Mobrey™ Hydratect 2462

Functional Safety Manual
Table of Contents

Contents

Section 1: Introduction
1.1 Scope and purpose of the safety manual ......................... 1
1.2 Skill level requirement ............................................. 1
1.3 Terms and definitions ............................................... 1
1.4 Documentation and standards .................................... 3

Section 2: Product Description
2.1 Operation principle .................................................. 5
2.2 Steam/water detection system purpose ............................. 5
2.3 Ordering information ................................................ 7

Section 3: Designing a Safety Function Using the Mobrey Hydratect
3.1 Safety function ...................................................... 9
3.2 Environmental limits ................................................ 9
3.3 Application limits ................................................... 9
3.4 Design verification .................................................. 9
3.5 SIL capability ........................................................ 10
  3.5.1 Systematic integrity ............................................ 10
  3.5.2 Random integrity .............................................. 10
  3.5.3 Safety parameters ............................................. 10
3.6 Connection of the Mobrey Hydratect to the SIS logic solver 11
3.7 General requirements ............................................... 12

Section 4: Installation and Commissioning
4.1 Installation .......................................................... 13
4.2 Physical location and placement .................................... 13
4.3 Electrical connections .............................................. 13
4.4 Configuration ........................................................ 14
  4.4.1 PCB jumper settings .......................................... 14
  4.4.2 Steam-normal/water-normal setting .......................... 14
  4.4.3 Low/high-sensitivity setting .................................. 14
  4.4.4 Electrode-contamination setting ............................. 14
  4.4.5 Electrode-contamination sensitivity setting ............... 14
4.4.6 Electrode-type setting ............................................................... 14
4.4.7 Status relay operation setting ............................................... 14
4.4.8 Configuration settings and output relays ................................ 14

Section 5: Operation and Maintenance

5.1 Proof-test requirement ............................................................ 17
5.2 Repair and replacement .......................................................... 17
5.3 Notification of failures ............................................................. 17

Appendix A: Specifications

A.1 General .................................................................................... 19
A.2 Useful life ................................................................................. 19
A.3 Useful lifetime .......................................................... 19

Appendix B: Proposed Comprehensive Proof-test Procedure

B.1 Suggested comprehensive proof-test (water-normal) .................. 21
B.2 Suggested comprehensive proof-test (steam-normal) ................. 24
B.3 Full proof-test coverage ............................................................ 27
B.4 Impact on SIF and process ....................................................... 27
B.5 Duration of full proof-test ........................................................ 27
B.6 System elements tested ............................................................ 27
B.7 Tools and data required ............................................................ 27
B.8 Personal safety concerns .......................................................... 28

Appendix C: Proposed Partial Proof-test Procedure

C.1 Suggested partial proof-test (water-normal) .............................. 29
C.2 Suggested partial proof-test (steam-normal) ............................. 32
C.3 Partial proof-test coverage ....................................................... 34
C.4 Impact on SIF and process ....................................................... 35
C.5 Duration of partial proof-test .................................................. 35
C.6 System elements tested ............................................................ 35
C.7 Tools and data required ............................................................ 35
C.8 Personal safety concerns ........................................................ 35
Section 1 Introduction

1.1 Scope and purpose of the safety manual

This safety manual contains the information to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Mobrey Hydratect 2462 Steam/Water Detection System (“Hydratect system”).

The manual provides the necessary requirements to enable the integration of the Hydratect system 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 Hydratect system. If these assumptions cannot be met by the application, the SIL capability of the Hydratect system may be adversely affected.

Note
For product support, use the contact details on the back page.

1.2 Skill level requirement

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

1.3 Terms and definitions

**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 greater than or equal to 1.

**Fail-safe State**

State where switch output is in the state corresponding to an alarm condition. In this condition the switch contacts will normally be open.

**Fail Dangerous**

Failure that does not respond to an input from the process (i.e. not switching to the fail-safe state).

**Fail Dangerous Detected**

Failure that is dangerous but is detected.

**Fail Dangerous Undetected**

Failure that is dangerous and that is not detected.
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 switch to go to the defined fail-safe state without an input from the process.

FMEDEA
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.

High demand
Mode of operation where the frequency of demands for operation on a safety-related system is greater than once per year.

Low demand
Mode of operation where the frequency of demands for operation made on a safety-related system is no greater than once per year.

PFD_{AVG}
Average Probability of Failure on Demand.

PFH
Probability of dangerous failure per hour.

Safety Demand Interval
The expected time between safety demands.

SFF
Safe Failure Fraction - a 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 - a 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 - a 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, and SIL 1 has the lowest level.

**SIS**

Safety Instrumented System - an instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensors, logic solvers, and final elements.

**Type A device**

A type A device is a simple device using discrete electronic and mechanical components only, as defined by the standard IEC 61508.

### 1.4 Documentation and standards

This section lists the documentation and standards referred to by this safety manual.

