SIL for FSE Actuator

Safety manual

SUG_19003_EN - Ind. B
Art : 5100710

TABLE OF CONTENTS

1 Introduction

1.1 Scope and purpose of the Safety Manual

This safety manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Bernard Controls FSE SELF CONTAINED ELECTRO-HYDRAULIC ACTUATOR.

This safety manual provides necessary requirements to enable the integration of the Bernard Controls FSE SELF CONTAINED ELECTRO-HYDRAULIC ACTUATOR when showing compliance with the IEC 61508 or IEC 61511 functional safety standards

It indicates all assumptions that have been made on the usage of the Bernard Controls FSE SELF CONTAINED ELECTRO-HYDRAULIC ACTUATOR. If these assumptions cannot be met by the application, the SIL capability of the Bernard Controls FSE SELF CONTAINED ELECTRO-HYDRAULIC ACTUATOR may be adversely affected.

1.2 Skill level required

System design, installation and commissioning, and repair and maintenance shall be carried out by suitably qualified personnel.

1.3 Terms, abbreviations and acronyms

Basic Safety
Freedom from unacceptable risk of harm.

BPCS
Basic Process Control System - a system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1.

Fail-safe State
State where FSE ESD solenoid valve is de-energized and the actuator spring is extended to move the attached valve.

Fail Annunciation Detected
Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.

Fail Annunciation Undetected
Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.

Fail Dangerous
Failure that does not respond to a demand from the process (i.e. being unable to go to the fail-safe state).

Fail Dangerous Detected
Failure that is dangerous but is detected as part of partial valve stroke testing.

Fail Dangerous Undetected
Failure that is dangerous and that is not detected as part of partial valve stroke testing.

Fail No Effect
Failure of a component that is part of the safety function but that has no effect on the safety function.

Fail Safe
Failure that causes the FSE to move the attached valve to go to the defined fail-safe state without a demand from the process.

FMEDA
Failure Modes, Effects and Diagnostics Analysis.

Functional safety
Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers.

FSE Actuator
Bernard Controls FSE SELF CONTAINED ELECTRO-HYDRAULIC ACTUATOR

HFT
Hardware Fault Tolerance

Low demand
Mode of operation, where the frequency of demands for operation made on a safety- related system is no greater than twice the proof test frequency.

MOC
Management of Change - specific procedures often done when performing any work activities in compliance with government regulatory authorities.

PFDAVG
Average Probability of Failure on demand.

PVST
Partial Valve Stroke Test.

SFF
Safe Failure Fraction - fraction of the overall random failure rate of a device that results in either a safe failure or a detected dangerous failure

SIF
Safety Instrumented Function - safety function with a specified SIL which is necessary to achieve functional safety. Typically a set of equipment intended to reduce the risk due to a specified hazard (a safety loop).

SIL
Safety Integrity Level - discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest level of safety integrity; SIL 1 has the lowest.

SIS
Safety Instrumented System - instrumented system used to implement on or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

1.4 Product Support & Service

Please refer to the contact information on the back cover of this document.

1.5 Related Documents

Hardware documents:

- Bernard Controls FSE Actuator Datasheet and Catalogue
- Bernard Controls Maintenance and installation manual (SUG_19002)

Guidelines/References:

- FMEDA report – ROT 18/03-043 R001

1.6 Reference standards

IEC 61508:2010
Functional Safety of Electrical/Electronic/Program-mable Electronic Safety-Related Systems

2 FSE Actuator Descriptions

With the combination of modern electronics and power of hydraulics, FSE series is super-efficient in providing precise control for high cyclic demand or ESD application. FSE series actuators are suitable for use in system integrated system (SIS). It has functional safety capability including and up to SIL 2 & SIL 3 to IEC 61508:2010.

FSE Actuator is suitable for rotary application. It can be customized to suit a given application. FSE series of actuator has an integral electronic control module which drives the electrical motor, pump and solenoid for operations. The logical module is responsible for diagnostics, alarms, fault messages and communication.

FSE Actuator can be specified to fail-safe close, open or as fail freeze based on emergency shut-down demand. It can be equipped with potential free switch for independent feedback and alarm status.

3 Designing a SIF using the FSE Actuator

3.1 Safety Function

The safety function for the FSE Actuator and the additional components in the subsystem is to move the attached valve to the safe position (which can be either open or closed as required by the application) within the specified safety time when the system is tripped.

3.2 Environmental limits

The designer of the **SIF** must check that the product is rated for use within the expected environmental limits, maximum working pressure and temperature.

Refer to the FSE Actuator datasheet for this information.

