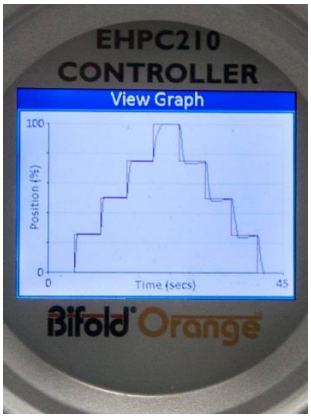
SIL – SM.014 Rev 0

EHPC210 Valve Controller

Compiled By : G. Elliott, Date: 15/11/17



Bifold Group
Bifold
Bifold FluidPower
Bifold Subsea
Bifold Marshalsea

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Innovative and Reliable Valve & Pump Solutions

Contents

Terminology Definitions 3
Acronyms & Abbreviations 4

1. Introduction 5
   1.1 Scope 5
   1.2 Relevant Standards 5
   1.3 Other related documents and papers 5
2. Device Description 5
   2.1 Safety Function 5
   2.2 Environmental Limits 5
   2.3 Application Limits 5
   2.4 Design Verification 5
   2.5 SIL Capability 6
   2.5.1 Systematic Integrity 6
   2.5.2 Random Integrity 6

3. Installation & Commissioning 7
   3.1 Installation 8
   3.2 Proof testing 8
   3.3 Repair & Replacement 9
   3.4 Useful Life 9
   3.5 Reporting Concerns to Bifold 9

Terminology Definitions:

Description	Explanation
Safety:	Freedom from unacceptable risk of harm
Functional Safety:	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment / machinery / plant / apparatus under control of the system.
Basic Safety:	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition.
Safety Assessment:	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems.
Fail-Safe State:	**The EHPC210 is non-interfering with a deenergise to trip safety function**
Safe Failure	Failure that causes the system to go to the defined fail-safe state without a demand from the process.
Dangerous Failure	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Dangerous Undetected Failure	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Dangerous Detected:	Failure that is dangerous but is detected by automatic stroke testing.
Fail Annunciation Undetected	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 Detected:	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 No Effect:	Failure of a component that is part of the safety function but that has no effect on the safety function.
Low demand mode:	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Acronyms / Abbreviations

Acronym / Abbreviation	Description	Explanation
CCF	Common Cause Failure	A common cause failure is one in which a single failure or condition affects the operation of multiple devices that would otherwise be considered independent. Common cause failures can result in the SIS failing to function when there is a process demand.
FITS	Failures in Time	The number of failures that can be expected in one billion (10^9) device-hours of operation.
FMEDA	Failure Modes, Effects & Diagnostics Analysis	A method of assessing a hardware device in order to predict failure rates and hence determine the applicable SFF.
HFT	Hardware Fault Tolerance	Ability of a functional device to continue to perform a required function when faults or errors are prevailing.
LOPA	Layers of Protection Analysis	LOPA is a methodology for hazard evaluation and risk assessment.
MTBF	Mean Time Between Failures	Mean time Between Failures. (1/ λ).
MTTR	Mean Time To Repair	Mean time between the occurrence of an error in a unit or system and its repair.
OIM	Operation & Installation Manual	Information on correct installation, maintenance and testing.
PFD	Probability of Failure on Demand	Probability of failures for a safety function on demand
PFDavg	Average Probability of Failure on Demand	Average Probability of failures for a safety function on demand
PTI	Proof Test Interval	The time between diagnostic testing or Partial Stroke Testing.
SIL	Safety Integrity Level	The international standard IEC61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for the failure of a safety function. The higher the SIL level the lower the probability that they will not perform the required safety function
SFF	Safe Failure Fraction	The proportion of non-hazardous failures.
λ	Failure Rate	Failure Rate – the ratio of the total number of failures in a given time period
λD	Dangerous Failure Rate	Failure Rate of Dangerous failures (per hour).
λDD	Dangerous Detected Failure rate	Failure Rate of Dangerous failures detected by diagnostic testing (per hour).
λDU	Dangerous Undetected Failure Rate	Failure Rate of Dangerous failures Undetected by diagnostic testing (per hour).
λS	Safe Failure Rate	Failure Rate of Safe failures (per hour).

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

1. Introduction

1.1 Purpose & Scope

This manual provides the results of a functional safety assessment by Exida Consulting in accordance with IEC61508: ed2: 2010.

The results of this provides the safety instrumentation engineer with the required failure data as per IEC61508 / IEC 61511, and confidence that sufficient attention has been given to systematic failures during the development of the device.

