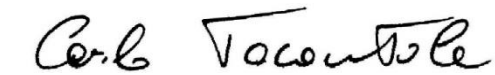
FMEDA REPORT

Report no.:	*18085 LA*
Rev. no.:	*0*
Date:	*2018-08-06*
Product:	*Partial stroke test device*
Models:	*Series SDCU-20*
Customer:	***DVG Automation S.p.A.*** *Via G. Rossetti, 2* *I-29016 Cortemaggiore (PC)*
Order no. / Date:	*DVG Automation order dated 2018-06-20*
Standards:	*IEC 61508: 2010 Part 1–7* *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems* *IEC 61511-1: 2016 + A1: 2017* *IEC 61511: 2016 Part 2–3* *Functional Safety – Safety Instrumented Systems for the process industry sector*
Issued by:	***CTAI S.r.l.*** *Viale Rimembranze, 46* *I-20020 Lainate (MI)*
Author:	*Carlo Tarantola*
(Signature)	

This document is only valid in its entirety and separation of any part is not allowed.

INDEX

1 INTRODUCTION

This report summarizes the results of a failure rates evaluation of partial stroke test device series SDCU-20 and it includes:

- list of reference documents
- general description of the product
- effects evaluated
- procedure used for the failure rates estimation, including:
  - description of the method used
  - assumptions used
- failure rates results

The inspection of the further requirements defined in IEC 61508 and IEC 61511 and applicable product standards are not scope of this job.

2 REFERENCE DOCUMENTS

2.1 Standards

No.	Reference	Title
[N1]	IEC 61508: 2010 Part 1–7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
[N2]	IEC 61511-1: 2016 + A1: 2017 IEC 61511: 2016 Part 2–3	Functional Safety – Safety Instrumented Systems for the process industry sector

2.2 Databases

No.	Reference	Title
[N3]	MIL-HDBK-217E Department of Defence, USA	Reliability Prediction of Electronic Equipment
[N4]	Telcordia SR-332	Reliability Prediction Procedure for Electronic Equipment
[N5]	SIEMENS SN 29500	Failure Rate of components
[N6]	RiAC NPRD-2016	Non electronic Parts Reliability Data
[N7]	RiAC FMD-97/2013	Failure Modes/Mechanism Distributions
[N8]	NSWC	Handbook of Reliability Prediction Procedures for Mechanical Equipment
[N9]	Exida	Safety Equipment Reliability Handbook
[N10]	OREDA	Offshore Reliability Data
[N11]	IEC/TR 62380	Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment (identical to RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication)
[N12]	IEC 61784-3:2016 + AMD1:2017	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

NOTES:

- For databases, where there is no indication of the publishing date it means that the reference is the latest edition
- [N12] is mentioned only for the method of calculation of the residual error rate

3 INSPECTION DOCUMENTS

3.1 Documentation provided by the customer

No.	Reference	Title
[D1]	DVG Automation document “SDCU-20 presentation”	Technical brochure
[D2]	DVG Automation documents no. LSboardPlus LSBplusBOTTOM	Electrical schemes
[D3]	DVG Automation document no. Diag-funct Rev. 01	Description of diagnostic functions and operation

3.2 Documentation prepared by CTAI

No.	Reference	Title
[R1]	18085 LA Rev. 0	SDCU - Random failure analysis

4 ABBREVIATIONS

Term	Definition
β, β_D	Beta common cause factor
λ_D	Failure rate of dangerous failures
λ_{DD}	Failure rate of detected dangerous failures
λ_{DU}	Failure rate of undetected dangerous failures
λ_{NE}	Failure rate of no effect failures
λ_S	Failure rate of safe failures
DC	Diagnostic coverage
DETT	De-energise-to-trip
ETT	Energise-to-trip
FMEDA	Failure modes, effects and diagnostic analysis
FST	Full stroke test
HFT	Hardware fault tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year
MRT	Mean repair time
PFD	Probability of failure on demand
PFD_{AVG}	Average probability of failure on demand
PFH	Probability of failure per hour
PST	Partial stroke test
PTC	Proof test coverage
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
TI	Test interval for proof test (full stroke)
TI_D (TI_{PS})	Test interval for diagnostic test (partial stroke)
Type A element	“Non-Complex” element (using discrete components)
Type B element	“Complex” element (using micro controllers or programmable logic)

NOTES:

- Terms and abbreviations that can be used in the report are listed in the table above.
- For definitions, standard [N1] (in particular, Part 4) applies.

5 PRODUCT DESCRIPTION

This report is related to partial stroke test (PST) device series SDCU-20.

The PST can be initiated via:

1. Local pushbutton
2. Remote command connected to one of the two digital inputs “Digital input 1” or “Digital Input 2”
3. Remote command via HART bus
4. Command from Local Control Panel (LCP), connected to the SDCU-20 via the optional board “I/O interface card”

The blocks used to perform the PST are the following:

Cases 1 and 2:

- Power supply blocks
- Digital input block
- Microcontroller
- PST actuation blocks
- Feedback blocks:
  - Contactless position sensor block
  - 4-20 mA conditioning circuit (pressure sensor input block)

Case 3:

- Power supply blocks
- HART Bus block
- Microcontroller
- PST actuation blocks
- Feedback blocks:
  - Contactless position sensor block
  - 4-20 mA conditioning circuit (pressure sensor input block)

Case 4:

- Power supply blocks
- I/O interface card
- CAN Bus block
- Microcontroller
- PST actuation blocks
- Feedback blocks:
  - Contactless position sensor block
  - 4-20 mA conditioning circuit (pressure sensor input block)

Detailed information is included in [D1]-[D3].