3.3 Application limits

The materials of construction of a FSE Actuator are specified in the FSE Actuator datasheet. It is especially important that the designer of the **SIF** checks for material compatibility considering on-site chemical contaminants and air/hydraulic (as appropriate) supply conditions. If the FSE Actuator is used outside the application limits or with incompatible materials, the reliability data and predicted SIL capability becomes invalid.

3.4 Design Verification

A detailed Failure Modes, Effects and Diagnostics Analysis (**FMEDA**) report is available for this product. This report details all failure rates and failure modes as well as expected lifetime of the product.

The achieved Safety Integrity Level (**SIL**) of an entire Safety Instrumented Function (**SIF**) design must be verified by the designer via a calculation of **PFDAVG** considering the architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failures rates of all equipment included in the **SIF**. Each subsystem must be checked to assure compliance with minimum Hardware Fault Tolerance (**HFT**) requirements.

When using the FSE Actuator in a redundant configuration, a common cause factor of at least 5% should be included in the safety integrity calculations.

The failure rate data listed in the **FMEDA** report is only valid for the useful lifetime of the FSE Actuator. The failure rates will increase after this useful lifetime period has expired. Reliability calculations based on the data listed in the **FMEDA** report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated SIL will not be achieved.

3.5 SIL Capability

3.5.1 Systematic Integrity

The FSE Actuator 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** higher than the statement without "prior use" justification by the end user, or verification of diverse technology in the design.

3.5.2 Random Integrity

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1H approach according to 7.4.4.2 of IEC 61508 or the 2H approach according to 7.4.4.3 of IEC 61508.

The 1H approach involves calculating the SFF for the entire element.

The 2H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508. The FSE actuator is classified as a device that is part of a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

The FSE actuator can be classified as a 2H device when the failure rates listed in the **FMEDA** report are used for the Design Verification calculations. When 2H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to **SIL** 2 at **HFT**=0 (or **SIL** 3 @ **HFT**=1) per Route 2H. If Route 2H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1H.

When the final element assembly consists of several components additional to FSE Actuator, the SIL must be verified for the entire assembly using the failure rates of all components. This analysis must account for architectural constraints by comparing both **SFF** and **HFT** with IEC61508-2, Table 2 if following Route 1H.

3.5.3 Safety Parameters

For detailed failure rate information refer to the FMEDA report ROT 18/03-043 R001.

3.6 Connection of the FSE actuator to the SIS Logic Solver

The FSE actuator should be assembled with a logic solver where all components are safety rated. The safety rated logic solver shall initiate the safety function as well as automatic diagnostics (if any) designed to diagnose potentially dangerous failures within the Bernard Controls FSE self-contained electro-hydraulic actuator, (i.e. partial valve stroke test).

3.7 General Requirements

The system and function response time shall be less than the process safety time. The FSE Actuator will move to its defined safe state in less than this time with relation to the specific hazard scenario. All **SIS** components including the FSE Actuator must be operational before process start-up. The User shall verify that the FSE Actuator is suitable for use in safety applications by confirming the FSE Actuator nameplate and model number is properly marked.

Personnel performing maintenance and testing on the FSE Actuator shall first be assessed as being competent to do so.

Results from periodic proof tests and partial valve stroke tests (if any) shall be recorded and periodically reviewed. The FSE Actuator shall not be operated beyond the useful lifetime as listed in paragraph 5.3 without undergoing overhaul or replacement.

IEC 61508 Failure Rates in FIT

(FIT = 1 failure per 10^9 hours)

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
FSE ESD function Stay Put on Loss of Power	0	1082	0	528

4 Installation & Commissioning

4.1 Installation

The FSE Actuator must be installed per the standard practices outlined in the Maintenance and Installation Instructions. The environment must be checked to verify that environmental conditions do not exceed the ratings. The FSE Actuator must be accessible for physical inspection.

4.2 Physical location and placement

The FSE Actuator shall be accessible with sufficient room for electrical connections to the actuator and shall allow for manual proof testing taking place. The FSE Actuator shall be mounted in a low vibration environment. If excessive vibration can be expected then special precautions shall be taken to ensure the integrity of hydraulic connections or the vibration should be reduced using appropriate damping mounts.

4.3 Electrical Connections

WARNING

Ensure all power supplies are isolated before removing actuator covers.

Check that the supply voltage agrees with that stamped on the actuator nameplate.

A switch or circuit breaker must be included in the wiring installation or the actuator. The switch or circuit breaker must meet the relevant requirements of IEC60947-1 and IEC60947-3 and be suitable for the application. The switch or circuit breaker must not disconnect the protective earth conductor. The switch or circuit breaker must be mounted as close to the actuator as possible and shall be marked to indicate that it is the disconnect device for that particular actuator. The actuator must be protected with a suitably rated overcurrent protection device. Power supply cables must have sufficient mechanical protection properties to meet installation requirements

and be screened to comply with EMC requirements of the installed actuator. Suitable methods include armoured and/or screened cables or cables contained within conduit.

