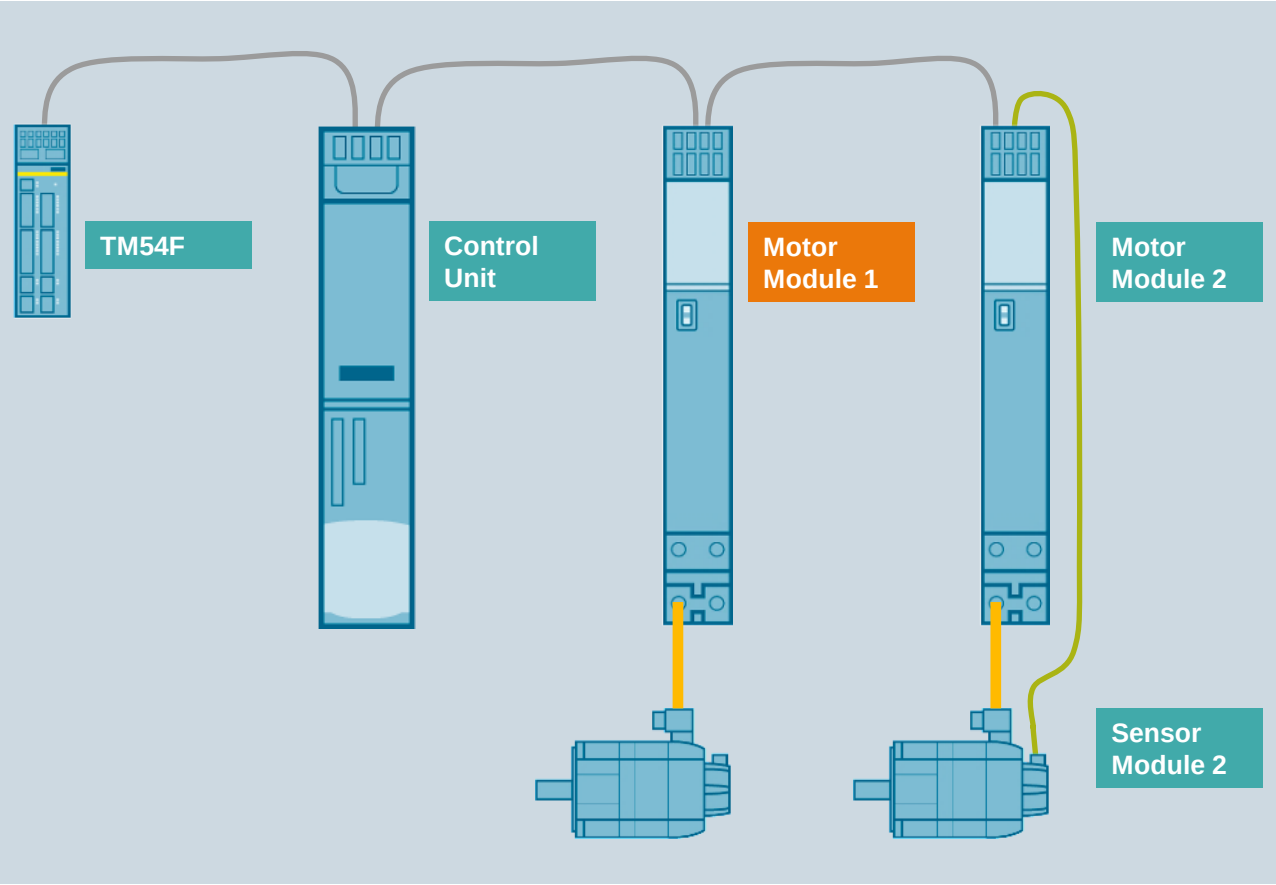
The Control Unit is replaced.
Which checksums change?

Response

The safety parameters are reloaded to the Control Unit

→ The time stamp (functional **r9782[0]** and hardware-related **r9782[1]**) change.

