PR Project name: RECIF Project - Safety system

Project file name:	C:\Users\ferrucci\OneDrive\UPF\projects\recif\studies\DD-019-note_calcul_systeme_securite\rev00\DD-019_rev01.ssm
Creation date:	05/04/2022 16:59:40
Project status:	Done
Project number:	
Project version:	
Authors:	Franco FERRUCCI
Project managers:	Pascal ORTEGA
Inspectors:	
Dangerous point/machine:	
Documentation:	In French: Système de sécurité projet RECIF
Document:	
Version of software:	2.0.8 build 4
Version of standard:	ISO 13849-1:2015, ISO 13849-2:2012
Checksum:	91dfcda8d7e857515123eae5fe44519c
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: Disconnection of fuel cell H2 solenoid valve power supply [SIF #1a]

Required: PLr d Reached: PL d PFHD [1/h]: 2E-7 Status: green

SF Name: Disconnection of electrolyzer power supply [SIF #1b]

Required: PLr d Reached: PL d PFHD [1/h]: 2,3E-7 Status: green

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Identifier of the Safety function:	SIF #1a
Safety function type:	Safety-related stop function initiated by safeguard
Triggering event:	Gas detection or fault detection in one of the two redundant gas detectors.
Reaction and Behaviour on power failure:	Trip of safety action.
Safe state:	
Operation mode:	
Demand rate:	
Running-on time:	
Priority:	
Documentation:	In French: Fermeture vanne alimentation H2 de la pile à combustible
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:	● S_2 → F_1 → P_2 → $\boxed{d}$
Documentation:	PL d: equivalent to SIL 2. The NF EN 60079-29-3 stays that it is rare for any risk study to determine a SIL higher than SIL 2 for a fixed gas detection system Note: NF EN 60079-29-3: Explosive atmospheres - Part 29-3: Gas detectors - Guidance on functional safety of fixed gas detection systems In French: Équivalent à SIL 2. La norme NF EN 60079-29-3 indique qu'une étude de risque ne détermine que rarement une intégrité de sécurité supérieure à SIL 2 pour un système fixe de détection de gaz. NB: NF EN 60079-29-3 : « Atmosphères explosives - Partie 29-3 : détecteurs de gaz - Recommandations relatives à la sécurité fonctionnelle des systèmes fixes de détection de gaz
Document:	

Performance Level Safety function

Reached PL: d	PFHD [1/h]: 2E-7

Status / Messages Safety function

Status:	green

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Subsystems (1 / 3)

SB Name: Hydrogen transmitters

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
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]: 1,9E-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]

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Requirements of the Category:	- 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]:	66,7 (High)
Mission time [a]: 20	Shortest mission time [a]: 20

Diagnostic coverage Subsystem

DCavg [%]:	60,1 (Low)

Common cause failure Subsystem

CCF Points:	90 (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. - Design / application / experience (5 Points) Components used are well-tried. - 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. - 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),

CCF Measures:	and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures. - 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 / 2)

BL Name: H2 transmitter #1

Reference designator: -B1	Inventory number:

Device details Block

Device Manufacturer:	GfG Gesellschaft für Gerätebau mbH	
Device Identifier:	CC28	
Device group:		
Part number:		Revision:
Function:	☑ Input □ Output	□ Logic □ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

Documentation Block

Documentation:	For monitoring combustible gases and vapors in hazardous areas, the CC28 transmitter in combination with GfG‘s proven gas measurement controllers is a reliable and economical solution. Short response times (t90=9s; depending on gas type and sensor) allow fast warning of gases such as methane or propane. The design is ATEX certified. With ignition protection types 'd'

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Documentation:	(flameproof enclosure) and 'e' (increased safety), safe use in Ex zone 1 is possible. In addition, the CC28 hardware complies with the European Functional Safety Standard DIN EN 61508-2: 2011 for many gases.
Document:	..\GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf

MTTFD and Mission time Block

MTTFD [a]: 1809,1 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Lambda [1/h]: 6,3E-8	RDF [%]: 100
Documentation:	Document: "Sl L-Declaration of Conformity EC28" GfG Gesellschaft für Gerätebau mbH File name: GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf lambda "du" (dangerous undetected) = 6.31 x 10-8 1/h Note: RDF stands for "ratio of dangerous failures". In this case I considered RDF=100% since the value of lambda I entered corresponds to the "dangerous undetected" type.

