File date: 24/05/2022 15:54:22 Report date: 10/06/2022 Checksum: 79e38934af00311620274f06c385e779

PR Project name: Automatic mounting machine

Project file name:	C:\Users\XF45871\OneDrive - INAIL\Documenti\ISSA\Control devices\toronto detroit may 2022\Presentazione\Example Validation ISSA FP.ssm
Creation date:	03/03/2022 14:24:23
Project status:	Completed
Project number:	1
Project version:	1.1
Authors:	FP
Project managers:	KB
Inspectors:	NA
Dangerous point/machine:	Movement of electrical driven parts inside a guarded space
Documentation:	- Instruction Handbook - Electrical diagramm - Logic block diagramm
Document:	..\automatic mounting machine.pdf
Version of software:	2.0.8 build 4
Version of standard:	ISO 13849-1:2015, ISO 13849-2:2012
Checksum:	79e38934af00311620274f06c385e779
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

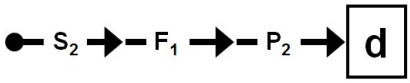
SF Name: Stop function [SF1]

Required: PLr d	Reached: PL d	PFHD [1/h]: 1,3E-7	Status: green

SF Safety function: Stop function

Identifier of the Safety function:	SF1
Safety function type:	Safety-related stop function initiated by safeguard
Triggering event:	Opening of the interlocked guard door
Reaction and Behaviour on power failure:	The dangerous movement will be stopped and unexpected start-up is prevented as long as the guard door is opened.
Safe state:	The dangerous movement is stopped (by de-energizing the power of the electrical motor).
Operation mode:	Automatic
Demand rate:	High (once an hour)
Running-on time:	less than 0,25 s
Priority:	High
Documentation:	ISO 13849-2
Document:	D:\Documents\ISO 13849-2.pdf

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:	ISO 13849-1
Document:	..\ISO 13849-1.pdf

Performance Level Safety function

Reached PL: d PFHD [1/h]: 1,3E-7

Status / Messages Safety function

Status:	green

Subsystems (1 / 1)

SB Name: complete control System

Reference designator: FP Inventory number: -

Device details Subsystem

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

SF Safety function: Stop function

Function:	☑ Input ☑ Logic ☑ Output ☐ unknown
Use case:	Complete category 3 subsystem
Description of the use case:	Diverse redundant and monitored structure for safety stop of electrical moved parts

Documentation Subsystem

Documentation:	Electrical diagram
Document:	..\electrical diagram.pdf

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]: 1,3E-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:	Block diagramm
Source (e.g. standard) Category:	ISO 13849-2
File:	D:\Documents\block diagram.pdf

MTTFD and Mission time Subsystem

MTTFD [a]:	42,3 (High)
Mission time [a]: 20	Shortest mission time [a]: 20

SF Safety function: Stop function

Diagnostic coverage Subsystem

DCavg [%]:	92,8 (Medium)

Common cause failure Subsystem

CCF Points:	85 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards. - Diversity (20 Points) Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electromechanical hardwired, — different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures. - Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc. - Environmental (25 Points) For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered. - Environmental (10 Points) Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).
Documentation:	
Document:	

SF Safety function: Stop function

Status / Messages Subsystem

Status:	green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 24,9

Blocks (1 / 3)

BL Name: Position switch B1

Reference designator: FP Inventory number: -

Device details Block

Device Manufacturer:	IX
Device Identifier:	B1
Device group:	Position switch (NC) with direct opening action
Part number: -	Revision: -
Function:	☑ Input ☐ Logic ☐ Output ☐ unknown
Technology:	electromechanic
Category:	-
Use case:	Input sensor subject to wear
Description of the use case:	The position switch in open state (guard open) causes the safe stop of the motor via PLC A that send a stop signal to T1 FC. This position switch has a direct opening action (NC) and is certified as manufactured in conformity with IEC 60947-5-1, Annex K.

