WESTLOCK CONTROLS

DIGITAL EPIC 2

SAFETY MANUAL

Before installation these instructions must be fully read and understood

TABLE OF CONTENTS

Safety manual

This document provides a Safety Manual for a Digital EPIC 2. A Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Digital EPIC.

1 INTRODUCTION

This safety manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the D-EPIC2. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.1 Terms and abbreviations

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	An investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems.
Fail-safe state	State where solenoid valve is de-energized and spring is extended.
Fail safe	Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Fail dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail dangerous undetected	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Fail 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 half the proof test frequency.

1.2 Acronyms

FMEDA	Failure modes, effects and diagnostic analysis.
HFT	Hardware fault tolerance.
MOC	Management of change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFDavg	Average probability of failure on demand.
SFF	Safe failure fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIF	Safety instrumented function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety integrity level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and safety integrity Level 1 has the lowest.
SIS	Safety instrumented system - implementation of one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

1.3 Product support
Product support can be obtained from:
Westlock Controls
280 Midland Ave.
Saddle Brook, NJ 07663
USA

1.4 Related literature
Hardware documents:
- D-EPIC2 Installation, Operation and Maintenance Instructions, Document Tech-491Q, Tech-511Q and QUICK START GUIDE VCIOM04592.

Guidelines/references:
- Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, ISBN 978-1-934977-03-3, Exida
- Control System Safety Evaluation and Reliability, 3rd Edition, ISBN 978-1-934394-80-9, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference standards
Functional Safety
- IEC 61508: 2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems.
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector.

2 DEVICE DESCRIPTION

The Digital EPIC Control Transmitter provides precision non-contact valve position feedback. Optional features include partial valve stroke testing.

3 DESIGNING A SIF USING A MANUFACTURER PRODUCT

3.1 Safety function
When used with a de-energize to trip final element subsystem, the D-EPIC2 will not interfere with the ability of the logic solver to bring the final element to its safe state. The D-EPIC2 is intended to be part of a final element subsystem as defined per IEC 61508 and the achieved SIL level of the designed function must be verified by the designer.

3.2 Environmental limits
The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the Westlock Controls D-EPIC2 Brochure for environmental limits.

3.3 Application limits
The materials of construction of a D-EPIC2 are specified in the Westlock Controls D-EPIC2 Brochure. It is especially important that the designer check for material compatibility considering on-site chemical contaminants. If the D-EPIC2 is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

3.4 Design verification
A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Westlock Controls. This report details all failure rates and failure modes as well as the expected lifetime.
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 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. The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the D-EPIC and its failure rates.
The failure rate data listed the FMEDA report are only valid for the useful life time of a D-EPIC2. The failure rates will increase sometime after this time period. 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 Safety Integrity Level will not be achieved.

3.5 Sil capability

3.5.1 Systematic integrity

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 without "prior use" justification by the end user or diverse technology redundancy in the design.

3.5.2 Random integrity

When the final element assembly consists of many components (D-EPIC, actuator, solenoid, quick exhaust valve, etc.) the SIL must be verified for the entire assembly using failure rates from all components. This analysis must account for any hardware fault tolerance and architecture constraints.

3.5.3 Safety parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the D-EPIC2.

3.6 Connection of the D-EPIC to the SIS logic-solver

The D-EPIC is connected to the safety rated logic solver which is actively performing the safety function as well as automatic diagnostics designed to diagnose potentially dangerous failures within the D-EPIC2, (i.e. partial valve stroke test).

3.7 General requirements

The system's response time shall be less than the process safety time.
All SIS components including the D-EPIC2 must be operational before process start-up.
User shall verify that the D-EPIC2 is suitable for use in safety applications by confirming the D-EPIC2's nameplate is properly marked.
Personnel performing maintenance and testing on the D-EPIC2 shall be competent to do so.
Results from the proof tests shall be recorded and reviewed periodically.
The useful life of the D-EPIC2 is listed in Section 5.4 and discussed in the Failure Modes, Effects and Diagnostic Analysis Report for the D-EPIC2.

4 INSTALLATION AND COMMISSIONING

4.1 Installation

The D-EPIC2 must be installed per standard practices outlined in the Installation Manual.
The environment must be checked to verify that environmental conditions do not exceed the ratings.
The D-EPIC2 must be accessible for physical inspection.