Diagnostic coverage Block

DC [%]: 81,4 (Low)	

Documentation:	Document: "Sl L-Declaration of Conformity EC28"
	GfG Gesellschaft für Gerätebau mbH
	
	File name:
	GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf
	lambda_du = 6.31e-8 1/h.
	lambda_dd = 2.77e-7 1/h.
	lambda_su = 6.10e-7 1/h.
	lambda_sd = 2.80e-8 1/h.
	
	DC = lambda_dd/lambda_d
	
	This last equation comes from IEC 61508-2:2010, Annex C.1, point "g".

Status / Messages Block

Status:	green

Blocks (2 / 2)

BL Name: H2 transmitter controller

Reference designator: -K.2.30	Inventory number:

Device details Block

Device Manufacturer:	GfG Gesellschaft für Gerätebau mbH
Device Identifier:	GMA 44
Device group:	

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

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]: 3869,7 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Lambda [1/h]: 2,9E-8	RDF [%]: 100
Documentation:	Document: "SIL-Declaration of Conformity GMA41/41B" GfG Gesellschaft für Gerätebau mbH File name: GfG_2010-01-29_SIL-Declaration-of-Conformity_GMA41(B).pdf lambda "du" (dangerous undetected) = 2.59 x 10-8 1/h Note: RDF stands for "ratio of dangerous failures". In this case I considered RDF=100% since the value of lambda I entered corresponds to the "dangerous undetected" type.

Diagnostic coverage Block

DC [%]: 89,5 (Low)	

Documentation:	Document: "Sl L-Declaration of Conformity EC28"
	GfG Gesellschaft für Gerätebau mbH
	
	File name:
	GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf
	lambda_du = 2.59e-8 1/h
	lambda_dd = 2.21e-7 1/h
	lambda_su = 1.65e-7 1/h
	lambda_sd = 1.26e-8 1/h
	
	DC = lambda_dd/lambda_d
	
	This last equation comes from IEC 61508-2:2010, Annex C.1, point "g".

Status / Messages Block

Status:	green

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 3

Blocks (1 / 1)

BL Name: H2 transmitter #2

Reference designator: -B3	Inventory number:

Device details Block

Device Manufacturer:	DEGA	
Device Identifier:	NSH-EL II LCD RE	
Device group:		
Part number:		Revision:
Function:	☑ Input □ Output	□ Logic □ unknown
Technology:	unknown	
Category:	-	
Use case:		
Description of the use case:		

Documentation Block

Documentation:	
Document:	

MTTFD and Mission time Block

MTTFD [a]: 3 (Low)	
Mission time [a]: 20	Shortest mission time [a]: 20
Rate of dangerous failure [FIT]: 38051,8	
Documentation:	

Diagnostic coverage Block

DC [%]: 60 (Low)	
Measure:	Processing unit: self-test by software (Logic) (60 % - 90 %)
Documentation:	

Status / Messages Block

Status:	green

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Subsystems (2 / 3)

SB Name: Safety programmable logic controller (PLC)

Reference designator: -K.2.53	Inventory number:

Device details Subsystem

Device Manufacturer:	ABB	
Device Identifier:	Pluto B46 v2	
Device group:		
Part number:		Revision:
Function:	□ Input □ Output	☑ Logic □ unknown
Use case:		
Description of the use case:		

Documentation Subsystem

Documentation:	Pluto B46 is a Safety PLC with 24 failsafe inputs and 4 failsafe relay outputs, 2 failsafe transistor outputs and safety bus connection.
Document:	..\Extract_2TLC172001M0212_A_Pluto_Hardware_Manual.pdf

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]: 2E-9

Documentation:

File name : 2TLC172001M0212_A_Pluto_Hardware_Manual.pdf
Document name: PLUTO Safety-PLC - Operating instructions - Hardware
Document code and version: 2TLC172001M0212_A, English v12A

