FLOWSERVE

MXa SIL Guidance and Certification

SIL 3 capable for critical applications

Experience In Motion

Functional Safety in Plants

Safety and instrumentation engineers demand that a functional safety system's probability of dangerous failures be greatly reduced in order to minimize the risk to humans and the environment. Functional safety can be defined as a safety function which insures that, when a device failure occurs, the device performs in a manner so as not to jeopardize plant safety. This means that the device performs its intended function when called upon (Emergency Shut Down or ESD mode) or its lack of performance (stay-put mode) does not increase the risk of further failure. A method for determining exposure levels of functional safety is defined in IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. It is complemented by IEC 61511, Functional safety — Safety Instrumented Systems for the Process Industry Sector. These two standards are used to aid engineers in designing systems that are functionally safe.

Safety Integrity Levels

Functional safety is vital in applications with potential to expose people and expensive equipment to random failures and their ramifications. This is especially true for equipment that employs microprocessors and programmable logic. Users want not only assurances, but also hard proof that confirms the equipment purchased for critical safety installations is safe, meeting the stipulations of IEC 61508. Plant operational functional safety categories are referred to as "SIL", or Safety Integrity Level, a measurement of risk reduction beginning with level 1 and ascending to level 4. Each category change, level 1 to level 2 for example, reduces the risk by a function of 10, as seen below:

SIL	PFD_{avg}	RRF (Risk Reduction Factor)
4	10^{-5} ... < 10^{-4}	10 000 to 100 000
3	10^{-4} ... < 10^{-3}	1000 to 10 000
2	10^{-3} ... < 10^{-2}	100 to 1000
1	10^{-2} ... < 10^{-1}	10 to 100

Safety Instrumented Systems and Probability of Failure on Demand

Each device installed into a Safety Instrumented System (SIS) should be evaluated independently to determine its FMEDA (Failure Modes Effects and Diagnostic Analysis) and subsequent safety tolerance values. Electric actuators do not, by themselves, comprise an SIS, but are an integral subset of others devices, i.e., typically a sensor of some nature (e.g., pressure sensor), a PLC or DCS (host device that receives the sensor input and outputs safety signal) and an operator, which may consist of a valve and an actuator. The components of an SIS should each have a SIL capable rating that enables a safety engineer to select the individual devices based upon their respective average Probability of Failure on Demand (PFD). PFD is the probability that a device will **not** function when called upon in an SIS. The average PFD for each device is added together to total the system PFD. This SIS total determines the overall SIL rating for the system in question. Selecting a low average PFD for each component in the SIS increases the risk tolerance of the safety system.

