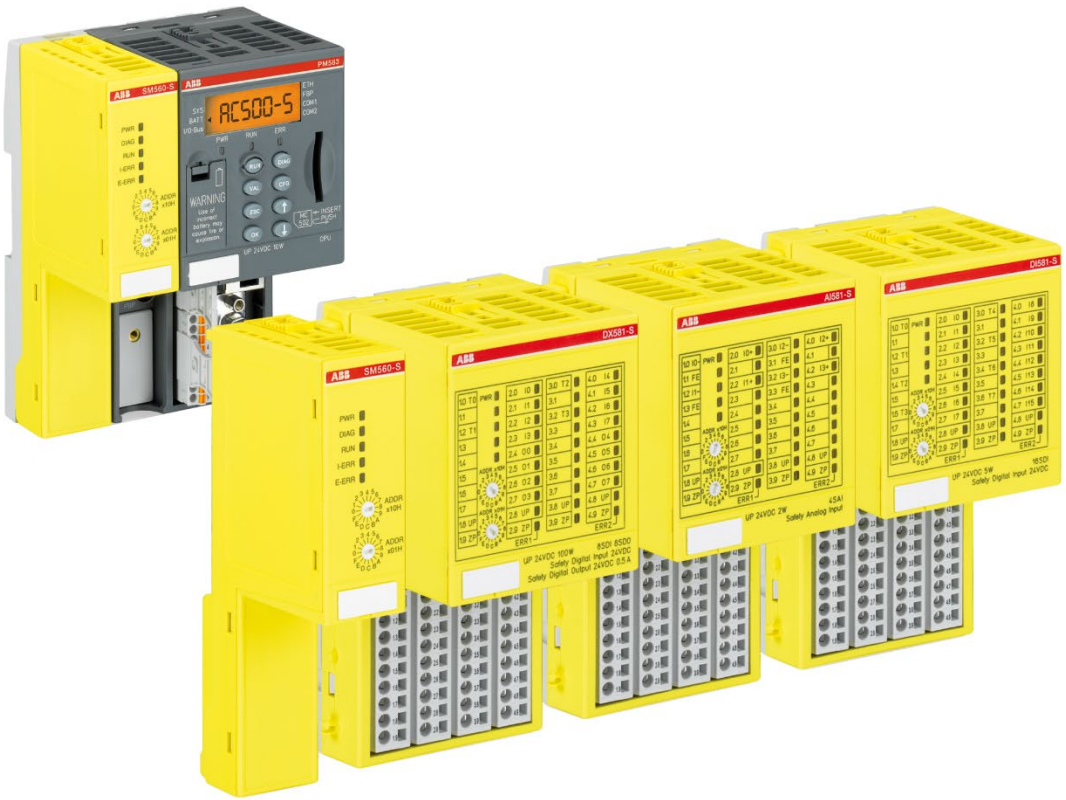
APPLICATION NOTE

AC500-S safety PLC

Usage of AC500 digital standard I/Os in functional safety applications up to PL c (ISO 13849-1)



Contents

1. Introduction 3
1.1. Purpose 3
1.2. Document history 3
1.3. Validity 3
1.4. Important user information 3
1.5. Definitions, expressions, abbreviations 4
1.6. References / related documents 4

2. Usage of digital standard I/Os in functional safety applications up to PL c 6
2.1. Overview 6
2.2. Task 7
2.3. Solution 8

3. Example 14
3.1. General 14
3.2. Safety function 14
3.3. Functional description 14
3.4. Design features 15
3.4.1. Implementation details 15
3.4.2. Common cause failures 17
3.4.3. Systematic failures 18
3.4.4. Safety function response time 18
3.5. Calculation of the probability of failure and correspondence to PL (ISO 13849-1) 19

4. Conclusion 21

1. Introduction

1.1. Purpose

The number of used digital safety input channels in safety applications is often significantly higher than the number of digital safety output channels. In some customer PLC applications, there are often free spare digital standard I/O channels. There is a question if these free spare digital standard I/O channels can be used together with SM560- S Safety CPU to realize functional safety functions. If yes, one could avoid using additional Safety I/O modules with digital safety input channels and, thus, save control system costs and reduce control cabinet dimensions in some customer applications.

We analyzed a possible usage of AC500 digital standard I/Os to realize functional safety functions. This application note describes a possible usage of digital standard I/O modules from AC500 platform (www.abb.com/PLC) in functional safety application up to PL c (ISO 13849-1). The functional safety calculation according to ISO 13849-1 is used as an example to show the compliance of the proposed approach with the relevant functional safety requirements for PL c (ISO 13849-1). The functional safety calculation according to IEC 62061 standard (applications up to SIL CL 1) can be similarly done, if required.

In special cases, digital standard I/O modules from AC500 platform can be also used in functional safety applications up to PL d (ISO 13849-1) and SIL CL 2 (IEC 62061). However, more detailed functional safety application analysis is required (contact AC500 technical support at www.abb.com/PLC for more details) and, thus, is not shown in this document.

1.2. Document history

Rev.	Description of version / changes	Who	Date
A (V1.0.0)	Final release	ABB	15.12.2015
B	Company name was changed. Various typos were corrected and various improvements in the texts and illustrations were made.	ABB	15.09.2021

1.3. Validity

The data and illustrations found in this documentation are not binding. ABB reserves the right to modify its products in line with its policy of continuous product development.

ABB assumes no liability or responsibility for any consequences arising from the use of this document information. ABB is in particular in no way liable for missed profits, loss of income, loss of life, loss of use, loss of production, capital costs or costs associated with an interruption to operation, the loss of expected savings or for indirect or follow up damages or losses no matter of what kind.

1.4. Important user information

This documentation is intended for qualified personnel familiar with Functional Safety. You must read and understand the safety concepts and requirements presented in AC500-S Safety User Manual [1.] as well as further referenced documents prior to operating AC500-S Safety PLC system.

The following special notices may appear throughout this documentation to warn of potential hazards or to call attention to specific information.

⚠ DANGER

The notices referring to your personal safety are highlighted in the manual by this safety alert symbol, which indicates that death or severe personal injury may result if proper precautions are not taken.

NOTICE

This symbol of importance identifies information that is critical for successful application and understanding of the product. It indicates that an unintended result can occur if the corresponding information is not taken into account.