Extract:
SAFETY PARAMETERS:

SIL according to IEC 61508	SIL 3
SIL according to EN 62061	SIL CL 3
PL according to EN ISO 13849-1	PL e
Category according to EN ISO 13849-1	4
DC avg according to EN ISO 13849-1	High
CCF according to EN ISO 13849-1	Meets the requirements
HFT (Hardware fault tolerance)	1
SFF (Safe failure fraction)	>99% for the single channel parts >90% for the double channel parts

Digital input to Safety output (Input to output (incl. AS-i and CAN bus))

PFD AV (for proof test interval = 20 years)	1.5x10-4
PFH D according to IEC 61508/EN 62061	2x10-9
MTTF d according to EN ISO 13849-1	High/1100 years

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Documentation:	Analogue inputs to Safety output (Pluto D20, D45) 2 inputs/sensors (see 4.3.2) 1 input/sensor (see 4.3.2) SIL according to IEC 61508/EN 62061 Up to SIL 3 Up to SIL 2 PL according to EN ISO 13849-1 Up to PL e Up to PL d DC avg according to EN ISO 13849-1 Up to High Up to Medium PFD AV (for proof test interval = 20 years) 1.5x10 -4 1.5x10 -3 PFH D according to IEC 61508/EN 62061 1.6x10 -9 5.8x10 -9 MTTF d according to EN ISO 13849-1 High/1100 years High/400 years
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: Safety expansion relay connected to PLC safety output

Reference designator: -K.2.54	Inventory number:

Device details Subsystem

Device Manufacturer:	ABB	
Device Identifier:	BT50	
Device group:		
Part number:		Revision:
Function:	☐ Input ☑ Output	☐ Logic ☐ unknown
Use case:		
Description of the use case:		

Documentation Subsystem

SF Safety function: Disconnection of fuel cell H2 solenoid valve power supply

Documentation:	Safety relay/expansion relay The BT50 is designed to connect safety devices, such as emergency stops, directly in the voltage supply circuit to the relay. Despite a maximum built-in width of 22.5 mm the relay is very powerful. This relay can be used to expand the safety outputs of Pluto. With 3 NO safety outputs, 1 NC output (for monitoring purposes), a test input and complete internal supervision, the BT50 is quite unique.
Document:	..\BT50_ABB.pdf

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]: 1,2E-8
Documentation:	From file name: \recif\datasheets\#functional_safety\ABB\Pluto\BT50\BT50_ABB.pdf Category 4/PL e (EN ISO 13849-1:2008) SIL 3 (EN 62061:2005) PFHd 1.22E-08 Functional test: The relays must be cycled at least once a year.
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: Disconnection of electrolyzer power supply

Identifier of the Safety function:	SIF #1b
Safety function type:	Safety-related stop function initiated by safeguard
Triggering event:	Gas detection or fault detection in one of the two redundant gas detectors.
Reaction and Behaviour on power failure:	Trip of safety action.
Safe state:	
Operation mode:	
Demand rate:	
Running-on time:	
Priority:	
Documentation:	In French: Coupure alimentation électrique de l'électrolyseur
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:	$\bullet\!- S_2 \rightarrow - F_1 \rightarrow - P_2 \rightarrow \boxed{d}$
Documentation:	PL d: equivalent to SIL 2. The NF EN 60079-29-3 stays that it is rare for any risk study to determine a SIL higher than SIL 2 for a fixed gas detection system Note: NF EN 60079-29-3: Explosive atmospheres - Part 29-3: Gas detectors - Guidance on functional safety of fixed gas detection systems In French: Équivalent à SIL 2. La norme NF EN 60079-29-3 indique qu'une étude de risque ne détermine que rarement une intégrité de sécurité supérieure à SIL 2 pour un système fixe de détection de gaz. NB: NF EN 60079-29-3 : « Atmosphères explosives - Partie 29-3 : détecteurs de gaz - Recommandations relatives à la sécurité fonctionnelle des systèmes fixes de détection de gaz
Document:	