Replacing components – S120
Checksums of the safety functions



Action

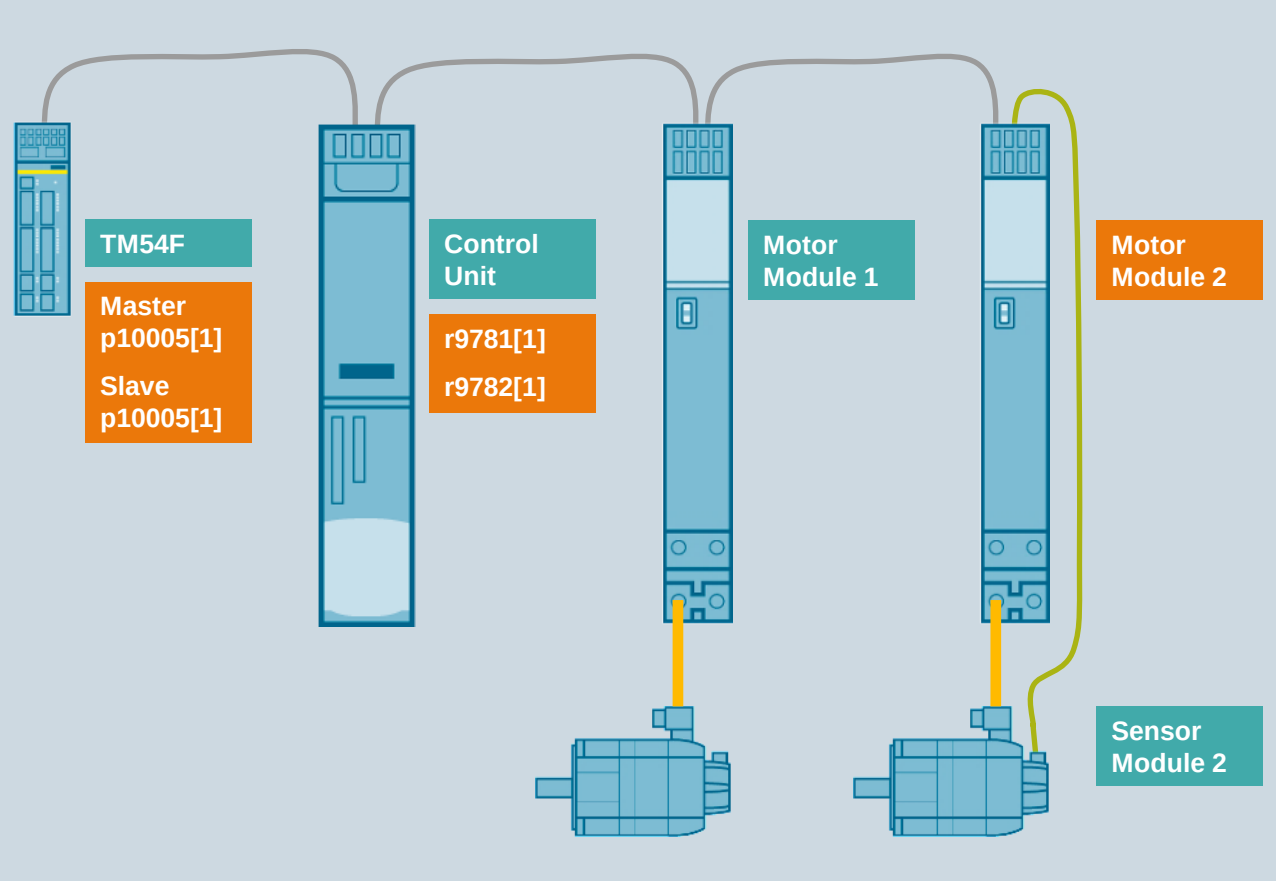
The Motor Module 1 is replaced.
Which checksums change?

Response

No checksum changes.

Reason: The Basic Functions are not controlled via the TM54F, but via terminal.

Replacing components – S120
Checksums of the safety functions



Action

The **Motor Module 2** is replaced.
Which checksums change?

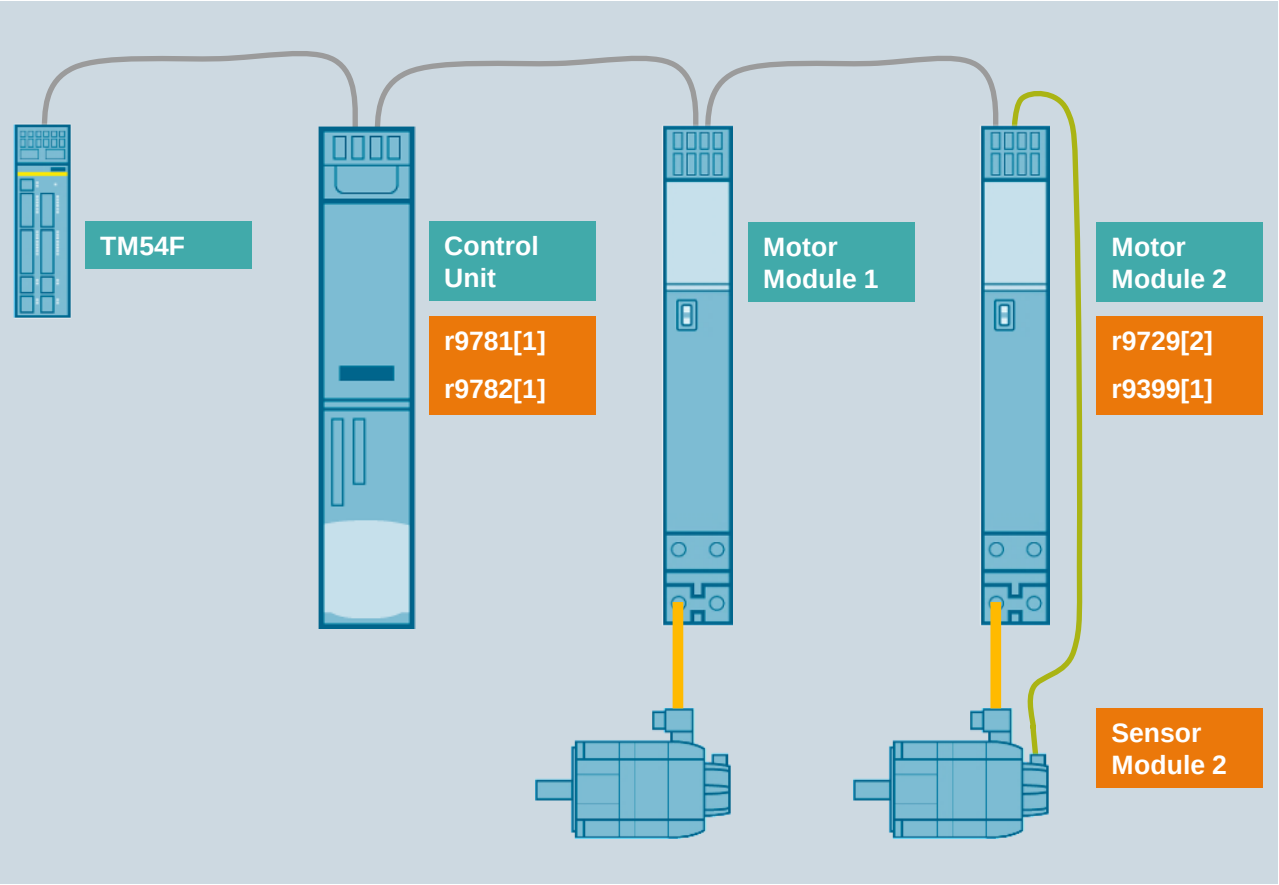
Response

- Checksum **p10005[1]** changes.

