DAPS
Semi-rotary Drive

Festo SE & Co. KG
Ruiter Sr. 82
73734 Esslingen
GERMANY
+49 0711/347-0

www.festo.com

8188700
2022-12a
[8188701]

SAFETY MANUAL

FOR

PNEUMATIC ACTUATOR

SMA202101

VERS.	DESCRIPTION	DATE	ISSUED	VERIFIED	APPROVED
0	First Issue	2021.05.24	FSM	EM	CEO
1					
2					
3					
4					
5					

SUMMARY

0 INTRUDUCTION....3

1 SAFETY FUNCTION(S) SPECIFICATION....3

2 CONFIGURATION OF THE PRODUCT....3

3 SERVICE CONDITION LIMITATIONS (LIMITATION OF USE)....4

4 EXPECTED LIFETIME....6

5 FAILURE MODES AND ESTIMATED FAILURE RATES....7

6 PERIODIC TEST AND MAINTENANCE REQUIREMENTS....7

7 CLASSIFICATION....14

8 ARCHITECTURAL CONSTRAINTS....14

9 MEAN REPAIR TIME....15

10 COMMON CAUSE FACTORS....15

11 SYSTEMATIC CAPABILITY....15

0 INTRUDUCTION

Purpose of this Safety Manual, written in compliance with IEC 61508-2, Annex D, is to give all necessary information to the system integrator for a correct use of the product in Safety Instrumented System for SIL classified applications

1 SAFETY FUNCTION(S) SPECIFICATION

The safety function is defined as follows:

SINGLE ACTING ACTUATOR:

a. CLOSE (C) - The Actuator performs a quarter turn rotation via the action of the spring, in order to close the shut-down valve (this operation is usually performed de-energizing a solenoid valve, and venting air via the control system), OR
b. OPEN (FO) - The Actuator performs a quarter turn rotation via the action of the spring, in order open the shut-down valve (this operation is usually performed by de-energizing a solenoid valve, and venting air via the control system)

From the point of view of the functioning of a single acting actuator, the two functions "a" (FC) and "b" (FO) are equivalent. The safety function is in both cases driven by the spring.

DOUBLE ACTING ACTUATOR:

a. The Actuator performs a quarter turn rotation, in order to close the shut-down valve; this operation is performed by depressurizing the OPEN chamber of the cylinder and pressurizing the CLOSE chamber, OR
b. The Actuator performs a quarter turn rotation, in order to open the shut-down valve. This operation is performed by depressurizing the CLOSE chamber of the cylinder and pressurizing the OPEN chamber.

From the point of view of the functioning of a double acting actuator, the two functions "a" and "b" are considered as equivalent.

The choice of the safety function to be implemented is responsibility of the system integrator.

2 CONFIGURATION OF THE PRODUCT

The configuration of the product is described in general way on the relevant sections of Installation, Maintenance and Instructions Manual: sectional drawing, part list and component description.

The reference document for the specific configuration of the product is the General Arrangement Drawing issued for job, approved by the customer and/or the final user, that contain any technical requirements of the product.

The product is named and coded as follow:

Type codes for DAPS

001	Series	
DAPS	Semi-rotary drive	

002	Size of valve actuator	
0008	0008	
0015	0015	
0030	0030	
0053	0053	
0060	0060	
0090	0090	
0106	0106	
0120	0120	
0180	0180	
0240	0240	
0360	0360	
0480	0480	
0720	0720	
0960	0960	
1440	1440	
1920	1920	
2880	2880	
3840	3840	
4000	4000	
5760	5760	
8000	8000	

003	Swivel angle	
90	90	

004	Closing direction	
R	Closes to the right	

005	Function	
	Double-acting	
S	Single-acting, pushing	

006	Spring force	
	None	
1	For connecting pressure of 2.8 bar	
2	For connecting pressure of 3.5 bar	
3	For connecting pressure of 4.2 bar	
4	For connecting pressure of 5.6 bar	

007	Flange pattern 1	
F03	Hole pattern F03	
F04	Hole pattern F04	
F05	Hole pattern F05	
F07	Hole pattern F07	
F10	Hole pattern F10	
F12	Hole pattern F12	
F14	Hole pattern F14	
F16	Hole pattern F16	
F25	Hole pattern F25	