1.5. Definitions, expressions, abbreviations

AC500	ABB PLC, refer also to www.abb.com/PLC for further details
AC500-S	ABB Safety PLC for applications up to SIL3 (IEC 61508 ed. 2 and IEC 62061) and PL e (ISO 13849-1), refer also to www.abb.com/PLC for further details
AB	Automation Builder (ABB Automation Builder is the integrated software suite for machine builders and system integrators which covers the engineering of ABB AC500 PLC, AC500-S Safety PLC, control panels, drives, motion and robots)
CCF	Common Cause Failure
CPU	Central Processing Unit
DCavg	Diagnostic Coverage - average
DPRAM	Dual-ported Random Access Memory
IEC	International Electro-technical Commission Standard
I/O	Input/Output
EMC	Electromagnetic compatibility
FB	Function Block
FSDT	Functional Safety Design Tool (ABB tool for functional safety calculation according to ISO 13849-1 and/or IEC 62061)
MTBF	Mean Time Between Failures
MTTFd	Mean Time To Failure dangerous
PFH	Probability of Failure per Hour (1/h)
PL	Performance Level according to ISO 13849-1
PLC	Programmable Logic Controller
SIL	Safety Integrity Level (IEC 61508 ed. 2)
TÜV	Technischer Überwachungs-Verein (Technical Inspection Association)

1.6. References / related documents

[1.] AC500-S Safety User Manual, 3ADR025091M0204

[2.] Cyclic Non-safe Data Exchange between SM560-S Safety CPU and PM5xx Non-Safety CPU, 3ADR025195M0201

[3.] BGIA Report 2/2008e, Functional safety of machine controls - Application of EN ISO 13849

[4.] AC500 Documentation, refer to www.abb.com/PLC and then navigate to Downloads area

2. Usage of digital standard I/Os in functional safety applications up to PL c

2.1. Overview

In this document, we discuss the usage of AC500 digital standard I/O modules on the input side of AC500-S Safety PLC. The output side has to be implemented using safety output modules as further explained in the notice below. SM560-S Safety CPU has to be used for safety logic processing and diagnostic measures for digital standard I/O modules.

NOTICE

Usage of standard output channels on standard I/O modules in AC500 platform for functional safety applications is not considered in this document because of the complexity of its implementation in practice and results in very limited cost saving (two output channels from two different standard output modules will be needed (contact ABB technical support at www.abb.com/PLC for more details)). As a result, safety output channels from DX581-S module [1.] or built-in drive safety functions (Safe Torque Off, Safe Stop 1, Safely Limited Speed, etc.) accessible through PROFINET / PROFIsafe [1.] shall be used on the output side of the Safety PLC.

Figure 1 gives an overview on the minimum exemplary AC500 configuration to be used for PL c safety functions with digital standard I/O modules (PM573 standard CPU and DC523 digital standard I/O modules are taken as examples here but other CPUs and I/O modules from the AC500 range could also be used).

DX581-S digital safety input/output module is included in Figure 1 as one of options for Safety PLC output part (another option is the usage of PROFINET/PROFIsafe communication to trigger safety functions in drives with safety option). In addition to available digital safety input channels on DX581-S, one can use digital standard I/O channels from standard I/O modules, like DC523.

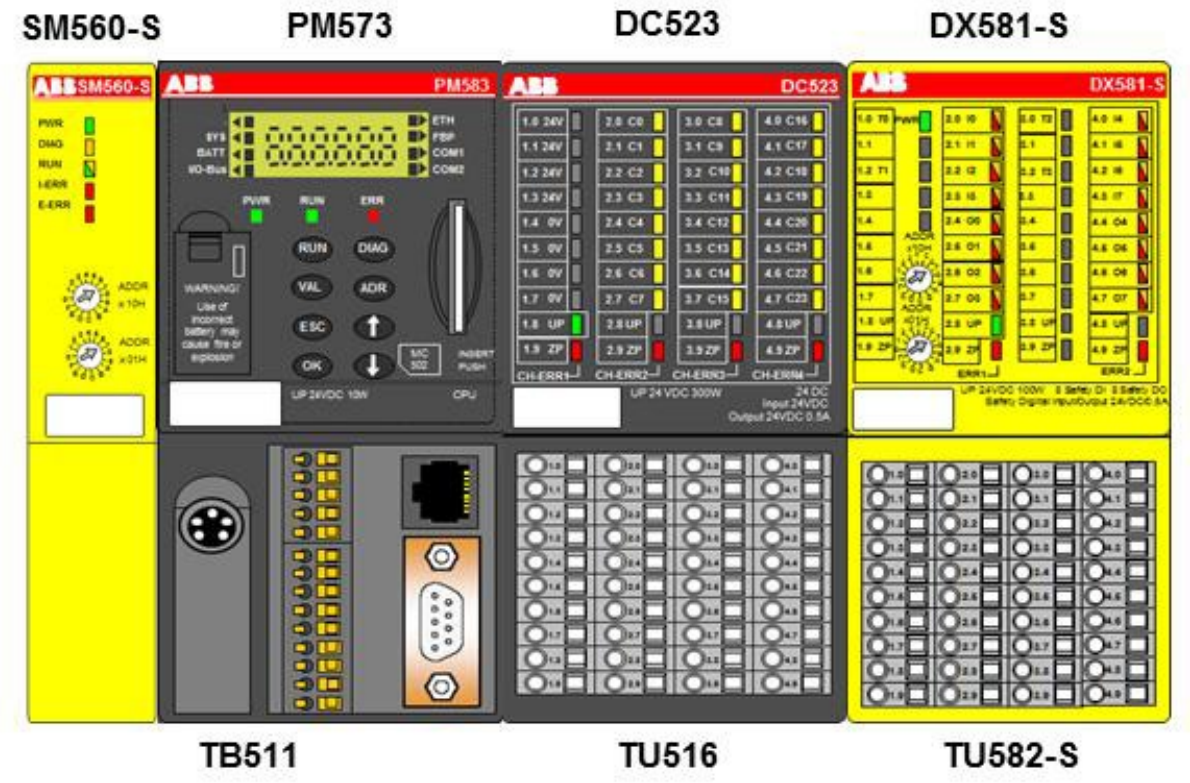


Figure 1. Basic setup with AC500/AC500-S modules for usage of AC500 digital standard I/O modules in functional safety application up to PL c

Remote digital standard I/O modules can be used as well (refer to www.abb.com/PLC for more details on available AC500 modules).

2.2. Task

We want to show and describe an approach how AC500 digital standard I/O channels can be used for functional safety applications up to PL c (ISO 13849-1) in combination with SM560-S Safety CPU.

NOTICE
It is always highly recommended to use digital safety input channels even for functional safety applications up to PL c (ISO 13849-1). Thus, the presented approach with the usage of digital standard I/O channels is only an option if spare digital standard I/O channels are available and their reuse for functional safety functions up to PL c is needed to satisfy specific customer requirements (e.g., limited space in the control cabinet to add additional digital safety I/O module, cost saving, etc.).

Customer benefits from using spare AC500 digital standard I/O channels for functional safety applications up to PL c (ISO 13849-1) are:

- Smaller control cabinet dimensions are possible
- Cost savings on additional Safety I/O modules.

2.3. Solution

The proposed solution is based on the design analysis and additional diagnostic safety measures which can be implemented using AC500/AC500-S setup shown in Figure 1 to enable usage of AC500 digital standard I/O channels in functional safety applications up to PL c (ISO 13849-1).