  Reason: The Extended/Advanced Functions are controlled via the TM54F.

- The changes are saved in the safety logbook (**r9781[1]**, **r9782[1]**).

Replacing components – S120
Checksums of the safety functions



Action

The **Sensor Module 2** is replaced.
Which checksums change?

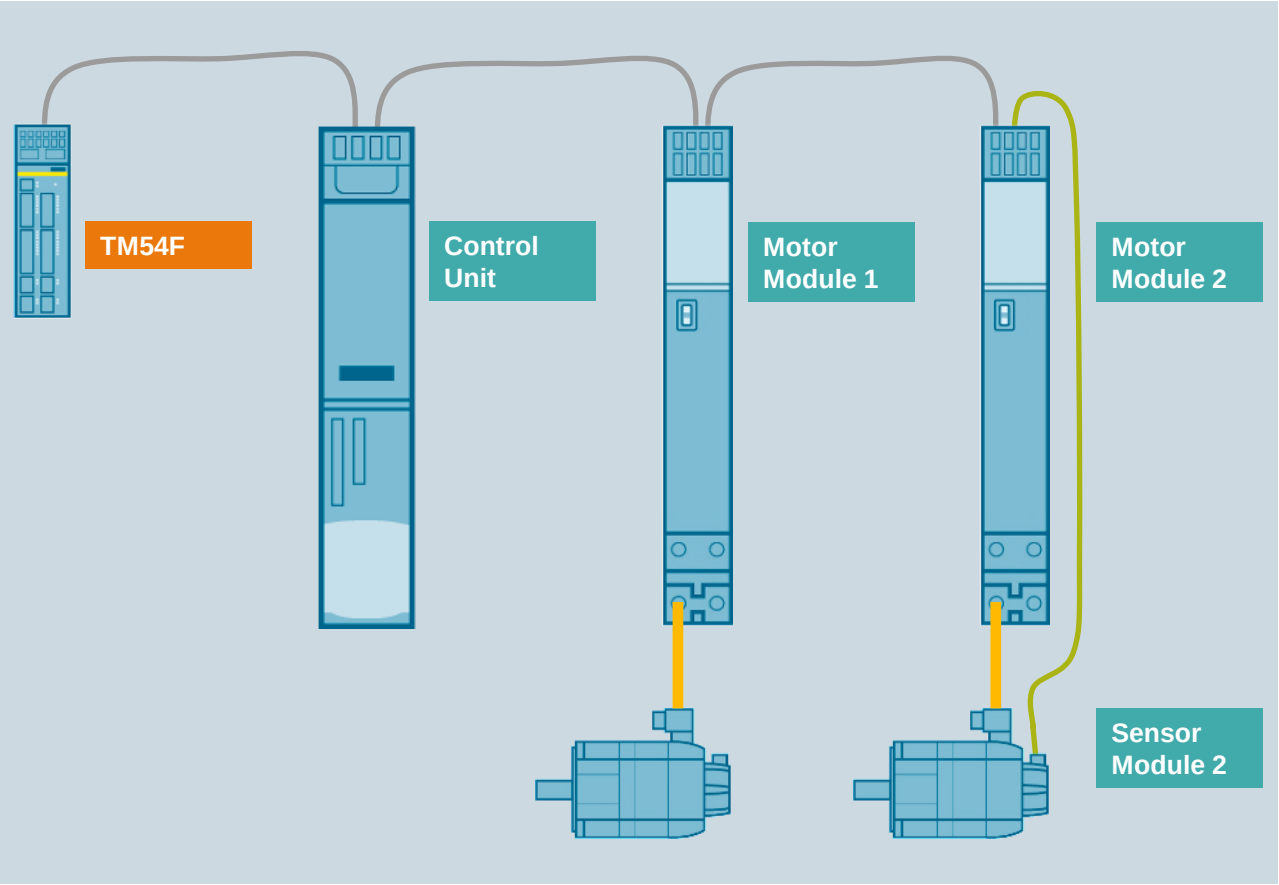
Response

- Checksums **p9729[2]** and **p9399[1]** change.

  Reason: The Extended/Advanced Functions are being used.

- The changes are saved in the safety logbook (**r9781[1]**, **r9782[1]**).