Electronic Actuators and SIL

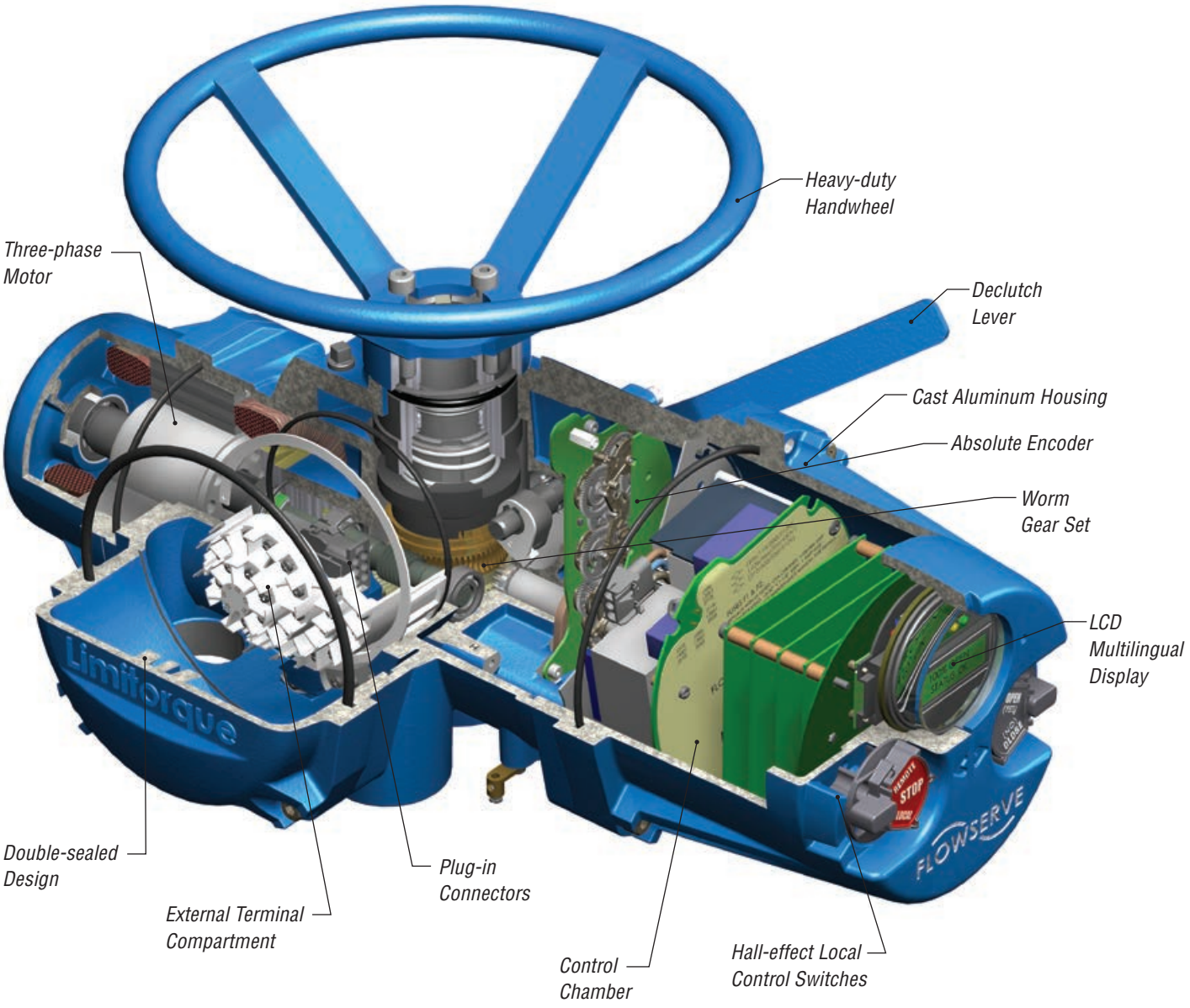
Electronic actuators are classified as type B, complex devices or devices containing microprocessors, microcontrollers, and ASICs by IEC 61508. Some electronic actuator manufacturers supply separate hardware devices to bypass their internal microprocessors in order to acquire SIL certification. Flowserve Limitorque's MXa is SIL certified without adding unique hardware modules, meaning that another potential point of failure is removed from the safety system. It is SIL 3 capable in "as built" configuration. In fact, when compared to other actuator providers, the MXa's PFD (Probability of Failure on Demand) is the lowest in the industry for a type B, complex device. The PFD can be improved by regularly exercising the actuator. This can be accomplished by performing a partial stroke test (PST), which is standard configuration for the MXa. It is highly recommended that a monthly PST be performed to improve the average PFD of the MXa.

For the MXa, SIL 2 is identified as Basic ESD and PST (moves when commanded) in a "1oo1" configuration (one out of one means that only one actuator is required to ensure the SIL 2 requirement is achieved). SIL 3 identified as Stay-put (no unsolicited movement), Enhanced ESD and PST in a "1oo2" configuration (one out of two means that redundant actuators and valves are required to ensure the SIL 3 requirement is achieved).

	Proof Test Interval		
Mission Time	1 year	3 years	5 years
10 yr	2.96 E-3	5.93 E-3	9.52 E-3
15 yr	3.22 E-3	6.51 E-3	9.77 E-3
20 yr	3.47 E-3	6.60 E-3	1.00 E-2

PFD table for MXa based upon monthly PST (Partial Stroke Test)

MX Multi-turn Smart Actuator



MXa—up to SIL 3 capable, even when option boards are installed!

MXa and SIL Certification

The SIL certification for the basic MXa, awarded by exida® Certification Services, now includes a suite of option boards which meet the requirements for systematic integrity up to SIL 3. A SIL 2 or SIL 3 capable MXa can include even network protocol field units, e.g., Foundation Fieldbus H1, Profibus DP & PA, DeviceNet HART and Modbus DDC. The MXa is identified as SIL 3 capable, meaning it is suitable for any safety integrity levels up to SIL 3, even with analog or digital out PCBs, or if installed into an arctic environment down to (-60°C). Please note that to meet the requirements of exida Certification for the SIL 2 or SIL 3 capable MXa the electronic actuator must be installed, configured and operated, and PST performed at regularly defined intervals. Please consult SIL Safety Manual, LMENIM2350, located on www.limitorque.com for complete instructions.

