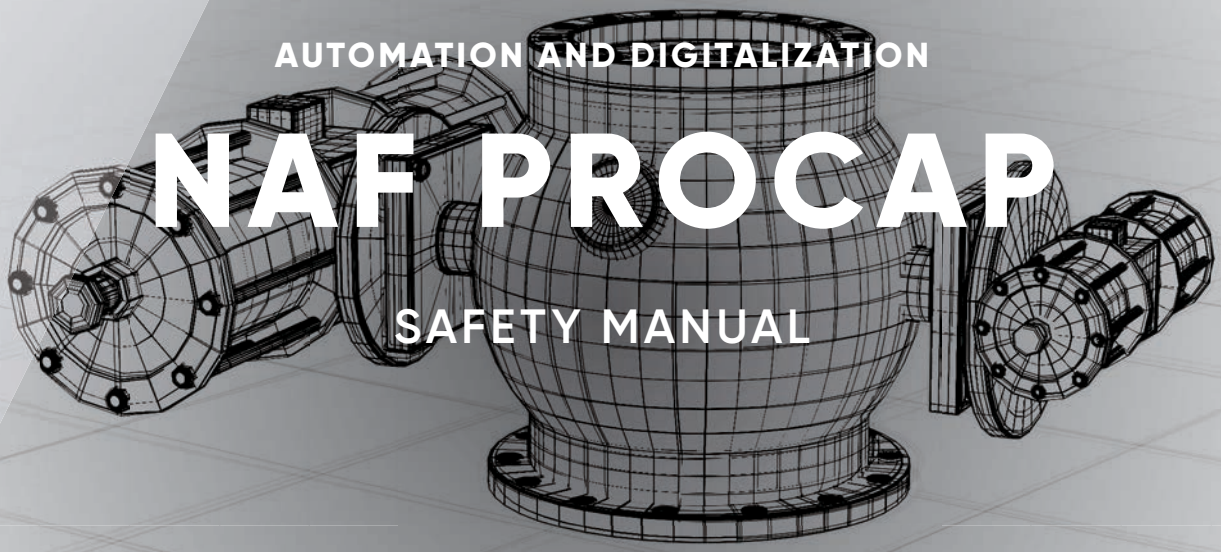
AUTOMATION AND DIGITALIZATION

NAF PROCAP

SAFETY MANUAL



V&A

ANDRITZ

ENGINEERED SUCCESS

CONTENTS

1 Introduction

1.1 SCOPE AND PURPOSE OF THE SAFETY MANUAL

This safety manual provides the information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the ProCap valve. This manual provides necessary requirements to enable the integration of the ProCap valve when showing compliance with the IEC 61508 or IEC 61511 functional safety standards.
This Safety Manual indicates all assumptions that have been made on the usage of the ProCap valve. If these assumptions cannot be met by the application, the SIL capability of the ProCap valve 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.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 solenoid valve is de-energized and spring is extended
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 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
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
PFD_{AVG}	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:

Fk 41.55GB, ProCap valve Datasheet

NFENIM4155, Procap valve Maintenance and installation instructions

Guidelines/References

FMEDA report - FLO 20-03-066 R001 V1R1 ProCap FMEDA
FMEDA report – FLO 20-03-066 R002 V1R1 Jammer FMEDA

1.6 REFERENCE STANDARDS

IEC 61508-2: 2010, Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-Related Systems
IEC 60654-1:1993-02, second edition, Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

2 ProCap valve Description

The NAF ProCap Capping Valve is intended to be used in batch digesters. The valve is mounted to the top flange of the digester and it automates the filling of wood chips into the digester. During the cooking sequence, the valve is closed and gives a tight seal to avoid gas/media leakage from the digester.

The valve consists of a single piece body housing and a ball sector. The ProCap valve has a unique design using eccentric hubs to load the seat and provide a tight shutoff.

The valve is automated and needs to follow correct sequence for opening and closing to work proberly. Refer to the ProCap valve datasheet for this information.

Jammer Function
The valve is locked in open and closed position by a jammer system that prevents the stem to operate.

3 Designing a SIF using the ProCap valve

3.1 SAFETY FUNCTION

Hazard Scenario
ProCap Valve opens while the digestor is pressurized.

Safety Function
The ProCap Safety Function is to remain closed (Stayput Function) once it has been put in the Cook position (sequence number 10).

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 ProCap valve datasheet for this information.

3.3 APPLICATION LIMITS

The materials of construction of a ProCap valve are specified in the NAF AB ProCap valve 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 ProCap valve 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 from NAF AB 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 PFD_{AVG} 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. The exida exSILentia™ tool is recommended for this purpose as it contains accurate models for the ProCap valve and its failure rates.

