SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine

Project name: **100384**

File date: 16.10.2026 10:12:30 Report date: 16.10.2026 Checksum: d49a78a07be8369be80d7d1cfb9a6b3b

PR Project name: 100384

Project file name:	C:\Users\jkhl\Documents\Projects\20211207-001\100384 Sistema Project - V3.0.4 - EN.ssm
Creation date:	14.12.2021 07:07:57
Project status:	
Project number:	
Project version:	
Authors:	
Project managers:	
Inspectors:	
Dangerous point/machine:	
Documentation:	
Document:	
Version of software:	3.0.4 build 3
Version of standard:	ISO 13849-1:2023, ISO 13849-2:2012
Checksum:	d49a78a07be8369be80d7d1cfb9a6b3b
Options:	☑ Use DC intermediate levels for calculation of PFH (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 documentations on SF, SB, BL and EL
- ☐ Show CCF and DC measures in detail
- ☑ Show requirements on PL and Category
- ☑ Show parameter documentations on PLr, PL, Category, CCF, MTTFD and DC
- ☑ Show messages

Contained safety functions

SF Name: STO

Required: PLr c **Reached: PL c** **PFH [1/h]: 1,15E-6** **Status: green**

List of documented messages:

- No messages known -

List of devices with a permissible operation time (T10D) of less than 20 years:

- No devices known -

SF Name: PUS

Required: PLr d **Reached: PL e** **PFH [1/h]: 4,29E-8** **Status: green**

PR Project name: 100384

List of documented messages:

- No messages known -

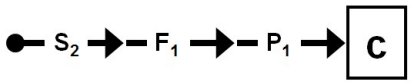
List of devices with a permissible operation time (T10D) of less than 20 years:

- No devices known -

SF Safety function: STO

Identifier of the Safety function:	
Safety function type:	
Triggering event:	
Reaction and Behaviour on power failure:	
Safe state:	
Operation mode:	
Interfaces:	
Demand rate:	
Running-on time:	
Priority:	
Documentation:	
Document:	

Required Performance Level Safety function

PLr (by risk graph):	c
Severity of injury (S):	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	**PFH [1/h]:**	1,15E-6

Electromagnetic immunity, EMI (Annex L) Safety function

Route for fulfilment of EMI measures:	n/a
Documentation:	
Document:	

List of devices with a permissible operation time (T10D) of less than 20 years:

Device list:

SF Safety function: STO

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:

Description of the use case:

Documentation Subsystem

Documentation:

Document:

Performance Level Subsystem

PL determination: Determine PL/PFH from Category, MTTFD and DCavg

Qualitative aspects (e.g. software, see sections 7, 10.3) Subsystem

Qualitative aspects suitable up to PL: n/a

Documentation:

Document:

Electromagnetic immunity, EMI (Annex L) Subsystem

Route for fulfilment of EMI measures: The fulfilment of the measures for electromagnetic immunity (EMI) was documented in the associated safety function.

PL requirements: fulfilled

The PL shall be determined by the estimation of the following aspects (section 6.1.1):
- Behaviour of the safety function under fault conditions [fulfilled]
- Safety-related software according to clause 7 and Annex J or no software included [fulfilled]
- Systematic failure (see clause 6.1.7 and Annex G) [fulfilled]
- Ability to perform a safety function under expected environmental conditions [fulfilled]

SF Safety function: STO

Reached PL:	c	**PFH [1/h]:**	1,15E-6

Documentation:

Category Subsystem

Cat.:	1
Category requirements:	fulfilled

Requirements for the category:
- Accordance with relevant standards to withstand the expected influences. [fulfilled]
- Basic safety principles are being used. [fulfilled]
- Well-tried components (clause 6.1.11) 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

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: 5/3-way valve

Reference designator:	Q2
Inventory number:	

Device details Block

Device Manufacturer:	
Device Identifier:	
Device group:	
Part number:	
Revision:	

Function:

- ☐ Input
- ☑ Output
- ☐ Logic
- ☐ unknown

SF Safety function: STO

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:			
Document:			