MXa and Failures in Time

For the user this means an MXa can be ordered with any combination of option boards, including network protocol field units, with the added confidence that each option has been analyzed by exida Certification. exida performed an FMEDA analysis for both the basic MXa and its associated option boards. Each option board was supplied an FIT (Failure in Time) calculation. A device failure is classified by IEC 61508 as a particular event which impacts proper and expected performance when requested. Failures In Time (FIT) is an indication of the number of failures in 10^9 hours, or approximately 114 000 years. So, an FIT of "1" would mean one failure can be expected every 114 000 years. The symbol used for the FIT calculation is Lambda (λ), and the subscript indicates the mode of failure, safe or dangerous, detected or undetected. The different classifications of "failures" and the expected response of an actuator are defined below:

- Fail-safe mode = Failure that causes the device to go to its defined fail-safe state without a demand from the process
  - ESD Mode = State in which the device is driven to its defined safe state (either open or close)
  - Stayput mode = State in which the actuator does not move (stays put)
- Safe detected = number of safe, detected failures in 10^9 hours. (λSD)
- Safe undetected = number of safe, but undetected failures in 10^9 hours (λ_{SU})
- Fail dangerous, detected = Failure that is potentially dangerous and is diagnosed by device diagnostics in 10^9 hours. (λ_{DD})
- Fail dangerous, undetected = Failure that is potentially dangerous and is not diagnosed by device diagnostics in 10^9 hours (λ_{DU})

The FIT for the MXa option boards are:

Failures in Time (FIT) of MXa Option Boards

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}
Arctic Option – ESD Mode	0	0	0	6
Backup Power Board – Stayput Mode	3	0	0	0
UPS Power Board – Stayput Mode	5	0	0	0
Analog Option Board – Stayput Mode	53	0	9	0
HART Board – Stayput Mode	51	0	9	0
HART Board – ESD Mode	0	0	60	0
DeviceNet Board – Stayput Mode	9	0	6	0
Foundation Fieldbus Board and Profibus PA – Stayput Mode	47	0	0	10
MODBus Board – Stayput Mode	7	0	6	0
ProfiBus DP Board – Stayput Mode	47	0	0	10
ProfiBus PA Board – ESD Mode	0	0	57	0
Relay Option Board – NI – Stayput Mode	11	0	6	0
Relay Option Board – Monitor – Stayput Mode	112	2	119	2
Arctic Option – Stayput Mode	0	9	0	0

MXa, Safe Failure Fraction (SFF), and Hardware Fault Tolerance (HFT)

The FIT for each option board can be used to develop a safety system's safe failure fraction (SFF) equation. An SFF is expressed in percent of safe failures which correspond to the overall failure rate. A high SFF value lowers the probability of a dangerous event impacting the SIS, e.g., 75% SFF is better than 50%.

The SFF determines the range of acceptable hardware fault tolerance (HFT) for the safety instrumented system. An HFT is the device's capability of acting on a safety signal in spite of system faults. The MXa and its suite of option boards has a Hardware Fault Tolerance of "0", as determined by exida Certification. This means that, for a SIL 2 application, the MXa with any combination of option boards having an HFT of "0" can be installed into an SIS requiring an SFF range from 90% to < 99%. For an SIL 3 application, redundant MXa actuators with any combination of option boards can be installed into an SIS requiring an SFF of >/= 99%.

MXa SIL Advantages

Advantages of the SIL certification for the MXa include continued torque and position protection, even when a safety event occurs. Also, the need to use external devices to track the position of the actuator is removed—the MXa's reliable Limigard feature insures the user's connection to the actuator's internal relays do not need to be bypassed. No peripheral wiring is required to isolate the actuator from its internal programmable logic for safe operation. The internal safeguard features of the MXa are sufficient to report the actuator status and respond when an ESD is asserted.

The addition of the option boards and arctic temperature components indicates Flowserve Limitorque's continued commitment to providing the safest, most reliable electronic actuator in the industry.