Documentation Block

Documentation:	ISO 138491
Document:	..\ISO 13849-1.pdf

MTTFD and Mission time Block

MTTFD [a]: 34722,2 (High)			
Mission time [a]: 20		Shortest mission time [a]: 20	
B10D [cycles]: 20000000		nop [cycles/a]: 5760	
Nop parameter:	Days: 240	Hours: 24	Seconds: 3600
Documentation:	Data from table C.1 (Manufactured according basic and well tried principle, application and operating conditions specified by manufacturer, the designer of the SRP/CS fulfils the basic and well-tried safety principles) B10D =20.000.000 dop= 240 g/a; hop=24 h; tcycle=3600 s		

SF Safety function: Stop function

Diagnostic coverage Block

DC [%]: 99 (High)	
Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (Input devices) (99 %)
Documentation:	Electrical diagramm Plausibility check is realized in both computer systems

Status / Messages Block

Status:	green

Blocks (2 / 3)

BL Name: PLCA

Reference designator: FP	Inventory number: -

Device details Block

Device Manufacturer:	LX
Device Identifier:	-
Device group:	-
Part number: -	Revision: -
Function:	☐ Input ☑ Logic ☐ Output ☐ unknown
Technology:	electronic
Category:	-
Use case:	Logic component (different technology from PLC B)
Description of the use case:	PLC A, when the guard door is open, provides a stop signal to T1 FC.

Documentation Block

Documentation:	Manufacturer data sheet
Document:	..\PLC A datasheet.pdf

MTTFD and Mission time Block

MTTFD [a]: 45 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Rate of dangerous failure [FIT]: 2536,8	
Documentation:	Data from the manufacturer of the PLC

Diagnostic coverage Block

DC [%]: 90 (Medium)	
Documentation:	- indirect monitoring by PLC B through G2 (pulse sensor)

SF Safety function: Stop function

Documentation:	- watcthdog monitoring (programm sequence) - cross monitoring with PLC B They result in a medium value of 90 %

Status / Messages Block

Status:	green

Blocks (3 / 3)

BL Name: T1FC

Reference designator: FP		Inventory number: -	

Device details Block

Device Manufacturer:	OX		
Device Identifier:	-		
Device group:	-		
Part number: -		Revision: -	
Function:	☐ Input ☑ Output	☐ Logic ☐ unknown	
Technology:	electronic		
Category:	-		
Use case:	Output component		
Description of the use case:	T1 FC brings the motor M to a safe stop when the guard is opened because it receives the stop signal from PLC A.		

Documentation Block

Documentation:	T1 datasheet
Document:	..\electrical diagram.pdf

MTTFD and Mission time Block

MTTFD [a]: 56 (High)		
Mission time [a]: 20	Shortest mission time [a]: 20	
Rate of dangerous failure [FIT]: 2038,5		
Documentation:	Data from the manufacturer of the T1 inverter	

Diagnostic coverage Block

DC [%]: 99 (High)	
Documentation:	- Plausibility check between theoretical braking ramp and signal from G2 (pulse sensor)

Status / Messages Block

SF Safety function: Stop function

Status:	green

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 55,7

Blocks (1 / 4)

BL Name: B2 position switch

Reference designator: FP Inventory number: -

Device details Block

Device Manufacturer:	IX
Device Identifier:	B2
Device group:	Position switch (NO)
Part number: -	Revision: 1.0)
Function:	☑ Input ☐ Logic ☐ Output ☐ unknown
Technology:	electromechanic
Category:	-
Use case:	Input sensor subject to wear
Description of the use case:	The position switch in open state (guard open) enables pulse blocking in T1 imp, de-energizing K1 (STO). This position switch has normally open contact (NO).

Documentation Block

Documentation:	ISO 138491
Document:	..\ISO 13849-1.pdf

MTTFD and Mission time Block

MTTFD [a]: 34722,2 (High)

Mission time [a]: 20		Shortest mission time [a]: 20	
B10D [cycles]: 20000000		nop [cycles/a]: 5760	
Nop parameter:	Days: 240	Hours: 24	Seconds: 3600
Documentation:		Data from table C.1 (Manufactured according basic and well tried principle, application and operating conditions specified by manufacturer, the designer of the SRP/CS fulfils the basic and well-tried safety principles) B10D =20.000.000 dop= 240 g/a; hop=24 h; tcycle=3600 s	

Diagnostic coverage Block

DC [%]: 99 (High)

Measure:	Plausibility check, e.g. use of normally open and normally

SF Safety function: Stop function

Measure:	closed mechanicall linked contacts (Input devices) (99 %)
Documentation:	Electrical diagramm Plausibility check is realized in both computer systems

