Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

PR Project name: HOACO

Project file name:	D:\HOACO.ssm
Creation date:	26/03/2020 09:10:13
Project status:	
Project number:	
Project version:	
Authors:	USER
Project managers:	
Inspectors:	
Dangerous point/machine:	
Documentation:	
Document:	
Version of software:	2.0.8 build 4
Version of standard:	ISO 13849-1:2015, ISO 13849-2:2012
Checksum:	5552651956d437729d6f50f3827e5c89
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 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

Solution Street Select Sel	Switch safety function
--	------------------------

Required: PLr d	Reached: PL e	PFHD [1/h]: 5.6E-8	Status: green
SF Name: A.2 Safety Lig	ht Curtain safety function		
Required: PLr d	Reached: PL d	PFHD [1/h]: 1.2E-7	Status: green
F Name: A.3 Safety En	coder safety function		
Required: PLr d	Reached: PL d	PFHD [1/h]: 1.3E-7	Status: green
F Name: A.4 Jog Grip	Switch safety function		
Required: PLr d	Reached: PL e	PFHD [1/h]: 8.9E-8	Status: green
F Name: A.5 LOCK Bu	tton safety function		
Required: PLr d	Reached: PL e	PFHD [1/h]: 9E-8	Status: green
F Name: B.1 Safety Co	ntact Sensor 1 safety fund	ction	
Required: PLr d	Reached: PL d	PFHD [1/h]: 1.3E-7	Status: green

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

PR Project name: HOACO

Required: PLr d	Reached: PL e	PFHD [1/h]: 9.5E-8	Status: green
SF Name: D.1 Emergend	cy Button safety function		
Required: PLr d	Reached: PL e	PFHD [1/h]: 8.9E-8	Status: green
F Name: D.2 Emergend	cy Cord safety function		
Required: PLr d	Reached: PL d	PFHD [1/h]: 1E-7	Status: green



Project name: HOACO

SF Safety function: A.1 MODE-Sele	ect Key Switch safety	function
Identifier of the Safety function:		
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 fund	ction	
PLr (by risk graph):	d	
Severity of injury (S): False	Serious (normally irrev	versible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuou	s / exposure time is long
Possibility of avoiding (P):	Possible under specifi	c conditions
Risk graph:	$\bullet S_2 \rightarrow F_2 -$	→ - P ₁ → d
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: e	PFHD [1/	h]: 5.6E-8
Status / Messages Safety function		
Status:	green	
Subsystems (1 / 2)		
SB Name: Key Switch		
Reference designator:	Inver	ntory number:
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revi	sion:
Function:	☐ Input ☐ Output	☐ Logic ☑ unknown

Project name: HOACO



Description of the use case: Documentation Subsystem		
Documentation Subsystem Documentation: Document: Performance Level Subsystem PL determination: Determine PL/PFHD from Category, MTTFD and DCavg Software suitable up to PL: In.a. PL requirements: The PL shall be determined by the estimation of the following aspects: In a step-related software according to clause 4.6 or no software included [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 environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Basic safety principles are being used. [fulfilled] - Basic safety principles are being used. [fulfilled] - A single fault tolerance and reasonable fault detection are gifulfilled] - 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] - The achieved score of the CCF-rating is at least 65. [fulfilled]	Use case:	
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: fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] Reached PL: e PFHD [1/h]: 2.5E-8 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expect influences. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled]	•	
Documents: 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: If utililed] - 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 environal conditions [fulfilled] - Ability to perform a safety function under expected environal conditions [fulfilled] Reached PL: e PFHD [1/h]: 2.5E-8 Documentation: Category Subsystem Cat.: 3 Category requirements: fulfilled - Basic safety principles are being used. [fulfilled] - Basic safety principles are being used. [fulfilled] - A single fault tolerance and reasonable fault detection are grifufilled] - MTTFD is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [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	Documentation Subsystem	
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 - Behaviour of the safety function under fault conditions (see the following aspects: If ulfilled] - 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 environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] Reached PL: e PFHD [1/h]: 2.5E-8 Documentation: Category Subsystem Cat: 3 Category requirements: 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 of [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - DCavg is at least Low or Medium; [fulfilled]	Documentation:	
PL determination: Determine PL/PFHD from Category, MTTFD and DCavg Software suitable up to PL: n.a. PL requirements: Interpretable of the following aspects: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - Ability to perform a safety function under expected environs conditions [fulfilled] - Ability to perform a safety function under expected environs conditions: The PL shall be determined by the estimation of the safety function under fault conditions (see [fulfilled] - Accordance with relevant standards to withstand the expect influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - Basic safety principles are being used. [fulfilled] - A single fault tolerance and reasonable fault detection are grufulfilled] - A single fault tolerance and reasonable fault detection are grufulfilled] - Docayg is at least Low or Medium; [fulfilled] - Docayg is at least Low or Medium; [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achi	Document:	
Software suitable up to PL: n.a. PL requirements: fulfilled The PL shall be determined by the estimation of the following aspects: fulfilled] - safety-related software according to clause 4.6 or no software included [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 environn conditions [fulfilled] Reached PL: e PFHD [1/h]: 2.5E-8 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expect influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - A single fault tolerance and reasonable fault detection are gruffilled] - MTTFD is at least Low or Medium; [fulfilled] - Docayg is at least Low or Medium; [fulfilled] - The achieved score of the CCF-rating is at least 65. [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	Performance Level Subsystem	
PL requirements: The PL shall be determined by the estimation of the Following aspects: The PL shall be determined by the estimation of the Following aspects: [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 environations [fulfilled] - Ability to perform a safety function under expected environations [fulfilled] Reached PL: e PFHD [1/h]: 2.5E-8 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expect 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 grundled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [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	PL determination:	Determine PL/PFHD from Category, MTTFD and DCavg
The PL shall be determined by the estimation of - Behaviour of the safety function under fault conditions (see the following aspects: fulfilled	Software suitable up to PL:	n.a.
the following aspects: [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 environn 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 expect 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 generated fulfilled] - MITTFD 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	PL requirements:	fulfilled
Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled Requirements of the Category: - Accordance with relevant standards to withstand the expect 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 of [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [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		[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
Category Subsystem Cat:: 3 Category requirements: fulfilled Requirements of the Category: - Accordance with relevant standards to withstand the expect 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 gas [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	Reached PL: e	PFHD [1/h]: 2.5E-8
Cate: Category requirements: Fulfilled Requirements of the Category: - Accordance with relevant standards to withstand the expect 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 go [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	Documentation:	
Cate: Category requirements: Fulfilled Requirements of the Category: - Accordance with relevant standards to withstand the expect 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 go [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	Catagory Subayatam	
Category requirements: Requirements of the Category: - Accordance with relevant standards to withstand the expect 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 g [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		3
Requirements of the Category: - Accordance with relevant standards to withstand the expect 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 general standards. [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] - The achieved score of the CCF-rating is at least 65. [fulfilled] Documentation: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem		
Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem		 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]
File: MTTFD and Mission time Subsystem		DCavg is at least Low or Medium; [fulfilled] The achieved score of the CCF-rating is at least 65. [fulfilled]
MTTFD and Mission time Subsystem	Documentation:	
	Source (e.g. standard) Category:	
= [-].	Source (e.g. standard) Category: File:	
	Source (e.g. standard) Category: File:	- The achieved score of the CCF-rating is at least 65. [fulfilled]
	Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem	

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: A.1 MODE-Select Key Switch safety function

CCF Points:	80 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example:
	i ^a separation in wiring/piping; i ^a detection of short circuits and open circuits in cables by dynamic
	test; i^a separate shielding for the signal path of each channel; i^a sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	- Design / application / experience (5 Points) Components used are well-tried.
	 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 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 C3-1).
	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 shoul 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).
Documentation:	
Document:	
Status / Messages Subsyste	m
Status:	green

Project name: HO400



afety function: A.1 MODE-Select Key	Switch safety function	
hannels / Test channels (1 / 2)		
H Name: Channel 1		
MTTFD [a]: 100		
Blocks (1 / 1)		
BL Name: Key Switch		
Reference designator:	Inventory number:	
Device details Block		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	✓ Input Logic Output unknown	
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
December 1 time District		
Documentation Block Documentation:		
Document:		
bocument.		
MTTFD and Mission time Block		
MTTFD [a]: 416.7 (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: Mode SW.1		
Reference designator:	Inventory number:	
Device details Element		
Device Manufacturer:	OMRON	
Device Identifier:		

Project name: HO400



	Device group:			
	Part number: A4EG-BM2B	041	Revision:	
	Function:		✓ Input ☐ Output	☐ Logic ☐ unknown
	Technology:		electronic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element	nt		
	Document:			
	MTTFD and Mission tir	ne Element		
	MTTFD [a]: 416.7 (High)			
	Mission time [a]: 20			
	B10 [cycles]: 200000		RDF [%]: 50	
	B10D [cycles]: 400000		nop [cycles/a]:	9600
	Nop parameter:	Days: 300	Hours: 8	Seconds: 900
	Documentation:			
	Diagnostic coverage E	lomont		
	DC [%]: 99 (High)	lement		
	Measure:		within the logic (L), an	nput signals and intermediate resul d temporal and logical software n flow and detection of static faults multiple I/O)
	Documentation:			
	Status / Messages Elei	ment		
	Status:		green	
hann	els / Test channels (2 / 2))		
	me: Channel 2			
	TFD [a]: 100			
	cks (1 / 1)			
	rioy Othicon			
BL	Name: Key Switch			

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: A.1 MODE-Select Key Switch safety function Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case: Description of the use case: Documentation Block Documentation: Document: MTTFD and Mission time Block MTTFD [a]: 416.7 (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: Mode SW.2 Reference designator: Inventory number: Device details Element Device Manufacturer: **OMRON** Device Identifier: Device group: Part number: A4EG-BM2B041 Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case:





	Description of the			
	use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time	e Element		
	Mission time [a]: 20			
	B10 [cycles]: 200000		RDF [%]: 50	
	B10D [cycles]: 400000		nop [cycles/a]: 9600	
	Nop parameter:	Days: 300	Hours: 8	Seconds: 900
	Documentation:			
	Diagnostic coverage Ele	ement		
	DC [%]: 99 (High)	inone		
	Measure:		within the logic (L), and ter	w and detection of static faults
	Documentation:			
	Status / Messages Elem	nent		
	Status:	ion	green	
Subsysten	22 (2 / 2)			
Subsysten	Safety PLC G9SP			
	ce designator:		Inventory number:	
	details Subsystem		inventory number.	
	lanufacturer:	OMRON		
Device lo	dentifier:			
Device g	roup:			
	nber: G9SP-N20S		Revision:	
Function	:	☐ Input ☐ Output	✓ Logic ☐ unknow	n
Use case):			





File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.1 MODE-Select Key Switch safety function Documentation Subsystem Documentation: Document: Performance Level Subsystem 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]: 3.2E-8 Documentation: Mission time [a]: 20 Shortest mission time [a]: 20 Category Subsystem 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: Status / Messages Subsystem Status: green



Project name: HO400

SF Safety function: A.2 Safety Light	Curtain safety function	
Identifier of the Safety function:		
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 func-	ion	
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 til	me is long
Possibility of avoiding (P):	Possible under specific conditions	
Risk graph:		d
Documentation:		
Document:		
Darfarmana Laval Cafaty function		
Performance Level Safety function Reached PL: d	PFHD [1/h]: 1.2E-7	
Status / Messages Safety function		
Status:	green	
Subsystems (1 / 4)		
SB Name: Safety Light Curtain		
Reference designator:	Inventory number:	
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	✓ Input Log	gic known

Project name: HO400



Safety function: A.2 Safety Light Cui	rtain safety function
Use case:	
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 [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]: 1.2E-8
Documentation:	
Category Subsystem	
Cat.:	4
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] Accumulation of faults does not lead to a loss of the safety function [fulfilled] MTTFD is at least High. [fulfilled] DCavg is at least High; [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]:	200 (High)
Mission time [a]: 20	Shortest mission time [a]: 20

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.2 Safety Light Curtain safety function

DCavg [%]:	99 (High)
Common cause failure Sub	system
CCF Points:	100 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: ¡a separation in wiring/piping; ¡a detection of short circuits and open circuits in cables by dynamic test; ¡a separate shielding for the signal path of each channel; ¡a sufficient clearances and creepage distances on printed-circuit boards.
	 Diversity (20 Points) Different technologies/design or physical principles are used, for example: i^a first channel electronic or programmable electronic and second channel electromechanical hardwired, i^a 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.
	 Design / application / experience (5 Points) Components used are well-tried. - 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 o 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"C3-1).

intake, drainage of compressed

requirements concerning purity of the pressure medium.