008	Flange pattern 2	
	None	
F05	Hole pattern F05	
F07	Hole pattern F07	
F10	Hole pattern F10	
F12	Hole pattern F12	
F16	Hole pattern F16	

009	Manual override	
	None	
MW	Handwheel	

010	Corrosion protection	
	Standard	
CR	Stainless steel	

011	Temperature range	
	Standard	
T4	0 ... +150°C	
T6	-50 ... +60°C	

For further information (eg. nominal pressure, output torque, rotation angle....) refer to the User's installation and maintenance manual.

3 SERVICE CONDITION LIMITATIONS (LIMITATION OF USE)

3.1 Ambient conditions

The following service condition limitations (Pressure Class, T(min), T(max), Rating) are included on product label (Fig. 1).

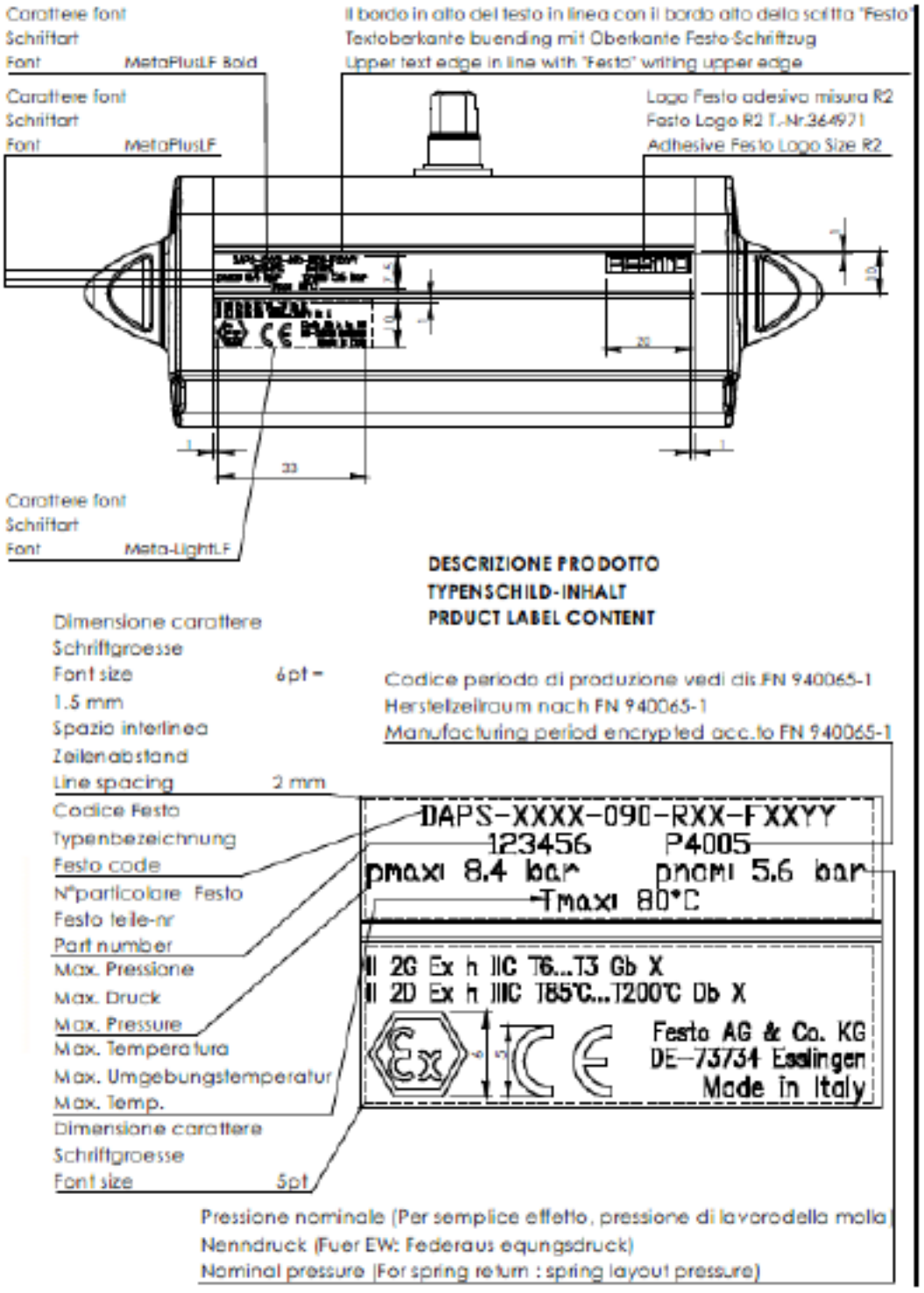
- **Supply operating media pressure.**

The maximum supply pressure is 8,4 bar (120 psi) (7 Bar for DAPS-8000)
Nominal supply pressure is 5,6 bar (80 psi), working pressure range from 2,5 bar (36 psi) up to 8,4 bar (120 psi) (7 Bar for DAPS-8000).

- **Operating temperature.**

Actuator standard working temperature range from –20°C to 80°C, are also available low temperature version from -50°C to + 60°C and high temperature version form –20°C to 150°C.

Fig. 1 - Product marking example



3.2 Use of double acting actuators in a Safety Instrumented System

In case of use of a double acting actuator in a Safety Instrumented System, the system shall respect all the requirements included in par. 11.2.11 of IEC 61511

3.3 Manual override

Manual override is not recommended for safety related applications as it can bypass the safety function. The manual override has to comply with the following:

1. The engage and disangage of the handwheel must be carried out according to the instructions in the installation and use manual.

2. To prevent an unauthorized use, the manual override shall be provided with a locking device (on request).

3. The engage signal is locally detected by the following operating instructions and described in detail in the instructions for use:

- Remove the cap to ensure there is no pressure in the actuator
- Engage the manual override and operate as required
- Disconnect the manual override (neutral position)
- Screw the cap

4. Before commissioning to ensure proper disengagement, perform an ON-OFF maneuverer of the actuator

3.4 Use of Double Acting actuators

