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

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

Required: PLr d | Reached: PL e | PFHD [1/h]: 5.6E-8 | Status: green

SF Name: A.2 Safety Light Curtain safety function

Required: PLr d | Reached: PL d | PFHD [1/h]: 1.2E-7 | Status: green

SF Name: A.3 Safety Encoder safety function

Required: PLr d | Reached: PL d | PFHD [1/h]: 1.3E-7 | Status: green

SF Name: A.4 Jog Grip Switch safety function

Required: PLr d | Reached: PL e | PFHD [1/h]: 8.9E-8 | Status: green

SF Name: A.5 LOCK Button safety function

Required: PLr d | Reached: PL e | PFHD [1/h]: 9E-8 | Status: green

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

Required: PLr d | Reached: PL d | PFHD [1/h]: 1.3E-7 | Status: green

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

PR Project name: HOACO

Required: PLr d	Reached: PL e	PFHD [1/h]: 9.5E-8	Status: green

SF Name: D.1 Emergency Button safety function

Required: PLr d	Reached: PL e	PFHD [1/h]: 8.9E-8	Status: green

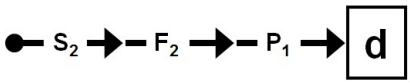
SF Name: D.2 Emergency Cord safety function

Required: PLr d	Reached: PL d	PFHD [1/h]: 1E-7	Status: green

SF Safety function: A.1 MODE-Select 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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: e	PFHD [1/h]: 5.6E-8

Status / Messages Safety function

Status:	green

Subsystems (1 / 2)

SB Name: Key Switch

Reference designator:	Inventory number:

Device details Subsystem

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

Function:	☐ Input	☐ Logic
	☐ Output	☑ unknown

SF Safety function: A.1 MODE-Select Key Switch 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 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]

Reached PL: e	PFHD [1/h]: 2.5E-8
Documentation:	

Category Subsystem

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

MTTFD and Mission time Subsystem

MTTFD [a]:	100 (High)

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

Diagnostic coverage Subsystem

DCavg [%]:	99 (High)

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

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. - 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 / Messages Subsystem

Status:	green

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

Channels / Test channels (1 / 2)

CH 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 ☐ Output	☐ Logic ☐ 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.1

Reference designator:		Inventory number:	

Device details Element

Device Manufacturer:	OMRON		
Device Identifier:			

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

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]: 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 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

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Key Switch

Reference designator:	Inventory number:

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 ☐ Output	☐ Logic ☐ 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 ☐ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		

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

Description of the use case:	

Documentation Element

Documentation:	
Document:	

MTTFD and Mission time 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 Element

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

Status / Messages Element

Status:	green

Subsystems (2 / 2)

SB Name: Safety PLC G9SP

Reference designator:		Inventory number:	

Device details Subsystem

Device Manufacturer:	OMRON		
Device Identifier:			
Device group:			
Part number: G9SP-N20S		Revision:	
Function:	☐ Input ☐ Output	☑ Logic ☐ unknown	
Use case:			
Description of the use case:			

SF 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:	

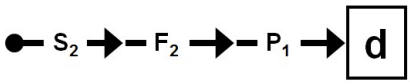
Status / Messages Subsystem

Status:	green

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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: 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 ☐ Output ☐ Logic ☐ unknown

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

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

Diagnostic coverage Subsystem

DCavg [%]:	99 (High)

Common cause failure Subsystem

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: ¡ª first channel electronic or programmable electronic and second channel electromechanical hardwired, ¡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 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.

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

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 Curtain

Reference designator:		Inventory 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:			

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)

SF 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:	☑ 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]: 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

SF 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 ☐ Output	☐ Logic ☐ 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:	
Function:	☑ Input ☐ Output	☐ Logic ☐ unknown	

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

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

Subsystems (2 / 4)

SB Name: Safety PLC G9SP

Reference designator:	Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: G9SP-N20S	Revision:	
Function:	☐ Input ☐ Output	☑ Logic ☐ unknown
Use case:		
Description of the use case:		

Documentation Subsystem

Documentation:	
Document:	

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

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 ☑ Output	☐ Logic ☐ 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

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 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: ¡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.

