SIL Manufacturer's Declaration Functional Safety According to IEC 61508 / 61511

Emerson Process Management Valve Automation, Inc.
19200 Northwest Freeway
Houston, TX. 77065
USA

Feb/06/2017

Emerson Process Management Valve Automation, Inc. hereby certifies that electric actuators CM32 are suitable to use in safety instrumented systems according to IEC 61508 and IEC 61511.

According to IEC 61508 the actuators correspond to

- SIL 0 (single device) without PVST
- SIL 1 (single device) with PVST
- SIL 2 (redundant configuration) by using a PVST.

The evidence is based on an FMEDA according to IEC 61508-2 and have been executed and verified by Exida.

General	Description
Safety Function	Move to Safety Position (ON/OFF)
Device Type According to IEC 61508	Type B^2
Operating Mode	Low demand mode
HW-Version	from 2014
SW-Version	from FW 1320
Hardware Fault Tolerance	0

FMEDA: CM32 with end position indication – IEC 61508:2010 Failure Rates

	Failure rates (in FIT), Profile 3 data	
Failure category	**Without PVST**	**With PVST [11]**
Safe Detected (λ_{SD})	**0**	**0**
Safe Undetected (λ_{SU})	**44**	**44**
Dangerous Detected (λ_{DD}) [12]	**571**	**1139**
Dangerous Detected (λ_{dd})	532	1100
Annunciation Detected (λ_{AD})	39	39
Dangerous Undetected (λ_{DU})	**804**	**236**
Annunciation Undetected (λ_{AU})	39	39
No effect	704	704
No part	123	123
PTC	**83%**	**33%**
Total failure rate (safety function)	**1419 FIT**	**1419 FIT**
SFF [13]	**43%**	**83%**
DC	**40%**	**82%**
SIL AC [14]	**---**	**SIL 1**
MTBF(in years)	50	50

[1] **Type A element**: Non-Complex element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2

[2] **Type B element**: Complex element (using microcontrollers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

[11] **PVST:** Partial Valve Stroke Test shall be performed at a rate at least ten times faster than the expected demand rate and carried out via the fail-safe mechanism

[12] **Torque/Force:** switch signal and end position signals are monitored by a safety PLC (control unit)

[13] **SFF:** The complete final element subsystem will need to be evaluated to determine the overall safe failure fraction. Number listed is for reference only.

[14] **SIL AC** (architectural constraints)**:** means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition, it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD value.

PTC = Proof Test Coverage (Diagnostic Coverage for Manual Proof Tests

All failure rates reflect random failures and include failures due to external events, such as unexpected use.
The failure rates are valid for useful life of the considered CM32 Electro-mechanical actuators when operating as defined in the considered scenarios.

FMEDA: CM32 without end position indication – IEC 61508:2010 Failure Rates

	Failure rates (in FIT), Profile 3 data	
Failure category	**Without PVST**	**With PVST [15]**
Safe Detected (λ_{SD})	**0**	**0**
Safe Undetected (λ_{SU})	**44**	**44**
Dangerous Detected (λ_{DD}) [16]	**465**	**924**
Dangerous Detected (λ_{dd})	426	885
Annunciation Detected (λ_{AD})	39	39
Dangerous Undetected (λ_{DU})	**682**	**223**
Annunciation Undetected (λ_{AU})	39	39
No effect	933	933
No part	123	123
PTC	**80%**	**30%**
Total failure rate (safety function)	**1191 FIT**	**1191 FIT**
SFF [17]	**42%**	**81%**
DC	**38%**	**80%**
SIL AC [18]	**---**	**SIL 1**
MTBF(in years)	50	50

[1] **Type A element**: Non-Complex element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2

[2] **Type B element**: Complex element (using microcontrollers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

[15] **PVST:** Partial Valve Stroke Test shall be performed at a rate at least ten times faster than the expected demand rate and carried out via the fail-safe mechanism

[16] **Torque/Force:** switch signal and end position signals are monitored by a safety PLC (control unit)

[17] **SFF:** The complete final element subsystem will need to be evaluated to determine the overall safe failure fraction. Number listed is for reference only.

[18] **SIL AC** (architectural constraints)**:** means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition, it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD value.

PTC = Proof Test Coverage (Diagnostic Coverage for Manual Proof Tests

All failure rates reflect random failures and include failures due to external events, such as unexpected use.
The failure rates are valid for useful life of the considered CM32 Electro-mechanical actuators when operating as defined in the considered scenarios.

Intended Use:
Internal company quality management system ensures information on safety related systematic faults which become evident in the future.
User manual should be observed
Safety manual should be observed

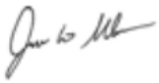
Actuator Series for CM32:

CM32 is included in this report.

Terms and Definitions:

DC	Diagnostic Coverage of dangerous failures (DC = λ_{dd} / (λ_{dd} + λ_{du}))
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test
	It is assumed that the Partial Stroke Testing, when performed, is performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Stroke Testing also has an impact on the Safe Failure Fraction.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A element	"Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.
Type B element	"Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

Quality Director



Justin DeClue

General Manager

Fayyad Sbaihat