



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

PR Project name: Safe stopping (SS1) AC15/20

Project file name:	C:\Users\GH111435\OneDrive - parkercorp\Documents\SISTEMA\Projects\en\PARKER AC15_20 STO 2022_12_20_E.ssm
Creation date:	-
Project status:	
Project number:	
Project version:	
Authors:	Günter Hog
Project managers:	
Inspectors:	
Dangerous point/machine:	Motor shaft
Documentation:	see safety function SS1
Document:	
Version of software:	2.0.8 build 4
Version of standard:	ISO 13849-1:2015, ISO 13849-2:2012
Checksum:	f13c14c87cf310aba3dd31ed995db735
Options:	☒ Use DC intermediate levels for calculation of PFHD (more precise) ☐ MTTFD capping for category 4 lower from 2500 to 100 years.
Status:	green
Note:	There are no warnings listed for this project (or it's subordinate basic elements).

Print options

- | | |
|--|---|
| ☒ Show device details | ☒ Show requirements on PL and Category |
| ☒ Show documentations on SF, SB, BL and EL | ☒ Show parameter documentations on PLr, PL, Category, CCF, MTTFD and DC |
| ☒ Show CCF and DC measures in detail | ☒ Show messages |

Contained safety functions

SF Name: SS1

Required: PLr d

Reached: PL d

PFHD [1/h]: 3,1E-8

Status: green



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

Identifier of the Safety function:

Safety function type: Emergency stop function

Triggering event: Stopping of the motor is initiated by actuation of the emergency stop button

Reaction and Behaviour on power failure: Immediately the safety control device UE410-MU, which is triggered by an 2-channel safety demand switch, requests via the output Q1 a braking ramp for the motor. Then after the delay time set on the safety control device UE410-MU the 2 STO channels of the AC15/20 drive are switched off by the outputs Q3 and Q4.

Safe state: STO
Remarks: During the braking ramp no safe state is ensured. The machine designer has to consider this in the risk analysis.

Operation mode:

Demand rate:

Running-on time:

Priority:

Documentation: see above

Document:

Required Performance Level Safety function

PLr (by direct input): d

Documentation:

Document:

Source (e.g. standard):

File:

Performance Level Safety function

Reached PL: d PFHD [1/h]: 3,1E-8

Status / Messages Safety function

Status: green

Subsystems (1 / 3)

SB Name: AC15/20 Drive

Reference designator: Inventory number:

Device details Subsystem

Device Manufacturer: Parker Hannifin

Device Identifier:

Device group:

Part number: Revision:



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

Function:	☒ Input	☒ Logic
	☒ Output	☐ unknown

Use case: Subsystem Safe Torque Off (STO)

Description of the use case: The STO function shall support the Safe Stop 1 safety function

Documentation Subsystem

Documentation:

Document: C:\Users\GH111435\OneDrive - parkercorp\STO\On Preparation\Hardware Design\DOC-0019-05-B_Didi_STO_Design_Description.doc

Performance Level Subsystem

PL determination: Enter PL/PFHD directly (manufacturer ensures compliance with the requirements of the Category and of the PL)

PL: d Software suitable up to PL: n.a.

Reached PL: d PFHD [1/h]: 4,6E-10

Documentation:

Mission time [a]: 20 Shortest mission time [a]: 20

Category Subsystem

Cat.: 3

Category requirements: fulfilled

Requirements of the Category: Since the category is given by the manufacturer he is responsible to satisfy the requirements.

Documentation:

Source (e.g. standard) Category:

File:

Status / Messages Subsystem

Status: green

Subsystems (2 / 3)

SB Name: Emergency stop switching device

Reference designator: Inventory number:

Device details Subsystem

Device Manufacturer:

Device Identifier:

Device group:

Part number: Revision:



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

Function:	☒ Input ☐ Output	☐ Logic ☐ unknown
Use case:	Emergency stop	
Description of the use case:	The emergency stop switching device shall support the safety function Safe Stop 1	

Documentation Subsystem

Documentation:	At a B10d value of 100,000 cycles and at 240 working days, 16 working hours and a cycle time of 1 hour, the result for nop is 3,840 cycles per year and for the MTTFd 260 years. Because the safety control device has a high quality fault detection with dynamic cross monitoring test pulses for the input signals the DC is 99%. Adequate measures against common cause failure (65 points): Over-voltage protection (15), using well-tried components (5), trained designers/maintainers (5), FMEA (5) and environmental conditions (25 + 10) are assumed.
----------------	---

Document:

Performance Level Subsystem

PL determination:	Determine PL/PFHD from Category, MTTFD and DCavg
Software suitable up to PL:	n.a.
PL requirements:	fulfilled
The PL shall be determined by the estimation of the following aspects:	- Behaviour of the safety function under fault conditions (see clause 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]

Reached PL: e PFHD [1/h]: 2,5E-8

Documentation:

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	- Accordance with relevant standards to withstand the expected influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - A single fault tolerance and reasonable fault detection are given. [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled]

Documentation:



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

Source (e.g. standard) Category:

File:

MTTFD and Mission time Subsystem

MTTFD [a]: 100 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

Diagnostic coverage Subsystem

DCavg [%]: 99 (High)

Common cause failure Subsystem

CCF Points: 75 (fulfilled)

CCF Measures:

- Design / application / experience (15 Points)
Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
- Competence / training (5 Points)
Training of designers to understand the causes and consequences of common cause failures.
- Assessment / analysis (5 Points)
For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.
- Environmental (25 Points)
For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1).
Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium.
NOTE For combined fluidic and electric systems, both aspects should be considered.
- Environmental (10 Points)
Other influences
Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).
- Separation / Segregation (15 Points)
Physical separation between signal paths, for example:
 - separation in wiring/piping;
 - detection of short circuits and open circuits in cables by dynamic test;
 - separate shielding for the signal path of each channel;
 - sufficient clearances and creepage distances on printed-circuit



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

CCF Measures: boards.