Fluidic systems: filtration of the pressure medium, prevention of dirt

air, e.g. in compliance with the component manufacturers;





CCF Measures:	NOTE For combined fluidic and electric systems, both aspects should be considered.
	 Environmental (10 Points) Other influences Consideration of the requirements for im
Documentation:	
Document:	
Status / Messages Subsystem	
Status:	green
Channels / Test channels (1 / 2)	
CH Name: Channel 1	
MTTFD [a]: 200	
Blocks (1 / 1)	
BL Name: Safety Light Curta	ain
Reference designator:	Inventory number:
Device details Block	
Device Manufacturer:	
Device Identifier:	
Device group:	
Part number:	Revision:
Function:	☐ Input ☐ Logic ☐ Output ☐ unknown
Technology:	electronic
Category:	-
Use case:	
Description of the use case:	
Documentation Block	
Documentation:	
Document:	
MTTFD and Mission time B	lock
MTTFD [a]: 200 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.2 Safety Light Curtain safety function Status / Messages Block Status: green **Elements (1 / 1)** EL Name: SC1.1 Reference designator: Inventory number: Device details Element Device Manufacturer: **LNTECH** Device Identifier: Device group: Part number: SND7220-PNP Revision: Function: Logic Input Output unknown Technology: electronic Category: Use case: Description of the use case: Documentation Element Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 200 (High) Mission time [a]: 20 Rate of dangerous failure [FIT]: 570.8 Documentation: Diagnostic coverage Element DC [%]: 99 (High) Documentation: Status / Messages Element Status: green Channels / Test channels (2 / 2) CH Name: Channel 2 MTTFD [a]: 200

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.2 Safety Light Curtain safety function Blocks (1 / 1) **BL** Name: Safety Light Curtain Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case: Description of the use case: Documentation Block Documentation: Document: MTTFD and Mission time Block MTTFD [a]: 200 (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: SC1.2 Reference designator: Inventory number: Device details Element Device Manufacturer: **LNTECH** Device Identifier: Device group: Part number: SND7220-PNP Revision:

InputOutput

Function:

Logic

unknown

Project name: HO400



Safety	function: A.2 Safety Lig	ght Curtain safety	function		
	Technology:		electronic		
	Category:		-		
	Use case:				
	Description of the use case:				
	Documentation Elemen	t			
	Documentation:				
	Document:				
	MTTFD (a): 200 (High)	ne Element			
	MTTFD [a]: 200 (High)				
	Mission time [a]: 20	EIT1 570.0			
	Rate of dangerous failure [F11]: 5/0.8			
	Documentation:				
	Diagnostic coverage El	ement			
	DC [%]: 99 (High)				
	Documentation:				
	Status / Messages Elen	nent			
	Status:		green		
Subsysten	ns (2 / 4)				
B Name:	Safety PLC G9SP				
Reference	ce designator:		Inventory nu	mber:	
Device	details Subsystem				
	Manufacturer:	OMRON			
Device lo	dentifier:				
Device g	group:				
Part num	nber: G9SP-N20S		Revision:		
Function	ו:	☐ Input ☐ Output		✓ Logic ☐ unknown	
Use case	e:				
Descript use case	ion of the e:				
Docume	entation Subsystem				
Docume	ntation:				
Docume	nt:				

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Second Se Performance Level Subsystem 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]: 3.2E-8 Documentation: Mission time [a]: 20 Shortest mission time [a]: 20 Category Subsystem 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: Status / Messages Subsystem Status: green Subsystems (3 / 4) SB Name: Contactor Reference designator: Inventory number: Device details Subsystem Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Use case: Description of the use case: Documentation Subsystem Documentation: Document: Performance Level Subsystem PL determination: Determine PL/PFHD from Category, MTTFD and DCavg

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: A.2 Safety Light Curtain safety function

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 [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]: 4.3E-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:				
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:	80 (fulfilled)			
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: ¡a separation in wiring/piping; ¡a detection of short circuits and open circuits in cables by dynamic test; ¡a separate shielding for the signal path of each channel; ¡a sufficient clearances and creepage distances on printed-circuit boards.			

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Second Se

CCF Measures:

- 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.

- 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"C3-1).

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).

- Competence / training (5 Points)

Training of designers to understand the causes and consequences of common cause failures.

- Design / application / experience (5 Points) Components used are well-tried.

Documentation:			
Document:			
Status / Messages Subsystem			
Status:	green		
Channels / Test channels (1 / 2	2)		
CH Name: Channel 1			
MTTFD [a]: 100			
Blocks (1 / 1)			
BL Name: Contactor			
Reference designator:		Inventory number:	
Device details Block			
Device Manufacturer:			

Project name: HOACO



Device Identifier:	
Device group:	
Part number:	Revision:
Function:	☐ Input ☐ Logic ☐ unknown
Technology:	electronic
Category:	-
Use case:	
Description of the use case:	
Documentation Block	
Documentation:	
Document:	
MTTFD and Mission time Block	
MTTFD and Mission time Block MTTFD [a]: 6944.4 (High)	
Diagnostic coverage Block	Shortest mission time [a]: 20
Diagnostic coverage Block DC [%]: 90 (Medium)	Shortest mission time [a]: 20
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block	Shortest mission time [a]: 20 green
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status:	
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1)	
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1)	
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3	green
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator:	green
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element	green Inventory number:
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer:	green Inventory number:
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier:	green Inventory number:
Device details Element Device Manufacturer: Device Identifier: Device group:	green Inventory number: SIEMENS
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02	green Inventory number: SIEMENS Revision: Input Logic
Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02 Function:	green Inventory number: SIEMENS Revision: Input Output Unknown

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.2 Safety Light Curtain safety function Documentation Element Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Days: 300 Hours: 8 Seconds: 300 Nop parameter: Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O) (Output device) (90 %)Documentation: Status / Messages Element Status: green Channels / Test channels (2 / 2) CH Name: Channel 2 MTTFD [a]: 100 Blocks (1 / 1) **BL** Name: Contactor Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case: Description of the use case:





Documentation Block			
Documentation:			
Document:			
MTTFD and Mission time Block			
MTTFD [a]: 6944.4 (High)			
Mission time [a]: 20		Shortest miss	ion time [a]: 20
Diagnostic coverage Block			
DC [%]: 90 (Medium)			
, ,			
Status / Messages Block			
Status:	9	reen	
Elements (1 / 1)			
EL Name: KM4			
Reference designator:		Inventory nu	umber:
Device details Element			
Device Manufacturer:		SIEMENS	
Device Identifier:			
Device group:			
Part number: 3RT60 16-1AB02		Revision:	
Function:		☐ Input ☑ Output	Logic unknown
Technology:		electronic	
Category:		-	
Use case:			
Description of the use case:			
Documentation Element			
Documentation:			
Document:			
MTTFD and Mission time Ele	ement		
MTTFD [a]: 6944.4 (High)	,		
Mission time [a]: 20			
B10D [cycles]: 20000000		nop [cycles/	'al· 28800
DIVDICACION, ZUUUUUU		Hop [cycles/	aj. 20000





	Documentation:			
	Diagnostic coverage Elem	nent		
	DC [%]: 90 (Medium)			
	Measure:	with	out detection tput device)	ng of output signals with dynamic test on of short circuits (for multiple I/O)
	Documentation:			
	Status / Messages Elemei	nt		
	Status:	gree	en	
ıboyotomo	. (4 / 4)			
Ibsystems Name: C	Converter U1 STO			
	designator:		nventory nur	mher·
	etails Subsystem		inventory nui	HIJOI.
	nufacturer:	OMRON		
Device Ide				
Device gro				
	er: R88D-1SN-10H-ECT		Revision:	
	er. Kood-13N-10H-ECT		REVISION.	TI ania
Function:		Input ✓ Output		Logic unknown
Use case:				
Descriptio use case:	n of the			
Documen	ntation Subsystem			
Document				
Document				
Dorforma	nce Level Subsystem			
PL determ				nanufacturer ensures compliance with the lory and of the PL)
PL: e			Software suit	able up to PL: n.a.
Reached P	PL: e		PFHD [1/h]: 3	·
Document	ation:			
Mission tir			Shortest miss	sion time [a]: 20
Category	Subsystem			
Cat.:	<i>-</i> Сироуотонн	3		
Category r		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:	



Project name: HO400

SF Safety function: A.3 Safety Enc	oder safety functi	on
Identifier of the Safety function:		
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 fund	ction	
PLr (by risk graph):	d	
Severity of injury (S): False	Serious (normally	y irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to conti	inuous / exposure time is long
Possibility of avoiding (P):	Possible under s	pecific conditions
Risk graph:	← S ₂ → −	$F_2 \longrightarrow P_1 \longrightarrow d$
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: d	PF	HD [1/h]: 1.3E-7
Status / Messages Safety function Status:	green	
Status.	green	
Subsystems (1 / 5)		
SB Name: Safety Encoder E1		
Reference designator:		Inventory number:
Device details Subsystem		
Device Manufacturer:	SICK	
Device Identifier:		
Device group:		
Part number: DFS60S-TDOC01024		Revision:
Function:	✓ Input Output	Logic unknown





Use case:			
Description of the use case:			
Documentation Subsystem			
Documentation:			
Document:			
Performance Level Subsystem			
PL determination:		lirectly (manufacturer ensures complianc he Category and of the PL)	e with th
PL: e	So	ftware suitable up to PL: n.a.	
Reached PL: e	PF	HD [1/h]: 1.7E-8	
Documentation:			
Mission time [a]: 20	Sh	ortest mission time [a]: 20	
Category Subsystem			
Cat.:	3		
Category requirements:	fulfilled		
Requirements of the Category:	Since the catego satisfy the requir	ry is given by the manufacturer he is respendents.	oonsible
Documentation:			
Source (e.g. standard) Category:			
File:			
Status / Messages Subsystem			
Status:	green		
bsystems (2 / 5)			
Name: Safety Relay S30-1			
Reference designator:	Inv	entory number:	
Device details Subsystem			
Device Manufacturer:	PILZ		
Device Identifier:			
Device group:			
Part number: S30	Re	vision:	
Function:	☐ Input ☐ Output	✓ Logic unknown	
Use case:			





Documentation Subsystem		
Documentation:		
Document:		
Performance Level Subsystem		
PL determination:		directly (manufacturer ensures compliance with the Category and of the PL)
PL: e	Sc	ftware suitable up to PL: n.a.
Reached PL: e	PF	HD [1/h]: 3.1E-9
Documentation:		
Mission time [a]: 20	St	ortest mission time [a]: 20
Category Subsystem		
Cat.:	4	
Category requirements:	fulfilled	
Requirements of the Category:	Since the categoral satisfy the requirements	ry is given by the manufacturer he is responsible ements.
Documentation:		
Source (e.g. standard) Category:		
File:		
Status / Messages Subsystem		
Status:	green	
psystems (3 / 5)		
Name: Safety PLC G9SP		
Reference designator:	In	ventory number:
Device details Subsystem		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: G9SP-N20S	Re	vision:
Function:	☐ Input ☐ Output	✓ Logic☐ unknown
Use case:		

Project name: HO400



Document:		
Performance Level Subsystem		
PL determination:	Enter PL/PFHD requirements of	directly (manufacturer ensures compliance with the the Category and of the PL)
PL: e	Si	oftware suitable up to PL: n.a.
Reached PL: e	P	FHD [1/h]: 3.2E-8
Documentation:		
Mission time [a]: 20	SI	hortest mission time [a]: 20
Category Subsystem		
Cat.:	4	
Category requirements:	fulfilled	
Requirements of the Category:	Since the categorial satisfy the requi	ory is given by the manufacturer he is responsible to rements.
Documentation:		
Source (e.g. standard) Category:		
File:		
Status / Magazagos Subayatam		
Status / Messages Subsystem Status:	green	
	g. 5.5.1	
Subsystems (4 / 5)		
Name: Contactor		
Reference designator:	In	ventory number:
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	R	evision:
Function:	☐ Input ☐ Output	☐ Logic ☑ unknown
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:	Pull rope switch	device
Document:		

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Secondary Safety Function: A.3 Safety Encoder safety function

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]: 4.3E-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:		
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:	80 (fulfilled)	
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: i ^a separation in wiring/piping; i ^a detection of short circuits and open circuits in cables by dynamic test; i ^a separate shielding for the signal path of each channel;	

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.3 Safety Encoder safety function

CCF Measures:

- $\mathbf{i}^{\mathbf{a}}$ sufficient clearances and creepage distances on printed-circuit boards.
- Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
- Design / application / experience (5 Points) Components used are well-tried.
- 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"C3-1).