4.2 Physical location and placement

The D-EPIC shall be accessible with sufficient room for connections and shall allow manual proof testing.
Pneumatic piping to the final element subsystem shall be kept as short and straight as possible to minimize the airflow restrictions and potential clogging. Long or kinked pneumatic tubes may also increase the valve closure time.
The D-EPIC shall be mounted in a low vibration environment. If excessive vibration can be expected special precautions shall be taken to ensure the integrity of pneumatic connectors or the vibration should be reduced using appropriate damping mounts.

4.3 Proof test without automatic testing

The objective of proof testing is to detect failures within a Westlock Controls D-EPIC2 that are not detected by any automatic diagnostics of the system. Of main concern are undetected failures that prevent the safety instrumented function from performing its intended function.
The frequency of proof testing, or proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which a Westlock Controls D-EPIC2 is applied. The proof tests must be performed at least as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The following proof test is recommended. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to Westlock Controls.
The suggested proof test consists of ensuring the electrical isolation between the D-EPIC2 and the solenoid circuit, see Table 1.

TABLE 1 - SUGGESTED PROOF TEST

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Use digital communications to retrieve any diagnostics and take appropriate action.
3	Disconnect the logic solver and solenoid from their terminal blocks on the D-EPIC2.
4	Ensure that there is no electrical continuity between the 4-20 mA terminals and the logic solver and solenoid terminals
5	Reconnect the logic solver and solenoid to their terminal blocks on the D-EPIC2.
6	Remove the bypass and otherwise restore normal operation.

This test will detect >99% of possible DU failures in the D-EPIC2.
The person(s) performing the proof test of a D-EPIC should be trained in SIS operations, including bypass procedures, valve maintenance and company Management of Change procedures.
No special tools are required.

4.4 Proof test with automatic partial valve stroke testing
An automatic partial valve stroke testing scheme that performs a full stroke of the isolation valves in the D-EPIC2 and measures valve movement timing will detect most potentially dangerous failure modes. It is recommended that a physical and electrical inspection (Table 1) be performed on a periodic basis with the time interval determined by plant conditions. A maximum inspection interval of five years is recommended.

4.5 Repair and replacement
Repair procedures in the D-EPIC2 Installation, Operation and Maintenance manual must be followed.

4.6 Useful life
The useful life of the D-EPIC2 is 50 years.

4.7 Manufacturer notification
Any failures that are detected and that compromise functional safety should be reported to Westlock Controls. Please contact Westlock Controls customer service.

APPENDIX A START-UP CHECKLIST

This appendix provides a Start-up Checklist for a PRODUCT. A Start-up Checklist will provide guidance during PRODUCT deployment.

1 Start-up checklist

The following checklist may be used as a guide to employ the D-EPIC in a safety critical SIF compliant to IEC61508/IEC 61511.

			Verified	
#	Activity	Result	By	Date
	Design			
	Target Safety Integrity Level and PFDavg determined			
	Correct valve mode chosen (Fail-closed, Fail-open)			
	Design decision documented			
	Pneumatic compatibility and suitability verified			
	SIS logic solver requirements for valve tests defined and documented			
	Routing of pneumatic connections determined			
	SIS logic solver requirements for partial stroke tests defined and documented			
	Design formally reviewed and suitability formally assessed			
	Implementation			
	Physical location appropriate			
	Pneumatic connections appropriate and according to applicable codes			
	SIS logic solver valve actuation test implemented			
	Maintenance instructions for proof test released			
	Verification and test plan released			
	Implementation formally reviewed and suitability formally assessed			

			Verified	
#	Activity	Result	By	Date
	Verification and testing			
	Electrical connections verified and tested			
	Pneumatic connection verified and tested			
	SIS logic solver valve actuation test verified			
	Safety loop function verified			
	Safety loop timing measured			
	Bypass function tested			
	Verification and test results formally reviewed and suitability formally assessed			
	Maintenance			
	Tubing blockage / partial blockage tested			
	Safety loop function tested			
	Maintenance			
	Tubing blockage / partial blockage tested			
	Safety loop function tested			

Engineering document reference
This safety manual is based on the latest engineering update, and forms part of the certification for the DEPIC-2 series. To ensure you have the most recent version of this document, please check the document library on our website (westlockcontrols.com).

Translations
Where translated the copy is taken from the original English document VCOSI-04978-EN as checked by the relevant certification body and therefore the original English document will prevail. No rights or liability can be derived from any translation.

Previous documents
VCIOM-04978 replaces all previous safety manuals for the DEPIC-2 series including SMAN-004.

WESTLOCK CONTROLS

www.westlockcontrols.com

Westlock. We reserve the right to change designs and specifications without notice.