Documentation:

Document:

Status / Messages Subsystem

Status: green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Switch channel 1

Reference designator:

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☒ Input
☐ Output

☐ Logic
☐ unknown

Technology:

mechanic

Category:

-

Use case:

Mechanical switch

Description of the
use case:

Documentation Block

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 260,4 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

Diagnostic coverage Block

DC [%]: 99 (High)

Status / Messages Block

Status: green



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1**Elements (1 / 1)****EL Name: Normally open contact**

Reference designator:

Inventory number:

Device details Element

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☒ Input
☐ Output

☐ Logic
☐ unknown

Technology:

mechanic

Category:

-

Use case:

Mechanical switch

Description of the
use case:*Documentation Element*

Documentation:

In this calculation only the probability of failure of the emergency stop switching device is considered, not the contacts of the safety door. At a B10d value of 100,000 cycles and at 240 working days, 16 working hours and a cycle time of 1 hour, the result for nop is 3,840 cycles per year and for the MTTFd 260 years. Because the safety control device has a high quality fault detection with dynamic cross monitoring test pulses for the input signals the DC is 99%.

Document:

MTTFD and Mission time Element

MTTFD [a]: 260,4 (High)

Mission time [a]: 20

B10D [cycles]: 100000

nop [cycles/a]: 3840

Documentation:

Diagnostic coverage Element

DC [%]: 99 (High)

Measure:

Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O) (Input devices) (99 %)

Documentation:



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1*Status / Messages Element*

Status: green

Channels / Test channels (2 / 2)**CH** Name: Channel 2

MTTFD [a]: 100

Blocks (1 / 1)**BL** Name: Switch channel 2

Reference designator:

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☒ Input
☐ Output

☐ Logic
☐ unknown

Technology:

mechanic

Category:

-

Use case:

Mechanical switch

Description of the
use case:*Documentation Block*

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 260,4 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

Diagnostic coverage Block

DC [%]: 99 (High)

Status / Messages Block

Status: green

Elements (1 / 1)**EL** Name: Normally open contact

Reference designator:

Inventory number:

Device details Element



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☒ Input
☐ Output

☐ Logic
☐ unknown

Technology:

mechanic

Category:

-

Use case:

Mechanical switch

Description of the
use case:*Documentation Element*

Documentation:

In this calculation only the probability of failure of the emergency stop switching device is considered, not the contacts of the safety door. At a B10d value of 100,000 cycles and at 240 working days, 16 working hours and a cycle time of 1 hour, the result for nop is 3,840 cycles per year and for the MTTFd 260 years. Because the safety control device has a high quality fault detection with dynamic cross monitoring test pulses for the input signals the DC is 99%.

Document:

MTTFD and Mission time Element

MTTFD [a]: 260,4 (High)

Mission time [a]: 20

B10D [cycles]: 100000

nop [cycles/a]: 3840

Documentation:

Diagnostic coverage Element

DC [%]: 99 (High)

Measure:

Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O) (Input devices) (99 %)

Documentation:

Status / Messages Element

Status:

green

Subsystems (3 / 3)**SB** Name: UE410_MU Safety control device



Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

SF Safety function: SS1

Reference designator:	Inventory number:	
<i>Device details Subsystem</i>		
Device Manufacturer:	Sick	
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	☒ Input ☒ Output	☒ Logic ☐ unknown
Use case:	Safe plc	
Description of the use case:	The safe plc has to carry out Safe Stop 1	
<i>Documentation Subsystem</i>		
Documentation:		
Document:	..\Flexi Classic - Modulare Sicherheits-Steuerung__2014-10-30__08-45-12.pdf	
<i>Performance Level Subsystem</i>		
PL determination:	Enter PL/PFHD directly (manufacturer ensures compliance with the requirements of the Category and of the PL)	
PL: e	Software suitable up to PL: n.a.	
Reached PL: e	PFHD [1/h]: 6E-9	
Documentation:	This product is certified according EN 61508.	
Mission time [a]: 20	Shortest mission time [a]: 20	
<i>Category Subsystem</i>		
Cat.:	4	
Category requirements:	fulfilled	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.	
Documentation:		
Source (e.g. standard) Category:		
File:		
<i>Status / Messages Subsystem</i>		
Status:	green	

Project name: Safe stopping (SS1) AC15/20

File date: 20.12.2022 11:10:42 Report date: 20.12.2022 Checksum: f13c14c87cf310aba3dd31ed995db735

EXCLUSION OF LIABILITY

Care has been taken in production of the software SISTEMA, which corresponds to the state of the art. It is made available to users free of charge.

Die Software wurde gemäß dem Stand von Wissenschaft und Technik sorgfältig erstellt. Sie wird dem Nutzer unentgeltlich zur Verfügung gestellt.

Die Haftung des IFAs/ DGUV ist damit auf Vorsatz und grobe Fahrlässigkeit (§ 521 BGB) bzw. bei Sach- und Rechtsmängel auf arglistig verschwiegene Fehler beschränkt (523, 524 BGB).

The IFA undertakes to keep its website free of viruses; nevertheless, no guarantee can be given that the software and information provided are virus-free. The user is therefore advised to take appropriate security precautions and to use a virus scanner prior to downloading software, documentation or information.

CONTACT

Institute for Occupational Health and Safety of German Social Accident Insurance (IFA)
Division 5: Accident Prevention / Product Safety
Alte Heerstr. 111, 53757 Sankt Augustin
E-mail: sistema@dguv.de
www.dguv.de/ifa (Webcode e561582)

Name in block letters:

Authors

Inspectors

Date, signature:

Authors

Inspectors