Status / Messages Block

Status:	green

Blocks (2 / 4)

BL Name: PLCB

Reference designator: FP	Inventory number: -

Device details Block

Device Manufacturer:	LY
Device Identifier:	-
Device group:	-
Part number: -	Revision: -
Function:	☐ Input ☑ Logic ☐ Output ☐ unknown
Technology:	unknown
Category:	-
Use case:	PLC B (different technology respect to PLC A)
Description of the use case:	PLC B, when the guard door is open, enables pulse blocking in T1 imp providing, de-energizing K1, the safe uncontrolled stop (STO) of the motor

Documentation Block

Documentation:	Manufacturer data sheet
Document:	..\PLC B datasheet.pdf

MTTFD and Mission time Block

MTTFD [a]: 56 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Rate of dangerous failure [FIT]: 2038,5	
Documentation:	Data from the manufacturer of the PLC

Diagnostic coverage Block

DC [%]: 90 (Medium)	
Documentation:	- indirect monitoring by PLC A by reading K1 - watcthdog monitoring (programm sequence) - cross monitoring with PLC B

SF Safety function: Stop function

Documentation:	They result in a medium value of 90 %

Status / Messages Block

Status:	green

Blocks (3 / 4)

BL Name: K1 relais

Reference designator: FP		Inventory number: -	

Device details Block

Device Manufacturer:	IY		
Device Identifier:	Relais		
Device group:			
Part number:		Revision:	
Function:	☐ Input ☐ Output	☑ Logic ☐ unknown	
Technology:	electromechanic		
Category:	-		
Use case:	component with a logic function subject to wear		
Description of the use case:	K1, when the guard is open, is deenergized by PLC B enabling impuls block in T1 imp that causes the safe uncontrolled stop (STO) of the motor		

Documentation Block

Documentation:	ISO 138491
Document:	..\ISO 13849-1.pdf

MTTFD and Mission time Block

MTTFD [a]: 34722,2 (High)			
Mission time [a]: 20		Shortest mission time [a]: 20	
B10D [cycles]: 20000000		nop [cycles/a]: 5760	
Nop parameter:	Days: 240	Hours: 24	Seconds: 3600
Documentation:	Data from table C.1 (Manufactured according basic and well tried principle, application and operating conditions specified by manufacturer, the designer of the SRP/CS fulfils the basic and well-tried safety principles) Relais with small load (overdimensioned for the current) B10D =20.000.000 dop= 240 g/a; hop=24 h; tcycle=3600 s		

Diagnostic coverage Block

DC [%]: 99 (High)

SF Safety function: Stop function

Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (Input devices) (99 %)
Documentation:	PLC A read K1 and makes a plausibility check with B1

Status / Messages Block

Status:	green

Blocks (4 / 4)

BL Name: T1imp

Reference designator: FP Inventory number: -

Device details Block

Device Manufacturer:	OX
Device Identifier:	-
Device group:	-
Part number: -	Revision: -
Function:	☐ Input ☐ Logic ☑ Output ☐ unknown
Technology:	electronic
Category:	-
Use case:	Output component
Description of the use case:	T1 imp brings the motor M1 to a uncontrolled safe stop (STO) when the guard is opened because PLC B, de-energizing K1, enables pulse blocking.

Documentation Block

Documentation:	Manufacturer data sheet
Document:	..\ISO 13849-1.pdf

MTTFD and Mission time Block

MTTFD [a]: 34722,2 (High)

Mission time [a]: 20		Shortest mission time [a]: 20	
B10D [cycles]: 20000000		nop [cycles/a]: 5760	
Nop parameter:	Days: 240	Hours: 24	Seconds: 3600
Documentation:		B10D =20.000.000 dop= 240 g/a; hop=24 h; tcycle=3600 s	

Diagnostic coverage Block

DC [%]: 99 (High)

SF Safety function: Stop function

Measure:	Plausibility check, e.g. use of normally open and normally closed mechanicall linked contacts (Input devices) (99 %)
Documentation:	Plausibility check by PLC A through B1 and pulse-blocking relay contact state (K1)

Status / Messages Block

Status:	green

EXCLUSION OF LIABILITY

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

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

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

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

CONTACT

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

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