Replacing components – S120
Checksums of the safety functions



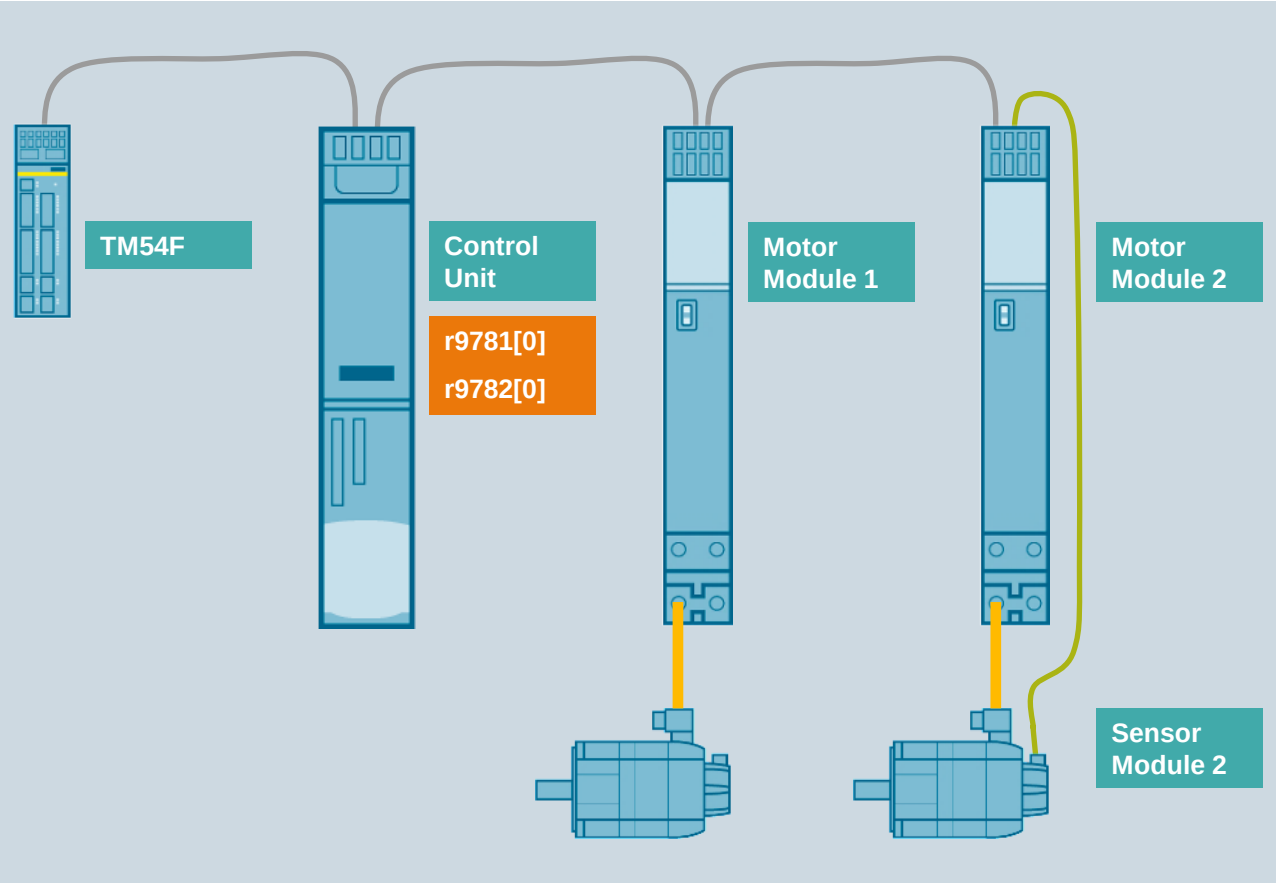
Action

The TM54F is replaced.
Which checksums change?

Response

No checksum changes.

Replacing components – S120
Checksums of the safety functions



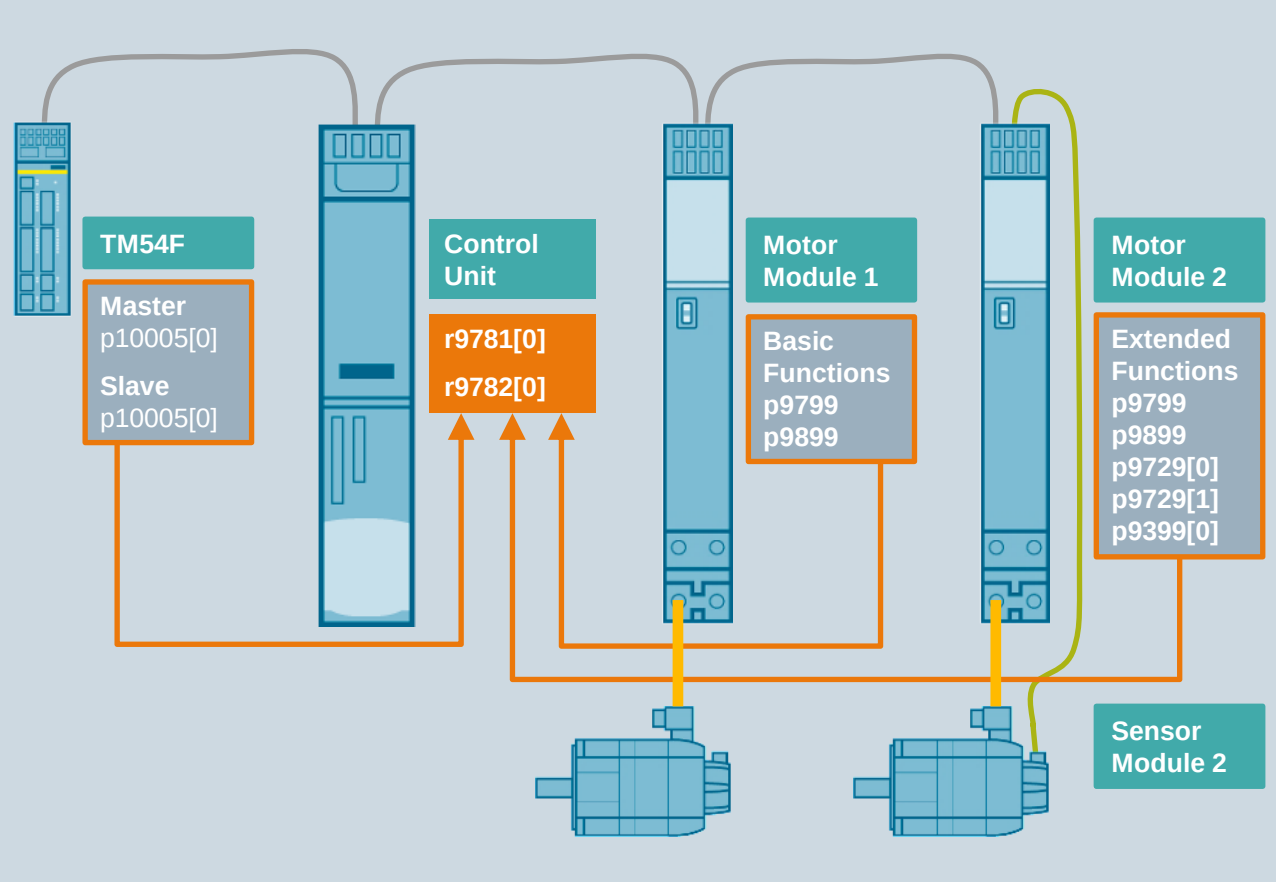
Action

A functional (i.e. not hardware-related) safety parameter is changed at any position.
Which checksums change?