Warning: when designing final elements subsystems including Double Acting actuators, be aware to comply with the requirements of IEC 61511-1 par.11.2.11.

4 EXPECTED LIFETIME

Product lifetime strongly depends on operating conditions and on materials of construction. As a general rule, the customer selects the main materials of construction.
For normal service conditions, the expected lifetime can be considered 20 years.
The above value is valid only if prescriptions in paragraph 6 of this manual are respected.

5 FAILURE MODES AND ESTIMATED FAILURE RATES

Please refer to the values included in the latest valid of SIL Certificate(s) (available on the Festo website or upon request)

NOTES:

- No internal diagnostics is included in the product.
- The failure rates are guaranteed:
  - For the service conditions listed in par. 3
  - For the expected lifetime declared in par. 4
  - Considering the periodic test and maintenance included in par. 6

The failure rates are determined performing a FMEDA based on the failure rates of components taken from industrial databases (NPRD-2016/FMD97/2016, EXIDA E&MCRH and NSWC-2011), integrated with field feedback using the Bayesian statistical approach mentioned in IEC 61508-2 Par. 7.4.4.3.3.

The system for reporting failures is based on field feedback from end users, with:

- Identification of the claim/failure
- Root cause analysis to identify cause and responsibility of the failure
- Identification of the possible effect of the failure on the Safety Function
- Classification of the failure considering the failure categories of IEC 61508-2 (Safe, Dangerous, No Effect)

Customer Service, Quality and Technical Department are responsible for the procedure, according to the respective role.

The requirements in IEC 61508-2 paragraphs 7.4.10.1 – 7.4.10.7 are fulfilled and assessed by Third Party.

6 PERIODIC TEST AND MAINTENANCE REQUIREMENTS

6.1 General

Please consider that the information in this paragraph is relevant only in regards of Reliability Tests; please refer to the IOM Manual for detailed information about product maintenance, handling and storage.

Tests may be carried out to increase the system reliability.
“On site” tests depend on Project/Plant facilities/requirements; however, a functional test must be executed on site, before product usage.