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).

Documentation:			
Document:			
Status / Manager Subay	votom		
Status / Messages Subsy	rstern		
Status:	green		
Channels / Test channe	els (1 / 2)		
CH Name: Channel 1			
MTTFD [a]: 100			
Blocks (1 / 1)			
BL Name: Contacto	or		
Reference designato	nr:	Inventory number:	

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.3 Safety Encoder safety function Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic ✓ Output unknown Technology: electronic Category: Use case: Description of the use case: Documentation Block Documentation: Document: MTTFD and Mission time Block MTTFD [a]: 6944.4 (High) Mission time [a]: 20 Shortest mission time [a]: 20 Diagnostic coverage Block DC [%]: 90 (Medium) Status / Messages Block Status: green **Elements (1 / 1) EL Name: KM3** Reference designator: Inventory number: Device details Element Device Manufacturer: **SIEMENS** Device Identifier: Device group: Part number: 3RT60 16-1AB02 Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case:





	Description of the			
	use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time MTTFD [a]: 6944.4 (High)	e Element		
	Mission time [a]: 20			
	B10D [cycles]: 20000000		nop [cycles/a]: 28800)
	Nop parameter:	Days: 300	Hours: 8	Seconds: 300
	Documentation:			
	Diagnostic coverage Ele	ment		
	DC [%]: 90 (Medium)			
	Measure:	W (0	cross monitoring of output without detection of short c Dutput device) 30 %)	
	Documentation:			
	Status / Messages Elem	ent		
	Status:	g	reen	
	els / Test channels (2 / 2)			
anne	cis / rest chamicis (2 / 2)			
	me: Channel 2			
Nar	me: Channel 2			
Nar MT1	TFD [a]: 100			
Nar MTT	TFD [a]: 100 cks (1 / 1)			
MTT Bloc	TFD [a]: 100 cks (1 / 1) Name: Contactor		Inventory number	
MTT Bloc	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator:		Inventory number:	
MTT Bloc BL I	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator: Device details Block		Inventory number:	
Blo I	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator:		Inventory number:	
Nar MTT Blog BL I	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator: Device details Block Device Manufacturer: Device Identifier:		Inventory number:	
Narr MTT Bloo BL	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group:			
Nar MTT Bloo BL I	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator: Device details Block Device Manufacturer: Device Identifier:	□ In	Revision:	ogic
Nam MTT Bloo BL	TFD [a]: 100 cks (1 / 1) Name: Contactor Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number:	□ In ▼ Ou elect	Revision: put	.ogic nknown





Use case:		
Description of the use case:		
Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 6944.4 (High)		
Mission time [a]: 20	Shortest mis	ssion time [a]: 20
Diagnostic coverage Block		
DC [%]: 90 (Medium)		
Status / Massagas Plack		
Status / Messages Block Status:	green	
Reference designator:	Inventory	number:
Reference designator:	Inventory	number:
Device details Element		
Device Manufacturer:	SIEMENS	
Device Identifier:		
Device group:		
Part number: 3RT60 16-1AB02	Revision:	
Function:	☐ Input ☑ Output	Logic unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Element		
Documentation:		
Document:		
Document: MTTFD and Mission time Element		





	B10D [cycles]: 20000000		nop [cycles/a]: 28800)
	Nop parameter:	Days: 300	Hours: 8	Seconds: 300
	Documentation:			
	Diamentia anyone Ele			
	Diagnostic coverage Elei DC [%]: 90 (Medium)	теп		
	Measure:	,	Cross monitoring of output without detection of short c (Output device) (90 %)	
	Documentation:			
	Status / Messages Eleme	ent		
	Status:		green	
Subsyste	ems (5 / 5)			
	e: Converter U1 STO			
Referer	nce designator:		Inventory number:	
Device	e details Subsystem			
Device	Manufacturer:	OMRON		
Device	Identifier:			
Device	group:			
Part nu	ımber: R88D-1SN-10H-ECT		Revision:	
Functio	on:	☐ Input ☑ Output	☐ Logic ☐ unknowi	n
Use cas	se:			
Descrip use cas	otion of the se:			
Docun	nentation Subsystem			
	entation:			
Docum	ent:			
Df				
	mance Level Subsystem ermination:		FHD directly (manufacturer ts of the Category and of the	r ensures compliance with the
PL: e			Software suitable up to PL:	: n.a.
Reache	ed PL: e		PFHD [1/h]: 3.2E-8	
Docum	entation:			
	n time [a]: 20		Shortest mission time [a]:	20

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Secondary Safety Function: A.3 Safety Encoder safety function

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



Project name: HO400

SF Safety function: A.4 Jog Grip S	witch safety function	
Identifier of the Safety function:		
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 fund	ction	
PLr (by risk graph):	d	
Severity of injury (S): False	Serious (normally irrev	ersible) 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:	$\bullet S_2 \rightarrow F_2 \rightarrow$	→ P ₁ → d
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: e	PFHD [1/h]: 8.9E-8
Status / Messages Safety function		
Status:	green	
Subsystems (1 / 3)		
SB Name: Jog Grip Switch / Contact	or	
Reference designator:	Inven	tory number:
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revis	ion:
Function:	☐ Input ☐ Output	☐ Logic ☑ unknown

Project name: HOACO



Use case:	
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 the following aspects:	of - Behaviour of the safety function under fault conditions (see clause [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]: 2.6E-8
Reached PL: e Documentation:	PFHD [1/h]: 2.6E-8
Documentation:	PFHD [1/h]: 2.6E-8
Documentation: Category Subsystem	
Documentation: Category Subsystem Cat.:	3
Documentation: Category Subsystem Cat.: Category requirements:	3 fulfilled
Documentation: Category Subsystem Cat.:	3
Documentation: Category Subsystem Cat.: Category requirements:	fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category:	fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category: Documentation:	fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category: Documentation: Source (e.g. standard) Category: File:	fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category: Documentation: Source (e.g. standard) Category:	fulfilled - 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]

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: A.4 Jog Grip Switch safety function

CCF Points:	80 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example:
	i ^a separation in wiring/piping; i ^a detection of short circuits and open circuits in cables by dynamic
	test; i^a separate shielding for the signal path of each channel; i^a sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	- Design / application / experience (5 Points) Components used are well-tried.
	 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 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 C3-1).
	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 shoul 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).
Documentation:	
Document:	
Status / Messages Subsyste	m
Status:	green

Project name: HO400



fety function: A.4 Jog Grip Switch s	safety function		
hannels / Test channels (1 / 2)			
H Name: Channel 1			
MTTFD [a]: 100			
Blocks (1 / 2)			
BL Name: Jog Grip Switch			
Reference designator:	Inventory r	number:	
Device details Block			
Device Manufacturer:			
Device Identifier:			
Device group:			
Part number:	Revision:		
Function:	✓ Input Output	Logic unknown	
Technology:	electronic		
Category:	-		
Use case:			
Description of the use case:			
D () D			
Documentation Block Documentation:			
Document:			
bocument.			
MTTFD and Mission time Block			
MTTFD [a]: 520.8 (High)			
Mission time [a]: 20	Shortest m	ission time [a]: 20	
Diagnostic coverage Block			
DC [%]: 99 (High)			
Status / Messages Block			
Status:	green		
Elements (1 / 1)			_
EL Name: Handle.1			
Reference designator:	Inventor	y number:	
Device details Element			
Device Manufacturer:	OMRON		
Device Identifier:			

Project name: HO400



	Device group:			
	Part number: A4EG-BM2B0	41	Revision:	
	Function:		✓ Input Output	Logic unknown
	Technology:		electronic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time	e Element		
	Mission time [a]: 20			
	B10 [cycles]: 100000		RDF [%]: 20	
	B10D [cycles]: 500000		nop [cycles/a]:	9600
	Nop parameter:	Days: 300	Hours: 8	Seconds: 900
	Documentation:	<u> </u>		
	Diagnostic coverage Ele	ment		
	DC [%]: 99 (High)		0	
	Measure:		within the logic (L), and	put signals and intermediate d temporal and logical softwa flow and detection of static nultiple I/O)
	Documentation:			
		ent		
	Documentation: Status / Messages Elementation:	ent	green	
	Status / Messages Elem Status:	ent	green	
	Status / Messages Elem Status: ocks (2 / 2)	ent	green	
	Status / Messages Elem Status: ocks (2 / 2) Name: Contactor	ent		
_	Status / Messages Elem Status: ocks (2 / 2)	ent	green Inventory number	:

Project name: HOACO



Device group:	
Part number:	Revision:
Function:	☐ Input ☐ Logic ☐ unknown
Technology:	electronic
Category:	-
Use case:	
Description of the use case:	
Documentation Block	
Documentation:	
Document:	
MTTFD and Mission time Block	
MTTFD [a]: 6944.4 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
DC [%]. 90 (Medium)	
Status / Messages Block	
Status / Messages Block	green
Status / Messages Block Status:	green
Status / Messages Block Status: Elements (1 / 1)	green
Status / Messages Block Status: Elements (1 / 1)	green Inventory number:
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3	
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator:	
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element	Inventory number:
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer:	Inventory number:
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier:	Inventory number:
Device details Element Device Manufacturer: Device Identifier: Device group:	Inventory number: SIEMENS
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02	Inventory number: SIEMENS Revision: Input Logic
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02 Function:	Inventory number: SIEMENS Revision: Input Output Unknown
Status / Messages Block Status: Elements (1 / 1) EL Name: KM3 Reference designator: Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02 Function: Technology:	Inventory number: SIEMENS Revision: Input Logic Output unknown electronic

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.4 Jog Grip Switch safety function Documentation Element Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Days: 300 Hours: 8 Seconds: 300 Nop parameter: Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O) (Output device) (90 %)Documentation: Status / Messages Element Status: green Channels / Test channels (2 / 2) CH Name: Channel 2 MTTFD [a]: 100 Blocks (1 / 2) **BL** Name: Jog Grip Switch Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case: Description of the use case:





Documentation Block		
Documentation block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 520.8 (High)		
Mission time [a]: 20	Shortest mis	sion time [a]: 20
Diagnostic coverage Block		
DC [%]: 99 (High)		
Status / Messages Block		
Status:	green	
Elements (1 / 1)		
EL Name: Handle.2		
Reference designator:	Inventory r	number:
Device details Element		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: A4EG-BM2B041	Revision:	
Function:	✓ Input Output	Logic unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Element		
Documentation:		
Document:		
MTTFD and Mission time Element		
MTTFD [a]: 520.8 (High)		
Mission time [a]: 20		
B10 [cycles]: 100000	RDF [%]: 2	0

Project name: HO400



	Nop parameter:	Days: 300	Hours: 8	Seconds: 900
	Documentation:			
	Diagnostic coverage Eleme	nt		
	DC [%]: 99 (High)			
	Measure:	within monito and sl	the logic (L), and ten or of the program flow nort circuits (for multip devices)	signals and intermediate nporal and logical softway and detection of static ple I/O)
	Documentation:			
	Status / Messages Element			
	Status:	green		
Blo	cks (2 / 2)			
	Name: Contactor			
-	Reference designator:		Inventory number:	
L	Device details Block			
Г	Device Manufacturer:			
-	Device Identifier:			
-	Device group:			
Ī	Part number:		Revision:	
	Function:	☐ Input ☑ Output		ogic Inknown
-	Technology:	electronic		
(Category:	-		
Ī	Use case:			
	Description of the use case:			
L	Documentation Block			
I	Documentation:			
	Document:			
ļ				
L	MTTFD and Mission time Block			
1	<i>MTTFD and Mission time Block</i> MTTFD [a]: 6944.4 (High)			

Project name: HOACO



Status / Messages Block			
Status:	g	reen	
Elements (1 / 1)			
EL Name: KM4			
Reference designator:		Inventory num	ber:
Device details Element		,	
Device Manufacturer:		SIEMENS	
Device Identifier:			
Device group:			
Part number: 3RT60 16-1AB0)2	Revision:	
Function:		☐ Input ☑ Output	Logic unknown
Technology:		electronic	
Category:		-	
Use case:			
Description of the use case:			
Documentation Element			
Documentation:			
Document:			
MTTFD and Mission time	Flement		
MTTFD [a]: 6944.4 (High)			
Mission time [a]: 20			
B10D [cycles]: 20000000		nop [cycles/a]:	28800
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
Documentation:			
Diagnostic coverage Elem	ment		
Measure:			utput signals with dynamic te nort circuits (for multiple I/O)
Documentation:			
Status / Messages Eleme	ent		
Status:	· · · ·	green	

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.4 Jog Grip Switch safety function Subsystems (2 / 3) Safety PLC G9SP Reference designator: Inventory number: Device details Subsystem Device Manufacturer: **OMRON** Device Identifier: Device group: Part number: G9SP-N20S Revision: Function: Input Logic Output unknown Use case: Description of the use case: Documentation Subsystem Documentation: Document: Performance Level Subsystem 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]: 3.2E-8 Documentation: Mission time [a]: 20 Shortest mission time [a]: 20 Category Subsystem 4 Cat.: fulfilled Category requirements: 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 (3 / 3)

SB Name: Converter U1 STO





Reference designator:	Inve	ntory number:
Device details Subsystem		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: R88D-1SN-10H-ECT	Rev	ision:
Function:	☐ Input ☑ Output	Logic unknown
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:		
Document:		
PL determination:		rectly (manufacturer ensures compliance with e Category and of the PL)
PL: e	Soft	ware suitable up to PL: n.a.
Reached PL: e	PFH	D [1/h]: 3.2E-8
Documentation:		
Mission time [a]: 20	Sho	rtest mission time [a]: 20
Category Subsystem		
Cat.:	3	
Category requirements:	fulfilled	
Requirements of the Category:	Since the category satisfy the require	y is given by the manufacturer he is responsibl ments.
Documentation:		
Source (e.g. standard) Category:		
File:		
Source (e.g. standard) Category: File:		
Status / Messages Subsystem		
Status:	green	



Project name: HO400

SF Safety function: A.5 LOCK Butto	on safety function
Identifier of the Safety function:	
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 fund	ction
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:	$- S_2 \rightarrow - F_2 \rightarrow - P_1 \rightarrow \boxed{d}$
Documentation:	
Document:	
Performance Level Safety function	
Reached PL: e	PFHD [1/h]: 9E-8
Status / Messages Safety function	
Status:	green
Subsystems (1 / 3)	
SB Name: Button / Contactor	
Reference designator:	Inventory number:
Device details Subsystem	
Device Manufacturer:	
Device Identifier:	
Device group:	
Part number:	Revision:
Function:	☐ Input ☐ Logic ☐ Output ☑ unknown

Project name: HOACO



Use case:	
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 the following aspects:	 of - Behaviour of the safety function under fault conditions (see clause [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]: 2.7E-8
Reached PL: e Documentation:	
Documentation: Category Subsystem	PFHD [1/h]: 2.7E-8
Documentation: Category Subsystem Cat.:	PFHD [1/h]: 2.7E-8
Documentation: Category Subsystem Cat.: Category requirements:	PFHD [1/h]: 2.7E-8 3 fulfilled
Documentation: Category Subsystem Cat.:	PFHD [1/h]: 2.7E-8
Category Subsystem Cat.: Category requirements:	PFHD [1/h]: 2.7E-8 3 fulfilled - 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]
Category Subsystem Cat.: Category requirements: Requirements of the Category:	PFHD [1/h]: 2.7E-8 3 fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category: Documentation:	PFHD [1/h]: 2.7E-8 3 fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category: Documentation: Source (e.g. standard) Category: File:	PFHD [1/h]: 2.7E-8 3 fulfilled - 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]
Documentation: Category Subsystem Cat.: Category requirements: Requirements of the Category: Documentation: Source (e.g. standard) Category:	PFHD [1/h]: 2.7E-8 fulfilled - 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]

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Sefety function: A.5 LOCK Button safety function

CCF Points:	80 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: ia separation in wiring/piping; ia detection of short circuits and open circuits in cables by dynamic test; ia separate shielding for the signal path of each channel; ia sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	- Design / application / experience (5 Points) Components used are well-tried.
	 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 o 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°C3-1). 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).
Documentation:	
Document:	
Status / Messages Subsystem	
Status:	green





fety function: A.5 LOCK Button safe	ety function	
hannels / Test channels (1 / 2)		
H Name: Channel 1		
MTTFD [a]: 100		
Blocks (1 / 2)		
BL Name: Button		
Reference designator:	Inventory number:	
Device details Block		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	✓ Input Log	gic known
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 1041.7 (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: Watch SW.1		
Reference designator:	Inventory number:	
Device details Element		
Device Manufacturer:	IDEC	
Device Identifier:		

Project name: HO400



	Device group:			
	Part number: AVLW32220DR		Revision:	
	Function:		✓ Input Output	☐ Logic ☐ unknown
	Technology:		electronic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time of MTTFD [a]: 1041.7 (High)	Element		
	Mission time [a]: 20			
	B10 [cycles]: 500000		RDF [%]: 50	
	B10D [cycles]: 1000000		nop [cycles/a]: 9	600
	Nop parameter:	Days: 300	Hours: 8	Seconds: 900
	Documentation:			
	Diagnostic coverage Elem	ent		
	DC [%]: 99 (High)			
			Cross monitoring of in	out signals and intermediate
	Measure:		within the logic (L), and	temporal and logical softwa flow and detection of static
	Measure: Documentation:		within the logic (L), and monitor of the program and short circuits (for m (Input devices)	temporal and logical softwa flow and detection of static
		nt	within the logic (L), and monitor of the program and short circuits (for m (Input devices)	temporal and logical softwa flow and detection of static
	Documentation:	nt	within the logic (L), and monitor of the program and short circuits (for m (Input devices)	temporal and logical softwa flow and detection of static
3lo	Documentation: Status / Messages Elemen	nt	within the logic (L), and monitor of the program and short circuits (for m (Input devices) (99 %)	temporal and logical softwa flow and detection of static
	Documentation: Status / Messages Element Status:	nt	within the logic (L), and monitor of the program and short circuits (for m (Input devices) (99 %)	temporal and logical softwa flow and detection of static
L	Documentation: Status / Messages Element Status: Cks (2 / 2)	nt	within the logic (L), and monitor of the program and short circuits (for m (Input devices) (99 %)	temporal and logical softwa flow and detection of static nultiple I/O)

Project name: HOACO



Device group:	
Part number:	Revision:
Function:	☐ Input ☐ Logic ☐ unknown
Technology:	electronic
Category:	-
Use case:	
Description of the use case:	
Documentation Block	
Documentation:	
Document:	
MTTFD and Mission time Block	
MTTFD and Mission time Block MTTFD [a]: 6944.4 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Status / Messages Block	
Status:	green
Elements (1 / 1)	
EL Name: KM3	
Reference designator:	Inventory number:
Device details Element	
Device details Element Device Manufacturer:	SIEMENS
	SIEMENS
Device Manufacturer:	SIEMENS
Device Manufacturer: Device Identifier:	SIEMENS Revision:
Device Manufacturer: Device Identifier: Device group:	
Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02	Revision:

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: A.5 LOCK Button safety function Documentation Element Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Days: 300 Hours: 8 Seconds: 300 Nop parameter: Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O) (Output device) (90 %)Documentation: Status / Messages Element Status: green Channels / Test channels (2 / 2) CH Name: Channel 2 MTTFD [a]: 100 Blocks (1 / 2) **BL** Name: Button Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electronic Category: Use case: Description of the use case:





Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 1041.7 (High)		
Mission time [a]: 20	Shortest mission tin	ne [a]: 20
Diagnostic coverage Block		
DC [%]: 99 (High)		
Status / Manages Black		
Status / Messages Block Status:	green	
Status.	green	
Elements (1 / 1)		
EL Name: Watch SW.2		
Reference designator:	Inventory number	:
Device details Element		
Device Manufacturer:	IDEC	
Device Identifier:		
Device group:		
Part number: AVLW32220DR	Revision:	
Function:	✓ Input Output	Logic unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Element		
Documentation:		
Document:		
MTTFD and Mission time Element		
MTTFD [a]: 1041.7 (High)		
Mission time [a]: 20		
B10 [cycles]: 500000	RDF [%]: 50	
B10D [cycles]: 1000000	nop [cycles/a]: 96	20

Project name: HO400



	Nop parameter:	Days: 300	Hours: 8	Seconds: 900
	Documentation:			
	Diagnostic coverage Elemei	nt		
	DC [%]: 99 (High)			
	Measure:	withi moni and	n the logic (L), and ter tor of the program flow short circuits (for multi it devices)	signals and intermediate nporal and logical softwark v and detection of static ple I/O)
	Documentation:			
	Status / Messages Element			
	Status:	gree	n	
Blo	cks (2 / 2)			
	Name: Contactor			
Ī	Reference designator:		Inventory number:	
	Device details Block		•	
	Device Manufacturer:			
Ī	Device Identifier:			
Ī	Device group:			
Ī	Part number:		Revision:	
I	Function:	☐ Input ☑ Outpu		_ogic unknown
-	Technology:	electron	C	
(Category:	-		
Į	Use case:			
	Description of the use case:			
L	Documentation Block			
I	Documentation:			
	Document:			
[
L	MTTFD and Mission time Block			
	<i>MTTFD and Mission time Block</i> MTTFD [a]: 6944.4 (High)			