Response

The changes are saved in the safety logbook of the assigned Control Unit (**r9781[0]**, **r9782[0]**).

Replacing components – S120
Summary



All changes to a functional safety parameter are documented and saved in the safety logbook!

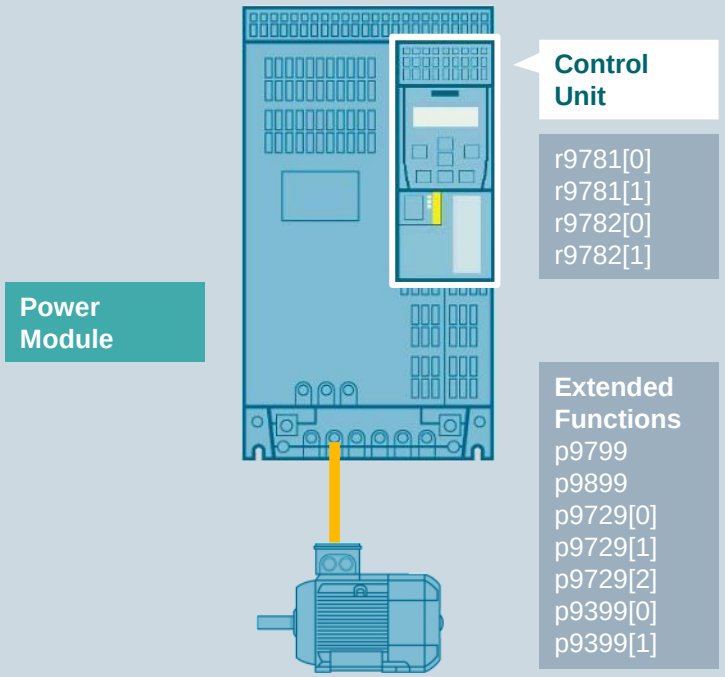
Replacing components – G120

Replacing components – G120
Components that can be replaced

Control Unit

Power Module

Replacing components – G120
Checksums of the safety functions

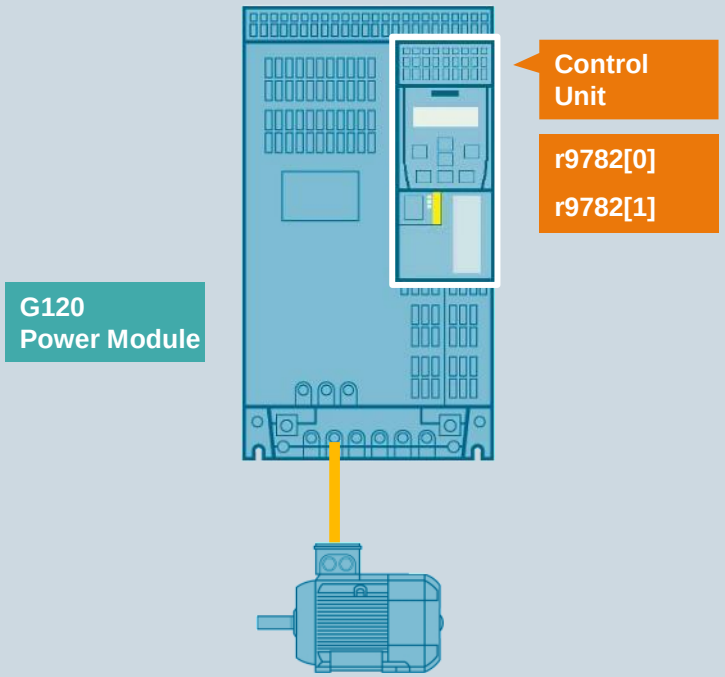


Example

The Extended Functions at a SINAMICS G120 are controlled.

The relevant checksums are shown in the diagram at the left.

Replacing components – G120
Checksums of the safety functions



Action

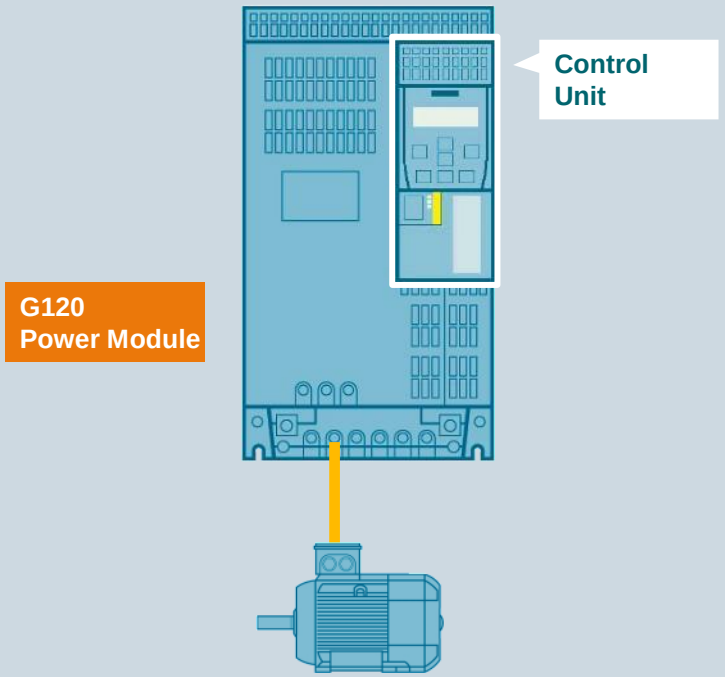
The **Control Unit** is replaced.
Which checksums change?