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

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)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Contactor

Reference designator: Inventory number:

Device details Block

Device Manufacturer:

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

Device Identifier:		
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

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 ☑ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

SF 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	
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
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 ☑ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

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

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: 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

Documentation:

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

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

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

Subsystems (4 / 4)

SB Name: Converter U1 STO

Reference designator: Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON
Device Identifier:	
Device group:	
Part number: R88D-1SN-10H-ECT	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

Cat.:	3
Category requirements:	fulfilled

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

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:	

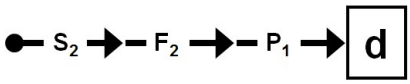
Status / Messages Subsystem

Status:	green

SF Safety function: A.3 Safety Encoder 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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: d	PFHD [1/h]: 1.3E-7

Status / Messages Safety function

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

SF Safety function: A.3 Safety Encoder safety function

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]: 1.7E-8
Documentation:		
Mission time [a]: 20		Shortest mission time [a]: 20

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.
Documentation:	
Source (e.g. standard) Category:	
File:	

Status / Messages Subsystem

Status:	green

Subsystems (2 / 5)

SB Name: Safety Relay S30-1

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	PILZ	
Device Identifier:		
Device group:		
Part number: S30		Revision:
Function:	☐ Input ☐ Output	☑ Logic ☐ unknown
Use case:		
Description of the use case:		

SF Safety function: A.3 Safety Encoder 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]: 3.1E-9
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 / 5)

SB Name: 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:	

SF Safety function: A.3 Safety Encoder 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

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 (4 / 5)

SB Name: Contactor

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:		
Device Identifier:		
Device group:		
Part number:		Revision:
Function:	☐ Input ☐ Output	☐ Logic ☑ unknown
Use case:		
Description of the use case:		

Documentation Subsystem

Documentation:	Pull rope switch device
Document:	

SF Safety function: A.3 Safety Encoder safety function

Performance Level Subsystem

PL determination:	Determine PL/PFHD from Category, MTTFD and DCavg
Software suitable up to PL:	n.a.
PL requirements:	fulfilled
The PL shall be determined by the estimation of the following aspects:	- Behaviour of the safety function under fault conditions (see clause 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]
Reached PL: e	PFHD [1/h]: 4.3E-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;

SF Safety function: A.3 Safety Encoder safety function

CCF Measures:

¡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 / Messages Subsystem

Status: green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Contactor

Reference designator: Inventory number:

SF Safety function: A.3 Safety Encoder safety function

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:		

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 ☑ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		

SF Safety function: A.3 Safety Encoder safety function

Description of the use case:

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

Nop parameter: Days: 300 Hours: 8 Seconds: 300

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: -

SF Safety function: A.3 Safety Encoder safety function

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: 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

Documentation:

Document:

MTTFD and Mission time Element

MTTFD [a]: 6944.4 (High)

Mission time [a]: 20

SF Safety function: A.3 Safety Encoder safety function

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 test without detection of short circuits (for multiple I/O) (Output device) (90 %)
Documentation:	

Status / Messages Element

Status:	green

Subsystems (5 / 5)

SB Name: Converter U1 STO

Reference designator:		Inventory number:	

Device details Subsystem

Device Manufacturer:	OMRON		
Device Identifier:			
Device group:			
Part number: R88D-1SN-10H-ECT		Revision:	
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		Shortest mission time [a]: 20	

SF 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:	

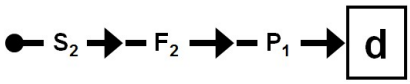
Status / Messages Subsystem

Status:	green

SF Safety function: A.4 Jog Grip 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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: e	PFHD [1/h]: 8.9E-8