Status / Messages Block

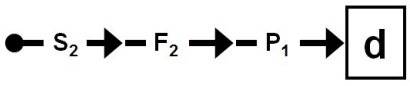
Status:	green

SF Safety function: PUS

Identifier of the Safety function:	
Safety function type:	
Triggering event:	
Reaction and Behaviour on power failure:	
Safe state:	
Operation mode:	
Interfaces:	
Demand rate:	
Running-on time:	
Priority:	
Documentation:	
Document:	

SF Safety function: PUS

Required Performance Level Safety function

PLr (by risk graph):	d
Severity of injury (S):	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	**PFH [1/h]:**	4,29E-8

Electromagnetic immunity, EMI (Annex L) Safety function

Route for fulfilment of EMI measures:	n/a

Documentation:

Document:

List of devices with a permissible operation time (T10D) of less than 20 years:

Device list:

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 ☐ Logic ☑ Output ☐ unknown

SF Safety function: PUS

Use case:

Description of the use case:

Documentation Subsystem

Documentation:

Document:

Performance Level Subsystem

PL determination: Determine PL/PFH from Category, MTTFD and DCavg

Qualitative aspects (e.g. software, see sections 7, 10.3) Subsystem

Qualitative aspects suitable up to PL: n/a

Documentation:

Document:

Electromagnetic immunity, EMI (Annex L) Subsystem

Route for fulfilment of EMI measures: The fulfilment of the measures for electromagnetic immunity (EMI) was documented in the associated safety function.

PL requirements: fulfilled

The PL shall be determined by the estimation of the following aspects (section 6.1.1):
- Behaviour of the safety function under fault conditions [fulfilled]
- Safety-related software according to clause 7 and Annex J or no software included [fulfilled]
- Systematic failure (see clause 6.1.7 and Annex G) [fulfilled]
- Ability to perform a safety function under expected environmental conditions [fulfilled]

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

Documentation:

Category Subsystem

Cat.: 3

Category requirements: fulfilled

Requirements for 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. [fulfilled]
- Requirement fulfilled because of the assumed limit value accuracy of 5 percentage points. [fulfilled]
- The achieved score of the CCF-rating is at least 65. [fulfilled]

Documentation:

SF Safety function: PUS

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)

Common cause failure Subsystem

CCF Points:	95 (fulfilled)

CCF Measures:
- 15 Points | Separation/segregation
- 20 Points | Diversity
- 15 Points | Protection against over-voltage, over-pressure, over-current, over-temperature
- 5 Points | Assessment/analysis
- 5 Points | Training
- 25 Points | Prevention of EMI or impurity of fluidic medium
- 10 Points | Other influences

Documentation:

Document:

Status / Messages Subsystem

Status:	green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: 5/3-way valve

Reference designator: Q2

Inventory number:

Device details Block

Device Manufacturer:

Device Identifier:

Device group:

Part number:
Revision:

SF Safety function: PUS

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:			
Document:			

Diagnostic coverage Block

DC [%]:	90 (Medium)
Measure:	Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators)
Documentation:	
Document:	

Status / Messages Block

Status:	green

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: 3/2-way valve

Reference designator:	Q1
Inventory number:	

SF Safety function: PUS

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]:	182648,4 (High)		
Mission time [a]:	20	**Shortest mission time [a]:**	20
B10 [cycles]:	10000000	**RDF [%]:**	50
B10D [cycles]:	20000000	**nop [cycles/a]:**	1095
Documentation:			
Document:			

Diagnostic coverage Block

DC [%]:	90 (Medium)
Measure: Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of machine actuators)	
Documentation:	
Document:	

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 Haftung des Institut für Arbeitsschutz der DGUV (IFA) ist damit auf Vorsatz und grobe Fahrlässigkeit (§ 521 BGB) bzw. bei Sach- und Rechtsmängel auf arglistig verschwiegene Fehler beschränkt (523, 524 BGB).

The Institute for Occupational Safety and Health of the German Social Accident Insurance 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.

German Social Accident Insurance (DGUV)
Glinkastraße 40
D-10117 Berlin

E-mail: info@dguv.de
Internet: www.dguv.de

NOTE

This document is not a complete technical documentation according to EN ISO 13849-1:2023, clause 12.

CONTACT

Company contact details unknown

Name in block letters	**Date, signature**
Authors	Authors
Inspectors	Inspectors