Response

The safety parameters are reloaded to the Control Unit

→ The time stamp (functional **r9782[0]** and hardware-related **r9782[1]**) change.

Replacing components – G120
Checksums of the safety functions



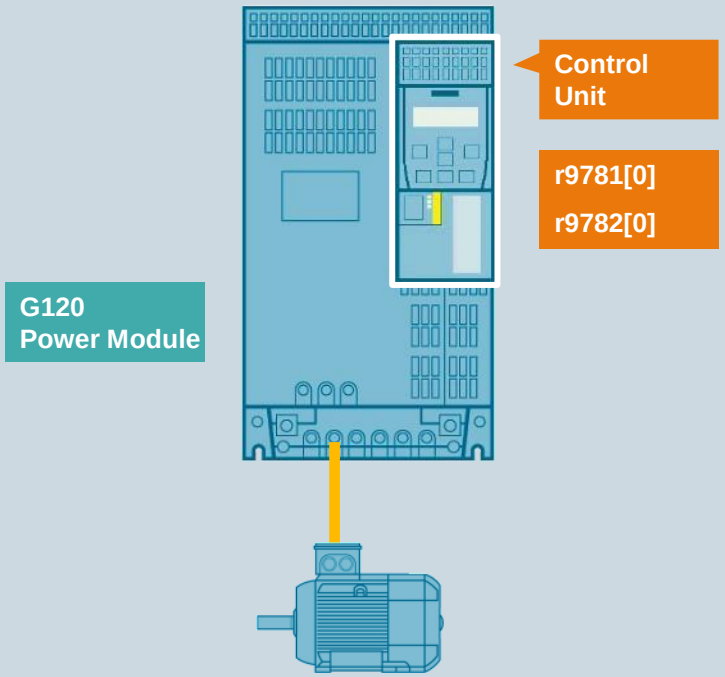
Action

The **Power Module** is replaced.
Which checksums change?

Response

No checksum changes.

Replacing components – G120
Checksums of the safety functions



Action

A functional (i.e. not hardware-related) safety parameter is changed at any position. Which checksums change?

Response

The changes are saved in the safety logbook of the assigned Control Unit (**r9781[0]**, **r9782[0]**).

Application examples

- Overview
- Selected examples

Overview

Overview
Broad selection of function examples and applications

DriveType | DriveFunction: Safety Integrated [46] | Control | EngineeringEnvironment | Communication
Speciality | Reset Filter

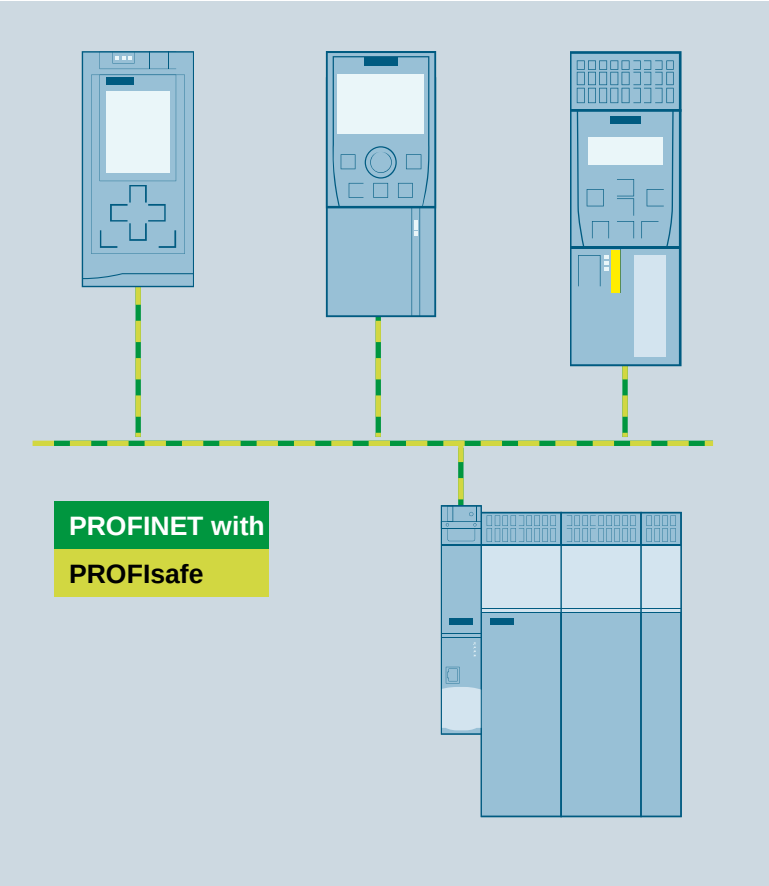
› Safety Integrated

Application	DriveType	DriveFunction	Control	EngineeringEnvironment	Communication	Speciality
› Controlling the Safety Integrated Functions of the SINAMICS S120 with a SIMATIC S7-1500F via PROFIsafe	S120	Safety Integrated	S7-1500	TIA-Portal	PROFINET	Startdrive
› SINAMICS, SIMOTION, SINUMERIK, SIMOTICS: Safety functions PFH/PFD - values	G110M G120 G120C G120D G120P G130 G150 S110 S210 S120 S150	Safety Integrated	- S7-1200 S7-1500 S7-1500T S7-300/400 SIMOTION D		- PROFIBUS PROFINET	
› SINAMICS G: SINAMICS G120 is controlled via PROFIsafe with a SIMATIC S7-1200 F-CPU	G120 G120C G120D	Speed control Safety Integrated	S7-1200	TIA-Portal	PROFINET	PROFISafe
› Safety position, standstill, direction and speed detection		Safety Integrated	S7-1500	TIA-Portal	PROFINET	
› SINAMICS G: Dimensioning and commissioning of serial hoisting equipment with G120	G120	Safety Integrated Hoist	-	-	-	-
› SINAMICS G: Positioning a G120 (Startdrive) with S7-1500 (TO) via PROFINET or PROFIBUS with Safety Integrated (via Terminal) and HMI	G110M G120 G120C G120D	Positioning Safety Integrated	S7-1500	TIA-Portal	PROFIBUS PROFINET	HMI
› SINAMICS G: Speed Control of a G120 (StartDrive) with S7-1200 (TIA Portal) via PROFINET/PROFIBUS DP with Safety Integrated (via Terminal) and HMI	G110M G120 G120C G120D G120P	Speed control Safety Integrated	S7-1200	TIA-Portal		

