



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

PR Project name: 20220131-001

Project file name:	C:\Users\jklh\OneDrive - Festo\Dokumente\Know-how\07 Paid Services\Application Notes\Projects\20220131-001 STO-Cat1-PLc-PUS-Cat3-PLd-5-3-Valve\20220131-001 Sistema Project - Basic - EN.ssm
Creation date:	14.12.2021 07:32:49
Project status:	
Project number:	
Project version:	
Authors:	
Project managers:	
Inspectors:	
Dangerous point/machine:	
Documentation:	
Document:	
Version of software:	2.0.8 build 3
Version of standard:	ISO 13849-1:2015, ISO 13849-2:2012
Checksum:	f17952d9676b23b64d63c8524512ebed
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: STO	Required: PLr c	Reached: PL c	PFHD [1/h]: 1,14E-6	Status: green
SF Name: PUS (operation pressure)	Required: PLr d	Reached: PL e	PFHD [1/h]: 4,28E-8	Status: green
SF Name: PUS (pilot pressure)	Required: PLr d	Reached: PL e	PFHD [1/h]: 4,29E-8	Status: green



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: STO

Safety function type:

Triggering event:

Reaction and
Behaviour on power failure:

Safe state:

Operation mode:

Demand rate:

Running-on time:

Priority:

Documentation:

Document:

Required Performance Level Safety function

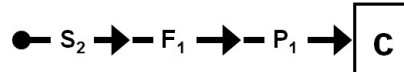
PLr (by risk graph): c

Severity of injury (S): False Serious (normally irreversible) injury or death

Frequency / exposure times to hazard (F): Seldom to less often / exposure time is short

Possibility of avoiding (P): Possible under specific conditions

Risk graph:



Documentation:

Document:

Performance Level Safety function

Reached PL: c PFHD [1/h]: 1,14E-6

Status / Messages Safety function

Status: green

Subsystems (1 / 1)

SB Name: Valves

Reference designator:

Inventory number:

Device details Subsystem

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☐ Output

☐ Logic
☒ unknown

Use case:



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: STO

Description of the
use case:

Documentation Subsystem

Documentation:

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: c PFHD [1/h]: 1,14E-6

Documentation:

Category Subsystem

Cat.: 1

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 components are being used. [fulfilled]
- Well-tried safety principles are being used. [fulfilled]
- MTTFD is at least High. [fulfilled]

Documentation:

Source (e.g. standard) Category:

File:

MTTFD and Mission time Subsystem

MTTFD [a]: 100 (High)

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

Status / Messages Subsystem

Status: green

Channels / Test channels (1 / 1)

CH Name: Channel 1



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: STO

MTTFD [a]: 380,5

Blocks (1 / 1)

BL Name: 5/3 Directional control valve

Reference designator: Q3

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Technology:

unknown

Category:

-

Use case:

Description of the
use case:

Documentation Block

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 380,5 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

B10 [cycles]: 10000000

RDF [%]: 50

B10D [cycles]: 20000000

nop [cycles/a]: 525600

Documentation:

Diagnostic coverage Block

DC [%]: not relevant

Measure:

Indirect monitoring (e.g monitoring by pressure switch,
electrical position monitoring of actuators)
(Output device)
(90 % - 99 % depending on the application)

Documentation:

Status / Messages Block

Status:

green



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (operation pressure)

Safety function type:

Triggering event:

Reaction and
Behaviour on power failure:

Safe state:

Operation mode:

Demand rate:

Running-on time:

Priority:

Documentation:

Document:

Required Performance Level Safety function

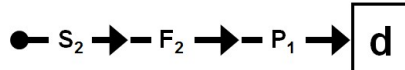
PLr (by risk graph): d

Severity of injury (S): False Serious (normally irreversible) injury or death

Frequency / exposure times to hazard (F): Frequent to continuous / exposure time is long

Possibility of avoiding (P): Possible under specific conditions

Risk graph:



Documentation:

Document:

Performance Level Safety function

Reached PL: e PFHD [1/h]: 4,28E-8

Status / Messages Safety function

Status: green

Subsystems (1 / 1)

SB Name: Valves

Reference designator:

Inventory number:

Device details Subsystem

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Use case:



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (operation pressure)

Description of the use case:

Documentation Subsystem

Documentation:

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]: 4,28E-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-tries 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:

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 [%]: 90 (Medium)



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (operation pressure)

Common cause failure Subsystem

CCF Points: 95 (fulfilled)

CCF Measures:

- 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 boards.
- Diversity (20 Points)
Different technologies/design or physical principles are used, for example:
 - first channel electronic or programmable electronic and second channel electromechanical hardwired,
 - different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or
 - digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or
 - Components of different manufactures.
- Design / application / experience (15 Points)
Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
- 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.
- Competence / training (5 Points)
Training of designers to understand the causes and consequences of common cause failures.
- 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



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (operation pressure)

CCF Measures: as, temperature, shock, vibra

Documentation:

Document:

Status / Messages Subsystem

Status: green

Channels / Test channels (1 / 2)**CH** Name: Channel 1

MTTFD [a]: 380,5

Blocks (1 / 1)**BL** Name: 5/3 Directional control valve

Reference designator: Q3

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Technology:

unknown

Category:

-

Use case:

Description of the
use case:*Documentation Block*

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 380,5 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

B10 [cycles]: 10000000

RDF [%]: 50

B10D [cycles]: 20000000

nop [cycles/a]: 525600

Documentation:

Diagnostic coverage Block

DC [%]: 90 (Medium)



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (operation pressure)

Measure: Indirect monitoring (e.g monitoring by pressure switch, electrical position monitoring of actuators)
(Output device)
(90 % - 99 % depending on the application)

Documentation:

Status / Messages Block

Status: green

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 91324,2

Blocks (1 / 1)

BL Name: 3/2 Directional control valve

Reference designator: Q1

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Technology:

unknown

Category:

-

Use case:

Description of the
use case:

Documentation Block

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 91324,2 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

B10 [cycles]: 10000000

RDF [%]: 50

B10D [cycles]: 20000000

nop [cycles/a]: 2190

Documentation:

Diagnostic coverage Block

DC [%]: 99 (High)



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (operation pressure)

Measure:	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements) (Output device) (99 %)
----------	---

Documentation:

Status / Messages Block

Status:	green
---------	-------



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (pilot pressure)

Safety function type:

Triggering event:

Reaction and
Behaviour on power failure:

Safe state:

Operation mode:

Demand rate:

Running-on time:

Priority:

Documentation:

Document:

Required Performance Level Safety function

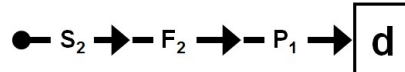
PLr (by risk graph): d

Severity of injury (S): False Serious (normally irreversible) injury or death

Frequency / exposure times to hazard (F): Frequent to continuous / exposure time is long

Possibility of avoiding (P): Possible under specific conditions

Risk graph:



Documentation:

Document:

Performance Level Safety function

Reached PL: e PFHD [1/h]: 4,29E-8

Status / Messages Safety function

Status: green

Subsystems (1 / 1)

SB Name: Valves

Reference designator:

Inventory number:

Device details Subsystem

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Use case:



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (pilot pressure)

Description of the use case:

Documentation Subsystem

Documentation:

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]: 4,29E-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-tries 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:

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 [%]: 90 (Medium)



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (pilot pressure)

Common cause failure Subsystem

CCF Points: 95 (fulfilled)

CCF Measures:

- 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 boards.
- Diversity (20 Points)
Different technologies/design or physical principles are used, for example:
 - first channel electronic or programmable electronic and second channel electromechanical hardwired,
 - different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or
 - digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or
 - Components of different manufactures.
- Design / application / experience (15 Points)
Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
- 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.
- Competence / training (5 Points)
Training of designers to understand the causes and consequences of common cause failures.
- 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



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (pilot pressure)

CCF Measures: as, temperature, shock, vibra

Documentation:

Document:

Status / Messages Subsystem

Status: green

Channels / Test channels (1 / 2)**CH** Name: Channel 1

MTTFD [a]: 380,5

Blocks (1 / 1)**BL** Name: 5/3 Directional control valve

Reference designator: Q3

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Technology:

unknown

Category:

-

Use case:

Description of the
use case:*Documentation Block*

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 380,5 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

B10 [cycles]: 10000000

RDF [%]: 50

B10D [cycles]: 20000000

nop [cycles/a]: 525600

Documentation:

Diagnostic coverage Block

DC [%]: 90 (Medium)



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (pilot pressure)

Measure: Indirect monitoring (e.g monitoring by pressure switch, electrical position monitoring of actuators)
(Output device)
(90 % - 99 % depending on the application)

Documentation:

Status / Messages Block

Status: green

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 91324,2

Blocks (1 / 1)

BL Name: 3/2 Directional control valve

Reference designator: Q2

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:

Revision:

Function:

☐ Input
☒ Output

☐ Logic
☐ unknown

Technology:

unknown

Category:

-

Use case:

Description of the
use case:

Documentation Block

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 91324,2 (High)

Mission time [a]: 20

Shortest mission time [a]: 20

B10 [cycles]: 10000000

RDF [%]: 50

B10D [cycles]: 20000000

nop [cycles/a]: 2190

Documentation:

Diagnostic coverage Block

DC [%]: 90 (Medium)



Project name: 20220131-001

File date: 18.08.2022 04:15:48 Report date: 18.08.2022 Checksum: f17952d9676b23b64d63c8524512ebed

SF Safety function: PUS (pilot pressure)

Measure:	Indirect monitoring (e.g monitoring by pressure switch, electrical position monitoring of actuators) (Output device) (90 % - 99 % depending on the application)
----------	--

Documentation:

Status / Messages Block

Status:	green
---------	-------

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