1.2 Relevant Standards

IEC 61508 (Parts 1 – 7) Ed2: 2010 - Functional Safety of Electrical /Electronic/Programmable Electronic Safety-Related Systems.

1.3 Other Related documents and papers

Device	Document ID	Document Type
EHPC210	ORM0012	Operating & Installation Manual
EHPC210	31 - Electro Hydraulic Power pack catalogue	Product Catalogue

2. Device Description

The EHPC210 Universal Controller allows the same platform to be used for hydraulic and pneumatic positional and Partial Stroke Test actuator systems. This incorporates graphic display, bluetooth communications, integral valve feedback measurement, low power modes, ESD monitoring and control, Partial Stroke Test and local control setting switch. The enclosure assembly allows installation in zone 1 or 2 hazardous areas.

The system monitors an incoming command signal and controls the operation of the hydraulic or pneumatic system opening and closing solenoids to position the actuator according to the actuator feedback position signal. The Universal Controller provides the correct fault action on loss of signals and / or power.

The Universal Controller positions a hydraulic or pneumatic actuated control valve from 0.25% accuracy with a resolution of 0.1% from the 4-20mA control signal. The valve actual position signal being available to the clients control system in the form of a 4-20mA signal externally powered.

The Universal Controller allows configuration by the user of the response tuning, actuator operation, clock, valve position calibration, valve feedback setting, analogue input setting and calibration, viewing faults and events, fault action setup, controller feedback, I/O configuration and monitoring, and pump control.

Partial Test: On receiving a command to carry out a Partial Stroke Test the Universal Controller will move the actuator to a preset position (typically 85% of open), a short pause, and then return to the fully open position.

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

During the Partial Stroke Test, with the addition of a pressure transmitter in the actuator control circuit, the pressure is recorded during the breakaway. This is used to measure the static friction in the valve. The Universal Controller will record the data during the test, the data will also be available for remote use via the Bifold app and HART communication.

2.1 Safety Function

In the event of the ESD Solenoid being de-energised this will overtake all other operation. The EHPC210 monitors the users ESD signal to the valve via an isolated safety relay ensuring this does not affect the ESD SIL rating. The EHPC210, therefore, has no specific Safety Function, other than to facilitate Partial Stroke Testing. The test exercises the solenoids and the valve to confirm they will operate in a shutdown situation. The EHPC210 performs a number of system tests during the operation of a partial test which are set up during commissioning.

The EHPC210 is non-interfering with a de-energise to trip safety function

The EHPC210 is designed to be part of a final element subsystem as defined by IEC61508 and the achieved SIL level of the designed function must be verified by the system designer.

2.2 Environmental Limits

The designer of a SIF must verify that the product is rated for use within the expected environmental limits.

For SIL rated devices the minimum operating temperature is -40°C.

Refer to Bifold Product Catalogue for more information.

2.3 Application Limits

The materials of construction are specified in the various Bifold Catalogues and Data Sheets. Maximum Operating Pressure is up to N/a.

2.4 Design Verification

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

2.5 SIL Capability

2.5.1 Systematic Integrity

The product has met manufacturers 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 the statement without “prior use” justification by end user or diverse technology redundancy in the design.

2.5.2 Random Integrity

The EHPC210 is non-interfering with a de-energise to trip safety function

3.0 Installation and Commissioning

3.1 Installation

The device must be installed per standard practices outlined in the Installation Manual. The environment must be checked to ensure that environmental conditions do not exceed the ratings.

The device must be accessible for physical inspection.

3.2 Proof Testing

The System should be subjected to a full test at least once every 12 months (or more frequently based on the desired PFDavg calculations – Ref Section 2.4). This would normally be conducted as part of a proof test or partial stroke test for the actuator under control. Partial stroke testing of the Safety Instrumented Function (SIF) must provide a full test of the device.

According to section 7.4.3.2.2 f) of IEC61508-2, proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

3.2.1 Suggested Proof Test

Proof testing is not applicable for the EHPC210 since the unit is non-interfering.

3.3 Repair and Replacement

Repair procedures must be implemented as per the Operation, Installation and Maintenance Manual for the device.

The SIL rating of the device will be voided if the repair is not performed with Genuine Bifold parts and serviced by a competent person.

3.4 Useful Lifetime for the Device.

The useful lifetime of the EHPC210 Valve Controller is 20 Years.

3.5 Reporting Concerns to Bifold

All faults to be reported to Bifold for recording purposes, by contacting the Quality Department at the supplying facility listed at the bottom of the page. All defective devices must be returned to Bifold for investigation and rectification by the Manufacturer. A Valve Return and Service Report form (VRSR) – available upon request, from the supplying facility - (Contact details at the foot of this page) must be completed and returned with the device.