Status / Messages Safety function

Status:	green

Subsystems (1 / 3)

SB Name: Jog Grip Switch / Contactor

Reference designator:	Inventory number:

Device details Subsystem

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

Function:	☐ Input	☐ Logic
	☐ Output	☑ unknown

SF Safety function: A.4 Jog Grip Switch 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 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]

Reached PL: e	PFHD [1/h]: 2.6E-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 [%]:	98.4 (Medium)

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

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. - 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 / Messages Subsystem

Status:	green

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

Channels / Test channels (1 / 2)

CH Name: Channel 1

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 ☐ Output	☐ Logic ☐ unknown	
Technology:	electronic		
Category:	-		
Use case:			
Description of the use case:			

Documentation Block

Documentation:	
Document:	

MTTFD and Mission time Block

MTTFD [a]: 520.8 (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: Handle.1

Reference designator:		Inventory number:	

Device details Element

Device Manufacturer:	OMRON		
Device Identifier:			

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

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 [%]: 20	
B10D [cycles]: 500000		nop [cycles/a]: 9600	
Nop parameter:	Days: 300	Hours: 8	Seconds: 900
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:

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

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

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 ☑ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

SF 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	
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
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 ☐ Output	☐ Logic ☐ unknown	
Technology:	electronic		
Category:	-		
Use case:			
Description of the use case:			

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

Documentation Block

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 520.8 (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: Handle.2

Reference designator: Inventory 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 [%]: 20

B10D [cycles]: 500000 nop [cycles/a]: 9600

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

Nop parameter:	Days: 300	Hours: 8	Seconds: 900
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:			
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

Diagnostic coverage Block

DC [%]: 90 (Medium)

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

Status / Messages Block

Status:	green

Elements (1 / 1)

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 ☑ Output	☐ Logic ☐ unknown	
Technology:	electronic		
Category:	-		
Use case:			
Description of the use case:			

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	
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
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

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

Subsystems (2 / 3)

SB Name: Safety PLC G9SP

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: G9SP-N20S		Revision:
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		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 / 3)

SB Name: Converter U1 STO

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

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: R88D-1SN-10H-ECT		Revision:
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		Shortest mission time [a]: 20

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.
Documentation:	
Source (e.g. standard) Category:	
File:	

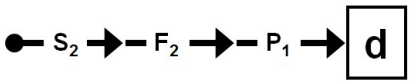
Status / Messages Subsystem

Status:	green

SF Safety function: A.5 LOCK Button 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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: e	PFHD [1/h]: 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

SF Safety function: A.5 LOCK Button 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 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]

Reached PL: e	PFHD [1/h]: 2.7E-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 [%]:	97.8 (Medium)

SF Safety function: A.5 LOCK Button safety function

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. - 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 / Messages Subsystem

Status:	green

SF Safety function: A.5 LOCK Button safety function

Channels / Test channels (1 / 2)

CH 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 ☐ Output	☐ Logic ☐ 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 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:			

SF Safety function: A.5 LOCK Button safety function

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]: 9600	
Nop parameter:	Days: 300	Hours: 8	Seconds: 900
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:	

SF Safety function: A.5 LOCK Button safety function

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

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 ☑ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

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	
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
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 ☐ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

SF Safety function: A.5 LOCK Button safety function

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.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]: 9600

SF Safety function: A.5 LOCK Button safety function

Nop parameter:	Days: 300	Hours: 8	Seconds: 900
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:			
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

Diagnostic coverage Block

DC [%]: 90 (Medium)

SF Safety function: A.5 LOCK Button safety function

Status / Messages Block

Status:	green

Elements (1 / 1)

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 ☑ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

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	
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
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

SF Safety function: A.5 LOCK Button safety function

Subsystems (2 / 3)

SB Name: Safety PLC G9SP

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: G9SP-N20S		Revision:
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		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 / 3)