Glossary:

- ESD = Emergency Shut Down – configuration of an actuator so that it enters a "safe state" when plant control issues an emergency signal.
- SIL = Safety Integrity Level – relative level of risk reduction required for a Safety Instrumented Function (SIF). SIL is generally identified by levels of risk reduction, where SIL 1 is the least dependable classification to SIL 4, the most dependable classification.
- SIF = Safety Instrumented Function – the specific control functions performed by a Safety Instrumented System (SIS).
- SIS = Safety Instrumented System – generally, a system that is instrumented with hardware and software which are specifically used in critical process applications. They may consist of a process monitoring device that is connected to a programmable logic device that transmits to equipment that controls the safety and reliability of the process.
- FMEDA = Failure Modes Effects and Diagnostic Analysis – generally a procedure to determine in detail the causes of errors and their impact on a system.
- PFD = Probability of Failure on Demand – the probability that a device will not safely function when a dangerous failure occurs.
- PST = Partial Stroke Test – a test scenario which partially strokes the actuator/valve combination when enabled. Its purpose is to routinely actuate a valve in order to preclude or diagnose a potentially dangerous undetected event before it occurs.
- FIT = Failures in Time – generally defined as the frequency of failure for an engineered system or component, expressed in hours. For SIL evaluations, FIT is expressed in number of events in 10^9 hours.
- SFF = Safe Failure Fraction – expressed in percent of safe failures which correspond to the overall failure rate, e.g., SFF = $\{1-(\lambda_{DD}\ (\lambda_{DD}) + (\lambda_{SD}) + (\lambda_{SU}) + (\lambda_{DU})\}$
- HFT = Hardware Fault Tolerance – the ability of the device to act upon a valid safety signal in spite of system faults. It is expressed in percentage.
- RRF = Risk Reduction Factor – the amount of reduction in risk gained by specifying an increase in SIL levels. An increase of one level (SIL 1 to SIL 2) reduces the RRF by a function of ten (10).


Certificate / Certificat
Zertifikat / 合格証
FLO 0810012 C001
exida hereby confirms that the:
MXa Electronic Valve Actuator and Option Boards
Flowserve Limitorque Lynchburg, VA - USA
Has been assessed per the relevant requirements of:
IEC 61508 : 2010 Parts 1-7
and meets requirements providing a level of integrity to:
Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B, Route 1_H Device
PFD_{avg} and Architecture Constraints must be verified for each application
Safety Function:
The Electronic Valve Actuator will move to the designed safe state per the actuator design within the specified safety time.
Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.
Evaluating Assessor
Certifying Assessor
Revision 2.4 April 7, 2016
Surveillance Audit Due July 1, 2018
ANSI Accredited Program PRODUCT CERTIFICATION #1064


Certificate / Certificat / Zertifikat / 合格証
FLO 081012 C001
Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B, Route 1_H Device
PFD_{avg} and Architecture Constraints must be verified for each application
MXa Electronic Valve Actuator and Option Boards
Systematic Capability:
The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.
Random Capability:
The SIL limit imposed by the Architectural Constraints must be met for each element.
The following option boards are covered by this certification: Backup Power Board, UPS Power Board, Analog Option Board, HART Board, DeviceNet Board, Foundation Fieldbus Board, MODBus Board, ProfiBus DP Board, Profibus PA Board, Relay Option Board – NI, and Relay Option Board – Monitor. The failure rates for these options are contained in the assessment and FMEDA reports.
SIL Verification:
The following documents are a mandatory part of certification:
Assessment Report: FLO 08-10-12 R002 V2 R4
Safety Manual: FCD LMENIM2350-01 – 9/13

For more information on the features, options and certifications of the Limitorque MX, consult Flowserve bulletin LMENBR2302.

www.limitorque.com

Flowserve Corporation
Flow Control

United States
Flowserve Limitorque
5114 Woodall Road
P.O. Box 11318
Lynchburg, VA 24506-1318
Phone: 434-528-4400
Facsimile: 434-845-9736

England
Flowserve Limitorque
Euro House
Abex Road
Newbury
Berkshire, RG14 5EY
United Kingdom
Phone: 44-1-635-46999
Facsimile: 44-1-635-36034

Japan
Limitorque – Nippon Gear Co., Ltd.
NOF Bldg. 9th Floor
1-11-11, Kita-Saiwai, Nishi-Ku
Yokohama (220-0004)
Japan
Phone: 81-45-326-2065
Facsimile: 81-45-320-5962

Singapore
Flowserve Limitorque
12, Tuas Avenue 20
Singapore 638824
Phone: 65-6868-4628
Facsimile: 65-6862-4940

China
Limitorque Beijing, Pte., Ltd.
RM A1/A2
22/F, East Area, Hanwei Plaza
No. 7 Guanghua Road, Chaoyang District
Beijing 100004, Peoples Republic of China
Phone: 86-10-5921-0606
Facsimile: 86-10-6561-2702

India
Flowserve Limitorque, Ltd.
Plot No 4
Export Promotional Industrial Park
Whitefield, Bangalore 560066
India
Phone: 91-80-40146200
Facsimile: 91-80-28410286

FCD LMENFL2351-02 May 2016