Project name: HOACO



Elements (1 / 1) EL Name: KM4 Reference designator: Inventory number: Device details Element Device group: Part number: 3RT60 16-1AB02 Revision: Function: □ Input □ Logic □ Output □ unknown Technology: electronic Category: - Use case: Description of the use case: Documentation: Document MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B100 [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamiwithout detection of short circuits (for multiple I/ (Output device) (90 %)	Status / Messages Block			
EL Name: KM4 Reference designator: Inventory number: Device details Element Device Manufacturer: SIEMENS Device Identifier: Device group: Part number: 3RT60 16-1AB02 Revision: Function: Input Logic Voutput unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 30: Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)		g	reen	
EL Name: KM4 Reference designator: Inventory number: Device details Element Device Manufacturer: SIEMENS Device Identifier: Device group: Part number: 3RT60 16-1AB02 Revision: Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 30 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Elements (1 / 1)			
Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02 Revision: Function: Input Logic unknown Technology: electronic Category: - Use case: Description of the use case: Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 Nop parameter: Days: 300 Hours: 8 Seconds: 301 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)				
Device details Element Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02 Revision: Function: Input Logic unknown Technology: electronic Category: - Use case: Description of the use case: Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 Nop parameter: Days: 300 Hours: 8 Seconds: 301 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Reference designator:		Inventory num	nber:
Device Manufacturer: Device Identifier: Device group: Part number: 3RT60 16-1AB02 Revision: Function:			,	
Device group: Part number: 3RT60 16-1AB02 Revision: Function:			SIEMENS	
Part number: 3RT60 16-1AB02 Revision: Function: □ Input □ Logic □ Output □ unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element Documents: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple Module of the control of the	Device Identifier:			
Part number: 3RT60 16-1AB02 Revision: Function:	Device group:			
Technology: electronic Category: - Use case: Description of the use case: Documentation Element Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %))2	Revision:	
Category: Use case: Description of the use case: Documentation Element Documents: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple Modure) (Output device) (90 %)	Function:			
Use case: Description of the use case: Documentation Element Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Technology:		electronic	
Description of the use case: Documentation Element Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Category:		-	
Documentation Element Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Use case:			
Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)				
MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Documentation Element			
MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Documentation:			
MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/(Output device) (90 %)	Document:			
MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	MTTED and Mission time	Flement		
B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)		Licinom		
B10D [cycles]: 20000000 nop [cycles/a]: 28800 Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Mission time [a]: 20			
Nop parameter: Days: 300 Hours: 8 Seconds: 300 Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)			nop [cycles/a]	: 28800
Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)		Days: 300		Seconds: 300
DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)		<u> </u>		
DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic without detection of short circuits (for multiple I/ (Output device) (90 %)	Diagnostic coverage Eler	nent		
without detection of short circuits (for multiple I/ (Output device) (90 %)				
Documentation:	Measure:		without detection of si (Output device)	
Dodanomaton.	Documentation:			
	Status / Messages Eleme	// IL	green	

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

Safety function: A.5 LOCK Button safety function Subsystems (2 / 3) Safety PLC G9SP Reference designator: Inventory number: Device details Subsystem **OMRON** Device Manufacturer: Device Identifier: Device group: Part number: G9SP-N20S Revision: Function: Input Logic Output unknown Use case: Description of the use case: Documentation Subsystem Documentation: Document: Performance Level Subsystem 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]: 3.2E-8 Documentation: Mission time [a]: 20 Shortest mission time [a]: 20 Category Subsystem 4 Cat.: fulfilled Category requirements: 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 (3 / 3)

SB Name: Converter U1 STO





OMRON
OMRON
Revision:
☐ Input ☐ Logic ☐ Unknown
Enter PL/PFHD directly (manufacturer ensures compliance with the requirements of the Category and of the PL)
Software suitable up to PL: n.a.
PFHD [1/h]: 3.2E-8
Shortest mission time [a]: 20
3
fulfilled
Since the category is given by the manufacturer he is responsible satisfy the requirements.



Project name: HO400

SF Safety function: B.1 Safety Con	tact Sensor 1 safety function	n
Identifier of the Safety function:		
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 fund	ction	
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 / expo	osure time is long
Possibility of avoiding (P):	Possible under specific condi	tions
Risk graph:	$\bullet S_2 \rightarrow F_2 \rightarrow F_1$	→ d
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: d	PFHD [1/h]: 1.3E-	7
Status / Messages Safety function		
Status:	green	
Subsystems (1 / 2)		
SB Name: Safety Contact Sensor		
Reference designator:	Inventory nui	mber:
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	✓ Input ☐ Output	☐ Logic ☐ unknown

Project name: HO400



Description of the use case: 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: The PL shall be determined by the estimation of the safety function under fault conditions (see content following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see content following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see content following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see content following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see content following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see content following fulfilled) - Ability to perform a safety function under expected environment conditions [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - 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] - MTTFD is at least Low or Medium; fulfilled] - DCavg is at least Low or Medium; fulfilled]		
Documentation Subsystem Document: Determine PL/PFHD from Category, MTTFD and DCavg 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: fulfilled - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environme conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Basic safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg 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	Use case:	
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 Behaviour of the safety function under fault conditions (see of [fulfilled]) - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environme conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expecte influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - Vell-tide safety principles are being used. [fulfilled] - A single fault tolerance and reasonable fault detection are given fulfilled and principles are being used. [fulfilled] - MITTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [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	•	
Document: Performance Level Subsystem PL determination: Determine PL/PFHD from Category, MTTFD and DCavg N.a. PL requirements: fulfilled The PL shall be determined by the estimation of the following aspects: safety-related software according to clause 4.6 or no software included [fulfilled] - safety function under fault conditions (see or [fulfilled]) - systematic failure (see Annex G) [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environme conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat.: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expecte 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 gin [fulfilled] - MTTFD is at least Low or Medium: [fulfilled] - DCavg is at least Low or Medium: [fulfilled] - DCavg is at least Low or Medium: [fulfilled] - DCavg is at least Low or Medium: [fulfilled] - DCavg is at least Low or Medium: [fulfilled] - DCavg is at least Low or Medium: [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled]	Documentation Subsystem	
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: - Safety-related software according to clause 4.6 or no software included [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] - Accordance with relevant standards to withstand the expected influences. [fulfilled] - Accordance with relevant standards to withstand the expected influences. [fulfilled] - Asingle fault tolerance and reasonable fault detection are given [fulfilled] - A single fault tolerance and reasonable fault detection are given [fulfilled] - MTTFD is at least Low or Medium: [fulfilled] - DCavg is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled] - DCavg is at least Low or Medium. [fulfilled]	Documentation:	
PL determination: Determine PL/PFHD from Category, MTTFD and DCavg Software suitable up to PL: n.a. PL requirements: Interpretable support of the safety function under fault conditions (see of the following aspects: The PL shall be determined by the estimation of the safety function under fault conditions (see of fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - Ability to perform a safety function under expected environme conditions [fulfilled] - Ability to perform a safety function under expected environme conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat: 3 Category subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expecte influences. [fulfilled] - Well-tried 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] - Docay gis at least Low or Medium; [fulfilled] - Docay gis at least Low or Medium; [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled]	Document:	
Software suitable up to PL: n.a. PL requirements: fulfilled The PL shall be determined by the estimation of the following aspects: Fulfilled - safety-related software according to clause 4.6 or no software included [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 environme conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expecte 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] - Docave is at least Low or Medium; [fulfilled] - Docay 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	Performance Level Subsystem	
PL requirements: The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects: [fulfilled] - safety-related software according to clause 4.6 or no softward included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environment conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expecte 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] - DCavg is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [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	PL determination:	Determine PL/PFHD from Category, MTTFD and DCavg
The PL shall be determined by the estimation of the following aspects: The PL shall be determined by the estimation of the following aspects:	Software suitable up to PL:	n.a.
the following aspects: [fulfilled] - safety-related software according to clause 4.6 or no softward included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ablitty to perform a safety function under expected environme conditions [fulfilled] Reached PL: d PFHD [1/h]: 1E-7 Documentation: Category Subsystem Cat.: 3 Category requirements: fulfilled - Accordance with relevant standards to withstand the expecte influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [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	PL requirements:	fulfilled
Documentation: Category Subsystem Cat:: Category requirements: Requirements of the Category: - Accordance with relevant standards to withstand the expecte 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: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem		[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
Category Subsystem Cat:: Category requirements: Requirements of the Category: - Accordance with relevant standards to withstand the expecte 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: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem	Reached PL: d	PFHD [1/h]: 1E-7
Cat.: 3 Category requirements: fulfilled Requirements of the Category: - Accordance with relevant standards to withstand the expecte 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: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem	Documentation:	
Cat:: Category requirements: Requirements of the Category: - Accordance with relevant standards to withstand the expecte 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: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem	Catagory Subayatam	
Category requirements: Requirements of the Category: - Accordance with relevant standards to withstand the expecte 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: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem		3
Requirements of the Category: - Accordance with relevant standards to withstand the expecte 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: Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem		
Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem		 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]
File: MTTFD and Mission time Subsystem		- The achieved score of the CCF-rating is at least 65. [fulfilled]
MTTFD and Mission time Subsystem	Documentation:	
	Source (e.g. standard) Category:	
	Source (e.g. standard) Category: File:	
Mission time [a]: 20 Shortest mission time [a]: 20	Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem	- The achieved score of the CCF-rating is at least 65. [fulfilled]
Diagnostic coverage Subsystem	Source (e.g. standard) Category: File: MTTFD and Mission time Subsystem MTTFD [a]: Mission time [a]: 20	- The achieved score of the CCF-rating is at least 65. [fulfilled]

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: B.1 Safety Contact Sensor 1 safety function

CCF Points:	80 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: ¡a separation in wiring/piping; ¡a detection of short circuits and open circuits in cables by dynamic test; ¡a separate shielding for the signal path of each channel; ¡a sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	- Design / application / experience (5 Points) Components used are well-tried.
	 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°C3-1). 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 shoul 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).
Documentation:	Televatii statiuatus).
Document:	
Status / Manages Subsuries	m
<i>Status / Messages Subsyste.</i> Status:	green





nnels / Test channels (1 / 2)	
Name: Channel 1	
MTTFD [a]: 100	
Blocks (1 / 1)	
L Name: Safety Contact Sensor	
Reference designator:	Inventory number:
Device details Block	
Device Manufacturer:	
Device Identifier:	
Device group:	
Part number:	Revision:
Function:	✓ Input Logic Output unknown
Technology:	electromechanic
Category:	-
Use case:	
Description of the use case:	
Documentation Block	
Documentation:	
Document:	
MTTFD and Mission time Block	
MTTFD [a]: 4166.7 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Diagnostic coverage Block	
DC [%]: 60 (Low)	
Status / Messages Block Status:	areen
Jialus.	green
Elements (1 / 1)	
EL Name: Guard-lock switch1.1	
Reference designator:	Inventory number:
Device details Element	
Device Manufacturer:	OMRON
Device Identifier:	

Project name: HO400



	Device group:			
	Part number: D4NS-4CF		Revision:	
	Function:		✓ Input ☐ Output	☐ Logic ☐ unknown
	Technology:		electromechanic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time Elen	nent		
	MTTFD [a]: 4166.7 (High)	non.		
	Mission time [a]: 20			
	B10 [cycles]: 500000		RDF [%]: 50	
	B10D [cycles]: 1000000		nop [cycles/a]:	2400
	Nop parameter:	Days: 300	Hours: 8	Seconds: 3600
	Documentation:			
	Diagnostic coverage Element DC [%]: 60 (Low)			
	Measure:		(Input devices)	nputs without dynamic test g on how often a signal change is
	Documentation:			•
	Status / Messages Element			
	Status:		green	
Chann	nels / Test channels (2 / 2)			
CH Na	me: Channel 2			
МТ	TFD [a]: 100			
Blo	ocks (1 / 1)			
BL	Name: Safety Contact Sensor			
	Reference designator:		Inventory numbe	er:

Project name: HO400



Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	✓ Input Output	☐ Logic ☐ unknown
Technology:	electromechanic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Block		
Documentation:		
Document:		
Mission time [a]: 20	Shortest miss	ion time [a]: 20
Diagnostic coverage Block		
DC [%]: 60 (Low)		
Status / Messages Block		
Status:	green	
Elements (1 / 1)		
EL Name: Guard-lock switch1.2		
	Inventor	ımhor
Reference designator:	Inventory no	umber:
Device details Element Device Manufacturer:	OMRON	
Device Identifier:	OWINGIN	
Device group:		
Part number: D4NS-4CF	Revision:	
Function:	✓ Input	Logic
. 410.001.	Output	unknown
Technology:	electromechanic	
Category:	-	





	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time	e Element		
	MTTFD [a]: 4166.7 (High)			
	Mission time [a]: 20			
	B10 [cycles]: 500000		RDF [%]: 50	
	B10D [cycles]: 1000000		nop [cycles/a]: 2400	
	Nop parameter:	Days: 300	Hours: 8	Seconds: 3600
	Documentation:			
	Diagnostic coverage Ele	ment		
	DC [%]: 60 (Low)			
	Measure:	(I (C	cross monitoring of inputs nput devices) 0 % - 99 % depending on one by the application)	without dynamic test
		(I (C	nput devices) 0 % - 99 % depending on	
	Measure: Documentation:	(I (C d	nput devices) 0 % - 99 % depending on	
	Measure:	(I (C d	nput devices) 0 % - 99 % depending on	
	Measure: Documentation: Status / Messages Elementation:	(I (C d	nput devices) 0 % - 99 % depending on one by the application)	
-	Measure: Documentation: Status / Messages Eleme Status: ns (2 / 2)	(I (C d	nput devices) 0 % - 99 % depending on one by the application)	
Name:	Measure: Documentation: Status / Messages Eleme Status: ns (2 / 2) Converter U1 STO	(I (C d	nput devices) 0 % - 99 % depending on one by the application) reen	
Name:	Measure: Documentation: Status / Messages Eleme Status: ns (2 / 2) Converter U1 STO ce designator:	(I (C d	nput devices) 0 % - 99 % depending on one by the application)	
Name: Reference	Measure: Documentation: Status / Messages Eleme Status: ns (2 / 2) Converter U1 STO de designator: details Subsystem	ent g	nput devices) 0 % - 99 % depending on one by the application) reen	
Name: Reference Device	Measure: Documentation: Status / Messages Eleme Status: ns (2 / 2) Converter U1 STO te designator: details Subsystem Manufacturer:	(I (C d	nput devices) 0 % - 99 % depending on one by the application) reen	
Name: Reference Device Device No	Measure: Documentation: Status / Messages Elementation: Status: Ins (2 / 2) Converter U1 STO The designator: In details Subsystem Manufacturer: Indentifier:	ent g	nput devices) 0 % - 99 % depending on one by the application) reen	
Name: Reference Device N Device N Device Ic	Documentation: Status / Messages Eleme Status: Ins (2 / 2) Converter U1 STO The designator: Indetails Subsystem Manufacturer: Identifier: Igroup:	ent g	nput devices) 0 % - 99 % depending on one by the application) reen Inventory number:	
Name: Reference Device N Device N Device Ic	Measure: Documentation: Status / Messages Elementation: Status: Ins (2 / 2) Converter U1 STO The designator: In details Subsystem Manufacturer: Indentifier:	ent g	nput devices) 0 % - 99 % depending on one by the application) reen	
Name: Reference Device N Device N Device Ic	Measure: Documentation: Status / Messages Eleme Status: Ins (2 / 2) Converter U1 STO De designator: Identifier: Igroup: Inber: R88D-1SN-10H-ECT	ent g	nput devices) 0 % - 99 % depending on one by the application) reen Inventory number:	how often a signal change
Reference Device No Device Identice generating Part num	Measure: Documentation: Status / Messages Eleme Status: Ins (2 / 2) Converter U1 STO De designator: Identifier: Igroup: Inber: R88D-1SN-10H-ECT In:	ent OMRON	nput devices) 0 % - 99 % depending on one by the application) reen Inventory number: Revision:	how often a signal change

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: B.1 Safety Contact Sensor 1 safety function Document: Performance Level Subsystem 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]: 3.2E-8 Documentation: Mission time [a]: 20 Shortest mission time [a]: 20 Category Subsystem 3 fulfilled Category requirements: 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



Project name: HO400

SF Safety function: C.1 Safety Con	tact Sensor 2/3 safety	function
Identifier of the Safety function:		
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 fund	ction	
PLr (by risk graph):	d	
Severity of injury (S): False	Serious (normally irrev	versible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuou	s / exposure time is long
Possibility of avoiding (P):	Possible under specifi	c conditions
Risk graph:	- S ₂ $-$ F ₂ $-$	→ -P ₁ → d
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: e	PFHD [1/	h]: 9.5E-8
Status / Messages Safety function		
Status:	green	
Subayatama (4.1.2)		
Subsystems (1 / 3) SB Name: Safety Contact Sensor		
	l	
Reference designator:	inver	ntory number:
Device details Subsystem Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revi	sion·
Fact number. Function:		
i unction.	✓ Input Output	Logic unknown

Project name: HO400



Use case:	
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 [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]: 3.2E-8
Documentation:	
Category Subsystem	2
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:	
Source (e.g. standard) Category:	
File:	
MTTFD and Mission time Subsystem	
and modern unito outboyoldin	400 (Himb)
MTTFD [a]:	100 (High)

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: C.1 Safety Contact Sensor 2/3 safety function

CCF Points:	80 (fulfilled)
CCF Measures:	 Separation / Segregation (15 Points) Physical separation between signal paths, for example:
	 i^a separation in wiring/piping; i^a detection of short circuits and open circuits in cables by dynamic test;
	i^a separate shielding for the signal path of each channel; i^a sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	- Design / application / experience (5 Points) Components used are well-tried.
	 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 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°C3-1).
	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 shoul 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).
Documentation:	
Document:	
Status / Messages Subsyste	m
Status:	green





File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: C.1 Safety Contact Sensor 2/3 safety function Channels / Test channels (1 / 2) CH Name: Channel 1 MTTFD [a]: 100 Blocks (1 / 2) **BL** Name: Safety Contact Sensor Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electromechanic Category: Use case: Description of the use case: Documentation Block Documentation: Document: MTTFD and Mission time Block MTTFD [a]: 4166.7 (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: Guard-lock switch2.1 Reference designator: Inventory number: Device details Element Device Manufacturer: **OMRON** Device Identifier:

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: C.1 Safety Contact Sensor 2/3 safety function Device group: Part number: D4NS-4CF Revision: Function: Input Logic Output unknown electromechanic Technology: Category: Use case: Description of the use case: Documentation Element Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 4166.7 (High) Mission time [a]: 20 B10 [cycles]: 500000 RDF [%]: 50 B10D [cycles]: 1000000 nop [cycles/a]: 2400 Days: 300 Hours: 8 Nop parameter: Seconds: 3600 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 Blocks (2 / 2) **BL** Name: Contactor Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier:

Project name: HO400



Device group:		
Part number:	Revision:	
Function:	☐ Input ☑ Output	Logic unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 6944.4 (High)		
Mission time [a]: 20	Shortest mission	time [a]: 20
Status / Messages Block	97000	
Status:	green	
Elements (1 / 1)		
EL Name: KM1		
Reference designator:	Inventory num	ber:
Device details Element		
Device Manufacturer:	SIEMENS	
Device Identifier:		
Device group:		
Part number: 3RT60 16-1AB02	Revision:	
Function:	☐ Input ☑ Output	Logic unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the		

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: C.1 Safety Contact Sensor 2/3 safety function Documentation Element Documentation: Document: MTTFD and Mission time Element MTTFD [a]: 6944.4 (High) Mission time [a]: 20 B10D [cycles]: 20000000 nop [cycles/a]: 28800 Days: 300 Hours: 8 Seconds: 300 Nop parameter: Documentation: Diagnostic coverage Element DC [%]: 90 (Medium) Measure: Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O) (Output device) (90 %)Documentation: Status / Messages Element Status: green Channels / Test channels (2 / 2) CH Name: Channel 2 MTTFD [a]: 100 Blocks (1 / 2) **BL** Name: Safety Contact Sensor Reference designator: Inventory number: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Revision: Function: Input Logic Output unknown Technology: electromechanic Category: Use case: Description of the use case:

Project name: HOACO



Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 4166.7 (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: Guard-lock switch2.2		
Reference designator:	Inventory number:	
Device details Element		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: D4NS-4CF	Revision:	
Function:	✓ Input Logi Output unki	
Technology:	electromechanic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Element		
Documentation:		
Document:		
MTTFD and Mission time Element		
MTTFD [a]: 4166.7 (High)		
Mission time [a]: 20		
B10 [cycles]: 500000	RDF [%]: 50	
B10D [cycles]: 1000000	nop [cycles/a]: 2400	

Project name: HO400



	Nop parameter:	Days: 300	Hours: 8	Seconds: 3600
	Documentation:			
	Diagnostic coverage Eleme	nt		
	DC [%]: 99 (High)			
	Measure:	within monito and sh	the logic (L), and ter or of the program flow nort circuits (for multi devices)	signals and intermediatenporal and logical softwork and detection of static ple I/O)
	Documentation:			
	Status / Messages Element			
	Status:	green		
Block	ks (2 / 2)			
	ame: Contactor			
Re	eference designator:		Inventory number:	
De	evice details Block			
	evice Manufacturer:			
De	evice Identifier:			
De	evice group:			
Pa	art number:		Revision:	
Fu	unction:	☐ Input ☑ Output		_ogic unknown
Te	echnology:	electronic		
Ca	ategory:	-		
Us	se case:			
	escription of the se case:			
Do	ocumentation Block			
Do	ocumentation:			
	ocument:			
Do				
	TTFD and Mission time Block			
M	<i>TTFD and Mission time Block</i> TTFD [a]: 6944.4 (High)			

Project name: HOACO



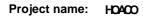
Status / Messages Block Status: Elements (1 / 1) EL Name: KM2 Reference designator: Device details Element	g	reen	
EL Name: KM2 Reference designator: Device details Element			
EL Name: KM2 Reference designator: Device details Element			
Reference designator: Device details Element			
Device details Element		Inventory n	umber:
Device Manufacturer:		SIEMENS	
Device Identifier:			
Device group:			
Part number: 3RT60 16-1AB02	2	Revision:	
Function:		☐ Input ☑ Output	Logic unknown
Technology:		electronic	
Category:		-	
Use case:			
Description of the use case:			
Documentation Element			
Documentation:			
Document:			
MTTFD and Mission time	Flement		
MTTFD [a]: 6944.4 (High)	Liomoni		
Mission time [a]: 20			
B10D [cycles]: 20000000		nop [cycles	/a]: 28800
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
Documentation:	•		
Diagnostic coverage Elem DC [%]: 90 (Medium)	ent		
Measure:			f output signals with dynamic ter short circuits (for multiple I/O)
Documentation:			

Project name: HOACO



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: C.1 Safety Contact Sensor 2/3 safety function Subsystems (2/3) Safety PLC G9SP Reference designator: Inventory number: Device details Subsystem **OMRON** Device Manufacturer: Device Identifier: Device group: Part number: G9SP-N20S Revision: Function: Input Logic Output unknown Use case: Description of the use case: Documentation Subsystem Documentation: Document: Performance Level Subsystem 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]: 3.2E-8 Documentation: Mission time [a]: 20 Shortest mission time [a]: 20 Category Subsystem 4 Cat.: fulfilled Category requirements: 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 (3 / 3) SB Name: Converter G1 STO