Figure 2 shows an overview on reachable Performance Levels depending on Category, DCavg and MTTFd values, as defined in ISO 13849-1. As one can see from Figure 2 (see a selection in blue), one of the most attractive approaches to satisfy PL c (MTTFd = High or Medium) and even PL d (MTTFd = High) requirements is the usage of Category 2, DCavg = Low.

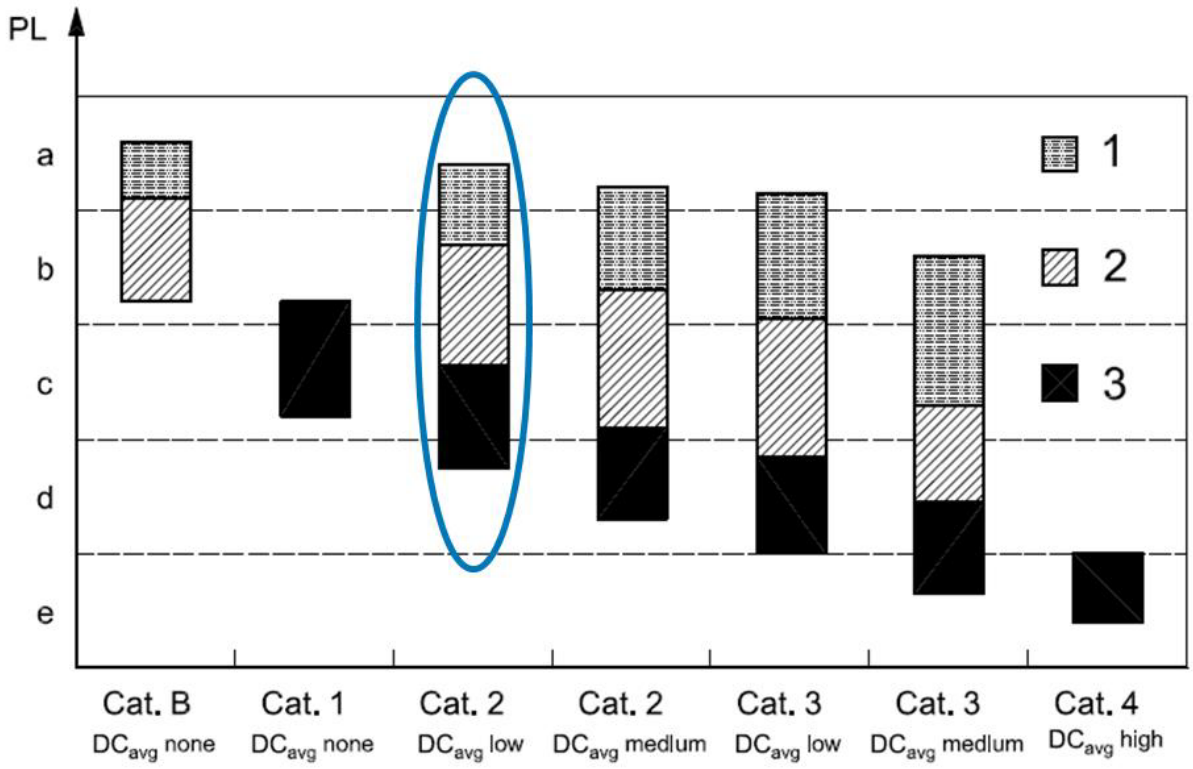
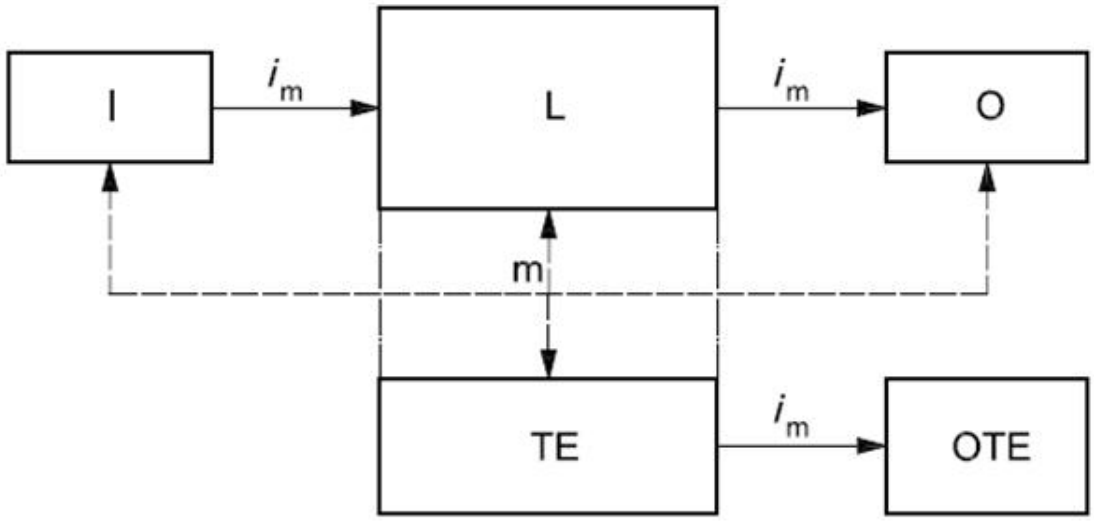


Figure 2. Relationship between Categories, DCavg, MTTFd of each channel and PL from ISO 13849-1 with a focus on Category 2

Category 2 architecture based on ISO 13849-1 is shown in Figure 3.



i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE

Figure 3. Category 2 architecture from ISO 13849-1

Key requirements for Category 2 (ISO 13849-1) are:

- Requirements of system B (refer to ISO 13849-1 for details) and the use of well-tried safety principles shall apply
- Safety function shall be checked at suitable intervals by the machine control system
- The occurrence of a fault can lead to the loss of the safety function between the checks
- The loss of safety function is detected by the check

Category 2 architecture realization using AC500/AC500-S modules (see Figure 1) is shown in Figure 4.