6.2 Full Stroke Test

The “Full Stroke Test” (“Online”) must be performed to satisfy the PFD_{AVG} (average probability of failure on demand) value.
The test frequencies shall be defined from the final integrator in relation to the defined SIL grade to achieve.

Procedure for Full Stroke Test

- Operate the Valve/Actuator assembly for No. 2 open/close complete cycles with complete closing of the valve.
- Verify the correct performing of open – close manoeuvre (e.g. check locally, or automatically via Logic solver, the correct movement of the valve/actuator assembly).

The achievement of the safe position (open or closed) shall be confirmed with the control of:

- The OPEN/CLOSED indications on actuator and the relative feedback to the logic solver, if existing.
  (see the specific operating manual for details)
- The mechanical position indicator on actuator, if existing;
  (see the specific operating manual and/or the assembly drawing for details)

The procedure can be performed manually or automatically. In the following, for both cases, the following points are listed:

- Parameters to be measured
- Instruments to be used
- Failure modes detected
- Diagnostic coverage/proof test coverage

Parameters to be measured:

The following parameters have to be measured for an effective Full Stroke Test:

- Angular position
- Time necessary to reach to final position
- Torque (as indirect measure, by means of the of pressure measurement in the actuator cylinder chamber)

NOTES:

- Not all parameters are needed, but the following combinations can be used:
  1. Measurement of angular position as function of time (pressure measurement is optional)
  2. Measurement of cylinder chamber pressure as function of time
  3. Verification of final position achievement in the established maximum time

Instruments / equipment to be used for the test:

Object	**Instruments / equipment**	
	Automatic Procedure	**Manual Procedure**
Angular Position	Case A: use of a Logic Solver: 1. Limit switches box, or 4÷20 mA position transmitter 2. Digital Input Module / Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 1. Limit switches box, or 4÷20 mA position transmitter 2. PST device with integrated SW function	1. Limit switches box, and/or visual indication 2. Skilled and trained personnel
Time necessary to reach the final position	As above	1. Limit switches box, and/or visual indication 2. Chronometer 3. Skilled and trained personnel
Torque (Pressure in the cylinder)	Case A: use of a Logic Solver: 1. Pressure transmitter connected to the cylinder chamber 2. Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 1. Pressure transmitter connected to the cylinder chamber 2. PST device with integrated SW function	Skilled and trained personnel (to check visible and/or audible partial sticking)

Failure modes detectable by the test:

Component	Detectable failure modes	
	Automatic Procedure	Manual Procedure
Spring Cartridge		
Spring	Breakage Weakened Worn Sticking	As per automatic procedure
Spring Flange	Breakage	
Head/end flange / bolts	Breakage Unscrewing	
Spring Rod	Breakage	
Spring Container	Total Breakage	
Scotch-Yoke mechanism		
Housing	Breakage	As per automatic procedure
Guide bar	Breakage	
Guide Block	Breakage	
Yoke	Breakage Sticking	
O-Rings	Breakage => External leakage	
Pneumatic cylinder		
Piston	Sticking	As per automatic procedure

NOTES:

- The ones listed above are the major failure modes of the main components
- In case of manual procedure, the detectable failure modes are the same as per automatic procedure. The test coverage is lower than the one for automatic mode, due to the human factor.
- The manual procedure cannot be considered as diagnostic.

Proof Test Coverage (PTC) / Diagnostic Coverage (DC)

Considering the application of the above described Test procedure, the “Test Coverage”, in case of automatic procedure, can be considered > 99% (it could be lower in case of test imperfections and/or use of un-calibrated instruments).

In case of manual procedure, the “Test Coverage” shall take into account also the test imperfection and the reliability/competence of the operator.

Note:

- if the test is automatic, then the Test Coverage is PTC, but can also considered as DC
- if the test is manual, then the Test Coverage is PTC, but cannot be considered as DC

6.3 Partial Stroke Test

The “Partial Stroke Test” (“Online”) can be performed to improve the PFD_{AVG} values.

A typical partial stroke value is 15% of the stroke.