6 EFFECTS EVALUATED

The failure rates are evaluated for the following effects:

1. *Failure of PST operation: the PST is not performed / not performed correctly*
2. *The PST gives as a result a signalling of "false positive": the PST is performed, but it can give a positive result when the result should be negative*
3. *Execution of a FST: a FST is performed instead of the PST*

NOTES:

- the failure rates are evaluated according to the above cases
- in the following, the notation "λ_D" is used to indicate:
  - for effect no. 1: the rate of failure of the device that can give as a result a non performing / non correct performing of PST
  - for effect no. 2: the rate of failure of the device that can give as a result a positive PST result when the result should be negative
  - for effect no. 3: the rate of failure of the device that can give as a result a FST instead of a PST
- in the following, the notation "λ_{DD}" is used to indicate that the failure is detected
- in the following, the notation "λ_{DU}" is used to indicate that the failure is undetected
- the three effects are evaluated for the four cases listed in par. 5
- effect no. 3 is evaluated also in case of presence of option "Position switch to eliminate spurious trips"

7 DETERMINATION OF FAILURE RATES

7.1 Procedure

The determination of random failure rates is performed with a Failure Modes, Effects and Diagnostic Analysis (FMEDA).

The procedure used for the determination of random hardware failures is the following:

1. FMEDA of the product, with classification of failure modes
2. Determination of λ values (final value)

The FMEDA is based on the documentation (drawings with components lists) provided by the manufacturer, and the other design documentation referenced in par. 3, and is documented in [R1].

The FMEDA includes the following information:

Item	**Meaning**
Position	Position of the component on the drawing
Component	Description of the component
Function	Function of the component
Quantity	No. of components which have the same function
Local Architecture	Local redundancy of the component (if any), to perform the specific function
Beta Factor	Parameter used in case of local redundancy
Failure rate	Total failure rate of the single component – Taken from the databases referenced in par. 2.2.
Total failure rate	Total failure rate, considering the values of Quantity and Beta Factor
Failure Mode	Failure Mode taken from the databases referenced in par. 2.2.
Failure Distribution	% of the total failure rate allocated to the specific failure mode
Mode failure rate	Failure rate of the specific failure mode
Effect	Effect of the failure mode on the safety function(s)
SIL Classification	Failure category according to [N1]. See par. 9.1.1.2 for details.
Diagnostics	Diagnostic test (internal or external) able to detect the specific failure mode
DC	Diagnostic Coverage of the identified diagnostic test
λ_S, λ_{DD}, λ_{DU}, λ_{NE}	Failure rate of the failure mode, for the specific failure category

7.2 Description of the failure categories

The following table lists:

- The failure types considered in the assessment
- The failure definition according to [N1]
- For each failure type, examples of failures considered for the specific product

Failure Type	Failure definition according to [N1]	Examples for the specific product
Safe	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a. results in the spurious operation of the safety function; or b. increases the probability of the spurious operation of the safety function	• No safe failures are considered
Dangerous	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode); or b. decreases the probability that the safety function operates correctly when required	For effect no. 1: • the input circuit does not work • the microcontroller does not work, • the activation command does not work • the feedback gives a non correct result (negative PST) For effect no. 2: • the feedback gives a non correct result (positive PST) For effect no. 3: • the command continues after the reaching of the PST position
No Effect	Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function	• Change in value of filtering components • Small change in feedback analog values
No Part	Failure of a component that plays no part in implementing the safety function	• Failure of components not involved in the PST function (e.g. LEDs, position feedback)

7.3 Assumptions

The following assumptions are used for the evaluation of random hardware failures:

- Failure rates are considered constant for the product lifetime.
- Failure rates and failure modes in the FMEDA are taken from databases [N3]–[N12] (mainly from [N9] and [N11]).
- Propagation of failures is considered not relevant, unless a clear propagation path is present: in this case, the failure is considered a single failure, with failure rate corresponding to the failure rate of the first failure.
- The components that are not part of the PST function and cannot influence it are excluded from the evaluation.
- The stress levels considered are average for an industrial environment (ground fixed, outdoor application).

7.4 Determination of λ values

The failure rates – λ values – are calculated from the FMEDA.

8 ASSESSMENT RESULTS

The results are included in the following table.

PST command	Effect evaluated	λ_{DD} [1/h]	λ_{DU} [1/h]
Case 1 / 2: Local command / digital input command	Failure of PST	1,04E-07	1,43E-07
	“False positive” PST	3,58E-08	6,62E-08
	Carry out of FST instead of PST	0,00E+00	2,37E-08
Case 3: Remote command via HART Bus	Failure of PST	1,07E-07	1,74E-07
	“False positive” PST	3,80E-08	7,94E-08
	Carry out of FST instead of PST	0,00E+00	2,37E-08
Case 4: LCP command via I/O Interface Card	Failure of PST	2,83E-07	2,29E-07
	“False positive” PST	4,20E-08	1,20E-07
	Carry out of FST instead of PST	0,00E+00	2,37E-08
Case 1 / 2 / 3 / 4: Presence of option “Position switch to eliminate spurious trips”	Carry out of FST instead of PST	0,00E+00	<1,00E-12

9 STATUS OF THE DOCUMENT

History: R 0: Initial release Date: 2018-08-06

Release status: Released to client

Author(s): Carlo Tarantola