SB Name: Converter U1 STO

SF Safety function: A.5 LOCK Button safety function

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: R88D-1SN-10H-ECT		Revision:
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		Shortest mission time [a]: 20

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.
Documentation:	
Source (e.g. standard) Category:	
File:	

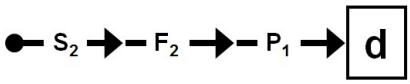
Status / Messages Subsystem

Status:	green

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

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: d	PFHD [1/h]: 1.3E-7

Status / Messages Safety function

Status:	green

Subsystems (1 / 2)

SB Name: Safety Contact Sensor

Reference designator:	Inventory number:

Device details Subsystem

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

Function:	☑ Input	☐ Logic
	☐ Output	☐ unknown

SF Safety function: B.1 Safety Contact Sensor 1 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 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: d	PFHD [1/h]: 1E-7
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 [%]:	60 (Low)

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

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. - 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 / Messages Subsystem

Status:	green

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

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 1)

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 [%]: 60 (Low)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: Guard-lock switch1.1

Reference designator:	Inventory number:

Device details Element

Device Manufacturer:	OMRON
Device Identifier:	

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

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 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 Element

DC [%]: 60 (Low)	
Measure:	Cross monitoring of inputs without dynamic test (Input devices) (0 % - 99 % depending on how often a signal change is done by the application)
Documentation:	

Status / Messages Element

Status:	green

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Safety Contact Sensor

Reference designator:	Inventory number:

Device details Block

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

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]: 4166.7 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20

Diagnostic coverage Block

DC [%]: 60 (Low)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: Guard-lock switch1.2

Reference designator:	Inventory number:	

Device details Element

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: D4NS-4CF	Revision:	
Function:	☑ Input ☐ Output	☐ Logic ☐ unknown
Technology:	electromechanic	
Category:	-	
Use case:		

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

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

Nop parameter: Days: 300 Hours: 8 Seconds: 3600

Documentation:

Diagnostic coverage Element

DC [%]: 60 (Low)

Measure: Cross monitoring of inputs without dynamic test (Input devices)
(0 % - 99 % depending on how often a signal change is done by the application)

Documentation:

Status / Messages Element

Status: green

Subsystems (2 / 2)

SB Name: Converter U1 STO

Reference designator: Inventory number:

Device details Subsystem

Device Manufacturer: OMRON

Device Identifier:

Device group:

Part number: R88D-1SN-10H-ECT Revision:

Function: ☐ Input ☐ Logic ☑ Output ☐ unknown

Use case:

Description of the use case:

Documentation Subsystem

Documentation:

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

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:	

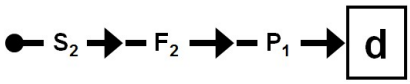
Status / Messages Subsystem

Status:	green

SF Safety function: C.1 Safety Contact 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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Frequent to continuous / exposure time is long
Possibility of avoiding (P):	Possible under specific conditions
Risk graph:	
Documentation:	
Document:	

Performance Level Safety function

Reached PL: e	PFHD [1/h]: 9.5E-8

Status / Messages Safety function

Status:	green

Subsystems (1 / 3)

SB Name: Safety Contact Sensor

Reference designator:	Inventory number:

Device details Subsystem

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

Function:	☑ Input	☐ Logic
	☐ Output	☐ unknown

SF Safety function: C.1 Safety Contact Sensor 2/3 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 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]: 3.2E-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 [%]:	95.6 (Medium)

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

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. - 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 / Messages Subsystem

Status:	green

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 ☐ Output	☐ Logic ☐ 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:	

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

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 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 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:	

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

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

Diagnostic coverage Block

DC [%]: 90 (Medium)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: KM1

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:		

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	
Nop parameter:	Days: 300	Hours: 8	Seconds: 300
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 ☐ Output	☐ Logic ☐ unknown	
Technology:	electromechanic		
Category:	-		
Use case:			
Description of the use case:			