Performance Level Safety function

Reached PL: d	PFHD [1/h]: 2,3E-7

SF Safety function: Disconnection of electrolyzer power supply

Status / Messages Safety function

Status:	green

Subsystems (1 / 4)

SB Name: Hydrogen transmitters

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
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]: 1,9E-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]

SF Safety function: Disconnection of electrolyzer power supply

Requirements of the Category:	- 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]:	66,7 (High)	
Mission time [a]: 20		Shortest mission time [a]: 20

Diagnostic coverage Subsystem

DCavg [%]:	60,1 (Low)

Common cause failure Subsystem

CCF Points:	90 (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. - Design / application / experience (5 Points) Components used are well-tried. - 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

SF Safety function: Disconnection of electrolyzer power supply

CCF Measures: as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).

- 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.

Documentation:

Document:

Status / Messages Subsystem

Status: green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 2)

BL Name: H2 transmitter #1

Reference designator: -B1 Inventory number:

Device details Block

Device Manufacturer: GfG Gesellschaft für Gerätebau mbH

Device Identifier: CC28

Device group:

Part number: Revision:

Function: ☑ Input ☐ Logic
☐ Output ☐ unknown

Technology: electronic

Category: -

Use case:

Description of the use case:

Documentation Block

Documentation: For monitoring combustible gases and vapors in hazardous areas, the CC28 transmitter in combination with GfG‘s proven gas measurement controllers is a reliable and economical

SF Safety function: Disconnection of electrolyzer power supply

Documentation:	solution. Short response times (t90=9s; depending on gas type and sensor) allow fast warning of gases such as methane or propane. The design is ATEX certified. With ignition protection types 'd' (flameproof enclosure) and 'e' (increased safety), safe use in Ex zone 1 is possible. In addition, the CC28 hardware complies with the European Functional Safety Standard DIN EN 61508-2: 2011 for many gases.
Document:	..\GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf

MTTFD and Mission time Block

MTTFD [a]: 1809,1 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Lambda [1/h]: 6,3E-8	RDF [%]: 100
Documentation:	Document: "Sl L-Declaration of Conformity EC28" GfG Gesellschaft für Gerätebau mbH File name: GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf lambda "du" (dangerous undetected) = 6.31 x 10-8 1/h Note: RDF stands for "ratio of dangerous failures". In this case I considered RDF=100% since the value of lambda I entered corresponds to the "dangerous undetected" type.

Diagnostic coverage Block

DC [%]: 81,4 (Low)	

Documentation:	Document: "Sl L-Declaration of Conformity EC28"
	GfG Gesellschaft für Gerätebau mbH
	
	File name:
	GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf
	lambda_du = 6.31e-8 1/h.
	lambda_dd = 2.77e-7 1/h.
	lambda_su = 6.10e-7 1/h.
	lambda_sd = 2.80e-8 1/h.
	
	DC = lambda_dd/lambda_d
	
	This last equation comes from IEC 61508-2:2010, Annex C.1, point "g".

Status / Messages Block

Status:	green

Blocks (2 / 2)

BL Name: H2 transmitter controller

Reference designator: -K.2.30	Inventory number:

Device details Block

SF Safety function: Disconnection of electrolyzer power supply

Device Manufacturer:	GfG Gesellschaft für Gerätebau mbH	
Device Identifier:	GMA 44	
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]: 3869,7 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
Lambda [1/h]: 2,9E-8	RDF [%]: 100
Documentation:	Document: "SIL-Declaration of Conformity GMA41/41B" GfG Gesellschaft für Gerätebau mbH File name: GfG_2010-01-29_SIL-Declaration-of-Conformity_GMA41(B).pdf lambda "du" (dangerous undetected) = 2.59 x 10-8 1/h Note: RDF stands for "ratio of dangerous failures". In this case I considered RDF=100% since the value of lambda I entered corresponds to the "dangerous undetected" type.

Diagnostic coverage Block

DC [%]: 89,5 (Low)	

Documentation:	Document: "Sl L-Declaration of Conformity EC28"
	GfG Gesellschaft für Gerätebau mbH
	
	File name:
	GfG_2016-02-08_SIL-Declaration-of-Conformity_CC28.pdf
	lambda_du = 2.59e-8 1/h
	lambda_dd = 2.21e-7 1/h
	lambda_su = 1.65e-7 1/h
	lambda_sd = 1.26e-8 1/h
	
	DC = lambda_dd/lambda_d
	
	This last equation comes from IEC 61508-2:2010, Annex C.1, point "g".