5 Operation & Maintenance

5.1 Proof Test requirement

During operation, a low demand mode **SIF** must be periodically proof tested. The objective of proof testing is to detect failures within the equipment in the **SIF** that are not detected by any automatic diagnostics of the system. Of main concern are undetected failures that prevent the **SIF** from performing its function. Periodic proof tests shall take place at the frequency (or interval) defined by a SIL verification calculation. The proof tests must be performed more frequently than (or as frequently as) specified in the SIL verification calculation in order to maintain the required safety integrity of the overall **SIF**. Results from periodic proof tests and partial valve stroke tests (if any) shall be recorded and periodically reviewed.

For detailed Proof Test information refer to the FMEDA report ROT 18/03-043 R001.

5.2 Repair and replacement

Repair procedures outlined in the Maintenance and Installation Instructions must be followed.

5.3 Useful life

Based on general field failure data and a low demand mode of operation, a useful life period of approximately 10 to 15 years is expected for the FSE Actuator

5.4 Notification of failures

In case of malfunction of the system or SIF, the FSE Actuator shall be put out of operation and the process shall be kept in a safe state by other measures. Bernard Controls must be informed (see back cover for contact information) when the FSE Actuator is required to be serviced, repaired or replaced due to failure. The occurred failure

shall be documented and reported to Bernard Controls representative. Contact details are on the back cover of this safety manual.

6 Restriction of use

For use of actuator, wherein ambient temperature is more than 50 °C, consult Bernard Controls prior to use.

BERNARD CONTROLS GROUP

CORPORATE HEADQUARTERS

4 rue d'Arsonval - CS 70091 / 95505 Gonesse CEDEX France
Tel. : +33 (0)1 34 7 71 00 / Fax : +33 (0)1 34 07 71 01 / mail@bernardcontrols.com

CONTACT BY OPERATING AREAS

> AMERICA

NORTH AMERICA
BERNARD CONTROLS UNITED STATES
HOUSTON
inquiry.usa@bernardcontrols.com
Tel. +1 281 578 66 66

SOUTH AMERICA
BERNARD CONTROLS LATIN AMERICA
inquiry.southamerica@bernardcontrols.com
Tel. +1 281 578 66 66

>ASIA

CHINA
BERNARD CONTROLS CHINA &
BERNARD CONTROLS CHINA NUCLEAR
BEIJING
inquiry.china@bernardcontrols.com
Tel. +86 (0) 10 6789 2861

KOREA
BERNARD CONTROLS KOREA
SEOUL
inquiry.korea@bernardcontrols.com
Tel. +82 2 553 6957

SINGAPORE
BERNARD CONTROLS SINGAPORE
SINGAPORE
inquiry.singapore@bernardcontrols.com
Tel. +65 65 654 227

> EUROPE

BELGIUM
BERNARD CONTROLS BENELUX
NIVELLES (BRUSSELS)
inquiry.belgium@bernardcontrols.com
inquiry.holland@bernardcontrols.com
Tel. +32 (0)2 343 41 22

FRANCE
BERNARD CONTROLS FRANCE &
BERNARD CONTROLS NUCLEAR FRANCE
GONESSE (PARIS)
inquiry.france@bernardcontrols.com
Tel. +33 (0)1 34 07 71 00

GERMANY
BERNARD CONTROLS DEUFRA
TROISDORF (KÖLN)
inquiry.germany@bernardcontrols.com
Tel. +49 2241 9834 0

ITALY
BERNARD CONTROLS ITALIA
RHO (MILANO)
inquiry.italy@bernardcontrols.com
Tel. +39 02 931 85 233

RUSSIA
BERNARD CONTROLS RUSSIA
inquiry.russia@bernardcontrols.com
Tel. +33 (0)1 34 07 71 00

SPAIN
BERNARD CONTROLS SPAIN
MADRID
inquiry.spain@bernardcontrols.com
Tel. +34 91 30 41 139

> INDIA, MIDDLE EAST & AFRICA

AFRICA
BERNARD CONTROLS AFRICA
ABIDJAN - IVORY COAST
inquiry.africa@bernardcontrols.com
Tel. + 225 21 34 07 82

INDIA
BERNARD CONTROLS INDIA
inquiry.india@bernardcontrols.com
Tel. +971 4 880 0660

MIDDLE-EAST
BERNARD CONTROLS MIDDLE-EAST
DUBAI - U.A.E.
inquiry.middleeast@bernardcontrols.com

BERNARD® CONTROLS

www.bernardcontrols.com