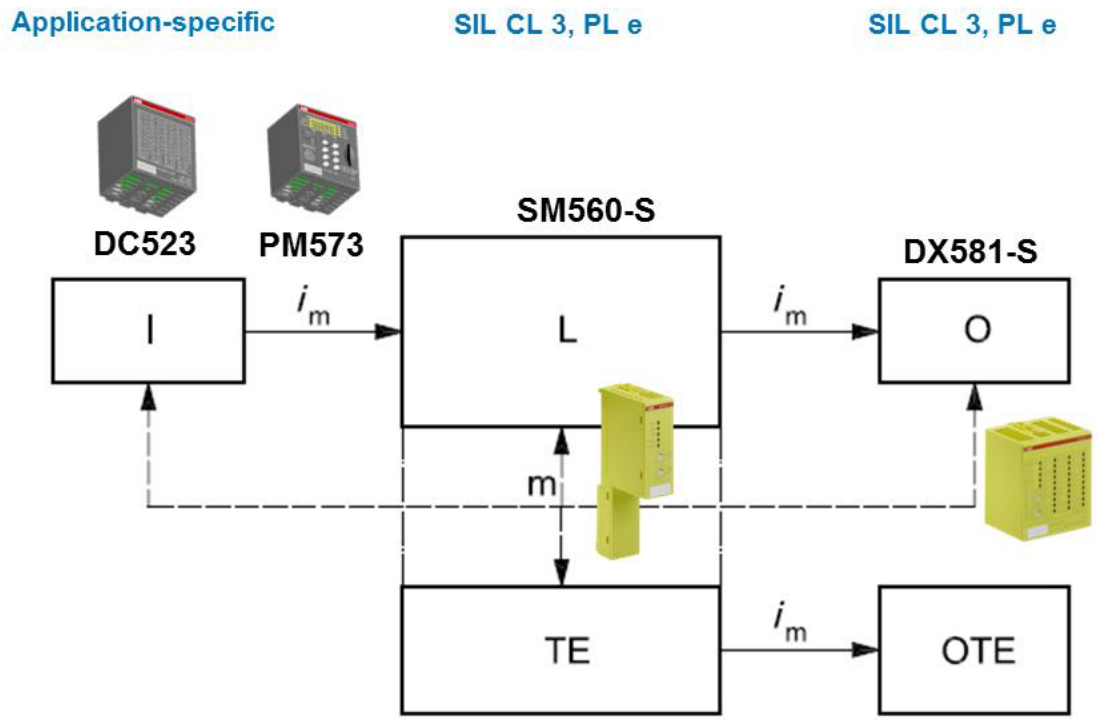


Figure 4. Category 2 equivalent architecture using AC500/AC500-S modules

As one can see from Figure 4, safety logic processing and safety output part are fully covered by SM560-S Safety CPU (SIL3, PL e) and DX581-S digital safety input/output module, which even significantly exceed the requirements from PL c (ISO 13849-1). Nevertheless, we need an additional analysis for the input part in which standard (nonsafety) AC500 modules (DC523 and PM573) are used. This input part will be always application-specific and will require additional measures to satisfy PL c requirements.

⚠ DANGER

In special cases (e.g., if two sensors are connected to two AC500 digital I/O channels from different I/O modules in parallel, etc.), digital standard I/O modules from AC500 platform can be also used in functional safety applications up to PL d (ISO 13849-1) and SIL CL 2 (IEC 62061). However, more detailed functional safety application analysis is required (contact AC500 technical support at www.abb.com/PLC for more details), which is not shown in this document.

To fulfill PL c (ISO 13849-1) requirements for input part, special DC measures shall be implemented according to ISO 13849-1. The following measure was selected for the input part:

- Cyclic test stimulus by dynamic change of the input signals, which provides DC = 90% (see Annex E, ISO 13849-1)

The exemplary realization of this measure in AC500/AC500-S setup is presented in Figure 5 and is based on some assumptions, which are later described in chapter 3 in details:

- Generation of dynamic pulses is done e.g., from non-safety PM5xx program but the supervision of the test pulse pattern is done on SM560-S Safety CPU
  - For data exchange between SM560-S and PM5xx two options can be used:
    - SF_DPRAM_PM5XX_S_REC and SF_DPRAM_PM5XX_S_SEND FBs from SafetyExt_ AC500_V22.lib [1.] or
    - Cyclic Non-safe Data Exchange [2.]

⚠ DANGER

50 Hz and 60 Hz frequencies shall be avoided for dynamic pulse generation to avoid electrical noise interference.

The safety reaction is triggered by SM560-S Safety CPU (in our example through DX581-S digital safety input/output module), if the expected test pattern is not available.

- Stuck-at-1 error are covered by the test pulse test
- Cross-talk between other channels can be implemented using time-shifted (unique) dynamic test pulses for different input channels or different test pulse frequencies

⚠ DANGER

Additional fault exclusion argumentation is required to exclude the availability of similar periodic signals (with the same frequency as that selected for dynamic test pulse generation on DC523 (see Figure 5)) within PM573 CPU.

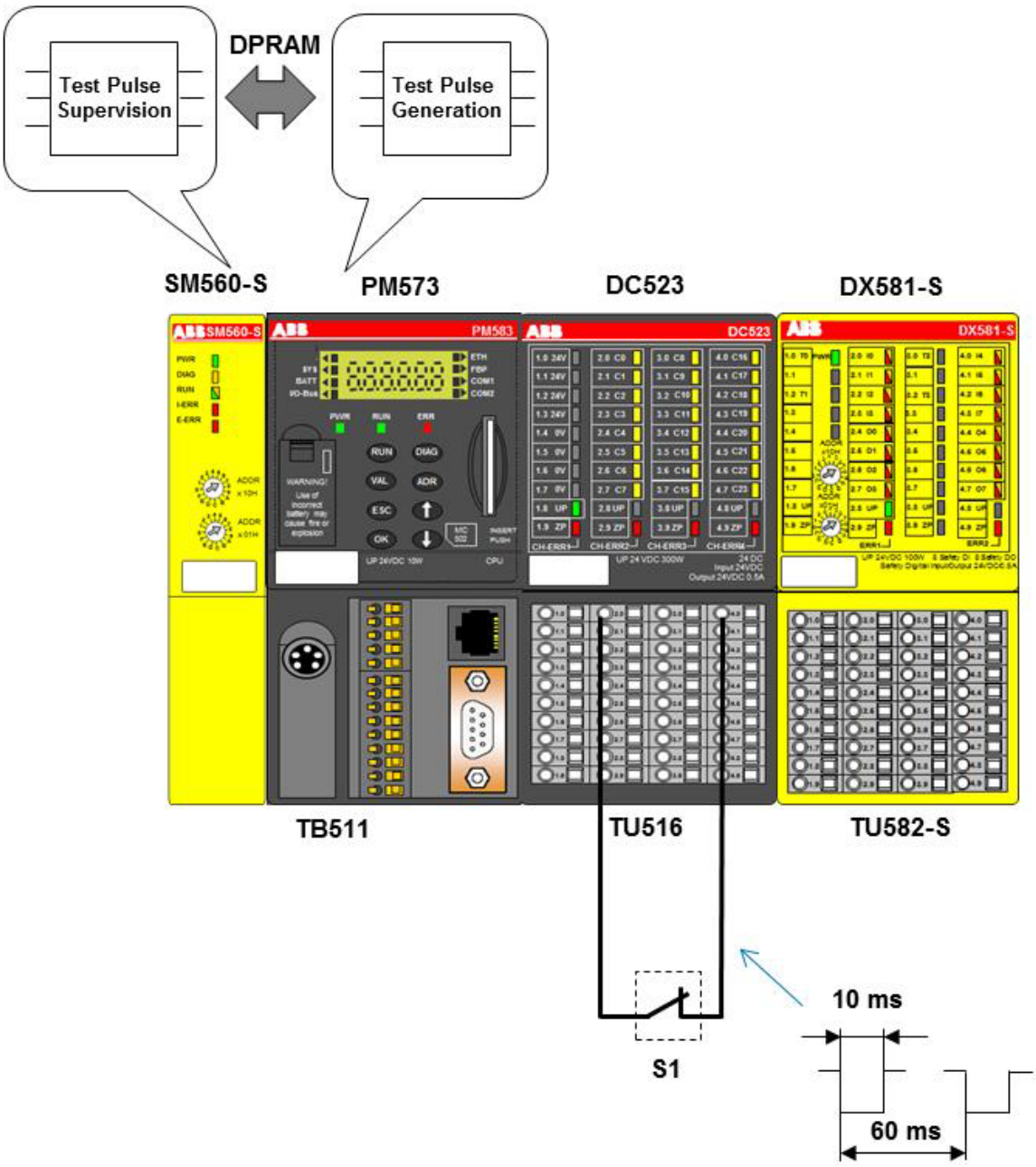


Figure 5. Exemplary realization of cyclic test stimulus by dynamic change of the input signals using AC500 digital standard I/O module