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

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 ☐ Logic ☐ Output ☐ unknown
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

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

Nop parameter:	Days: 300	Hours: 8	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:			
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

Diagnostic coverage Block

DC [%]: 90 (Medium)

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

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: KM2

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:	

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 test without detection of short circuits (for multiple I/O) (Output device) (90 %)
Documentation:	

Status / Messages Element

Status:	green

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

Subsystems (2 / 3)

SB Name: Safety PLC G9SP

Reference designator:		Inventory number:	

Device details Subsystem

Device Manufacturer:	OMRON		
Device Identifier:			
Device group:			
Part number: G9SP-N20S		Revision:	
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		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 / 3)

SB Name: Converter G1 STO

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

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON	
Device Identifier:		
Device group:		
Part number: R88D-1SN-10H-ECT		Revision:
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		Shortest mission time [a]: 20

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.
Documentation:	
Source (e.g. standard) Category:	
File:	

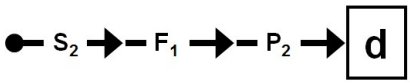
Status / Messages Subsystem

Status:	green

SF Safety function: D.1 Emergency Button 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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Seldom to less often / exposure time is short
Possibility of avoiding (P):	Scarcely possible
Risk graph:	
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: Emergency Button / Contactor

Reference designator:	Inventory number:

Device details Subsystem

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

Function:	☐ Input	☐ Logic
	☐ Output	☑ unknown

SF Safety function: D.1 Emergency Button safety function

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 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]

Reached PL: e	PFHD [1/h]: 2.6E-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 [%]:	98.5 (Medium)

SF Safety function: D.1 Emergency Button safety function

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. - 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 / Messages Subsystem

Status:	green

SF Safety function: D.1 Emergency Button safety function

Channels / Test channels (1 / 2)

CH 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 ☐ Output	☐ Logic ☐ 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: ES-ZP.1

Reference designator:		Inventory number:	

Device details Element

Device Manufacturer:	Schneider		
Device Identifier:			

SF Safety function: D.1 Emergency Button safety function

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 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 Element

DC [%]: 99 (High)	
Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (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:	
Device group:	
Part number:	Revision:

SF Safety function: D.1 Emergency Button safety function

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

Diagnostic coverage Block

DC [%]: 90 (Medium)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: KM1

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:

SF Safety function: D.1 Emergency Button safety function

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 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: Emergency Button

Reference designator:		Inventory 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:			

Documentation Block

Documentation:	

SF Safety function: D.1 Emergency Button safety function

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: ES-ZP.2

Reference designator: Inventory number:

Device details Element

Device Manufacturer:	Schneider	
Device Identifier:		
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 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 Element

SF Safety function: D.1 Emergency Button safety function

DC [%]: 99 (High)

Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (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:			
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

Diagnostic coverage Block

DC [%]: 90 (Medium)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: KM2

SF Safety function: D.1 Emergency Button safety function

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:	

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 test without detection of short circuits (for multiple I/O) (Output device) (90 %)
Documentation:	

Status / Messages Element

Status:	green

Subsystems (2 / 3)

SB Name: Safety PLC G9SP

Reference designator:		Inventory number:	

Device details Subsystem

Device Manufacturer:	OMRON

SF Safety function: D.1 Emergency Button safety function

Device Identifier:		
Device group:		
Part number: G9SP-N20S	Revision:	
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	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:	..\Å·Ä·ÁúNXÏµÁÐ°²È«²úÆ·.pdf

Status / Messages Subsystem

Status:	green

Subsystems (3 / 3)

SB Name: Converter U1 STO

Reference designator:	Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON
Device Identifier:	
Device group:	

SF Safety function: D.1 Emergency Button safety function

Part number: R88D-1SN-10H-ECT		Revision:
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	Shortest mission time [a]: 20