SF Safety function: Disconnection of electrolyzer power supply

Status / Messages Block

Status:	green

Channels / Test channels (2 / 2)

CH Name: Channel 2

MTTFD [a]: 3

Blocks (1 / 1)

BL Name: H2 transmitter #2

Reference designator: -B3	Inventory number:

Device details Block

Device Manufacturer:	DEGA	
Device Identifier:	NSH-EL II LCD RE	
Device group:		
Part number:	Revision:	
Function:	☑ Input ☐ Output	☐ Logic ☐ unknown
Technology:	electronic	
Category:	-	
Use case:		
Description of the use case:		

Documentation Block

Documentation:	DEGA NS II LCD transmitter is a part of the gas detection system. Transmitter is located in monitored premises in which critical situations due to accumulation of flammable or toxic substances can occur. The transmitter has an LCD display to show measured concentrations of detected substances in real time.
Document:	

MTTFD and Mission time Block

MTTFD [a]: 3 (Low)	
Mission time [a]: 20	Shortest mission time [a]: 20
Rate of dangerous failure [FIT]: 38051,8	
Documentation:	

Diagnostic coverage Block

DC [%]: 60 (Low)	
Measure:	Processing unit: self-test by software (Logic)

SF Safety function: Disconnection of electrolyzer power supply

Measure:	(60 % - 90 %)
Documentation:	

Status / Messages Block

Status:	green

Subsystems (2 / 4)

SB Name: Safety programmable logic controller (PLC)

Reference designator: -K.2.53	Inventory number:

Device details Subsystem

Device Manufacturer:	ABB	
Device Identifier:	Pluto B46 v2	
Device group:		
Part number:		Revision:
Function:	□ Input □ Output	☑ Logic □ unknown
Use case:		
Description of the use case:		

Documentation Subsystem

Documentation:	Pluto B46 is a Safety PLC with 24 failsafe inputs and 4 failsafe relay outputs, 2 failsafe transistor outputs and safety bus connection.
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]: 2E-9
Documentation:	File name : 2TLC172001M0212_A_Pluto_Hardware_Manual.pdf Document name: PLUTO Safety-PLC - Operating instructions - Hardware Document code and version: 2TLC172001M0212_A, English v12A Extract: SAFETY PARAMETERS: SIL according to IEC 61508: SIL 3 SIL according to EN 62061: SIL CL 3 PL according to EN ISO 13849-1: PL e Category according to EN ISO 13849-1: 4 DC avg according to EN ISO 13849-1: High CCF according to EN ISO 13849-1: Meets the requirements HFT (Hardware fault tolerance): 1 SFF (Safe failure fraction): >99% for the single channel parts, >90% for the double channel parts

SF Safety function: Disconnection of electrolyzer power supply

Documentation:	Digital input to Safety output (Input to output (incl. AS-i and CAN bus)) PFD AV (for proof test interval = 20 years): 1.5x10-4 PFH D according to IEC 61508/EN 62061: 2x10-9 MTTF d according to EN ISO 13849-1: High/1100 years
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: Safety expansion relay connected to PLC safety output

Reference designator: -K.2.54	Inventory number:

Device details Subsystem

Device Manufacturer:	ABB	
Device Identifier:	BT50	
Device group:		
Part number:	Revision:	
Function:	□ Input ☑ Output	□ Logic □ unknown
Use case:		
Description of the use case:		

Documentation Subsystem

Documentation:	Safety relay/expansion relay The BT50 is designed to connect safety devices, such as emergency stops, directly in the voltage supply circuit to the relay. Despite a maximum built-in width of 22.5 mm the relay is very powerful. This relay can be used to expand the safety outputs of Pluto. With 3 NO safety outputs, 1 NC output (for monitoring purposes), a test input and complete internal supervision, the BT50 is quite unique.
Document:	