Recommended Test Interval = 1 ÷ 3 months

Procedure for Partial Stroke Test

- Operate the Valve/Actuator assembly for No° 1 open/close cycles 15% of the stroke.
- Verify the correct performing of partial stroke manoeuvre (e.g. check locally, or automatically via Logic solver, or via the PST system the correct movement of the valve/actuator till 15% of the stroke).

The achievement of the partial stroke position shall be confirmed with the simultaneous control of:

- The indications of INTERMEDIATE POSITION on actuator display or PST device and the relative feedback to the logic solver, if existing
- The mechanical position indicator on actuator, if existing

The procedure can be performed manually or automatically. In the following, for both cases, the following points are listed:

- Parameters to be measured
- Instruments to be used
- Failure modes detected
- Diagnostic coverage/ test coverage

Parameters to be measured:

The following parameters have to be measured for an effective Partial Stroke Test:

- Angular position;
- Time necessary to reach to final position;
- Output torque (as indirect measure, by means of the of pressure measurement in the cylinder chamber)

NOTE:

- Not all parameters are needed, but the following combinations can be used:
    1. Measurement of position as function of time (pressure measurement is optional)
    2. Measurement of cylinder chamber pressure as function of time
    3. Verification of final position achievement in the established maximum time.

The parameters to be measured depends upon the partial stroke test system available.

Instruments / equipment to be used for the test:

The Partial Stroke Test can be executed in the following way:

1. Using commercial PST device, measuring/verifying:
    a. angular position as function of time
    b. cylinder chamber pressure as function of time (optional)
    c. final position achievement in the established maximum time.
2. By means of Logic Solver, measuring/verifying:
    a. angular position as function of time
    a. cylinder chamber pressure as function of time (optional)
    b. final position achievement in the established maximum time.
3. By means of a manual PST system (slightly different systems can be available: please make reference to the documentation of the specific project)

Instruments / equipment to be used for the test:

Object	**Instruments / equipment**	
	Automatic Procedure	**Manual Procedure**
Angular Position	Case A: use of a Logic Solver: 1. Limit switches box, or 4÷20 mA position transmitter 2. Digital Input Module / Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 1. Limit switches box, or 4÷20 mA position transmitter 2. PST device with integrated SW function	1. Limit switches box, and/or visual indication 2. Skilled and trained personnel
Time necessary to reach the final position	As above	1. Limit switches box, and/or visual indication 2. Chronometer 3. Skilled and trained personnel

Object	Instruments / equipment	
	Automatic Procedure	Manual Procedure
Torque (Pressure in the cylinder)	Case A: use of a Logic Solver: 1. Pressure transmitter connected to the cylinder chamber 2. Analog Input Module included in the Logic Solver 3. Application SW function (to compare the actual trend with the one stored during SAT) Case B: use of a PST device: 1. Pressure transmitter connected to the cylinder chamber 2. PST device with integrated SW function	Skilled and trained personnel (to check visible and/or audible partial sticking)

Failure modes detectable by the test:

Component	Detectable failure modes	
	Automatic Procedure	Manual Procedure
Spring Cartridge		
Spring	Breakage Weakened Worn Sticking	As per automatic procedure
Spring Flange	Breakage	
Head/end flange / bolts	Breakage Unscrewing	
Spring Rod	Breakage	
Spring Container	Total Breakage	
Scotch-Yoke mechanism		
Housing	Breakage	As per automatic procedure
Guide bar	Breakage	
Guide Block	Breakage	
Yoke	Breakage Sticking	
O-Rings	Breakage => External leakage	
Pneumatic cylinder		
Piston	Sticking	As per automatic procedure

NOTES:

- The ones listed above are the major failure modes of the main components
- In case of manual procedure, the detectable failure modes are the same as per automatic procedure. The test coverage is lower than the one for automatic mode, due to the human factor
- The manual procedure cannot be considered as diagnostic. The test can be considered as "non-perfect Proof Test", and can be considered in the estimation of PFD_{AVG}, while it is not considered for the estimation of SFF

Partial Stroke Diagnostic Coverage / Test Coverage

Considering the application of the above described Partial Stroke Test procedure, for all automatic methods indicated, the "Diagnostic Coverage" can be considered >90% (it could be lower in case of test imperfections and/or use of un-calibrated instruments).