When using the ProCap valve in a redundant configuration, a common cause factor or 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 ProCap valve. 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 ProCap valve has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. 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 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.
The 1_H approach involves calculating the Safe Failure Fraction for the entire element.
The 2_H approach involves assessment of the reliability

data for the entire element according to 7.4.4.3.3 of IEC 61508.
The ProCap Valve 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 ProCap Valve can be classified as a 2_H device when the failure rates listed in the FMEDA report are used for the Design Verification calculations. When 2_H 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 per Route 2_H. If Route 2_H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1_H.

When the final element assembly consists of several components additional to ProCap valve, 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 1_H

3.5.3 SAFETY PARAMETERS

For detailed failure rate information refer to the FMEDA report for the ProCap valve.

3.6 CONNECTION OF THE PROCAP VALVE TO THE SIS LOGIC SOLVER BALL VALVE TO THE SIS LOGIC SOLVER

The ProCap should be connected to a logic solver where all components are safety rated. The safety rated logic solver shall actively perform the safety function as well as automatic diagnostics (if any) designed to diagnose potentially dangerous failures within the ProCap valve, (i.e. monitoring of position- and pressure switches).

3.7 GENERAL REQUIREMENTS

The system and function response time shall be less than the process safety time. The ProCap valve will remain in its safe state during the cocking cycle of the digester.
All SIS components including the ProCap valve must be operational before process start-up.
The User shall verify that the ProCap valve is suitable for use in safety applications by confirming the ProCap valve nameplate and model number is properly marked.
The system must contain components (ie pressure switches) to verify that the pressure in the digester is zero before the ProCap valve receives the signal to start opening sequence. It is recommended to have a redundant function.
Personnel performing maintenance and testing on the ProCap valve 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 ProCap valve shall not be operated beyond the useful lifetime as listed in paragraph 5.4 without undergoing overhaul or replacement.

4 Installation & Commissioning

4.1 INSTALLATION

The ProCap valve 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 ProCap valve must be accessible for physical inspection.

4.2 PHYSICAL LOCATION AND PLACEMENT

The ProCap valve shall be accessible with sufficient room for pneumatic connections to the actuator and shall allow for manual proof testing to take place.
The ProCap valve 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 pneumatic connectors or the vibration should be reduced using appropriate damping mounts.

4.3 PNEUMATIC CONNECTIONS

Pneumatic piping to the valve actuator shall be kept as short and straight as possible to minimize airflow restrictions and potential clogging. Long or kinked pneumatic tubes may also increase valve closure time.
Only dry instrument air filtered to 50 micron level or better shall be used.
The process air pressure shall meet the requirements set forth in the actuator installation manual.
The process air capacity shall be sufficient to move the valve within the required time.

4.4 WIRING OF LIMIT SWITCH UNITS FOR THE JAMMER

The mechanical locking of the valve is made by two jammer cylinder and their function are a crucial part of the safety system. They prevent unintentional opening of the valve while the digester is pressurized.

There are two limit switch units, sitting on the jammer cylinders. These should be wired so a serial function is achieved. Both jammers shall be in their locked position for the sequence to continue.

4.5 COMMISSIONING

Prior to start up, during commissioning, the correct function of the limit switches of the mechanical locking device (jammer) must be verified. Without supply air and the ProCap valve in closed, the inner limit switches shall be activated.

5 Operation & Maintenance

5.1 PROOF TEST REQUIREMENT

During operation, a low demand mode SIF must be 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. A sample procedure is provided in Table 1. Results from periodic proof tests shall be recorded and periodically reviewed.
For detailed Proof Test information refer to the FMEDA report for the ProCap valve.

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 20 to 25 years is expected for the ProCap valve, provided regular maintenance is done every 3-8 years, depending of application needs.

5.4 NOTIFICATION OF FAILURES

In case of malfunction of the system or SIF, the ProCap valve shall be put out of operation and the process shall be kept in a safe state by other measures.
NAF AB must be informed when the ProCap valve is required to be replaced due to failure. The occurred failure shall be documented and reported to ANDRITZ NAF representative or directly to NAF AB using the contact details on the back cover of this safety manual.

Valve & Automation
Total Valve & Control Solutions®

JOHANNESBURG
Tel: 011 397 2833

DURBAN
Tel: 031 579 2593

South Africa:
0861 103 103

E-mail: sales@valve.co.za
www.valve.co.za

SCAN ME