Safety function: Disconnection of electrolyzer power supply

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]: 1,2E-8
Documentation:	From file name: \recif\datasheets\#functional_safety\ABB\Pluto\BT50\BT50_ABB.pdf Category 4/PL e (EN ISO 13849-1:2008) SIL 3 (EN 62061:2005) PFHd 1.22E-08 Functional test: The relays must be cycled at least once a year.	
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 / 4)

Name: Two trip contactors connected to expansion relay

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:	

SF Safety function: Disconnection of electrolyzer power supply

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)

Common cause failure Subsystem

CCF Points:	75 (fulfilled)
CCF Measures:	- Design / application / experience (5 Points) Components used are well-tried. - Design / application / experience (15 Points)

CCF Measures:	Protection against over-voltage, over-pressure, over-current, over-temperature, etc. - Competence / training (5 Points) Training of designers to understand the causes and consequences of common cause failures. - Environmental (25 Points) For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers’ requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered. - Environmental (10 Points) Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards). - 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.
Documentation:	
Document:	

Status / Messages Subsystem

Status:	green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Trip contactor #1

Reference designator: -K.2.50 Inventory number:

Device details Block

Device Manufacturer:	Schneider electric
Device Identifier:	LC1DT40BL + LAD4TBDL

SF Safety function: Disconnection of electrolyzer power supply

Device group:		
Part number:		Revision:
Function:	□ Input ☑ Output	□ Logic □ unknown
Technology:	electromechanic	
Category:	-	
Use case:		
Description of the use case:		

Documentation Block

Documentation:	TeSys Deca contactor, 4P(4NO), AC-1, <=440V 40A, 24V DC low consumption coil Auxiliary contacts: - type type mechanically linked 1 NO + 1 NC conforming to IEC 60947-5-1 - type mirror contact 1 NC conforming to IEC 60947-4-1
Document:	..\LC1DT40BL_en.pdf

MTTFD and Mission time Block

MTTFD [a]: 1141552,5 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
B10D [cycles]: 1369863	nop [cycles/a]: 12
Documentation:	From product datasheet: Safety reliability level: - B10d = 1369863 cycles contactor with nominal load conforming to EN/ISO 13849-1 - B10d = 20000000 cycles contactor with mechanical load conforming to EN/ISO 13849-1

Diagnostic coverage Block

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

Status / Messages Block

Status:	green

Channels / Test channels (2 / 2)

CH Name: Channel 2

SF Safety function: Disconnection of electrolyzer power supply

MTTFD [a]: 100

Blocks (1 / 1)

BL Name: Trip contactor #2

Reference designator: -K.2.51 Inventory number:

Device details Block

Device Manufacturer:	Schneider electric	
Device Identifier:	LC1DT40BL + LAD4TBDL	
Device group:		
Part number:		Revision:
Function:	□ Input ☑ Output	□ Logic □ unknown
Technology:	electromechanic	
Category:	-	
Use case:		
Description of the use case:		

Documentation Block

Documentation:	TeSys Deca contactor, 4P(4NO), AC-1, <=440V 40A, 24V DC low consumption coil Auxiliary contacts: - type type mechanically linked 1 NO + 1 NC conforming to IEC 60947-5-1 - type mirror contact 1 NC conforming to IEC 60947-4-1
Document:	..\LC1DT40BL_en.pdf

MTTFD and Mission time Block

MTTFD [a]: 1141552,5 (High)	
Mission time [a]: 20	Shortest mission time [a]: 20
B10D [cycles]: 1369863	nop [cycles/a]: 12
Documentation:	From product datasheet: Safety reliability level: - B10d = 1369863 cycles contactor with nominal load conforming to EN/ISO 13849-1 - B10d = 20000000 cycles contactor with mechanical load conforming to EN/ISO 13849-1

Diagnostic coverage Block

DC [%]: 99 (High)	
Measure:	Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)

SF Safety function: Disconnection of electrolyzer power supply

Measure:	(Output device) (99 %)
Documentation:	

Status / Messages Block

Status:	green

EXCLUSION OF LIABILITY

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

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

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

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

CONTACT

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