In Figure 5, Channel C16 of DC523 is configured as an output and Channel C0 is configured as an input. Test pulses (for example, with LOW phase duration of 10 ms, HIGH phase duration of 50 ms and a period of 60 ms) are generated on Channel C16 using PM573 application program and are read back through Channel C0 to which normally-closed position switch S1 is connected. Using DPRAM data exchange (two options are available, refer to [1.] and [2.], respectively), one can transfer the observed signal pattern to SM560-S Safety CPU for supervision. If the test pulse pattern (both LOW and HIGH phases are supervised) is not available, the safety reaction is triggered to stop the machine, e.g., through DX581-S digital safety input/output module.

Figure 6 shows how dynamic signal is transferred from position switch S1 (there could be also two position switches, as it is shown in Figure 6, e.g., if PL d (ISO 13849-1) safety applications have to be realized) to SM560-S Safety CPU and then, if safety request exists, further through DX581-S to the actuator, which

was not shown in Figure 5 for simplicity (refer to [1.] on details for connections of actuators to DX581-S outputs).

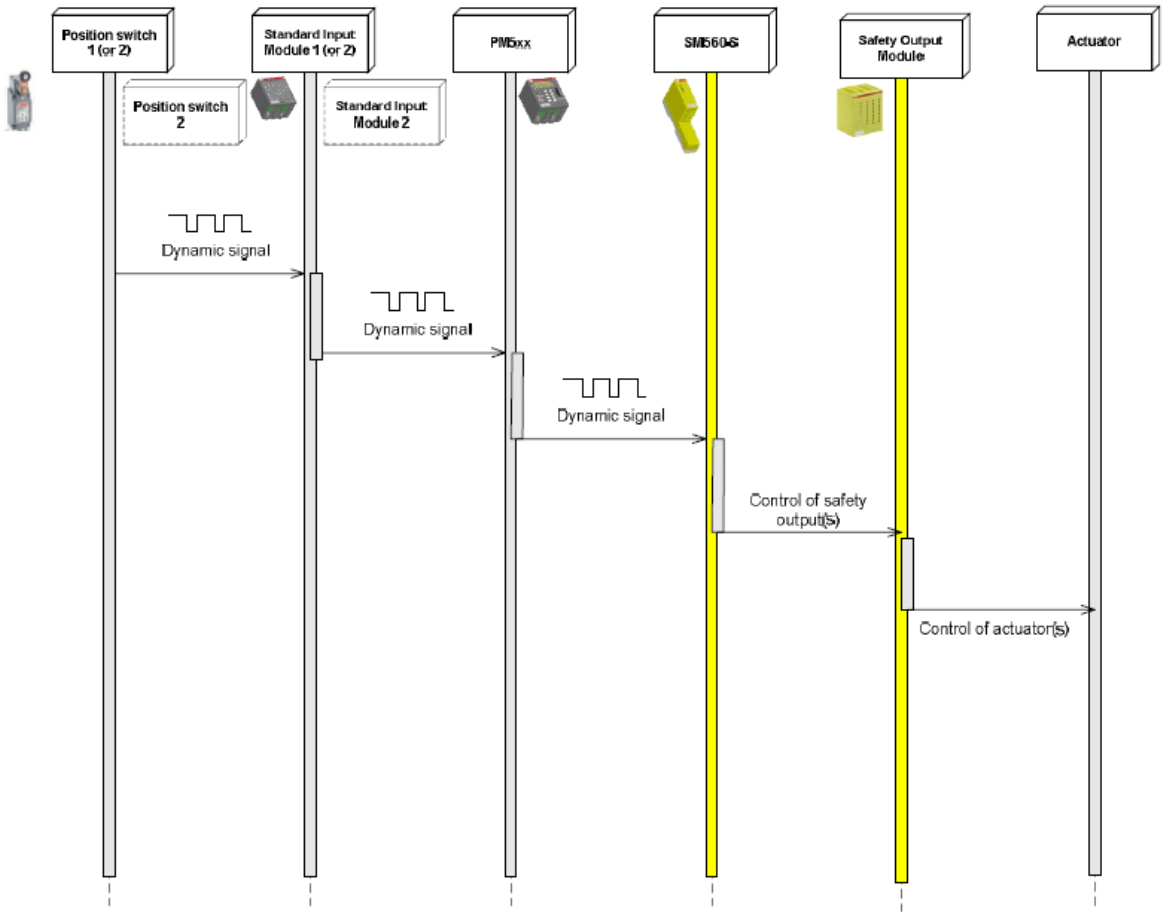


Figure 6. Sequence diagram for dynamic signal supervision using SM560-S Safety CPU

The proposed approach with AC500 digital standard I/O modules in functional safety applications up to PL c (ISO 13849-1) is analysed with more details in an example in chapter 3.

3. Example

The following example describes the safety analysis and implementation needed for AC500 digital standard I/O module usage in functional safety applications up to PL c (ISO 13849-1). In our example, we refer to the AC500/AC500-S setup described in Figure 5.

3.1. General

We will provide only a safety analysis with the supporting calculation for the Safety PLC part in the safety loop, which means that values for sensor and actuator parts will be omitted for simplicity. We aim to reach ~ 15 % of safety loop PFH equivalent for PL c (ISO 13849-1), as it is shown in Figure 7 [1].