In case of manual procedure, the "Test Coverage" shall take into account also the test imperfection and the reliability/competence of the operator.

Note:

- if the test is automatic, then the Test Coverage can also considered as DC
- if the test is manual, then the Test Coverage cannot be considered as DC

6.4 Periodic Maintenance

No particular periodic maintenance is requested.

7 CLASSIFICATION

The product is classified Type A according to IEC 61508-2.

8 ARCHITECTURAL CONSTRAINTS

For the evaluation of the conformity to the requirement of Hardware safety integrity architectural constraints of the standard IEC 61508, both Route 1_H and Route 2_H are used.

Route 1_H

- The product has a single channel configuration, HFT=0

- Safe failure rate λ_S:
  - **Single Acting Actuators:** According to IEC 61508 definitions (in particular definitions 3.6.8 and 3.6.13 of IEC 61508-4), no Safe Failures are possible in a Single Acting actuator. Each failure mode of the actuator itself shall be classified as "Dangerous" or "No Effect" (failures which can generate the spurious operation of the safety function are only external to the actuator itself, or are related to components that "plays no part in implementing the safety function", e.g. components of the pneumatic cylinder. Therefore, according to definition 3.6.13 of IEC 61508- 4, they cannot be used for the calculation of the SFF (SFF = Safe Failure Fraction). Hence **λ_S=0 for each type of single acting actuator**.
  - **Double Acting Actuators**: According to IEC 61508 definitions (in particular definitions 3.6.8 and 3.6.13 of IEC 61508-4), no Safe Failures are possible in a Double Acting actuator. Each failure mode of the actuator itself shall be classified as "Dangerous" or "No Effect" (failures which can generate the spurious operation of the safety function are only external to the actuator itself, and in the case of loss of power supply the actuator "stays put"). Therefore, according to definition 3.6.13 of IEC 61508- 4, they cannot be used for the calculation of the SFF (SFF = Safe Failure Fraction). Hence **λ_S=0 for each type of Double Acting actuator**.

For this reason, according to definition 3.6.15 of IEC 61508-4, we have:

- SFF=0 without external diagnostic tests;
- SFF>0 with external diagnostic tests, carried out according to definition 3.8.7 of IEC 61508-4, and according to what written in Par. 6 above (see the same paragraph for the SFF / DC reachable).

Route 2_H

The application of Route 2_H ("proven in use approach") is evaluated according to paragraphs 7.4.10.1÷7.4.10.7 of IEC 61508-2. Evidence was identified for each specific point.
As the product is classified as "Type A", no requirements for SFF are given for Route 2_H.

In conclusion:

The product can be used in single channel configuration up to:

- SIL 2 without external diagnostic tests
- SIL 3 considering external diagnostic tests

9 MEAN REPAIR TIME

The Mean Repair Time (MRT) is indicated in the following table:

TYPE	SIZE	MRT [h]
DOUBLE ACTING	DAPS 08-960	8
SPRING RETURN	DAPS 15-480	
DOUBLE ACTING	DAPS 1440-4000	16
SPRING RETURN	DAPS 720- DAPS 2880	

The MRT considered is the Technical Mean Repair Time, i.e., it takes in consideration availability of skilled personnel, adequate tools and spare parts.

10 COMMON CAUSE FACTORS

The product has a single channel configuration, HFT=0.
The β factors can be used when performing PFD_{AVG} calculations for redundant architectures.
The Common Cause factors, relevant when the product is used in redundant configuration, are:

$\beta=\beta_D=0,05$

NOTES:

- The above value is the value for 1oo2 architecture. The values for other architectures shall be calculated according to IEC 61508 Part 6, Table D.5.
- The above value is calculated in the hypothesis of redundancy without diversity

11 SYSTEMATIC CAPABILITY

The systematic capability of the product is 3.

This systematic capability is guaranteed only if the user:

1. Use the product according to the instructions for use and to the present Manual
2. Use the product in the appropriate environment (limitation of use)