Reference designator:	Inve	ntory number:
Device details Subsystem		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: R88D-1SN-10H-ECT	Rev	ision:
Function:	☐ Input ☑ Output	Logic unknown
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:		
Document:		
PL determination:		rectly (manufacturer ensures compliance with t e Category and of the PL)
PL: e	Soft	ware suitable up to PL: n.a.
Reached PL: e	PFH	D [1/h]: 3.2E-8
Documentation:		
Mission time [a]: 20	Sho	rtest mission time [a]: 20
Category Subsystem		
Cat.:	3	
Category requirements:	fulfilled	
Requirements of the Category:	Since the category satisfy the require	y is given by the manufacturer he is responsible ments.
Documentation:		
Source (e.g. standard) Category:		
File:		
File:		
Ctatus / Managers Cuba vatars		
Status / Messages Subsystem Status:	green	



Project name: HO400

SF Safety function: D.1 Emergency	Button safety function	n
Identifier of the Safety function:		
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 fund	ction	
PLr (by risk graph):	d	
Severity of injury (S): False	Serious (normally irrev	ersible) injury or death
Frequency / exposure times to hazard (F):	Seldom to less often /	exposure time is short
Possibility of avoiding (P):	Scarcely possible	
Risk graph:	$\bullet S_2 \rightarrow F_1 - F_1$	>- P₂ → d
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: e	PFHD [1/I	n]: 8.9E-8
Status / Messages Safety function		
Status:	green	
Subsystems (1 / 3)		
SB Name: Emergency Button / Conta	actor	
Reference designator:		ntory number:
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revis	sion:
Function:	Input Output	☐ Logic ☑ unknown

Project name: HOACO



Use case:	
Description of the use case:	
Documentation Subsystem	
Documentation:	Pull rope switch device
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:	F - Behaviour of the safety function under fault conditions (see clause [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]: 2.6E-8
Documentation:	
Catagony Cubayatam	
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:	
Source (e.g. standard) Category:	
File:	
MTTFD and Mission time Subsystem	
MTTFD and Mission time Subsystem MTTFD [a]:	100 (High)

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: D.1 Emergency Button safety function

CCF Points:	80 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: i ^a separation in wiring/piping; i ^a detection of short circuits and open circuits in cables by dynamic test; i ^a separate shielding for the signal path of each channel; i ^a sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	- Design / application / experience (5 Points) Components used are well-tried.
	 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 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°C3-1). 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
Documentation:	relevant standards).
Document:	
Status / Managas Subayatam	
Status / Messages Subsystem Status:	green



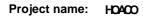


annels / Test channels (1 / 2)		
Name: Channel 1		
 MTTFD [a]: 100		
Blocks (1 / 2)		
BL Name: Emergency Button		
Reference designator:	Inventory number:	
Device details Block		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revision:	
Function:	✓ Input Logic ☐ Output unkno	own
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 416.7 (High)		
Mission time [a]: 20	Shortest mission time [a]: 2	0
Diagnostic coverage Block		
DC [%]: 99 (High)		
Status / Messages Block		
Status:	green	
Elements (1 / 1)		
EL Name: ES-ZP.1		
Reference designator:	Inventory number:	
Device details Element		
Device Manufacturer:	Schneider	
Device Identifier:		

Project name: HO400



	Device group:			
	Part number: XB2BS542C		Revision:	
	Function:		✓ Input ☐ Output	Logic unknown
	Technology:		electronic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time	e Element		
	MTTFD [a]: 416.7 (High)			
	Mission time [a]: 20			
	B10D [cycles]: 100000		nop [cycles/a]	: 2400
	Nop parameter:	Days: 300	Hours: 8	Seconds: 3600
	Documentation:			
	Diagnostic coverage Ele	ment		
	Measure:		Plausibility check, e.g closed mechanicall lii (Input devices) (99 %)	g. use of normally open and n nked contacts
	Documentation:			
	Status / Messages Elem	ent		
	Status:		green	
Bloc	ks (2 / 2)			
BL N	lame: Contactor			
_	eference designator:		Inventory numb	er:
R	~		,	
	evice details Block			
D	evice details Block evice Manufacturer:			





Shortest mission time [a]: 20
en
Inventory number:
SIEMENS
Revision:
☐ Input ☐ Logic ☑ Output ☐ unknow
electronic
-





	MTTFD (a), 4044 4 (High)	ne Element		
	MTTFD [a]: 6944.4 (High)			
	Mission time [a]: 20		F 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	•
	B10D [cycles]: 20000000	.	nop [cycles/a]: 2880	
	Nop parameter:	Days: 300	Hours: 8	Seconds: 300
	Documentation:			
	Diagnostic coverage E	lement_		
	DC [%]: 90 (Medium)			
	Measure:		Cross monitoring of output without detection of short (Output device) (90 %)	
	Documentation:			
	Status / Messages Elei	ment		
	Status:		green	
Naı	els / Test channels (2 / 2) me: Channel 2		g.co.,	
Nai MT			3	
MT Blo	me: Channel 2 TFD [a]: 100		g. co	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2)		Inventory number:	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator:			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block Device Manufacturer:			
MT Blo BL	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block Device Manufacturer: Device Identifier:			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group:	on ✓	Inventory number: Revision:	Logic
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number:	on V I	Inventory number: Revision:	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Function:	on V I	Inventory number: Revision: nput	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Butto Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Function: Technology:	on V I	Inventory number: Revision: nput	





MTTFD and Mission time Block MTTFD [a]: 416.7 (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: ES-ZP.2 Reference designator: Inventory number: Device Manufacturer: Schneider Device Identifier: Device group: Part number: XB2BS542C Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element Documentation:			
Mission time [a]: 20 Diagnostic coverage Block DC [%]: 99 (High) Status / Messages Block Status: green Elements (1 / 1) EL Name: ES-ZP.2 Reference designator: Inventory number: Device Manufacturer: Schneider Device Identifier: Device group: Part number: XB2BS542C Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element	D and Mission time Block		
Diagnostic coverage Block DC [%]: 99 (High) Status / Messages Block Status: green Elements (1 / 1) EL Name: ES-ZP.2 Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device group: Part number: XB2BS542C Revision: Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element) [a]: 416.7 (High)		
DC [%]: 99 (High) Status / Messages Block Status: green Elements (1 / 1) EL Name: ES-ZP.2 Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device group: Part number: XB2BS542C Revision: Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element	n time [a]: 20	Shortest n	mission time [a]: 20
DC [%]: 99 (High) Status / Messages Block Status: green Elements (1 / 1) EL Name: ES-ZP.2 Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device group: Part number: XB2BS542C Revision: Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element	ostic coverage Block		
Elements (1 / 1) EL Name: ES-ZP.2 Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device group: Part number: XB2BS542C Revision: Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element			
Elements (1 / 1) EL Name: ES-ZP.2 Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device group: Part number: XB2BS542C Revision: Function: Input Logic Output unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element	s / Messages Block		
Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device Identifier: Device group: Part number: XB2BS542C Revision: Function: Input Logic unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element	:	green	
Reference designator: Inventory number: Device details Element Device Manufacturer: Schneider Device group: Part number: XB2BS542C Revision: Function: Input Logic unknown Technology: electronic Category: - Use case: Description of the use case: Documentation Element	ents (1 / 1)		
Device details Element Device Manufacturer: Schneider Device Identifier: Device group: Part number: XB2BS542C Revision: Function: ✓ Input			
Device Manufacturer: Device Identifier: Device group: Part number: XB2BS542C Revision: Function: ✓ Input Output unknown Technology: Category: Use case: Description of the use case: Documentation Element	ference designator:	Inventor	ry number:
Device Identifier: Device group: Part number: XB2BS542C Revision: Function: Input Output unknown Technology: Category: Use case: Description of the use case: Documentation Element	evice details Element		
Device group: Part number: XB2BS542C Revision: Function: Input Output unknown Technology: Category: Use case: Description of the use case: Documentation Element	vice Manufacturer:	Schneider	
Part number: XB2BS542C Revision: Function: Input Logic Output unknown Technology: Category: Use case: Description of the use case: Documentation Element	vice Identifier:		
Function: Input Logic Output unknown Technology: Category: Use case: Description of the use case: Documentation Element	vice group:		
Technology: electronic Category: - Use case: Description of the use case: Documentation Element	rt number: XB2BS542C	Revision:	
Category: - Use case: Description of the use case: Documentation Element	nction:		
Use case: Description of the use case: Documentation Element	chnology:	electronic	
Description of the use case: Documentation Element	itegory:	-	
use case: Documentation Element	se case:		
Documentation:	ocumentation Element		
Document:	ocument:		
MTTFD and Mission time Element MTTFD [a]: 416.7 (High)		nt	
Mission time [a]: 20	ssion time [a]: 20		
B10D [cycles]: 100000 nop [cycles/a]: 2400	0D [cycles]: 100000	nop [cyc	cles/a]: 2400
Nop parameter: Days: 300 Hours: 8 Seconds:	pp parameter: Day	vs: 300 Hours	s: 8 Seconds: 360

Project name: HO400



DO	C [%]: 99 (High)	
Me	easure:	Plausibility check, e.g. use of normally open and no closed mechanicall linked contacts (Input devices) (99 %)
Do	ocumentation:	
St	atus / Messages Element	
St	atus:	green
Blocks (2	2 / 2)	
L Nam	e: Contactor	
Refere	ence designator:	Inventory number:
	e details Block	
Device	e Manufacturer:	
Device	e Identifier:	
Device	e group:	
Part n	umber:	Revision:
Functi	on:	☐ Input ☐ Logic ☐ unknown
Techn	ology:	electronic
Catego	ory:	-
Use ca	ase:	
Descri use ca	iption of the use:	
Docui	mentation Block	
Docun	nentation:	
Docun	nent:	
	FD and Mission time Block	
	D [a]: 6944.4 (High)	
Missio	on time [a]: 20	Shortest mission time [a]: 20
Diagn	ostic coverage Block	
DC [%]: 90 (Medium)	
Status	s / Messages Block	
Status		green

Project name: HO400



	Reference designator:		Inventory number	er:
	Device details Element			
	Device Manufacturer:		SIEMENS	
	Device Identifier:			
	Device group:			
	Part number: 3RT60 16-1AB0	2	Revision:	
	Function:		☐ Input ☑ Output	☐ Logic ☐ unknown
	Technology:		electronic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time MTTFD [a]: 6944.4 (High)	Element		
	Mission time [a]: 20			
	B10D [cycles]: 20000000		nop [cycles/a]: 2	28800
	Nop parameter:	Days: 300	Hours: 8	Seconds: 300
	Documentation:			
	Diagnostic coverage Elem DC [%]: 90 (Medium)	nent		
	Measure:			tput signals with dynamic test ort circuits (for multiple I/O)
	Documentation:			
	Status / Messages Eleme	nt		
	Status:		green	
ubsvste	ms (2 / 3)			
	:: Safety PLC G9SP			
	nce designator:		Inventory number:	
	e details Subsystem		inventory number.	
	Manufacturer:	OMRON		

Project name: HOACO



Device Identifier:		
Device group:		
Part number: G9SP-N20S	Revision:	
Function:	☐ Input ☑ Logic ☐ Output ☐ unknown	
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:		
Document:		
Performance Level Subsystem		
PL determination:	Enter PL/PFHD directly (manufacturer ensures compliar requirements of the Category and of the PL)	nce with th
PL: e	Software suitable up to PL: n.a.	
Reached PL: e	PFHD [1/h]: 3.2E-8	
Documentation:		
Mission time [a]: 20	Shortest mission time [a]: 20	
Category Subsystem		
Cat.:	4	
Category requirements:	fulfilled	
Requirements of the Category:	Since the category is given by the manufacturer he is re satisfy the requirements.	sponsible
Documentation:		
Source (e.g. standard) Category:		
File:	∖Å∙Ä∙ÁúNXϵÁа²È«²úÆ∙.pdf	
Status / Messages Subsystem		
Status:	green	
bsystems (3 / 3)		
Name: Converter U1 STO		
Reference designator:	Inventory number:	
Device details Subsystem		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		