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.
Documentation:	
Source (e.g. standard) Category:	
File:	..\1SËÅ·þÊ¹ÓÃÊÖ²á.pdf

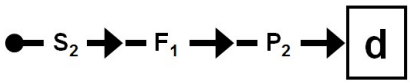
Status / Messages Subsystem

Status:	green

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 function

PLr (by risk graph):	d
Severity of injury (S): False	Serious (normally irreversible) injury or death
Frequency / exposure times to hazard (F):	Seldom to less often / exposure time is short
Possibility of avoiding (P):	Scarcely possible
Risk graph:	
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 / Contactor

Reference designator:	Inventory number:

Device details Subsystem

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

Function:

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

SF Safety function: D.2 Emergency Cord safety function

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 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]: 3.8E-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 [%]:	92.6 (Medium)

SF Safety function: D.2 Emergency Cord safety function

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. - 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 / Messages Subsystem

Status:	green

SF Safety function: D.2 Emergency Cord safety function

Channels / Test channels (1 / 2)

CH 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 ☐ Logic ☐ Output ☐ 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 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:	Inventory number:

Device details Element

Device Manufacturer:	Schneider
Device Identifier:	

SF Safety function: D.2 Emergency Cord safety function

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]: 2400	
Nop parameter:	Days: 300	Hours: 8	Seconds: 3600
Documentation:			

Diagnostic coverage Element

DC [%]: 99 (High)	
Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (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:	
Device group:	
Part number:	Revision:

SF Safety function: D.2 Emergency Cord safety function

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

Diagnostic coverage Block

DC [%]: 90 (Medium)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: KM1

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:	

SF Safety function: D.2 Emergency Cord safety function

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 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: 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:	

SF Safety function: D.2 Emergency Cord safety function

Document:

MTTFD and Mission time Block

MTTFD [a]: 16666.7 (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: LaSheng-SW1.2

Reference designator: Inventory number:

Device details Element

Device Manufacturer: Schneider

Device Identifier:

Device group:

Part number: XY2CH13290 Revision:

Function: ☑ Input ☐ Logic ☐ Output ☐ 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]: 2400

Nop parameter: Days: 300 Hours: 8 Seconds: 3600

Documentation:

Diagnostic coverage Element

SF Safety function: D.2 Emergency Cord safety function

DC [%]: 99 (High)

Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (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:		
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

Diagnostic coverage Block

DC [%]: 90 (Medium)

Status / Messages Block

Status:	green

Elements (1 / 1)

EL Name: KM2

SF Safety function: D.2 Emergency Cord safety function

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:	

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 test without detection of short circuits (for multiple I/O) (Output device) (90 %)
Documentation:	

Status / Messages Element

Status:	green

Subsystems (2 / 3)

SB Name: Safety PLC G9SP

Reference designator:		Inventory number:	

Device details Subsystem

Device Manufacturer:	OMRON

SF Safety function: D.2 Emergency Cord safety function

Device Identifier:		
Device group:		
Part number: G9SP-N20S	Revision:	
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	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:	..\Å·Ä·ÁúNXÏµÁÐ°²È«²úÆ·.pdf

Status / Messages Subsystem

Status:	green

Subsystems (3 / 3)

SB Name: Converter U1 STO

Reference designator:		Inventory number:

Device details Subsystem

Device Manufacturer:	OMRON
Device Identifier:	
Device group:	

SF Safety function: D.2 Emergency Cord safety function

Part number: R88D-1SN-10H-ECT		Revision:
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	Shortest mission time [a]: 20

Category Subsystem

Cat.:	3
Category requirements:	fulfilled
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.
Documentation:	
Source (e.g. standard) Category:	
File:	..\1SËÅ·þÊ¹ÓÃÊÖ²á.pdf

Status / Messages Subsystem

Status:	green

EXCLUSION OF LIABILITY

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

Die Software wurde 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