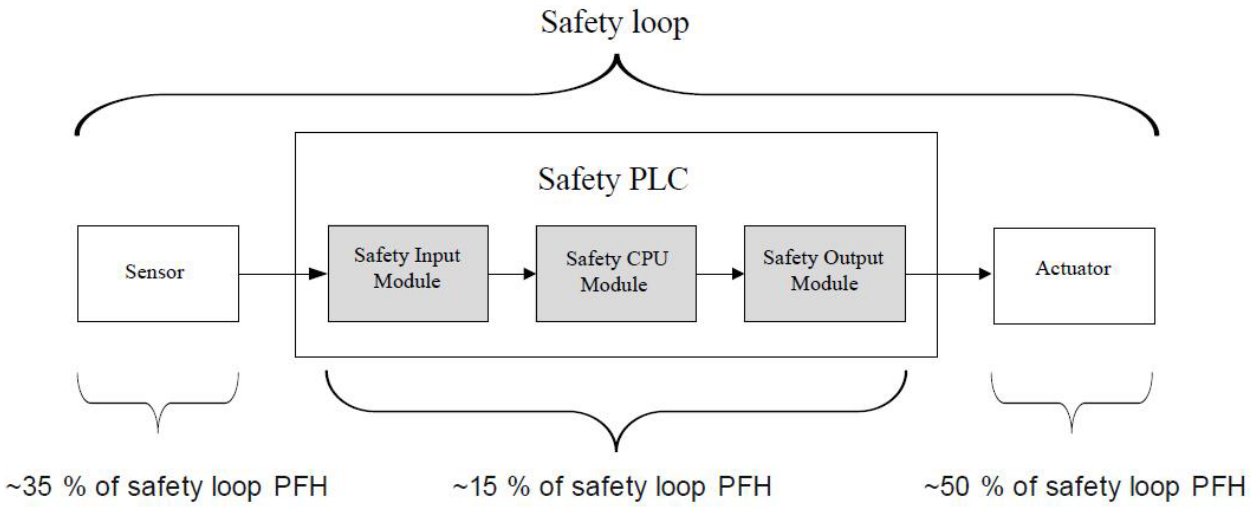


Figure 7. A typical safety loop with Safety PLC [1]

The safe stopping of the woodworking machine with PL c (ISO 13849-1) is discussed in our example. The presented safety analysis for Safety PLC part can be similarly applied for other safety functions up to PL c (ISO 13849-1).

3.2. Safety function

The safety function in this example is the actuation of the “Off” switch (see S1 in Figure 5), which leads to SS1 (Safe Stop 1) with a controlled stop of the motor within a maximum permissible time.

3.3. Functional description

- The motor stop is initiated by the actuation of “Off” switch S1 (Normally-closed contact) which is connected to DC523 digital standard input channel. DC523 digital standard input channel is read by the Safety CPU SM560-S. The digital safety output channel of the DX581-S safety I/O module is connected to SS1 terminal of the drive with safety option (this part is omitted in Figure 5 for simplicity). DX581-S safety output channels are controlled from SM560-S Safety CPU and can be deactivated if the safety reaction is requested through S1. The drive with built-in safety option is responsible for safe braking.

- SM560-S Safety CPU, DX581-S digital safety I/O module and safety option of the drive are all certified for SIL CL 3 (IEC 62061) and PL e (ISO 13849-1). In this example, we will further analyse only Safety PLC (Input, Logic Processing and Output) parts. The safety analysis of “Off” switch S1 and drive with safety option is omitted for simplicity.
- A special measure “Cyclic test stimulus by dynamic change of the input signal” for fault detection is implemented for digital standard input channel on DC523 module, as it is shown in Figure 5. This test signal is able to detect “Stuck-At-1” errors on the path from digital standard input channel on DC523 module until the signal is available on the Safety CPU SM560-S. Short-circuit on the input channel of DC523 module against the ground is a safe error which leads to a safe state. If needed in the given application (if more than one input channels on DC523 module are used), cross-talk failures against other dynamic signals for other input channels on DC523 or other input modules can be implemented in the application program on SM560-S as well. For example, phase-shifted pulses or pulses with different frequencies shall be used for selected channels in the latter case and an additional supervision on SM560-S application program shall be implemented (it is always application-specific).
- Fault exclusion for dynamic signal with the same frequency as one used on the digital standard input channel of DC523 shall be performed for AC500 implementation part (all data transfer paths from DC523 till SM560-S Safety CPU).

⚠ DANGER

Fault exclusion for dynamic signal with the same frequency shall be performed not only as part of wire cross-talk detection but also as a part of standard (non-safe) signal state transfer from DC523 module to the SM560-S Safety CPU through internal I/O bus, PM573 CPU and then internal coupler bus communication to SM560-S Safety CPU.

3.4. Design features

3.4.1. Implementation details

The following steps shall be considered during the implementation of the proposed approach (see Figure 5) for usage of digital standard I/Os in functional safety applications up to PL c (ISO 13849-1) in our example:

1. Use channel C16 of DC523 as an output in PM573 standard CPU program and implement continuous pulsing (periodic TRUE and FALSE phases), as it is specified in Figure 5, using e.g., TON FB. One can also define a dedicated cyclic task on PM573 with 5 ms cycle and priority = 10 to continuously change the value of channel C16 in the software loop keeping the periodic pulse behaviour as it is shown in Figure 5.

NOTICE

The selected cycle time for test pulse generation task on standard CPU program will influence the generated test pulse pattern.

The supervision of the test pattern (length of LOW and HIGH phases) will be implemented on the Safety CPU. Thus, any deviation of the test pulse pattern will be detected by the Safety CPU, which will have to trigger the safe state for the given input channel in case of a wrong test pattern.

2. Continuously read C0 input channel (with input delay parameter (refer to [4.] for details) set to 1 ms for input channels) of DC523 module in the application program on PM573 CPU (make sure that the cycle time on the PM573 task is properly selected, e.g., 2 ms cycle time with cyclic behaviour and priority = 11 for the task are proper ones for the given example).

3. Activate continuous sending of C0 channel value from PM573 application program to SM560-S Safety CPU application program for safe test pattern supervision. To send C0 channel value to SM560-S from PM573, one can use:

   a) SF_DPRAM_PM5XX_S_REC and SF_DPRAM_PM5XX_S_SEND FBs from SafetyExt_AC500_V22.lib [1.] or

   b) Cyclic Non-safe Data Exchange [2.], which has higher performance of data transfer than using SF_DPRAM_PM5XX_S_REC and SF_DPRAM_PM5XX_S_SEND FBs.

⚠ DANGER

You have to keep in mind that data transfer from PM573 to SM560- S (both using FBs SF_DPRAM_PM5XX_S_REC and SF_DPRAM_PM5XX_S_SEND and Cyclic Non-safe Data Exchange) and backwards is a non-safe function. The usage of this communication is suitable for PL c (ISO 13849-1) only as application specific implementation with the usage of described test pulsing and test pattern supervision on SM560-S Safety CPU.

The implementation, verification and validation of the approach in practice according to ISO 13849-1 and/or IEC 62061 will remain always application specific because standard (non-safety) AC500 modules become involved in the execution of functional safety functions. Thus, the responsibility for correct implementation, verification and validation of the proposed approach is fully within the end-customer responsibility.

NOTICE

Make sure that proper "Min Update Time" setting is selected for SM560-S Safety CPU in Automation Builder. 2 or 3 ms are recommended for the proposed example.

NOTICE

Make sure that proper cycle time value is used in SM560-S Safety CPU application program, e.g., the maximum cycle time of 3 ms for SM560-S Safety CPU is acceptable for the given application example.