Project name: HO400



Part number: R88D-1SN-10H-ECT	Rev	rision:
Function:	☐ Input ☑ Output	Logic unknown
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:		
Document:		
Performance Level Subsystem		
PL determination:		irectly (manufacturer ensures compliance with the category and of the PL)
PL: e	Sof	tware suitable up to PL: n.a.
Reached PL: e	PFI	HD [1/h]: 3.2E-8
Documentation:		
Mission time [a]: 20	Sho	ortest mission time [a]: 20
Category Subsystem		
Cat.:	3	
Category requirements:	fulfilled	
Requirements of the Category:	Since the categor satisfy the require	y is given by the manufacturer he is responsible tements.
Documentation:		
Source (e.g. standard) Category:		
File:	\1SËÅ∙þʹÓÃÊĊ	⁾ ² á.pdf
Status / Messages Subsystem		



Project name: HO400

SF Safety function: D.2 Emergency	Cord safety function	
Identifier of the Safety function:		
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 fund	ction	
PLr (by risk graph):	d	
Severity of injury (S): False	Serious (normally irre	versible) injury or death
Frequency / exposure times to hazard (F):	Seldom to less often /	exposure time is short
Possibility of avoiding (P):	Scarcely possible	
Risk graph:	← S ₂ → − F ₁ −	→ -P ₂ → d
Documentation:		
Document:		
Performance Level Safety function		
Reached PL: d	PFHD [1	h]: 1E-7
Status / Messages Safety function		
Status:	green	
Subsystems (1 / 3)		
SB Name: Emergency Cord / Contact	ctor	
Reference designator:		ntory number:
Device details Subsystem		
Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:	Revi	sion:
Function:	Input Output	☐ Logic ☑ unknown

Project name: HOACO



Use case:	
Description of the use case:	
Documentation Subsystem	
Documentation:	Pull rope switch device
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 [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]: 3.8E-8
Documentation:	
0.4	
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:	
Source (e.g. standard) Category:	
File:	
MTTFD and Mission time Subsystem	
MTTFD and Mission time Subsystem MTTFD [a]:	100 (High)

Project name: HO400



File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

SF Safety function: D.2 Emergency Cord safety function

CCF Points:	80 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example:
	i ^a separation in wiring/piping; i ^a detection of short circuits and open circuits in cables by dynamic
	test; i^a separate shielding for the signal path of each channel; i^a sufficient clearances and creepage distances on printed-circuit boards.
	 Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc.
	 Design / application / experience (5 Points) Components used are well-tried.
	 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 C3-1). 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 shoul 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).
Documentation:	
Document:	
Status / Messages Subsyster	m
Status:	green





fety function: D.2 Emergency Cord	safety function		
hannels / Test channels (1 / 2)			
Name: Channel 1			
MTTFD [a]: 100			
Blocks (1 / 2)			
BL Name: Emergency Cord			
Reference designator:	Inventory	number:	
Device details Block	-		
Device Manufacturer:			
Device Identifier:			
Device group:			
Part number:	Revision:		
Function:	✓ Input Output	Logic unknown	
Technology:	electromechanic		
Category:	-		
Use case:			
Description of the use case:			
Documentation Block			
Documentation:			
Document:			
MTTFD and Mission time Block			
MTTFD [a]: 16666.7 (High)			
Mission time [a]: 20	Shortest r	mission time [a]: 20	
Diagnostic coverage Block			
DC [%]: 99 (High)			
Status / Messages Block			
Status:	green		
Elements (1 / 1)			
EL Name: LaSheng-SW1.1			
Reference designator:	Invento	ry number:	
Device details Element Device Manufacturer:	Schneider		
Device Identifier:	Connect		





	Device group:			
	Part number: XY2CH13290		Revision:	
	Function:		✓ Input Output	Logic unknown
	Technology:		electromechanic	
	Category:		-	
	Use case:			
	Description of the use case:			
	Documentation Element			
	Documentation:			
	Document:			
	MTTFD and Mission time	: Element		
	MTTFD [a]: 16666.7 (High)			
	Mission time [a]: 20			
	B10D [cycles]: 4000000		nop [cycles/a]: 24	400
	Nop parameter:	Days: 300	Hours: 8	Seconds: 3600
	Documentation:			
	Diagnostic coverage Element DC [%]: 99 (High)	ment		
	Measure:		Plausibility check, e.g. u closed mechanicall links (Input devices) (99 %)	use of normally open and no ed contacts
	Documentation:			
	Status / Messages Eleme	ent		
	Status:		green	
Bloc	cks (2 / 2)			
BL N	Name: Contactor			
F	Reference designator:		Inventory number:	
	Device details Block		,	
E				
	Device Manufacturer:			

Project name: HO400



Function:	☐ Input ☑ Output	Logic unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		
Documentation Block		
Documentation:		
Document:		
MTTFD and Mission time Block		
MTTFD [a]: 6944.4 (High)		
Mission time [a]: 20	Shortest mis	ssion time [a]: 20
Status: Elements (1 / 1)	green	
EL Name: KM1		
Reference designator:	Inventory	number:
Device details Element		
Device Manufacturer:	SIEMENS	
Device Identifier:		
Device group:		
	Revision:	
Part number: 3RT60 16-1AB02		
Part number: 3RT60 16-1AB02 Function:	☐ Input ☑ Output	☐ Logic ☐ unknown
Function:	✓ Output	
Function: Technology:	✓ Output electronic	





	MTTFD (a) (044.4 (Uinh)	ne Element		
	MTTFD [a]: 6944.4 (High)			
	Mission time [a]: 20			
	B10D [cycles]: 20000000		nop [cycles/a]: 28	800
	Nop parameter:	Days: 300	Hours: 8	Seconds: 300
	Documentation:			
	Diagnostic coverage El	lement		
	Measure:			out signals with dynamic tes t circuits (for multiple I/O)
	Documentation:			
	Status / Messages Elei	ment		
	Status:			
Naı	els / Test channels (2 / 2) me: Channel 2		green	
Nai MT			green	
MT ⁻	me: Channel 2 TFD [a]: 100		green	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2)		Inventory number:	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord Reference designator:			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Coro Reference designator: Device details Block			
MTT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord Reference designator: Device details Block Device Manufacturer:			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord Reference designator: Device details Block Device Manufacturer: Device Identifier:			
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group:	i I	Inventory number:	Logic
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Coro Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number:	i V	Inventory number: Revision:	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Function:	i V	Inventory number: Revision: Input Output	
MT Blo	me: Channel 2 TFD [a]: 100 cks (1 / 2) Name: Emergency Cord Reference designator: Device details Block Device Manufacturer: Device Identifier: Device group: Part number: Function: Technology:	i V	Inventory number: Revision: Input Output	

Project name: HO400



Document:			
MTTFD and Mission time Blo	ock		
MTTFD [a]: 16666.7 (High)			
Mission time [a]: 20		Shortest missio	n time [a]: 20
Diagnostic coverage Block			
DC [%]: 99 (High)			
Status / Messages Block			
Status:	gı	reen	
Elements (1 / 1)			
EL Name: LaSheng-SW1	.2		
Reference designator:		Inventory nun	nber:
Device details Element			
Device Manufacturer:		Schneider	
Device Identifier:			
Device group:			
Part number: XY2CH13290		Revision:	
Function:		✓ Input Output	Logic unknown
Technology:		electromechanic	
Category:		-	
Use case:			
Description of the use case:			
Documentation Element			
Documentation:			
Document:			
MTTFD and Mission time	e Element		
MTTFD [a]: 16666.7 (High)			
Mission time [a]: 20			
B10D [cycles]: 4000000		nop [cycles/a]]: 2400
Nop parameter:	Days: 300	Hours: 8	Seconds: 360

Project name: HOACO



	DC [%]: 99 (High)	
	Measure:	Plausibility check, e.g. use of normally open and normal closed mechanical linked contacts (Input devices) (99 %)
	Documentation:	
	Status / Messages Element	
	Status:	green
3lock	cs (2 / 2)	
≩L Na	ame: Contactor	
Re	eference designator:	Inventory number:
	evice details Block	
De	evice Manufacturer:	
De	evice Identifier:	
De	evice group:	
Pa	art number:	Revision:
Fu	unction:	☐ Input ☐ Logic ☐ unknown
Te	chnology:	electronic
Ca	ategory:	-
Us	se case:	
	escription of the se case:	
Do	ocumentation Block	
Do	ocumentation:	
Do	ocument:	
	TTFD and Mission time Block	
M	TTFD [a]: 6944.4 (High)	
Mi	ssion time [a]: 20	Shortest mission time [a]: 20
Di	agnostic coverage Block	
DC	C [%]: 90 (Medium)	
St	atus / Messages Block	
	atus:	green

Project name: HOACO



	Reference designator:		Inventory number:		
	Device details Element				
	Device Manufacturer:		SIEMENS		
	Device Identifier:				
	Device group:				
	Part number: 3RT60 16-1AB0)2	Revision:		
	Function:		☐ Input ☑ Output	Logic unknown	
	Technology:		electronic		
	Category:		-		
	Use case:				
	Description of the use case:				
	Documentation Element Documentation:				
	Document:				
	Mission time [a]: 20 B10D [cycles]: 20000000		nop [cycles/a]: 28800		
	Nop parameter:	Days: 300	Hours: 8	Seconds: 300	
	Documentation:	<u> </u>			
	Diagnostic coverage Element DC [%]: 90 (Medium)				
	Measure:			tput signals with dynamic test ort circuits (for multiple I/O)	
	Documentation:				
	Status / Messages Eleme	ent			
	Status:		green		
Subsvs	tems (2 / 3)				
	ne: Safety PLC G9SP				
	rence designator:		Inventory number:		
	ce details Subsystem		sales y manibori		
	of adiano casoyotom				

Project name: HOACO



Device Identifier:		
Device group:		
Part number: G9SP-N20S	Revis	sion:
Function:	☐ Input ☐ Output	✓ Logic □ unknown
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:		
Document:		
Performance Level Subsystem		
PL determination:		rectly (manufacturer ensures compliance with the Category and of the PL)
PL: e	Software suitable up to PL: n.a.	
Reached PL: e	PFHD	D [1/h]: 3.2E-8
Documentation:		
Mission time [a]: 20	Short	test mission time [a]: 20
Category Subsystem		
Cat.:	4	
Category requirements:	fulfilled	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible satisfy the requirements.	
Documentation:		
Source (e.g. standard) Category:		
File:	\Å·Ä·ÁúNXϵÁа²	ÈײúÆ∙.pdf
Status / Messages Subsystem		
Status:	green	
ıbsystems (3 / 3)		
Name: Converter U1 STO		
Reference designator:	Inver	ntory number:
Device details Subsystem		
Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		





Part number: R88D-1SN-10H-ECT	Re	vision:
Function:	☐ Input ☑ Output	Logic unknown
Use case:		
Description of the use case:		
Documentation Subsystem		
Documentation:		
Document:		
Performance Level Subsystem		
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]: 3.2E-8	
Documentation:		
Mission time [a]: 20	Sh	ortest 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:	\1SËÅ∙þʹÓÃÊ¢	Ö²á.pdf
Ctatus / Managers Culturaters		
Status / Messages Subsystem Status:	green	
	J	



Project name: HOACO

File date: 22/05/2020 17:30:32 Report date: 2020/5/22 Checksum: 5552651956d437729d6f50f3827e5c89

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 gem?? dem Stand von Wissenschaft und Technik sorgf?ltig erstellt. Sie wird dem Nutzer unentgeltlich zur Verf "1gung gestellt.

Die Haftung des IFAs/ DGUV ist damit auf Vorsatz und grobe Fahrl?ssigkeit (¡ì 521 BGB) bzw. bei Sach- und Rechtsm?ngel auf arglistig verschwiegene Fehler beschr?nkt (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:	Date, signature:	
Authors	Authors	
Inspectors	Inspectors	