SINAMICS application examples

Selected examples

Selected examples
LDrvSafe failsafe library

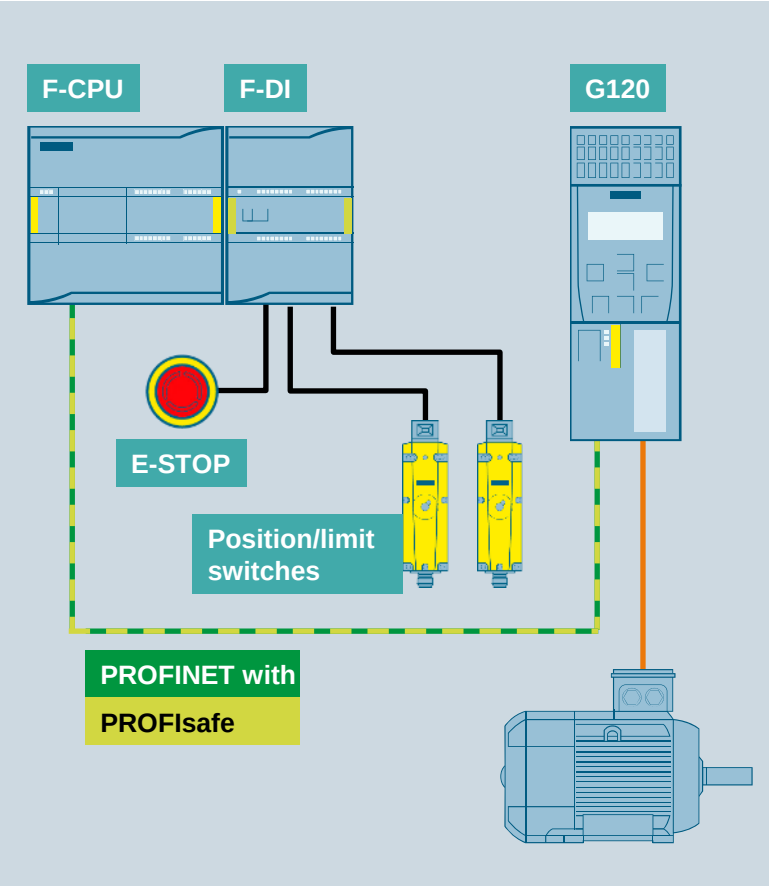


LDrvSafe failsafe library in the SINAMICS Safety Integrated environment

- Simple control and evaluation of all PROFIsafe telegrams
- Winder application – failsafe web velocity monitoring: Speed is safely corrected as a function of the roll diameter
- Acyclic blocks for
  - Safe referencing
  - Acknowledging hardware replacement
- Controlling and evaluating the Safety Info and Control Channels

SIOS-ID 109485794

Selected examples
Controlling SINAMICS G120 using PROFIsafe

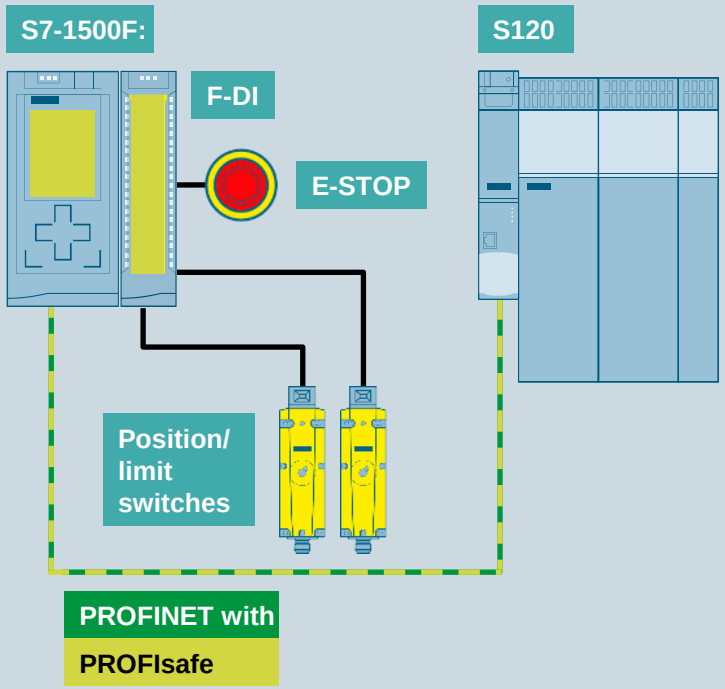


Controlling a SINAMICS G120 via PROFIsafe with a SIMATIC S7-1200 F-CPU

- Configuring and parameterizing a S7-1200 F-CPU via the TIA Portal
- Configuring safety-relevant communication between S7-1200 F-CPU and SINAMICS G120 via PROFIsafe
- Controlling Safety Extended Functions of the SINAMICS G120