4. Continuously read C0 channel value on SM560-S safety application program (the implementation depends on which method was selected in Step 3) and supervise the pattern availability using safety application logic, for example, using safety TON FBs [1.]. Another option is to use two SF_Antivalent FB instances [1.]:

   a) **For LOW (0 V) phase supervision:** Selected SF_Antivalent inputs are, for example, S_ChannelNC := FALSE, S_ChannelNO:= IS_DC523_S1, DiscrepancyTime := T#35ms;

   b) **For HIGH (+24 V) phase supervision:** Selected SF_Antivalent inputs are, for example, S_ChannelNC := IS_DC523_S1, S_ChannelNO:= TRUE, DiscrepancyTime := T#400ms

Where IS_DC523_S1 is the variable name of the transferred C0 channel value on SM560-S Safety CPU application program. "Error" outputs of SF_Antivalent FB shall be used as a result of safety pattern supervision on DC523 input channel C0 and shall be further used in SF_EmergencyStop and SF_SafetyRequest FBs (see [1.] for more details) to properly implement emergency stop functionality.

NOTICE

The data transfer (C0 channel state) from DC523 to PM573 and then further to SM560-S Safety CPU introduces some time jitter. The largest introduced time jitter is usually caused by SF_DPRAM_PM5XX_S_REC and SF_DPRAM_PM5XX_S_SEND FBs. This leads to longer supervised time values (e.g., LOW phase of 35 ms and HIGH phase of 400 ms can be used as limits) than those specified in Figure 5. These limit values can, however, vary depending on selected settings for tasks on PM573, SM560-S, "Min Update Time" parameter for SM560-S and selected data transfer method between PM573 and SM560-S.

NOTICE

Due to the introduced jitter in the used test signal pattern, as one could see from Step 4, the effective input delay used for C0 input channel becomes 35 ms (DiscrepancyTime := T#35ms, see Step 4 above). The longest tolerated HIGH phase (+24 V) before "Stuck- At-1" error is detected and then safe reaction is triggered (to be implemented as part of the safety application program) becomes (DiscrepancyTime := T#400ms, see Step 4 above). These values shall be further used in SFRT and fault reaction time calculations.

NOTICE

The test rate (the test period of 450 ms was used in the given example) for input part of the safety function shall be at least 100 times greater than the demand rate upon the safety function, as required for Category 2 (ISO 13849-1).

This requirement is fulfilled in the given example for PL c safety function if the demand is less than 1 per 45 seconds.

3.4.2. Common cause failures

All measures for CCF are already covered for AC500-S Safety PLC modules like SM560-S and DX581-S, which are certified for up to PL e (ISO 13849-1) and SIL CL 3 (IEC 62061) safety applications. However, for all AC500 standard (non-safety) modules, like PM573 and DC523, the estimation of CCF effect shall be performed using Annex F, ISO 13849-1.

We use below the scoring process and quantification of measures against CCF based on Annex F, ISO 13849-1:

1. Physical separation between signal paths, refer to AC500 design process (see chapter 3.4.3) – **15 points**
    - Sufficient clearances and creepage distances on printed-circuit boards
2. Design/application/experience (Protection against overvoltage), refer to AC500 design process (see chapter 3.4.3) – **15 points**
3. Environmental (EMC, etc.), refer to CE declaration type test report for a given AC500 product – **25 points**
4. Environmental (Other influences - shock, vibration and temperature), refer to CE declaration type test report for a given AC500 product – **10 points**

Total sum of points: **65 points**

As a result, according to ISO 13849-1, CCF requirements for usage of AC500 products are fulfilled because 65 points are needed for this based on Annex F, ISO 13849-1.

⚠ DANGER

A physical separation of signal lines for AC500 standard input channels have to be considered on the application level as well. Thus, the responsibility for this part remains fully within the end-customer responsibility.

3.4.3. Systematic failures

Measures for the control and avoidance of systematic failures from Annex G, ISO 13849-1 shall be considered for standard (non-safety) AC500 components separately (all these measures are already covered for AC500-S Safety PLC modules like SM560- S and DX581-S, which are certified for up to PL e (ISO 13849-1) and SIL CL 3 (IEC 62061) safety applications). The AC500 product requirements for the control and avoidance of systematic failure in PL c (ISO 13849-1) applications are satisfactorily covered in the proposed implementation (refer to the system setup in Figure 5) through ABB AC500 product development model:

- Usage of Integrated Management System which is ISO 9001 certified by external certification body
- Quality guidelines for software development
- Hardware development process including hardware quality statistics for at least last 3 years
- Continuous analysis of all critical bug entries in the bug tracking system

All used AC500 modules have CE declaration (European Conformity) available which means that they satisfy Low Voltage Directive 2006/95/EG, EMC Directive 2004/108/EG and IEC 61131-2:2007 standard requirements in addition to various other standards (refer to www.abb.com/PLC for details).

⚠ DANGER

If standard (non-safety) modules are used for safety functions, one still have to perform a systematic failure analysis (refer to Annex G, ISO 13849-1) on the application level for the application part in which standard (non-safety) modules are used.

3.4.4. Safety function response time

SFRT calculation shall be done based on the data presented in chapter 5 [1.]. It is straight-forward for all functional safety modules, like SM560-S and DX581-S, but require additional analysis for standard (non-safety) ones, like PM573 and DC523.

Under assumptions and implementation aspects listed in chapter 3.4.1, one can add the following fault error reaction time (e.g., for Stuck-At-1 errors) for DC523 input channel:

- 400 ms, if supervised as proposed in chapter 3.4.1.

As for SFRT input part (it means SFRT up to SM560-S Safety CPU only), one shall add the fault error reaction time for DC523 path (400 ms in the given example, refer to chapter 3.4.1) to a LOW phase supervision time (35 ms in the given example, refer to chapter 3.4.1) as the overall worst-case response time, which will result in SFRT for input part:

- 435 ms, if supervised as proposed in chapter 3.4.1

⚠ DANGER

You still have to do a complete SFRT calculation for the safety loop(s) (not only input part but also logic processing and output parts) in your application (see chapter 5 [1.]).

3.5. Calculation of the probability of failure and correspondence to PL (ISO 13849-1)

For calculation of the probability of failure for Safety PLC part, we will use ABB FSDT software (see www.abb.com). Our goal is to confirm that PFHavg is (refer to Figure 7) below or equal to 15% of PL c for Category 2 (refer also to PFHavg values listed in Table K1 of ISO 13849-1 for given Category, DC and MTTFd values).