SIOS-ID 109746271

Selected examples
Controlling safety functions via PROFIsafe

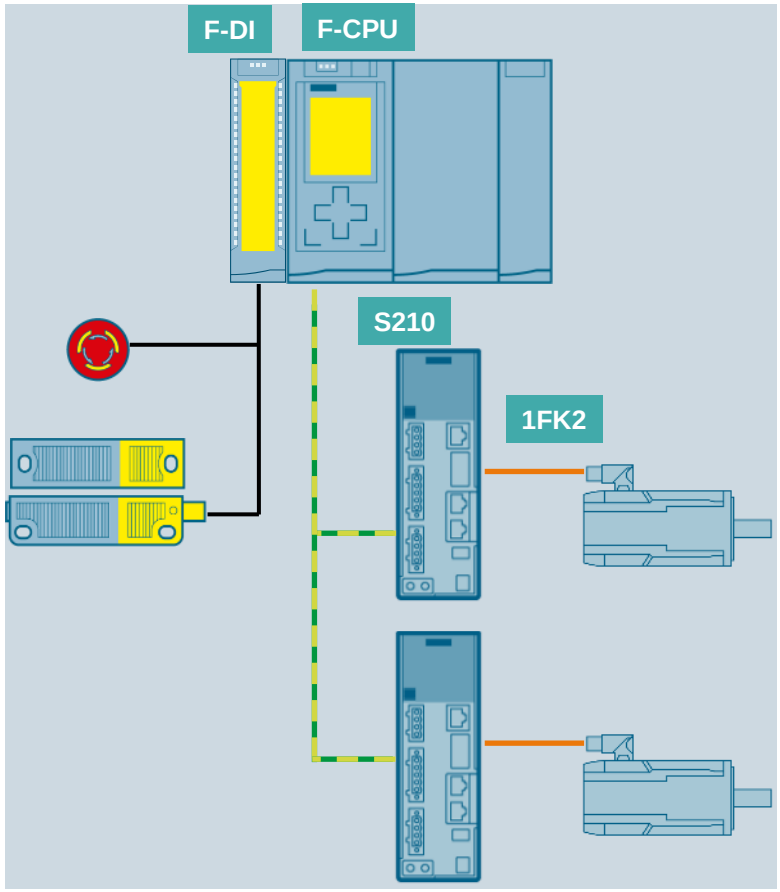


Controlling Safety Integrated Functions of the SINAMICS S120 with SIMATIC S7-1500F via PROFIsafe

- Configuring PROFIsafe telegram
- Configuring Safety Integrated Functions in the drive
- Writing F-program code for Safety Integrated Functions
- Commissioning Safety Integrated Functions

SIOS-ID 109749224

Selected examples
Controlling the Safety Integrated Functions of the SINAMICS S210 with SIMATIC S7-1500TF via PROFIsafe

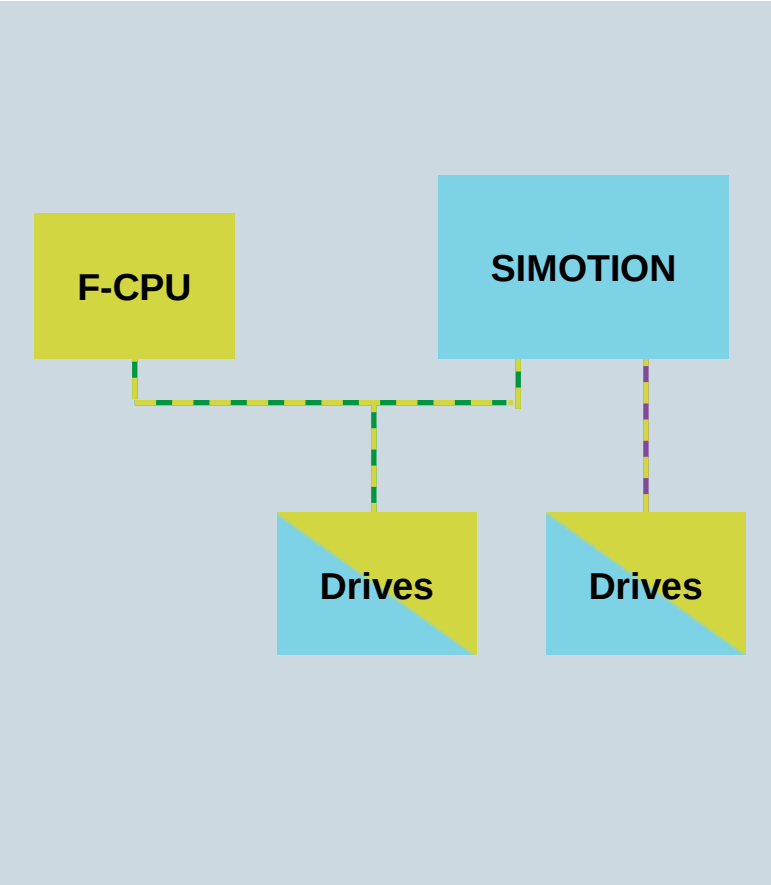


In addition to the standard drive functions, using a SIMATIC F-PLC the (Extended) Safety Integrated Functions of the SINAMICS S210 can be controlled using PROFIsafe.

- SIMATIC S7-1500 PLCs support the connection of drives as speed axis, positioning axis or synchronous operation axis via PROFINET or PROFIBUS.
- In the TIA Portal, it is possible to control a SINAMICS S210 drive in a TIA Portal program, and operate it using motion control instructions.

SIOS-ID 109760341

Selected examples
Controlling safety functions via SIMOTION



Controlling safety functions integrated in the drive using SIMOTION via PROFIsafe (I-Device F-Proxy)

- From SIMOTION V4.2, the *F-Proxy for PROFINET* functionality is available to connect SINAMICS drives (controlled from a SIMOTION control system) via PROFIsafe.
- The F-Proxy forms the interface between the F-CPU and the drive, and facilitates transparently transferring PROFIsafe telegrams from the F-CPU via the SIMOTION I-Device to the associated SIMOTION IO controller (PROFINET) where the drive is configured.

SIOS-ID 50207350