NOTICE

MTTFd values for AC500 standard (non-safety) modules were obtained based on MTBF values (contact AC500 technical support at www.abb.com/PLC to obtain MTBF values for selected AC500 modules). The following relation, which complies with ISO 13849-1, was used:

MTTFd = 2 * MTBF

This relationship is based on the following assumptions:

- **It is assumed that statistically only every second failure is a potentially dangerous failure**
- **The permissible ambient conditions are met**
- **Mean Time to Repair (MTTR) is significantly less than the MTBF.**

The following MTTFd values were used in the calculation for AC500 standard modules

(all AC500 modules, which are involved in the internal communication of dynamic test

pulses up to SM560-S Safety CPU):

- PM573-ETH → 2 * 170 years = 340 years
- DC523 → 2 * 88 years = 176 years
- DX581-S (1 out of 3 electronic boards is involved in the internal communication) → 2 * (3 * 73 years) = 438 years
- TB511-ETH → 2 * 292 years = 584 years
- TU582-S → 2 * 2757 years = 5514 years
- TU516 → 2 * 2942 years = 5884 years

Using formula D.1 from Annex D, ISO 13849-1, MTTFd value for the input part, which is composed of all components contributing to the safety function and listed above, was calculated:

- MTTFd for input part in Figure 5 → 77 years

DC = 90% was used for standard modules in the input path (see Figure 5). All safety values for safety modules SM560-S and DX581-S are available from the TUV certification process and are a part of the FSDT library.

Figure 8 shows a screen shot from FSDT safety calculation.

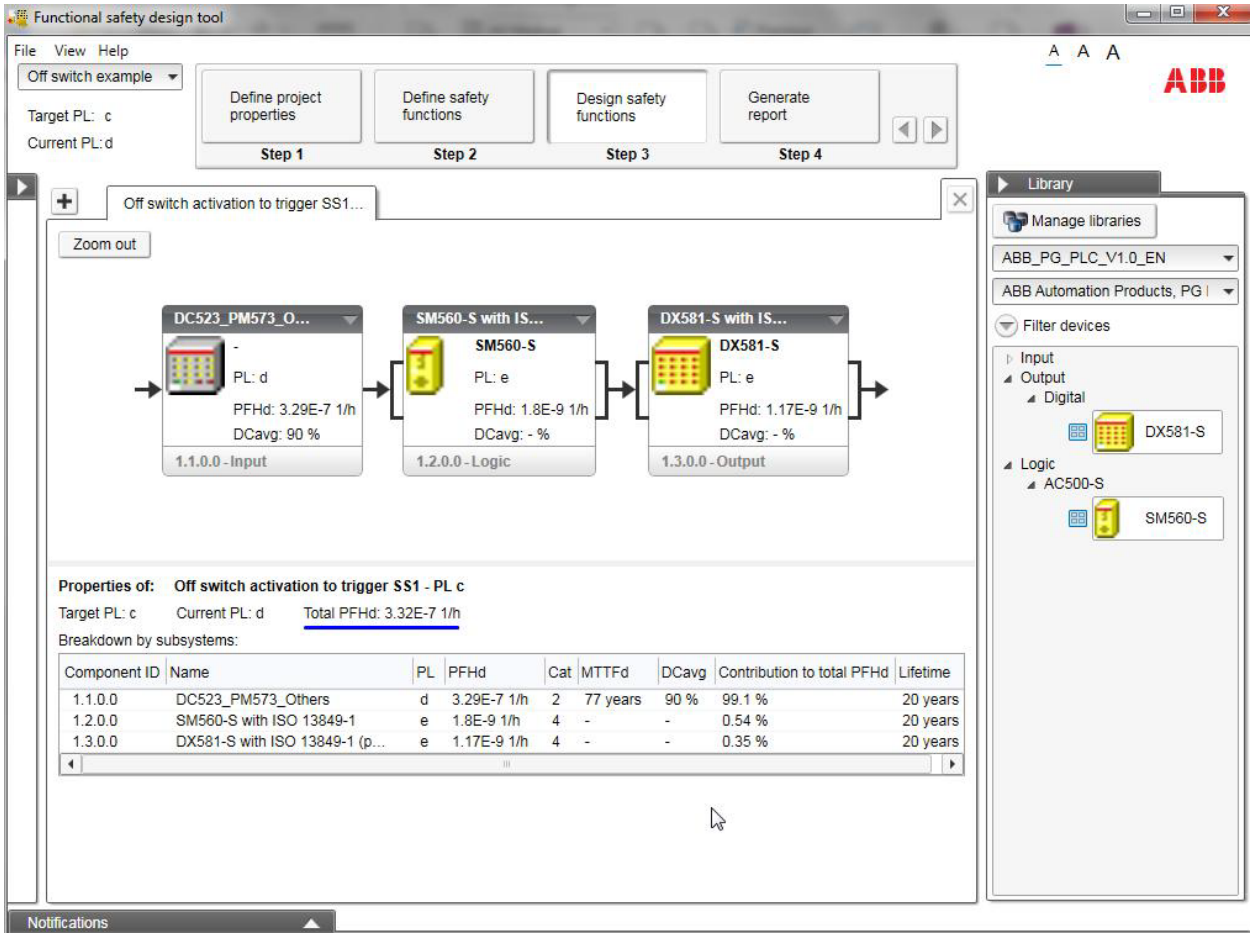


Figure 8. FSDT safety calculation for selected safety function

The safety calculation result (see Figure 8) is the PFHavg value of 3.32E-7 1/h for the safety function (actuation of the “Off” switch S1, which leads to SS1 (Safe Stop 1) with a controlled stop of the motor within a maximum permissible time).

NOTICE

The mission time for implemented safety functions up to PL c is 20 years and cannot be extended because standard components are used in the input part of the safety function.

This value is better than the required limit value 4.50E-7 1/h (15 % of PFHavg (3E-6 1/h) from Table K1 of ISO 13849-1 for PL c), which means that the proposed approach is suitable for usage in safety application up to PL c (ISO 13849-1).

4. Conclusion

The results of our safety analysis confirm that AC500 digital standard I/O channels can be used in functional safety applications up to PL c (ISO 13849-1). The functional safety calculation according to IEC 62061 standard (applications up to SIL CL 1) can be similarly done, if required.

⚠ DANGER

The presented approach enables the usage of AC500 digital standard I/O modules in functional safety applications up to PL c (ISO 13849-1). However, the implementation, verification and validation of the approach in practice according to ISO 13849-1 and/or IEC 62061 will remain always application specific because standard (non-safety) AC500 modules become involved in the execution of functional safety functions. Thus, the responsibility for correct implementation, verification and validation of the proposed approach is fully within the end-customer responsibility.

In special cases, digital standard I/O modules from AC500 platform can be also used in functional safety applications up to PL d (ISO 13849-1) and SIL CL 2 (IEC 62061). However, more detailed functional safety application analysis is required (contact AC500 technical support at www.abb.com/PLC for more details), which is not shown in this document.

3ADR025245M0201, REV B, en_US, 2021/09/15

ABB AG
Eppelheimer Straße 82
69123 Heidelberg, Germany
Phone: +49 62 21 701 1444
Fax: +49 62 21 701 1382
Mail: plc.support@de.abb.com
www.abb.com/plc