**Table 1-1. Associated Documentation**

<table>
<thead>
<tr>
<th>Documents</th>
<th>Purpose of documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOB 16-02-064 R001 V1R1 FMEDA Hydratect</td>
<td>FMEDA Report Version 01, Revision 01, or later, for the Mobrey Hydratect</td>
</tr>
<tr>
<td>BP2462</td>
<td>Mobrey Hydratect Product Data Sheet</td>
</tr>
<tr>
<td>24625020</td>
<td>Mobrey Hydratect Reference Manual</td>
</tr>
</tbody>
</table>

**Table 1-2. Associated Standards**

<table>
<thead>
<tr>
<th>Standards</th>
<th>Purpose of standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61511 (ANSI/ISA 84.00.01-2004)</td>
<td>Functional safety - Safety instrumented systems for the process industry sector</td>
</tr>
<tr>
<td>IEC 60664-1</td>
<td>Insulation coordination for equipment with low voltage systems</td>
</tr>
<tr>
<td>IEC 61984</td>
<td>Connectors - Safety requirements and test</td>
</tr>
<tr>
<td>HRD 5:1994</td>
<td>Handbook of Reliability Data for Components used in Telecommunication systems</td>
</tr>
</tbody>
</table>
Section 2  Product Description

2.1 Operation principle

The Mobrey Hydratect 2462 Steam/Water Detection System ("Hydratect system") consists of a dual-channel electronic control unit with electrodes (Figure 2-1). The electrodes are mounted in plant pipe-work using Inserts, or within an Emerson supplied manifold. They are connected to each channel of the control unit which then gives an indication of the presence of water or steam where the associated electrode is installed.

When in contact with water, the resistance of the electrode measures between 2 kΩ and 100 kΩ. In steam, the resistance of the electrode rises to greater than 10 MΩ. The control unit measures the resistance of each electrode continuously, basing each channel indication upon this measurement.

Each channel is independently powered via separate power supply circuitry to ensure one channel remains active in event of failure of the other’s supply. In addition, output stage circuitry is triplicated such that the output would still continue to operate normally in the event of the failure of two output stages.

Note
For all product information and documentation downloads, visit Emerson.com/Mobrey.

Figure 2-1. Hydratect Electronics Control Unit and Electrodes

A. Electronics Control Unit.  B. Electrodes

2.2 Steam/water detection system purpose

Each Hydratect channel indicates, by means of a relay output, the presence of water or steam in the proximity of its associated electrode. See Figure 2-2 and Figure 2-3 on page 6 for example applications.
Figure 2-2. Example Application: High Water Level Detection in Drain Pot

A. Superheat steam line.  
B. Drain pot.  
C. Isolation valve.  
D. Drain line.  
E. High alarm signal.  
F. In-line manifold with two electrodes (channels 1 and 2).

Figure 2-3. Example Application: Water Level Detection in Boiler Drum

A. High-high level electrode.  
B. High level electrode.  
C. Low level electrode.  
D. Low-low level electrode.  
E. High alarm and trip signal output from Control Unit.  
F. Low alarm and trip signal output from Control Unit.
2.3 Ordering information

Hydratect systems consist of a control unit and two electrodes. The electrodes must be of the same type. In addition, a cable, cover and insert must also be ordered for each electrode.

**Control units** are ordered using the following order number and option codes.

Typical control unit model number: 2462 A QT

The option code after “2462” indicates the output and power supply type:
- **A** = AC power supply, single pole single throw relay outputs
- **C** = DC power supply, single pole single throw relay outputs
- **E** = AC power supply, two pole changeover relay outputs

**Electrodes** are ordered using the following order number and option codes.

Typical electrode model number: 246785 A

The option code after “246785” indicates the electrode type:
- **A** = Extended range (300 bar/4350 psi, 560 °C/1040 °F) electrode
- **Z** = Standard range (210 bar/3045 psi, 370 °C/698 °F) electrode

**Cables** are ordered using the following order number and option codes.

Typical cable model number: 2462020 4A

The option code after “2462020” indicates the cable length:
- **4A** = 3 m/10 ft.
- **5A** = 10 m/33 ft.
- **6A** = 18 m/60 ft.
- **7A** = 30 m/98 ft.

**Inserts** are available using the following order number and option codes.

- 24673540B = 316 stainless steel
- 24673548B = F22 modified NQT alloy steel
- 24673549B = Grade 91 alloy steel

One type of **electrode cover** is available for ordering with the code 24670118A.

Hydratect systems consisting of the above elements have achieved a SIL rating. Refer to Table 3-1 and Table 3-2 on page 11 for the associated Safety Instrumented System (SIS) parameters.

Control Units with the QT option code are supplied with a third party certificate of SIL capability, and approved for usage in SIS applications.
Section 3  Designing a Safety Function Using the Mobrey Hydratect

3.1 Safety function

Each channel of the Mobrey Hydratect 2462 Steam/Water Detection System ("Hydratect system") can be configured to indicate, using its relay output, when the associated electrode is in water or steam conditions. It is important that the Hydratect system is user-configured for the correct application.

3.2 Environmental limits

The designer of the SIF (Safety Instrumented Function) must check that the Hydratect system is rated for use within the expected environmental limits. See the Mobrey Hydratect Product Data Sheet for environmental limits.

Note
For all product information and documentation downloads, see the on-line Mobrey Hydratect web page at Emerson.com/Mobrey.

3.3 Application limits

It is very important that the SIF designer checks for material compatibility by considering process liquids and on-site chemical contaminants. If the Hydratect system is used outside the application limits or with incompatible materials, the reliability data and predicted SIL capability becomes invalid.

The construction materials of a Hydratect system are specified in the product data sheet and the product reference manual (Table 1-1 on page 3). Use the model code on the product label, and the ordering information table and specification in these product documents, to determine the construction materials.

3.4 Design verification

A detailed Failure Modes, Effects and Diagnostics Analysis (FMEDA) report for the Hydratect system is available from Emerson. This report details all failure rates and failure modes as well as expected lifetime.

Note
The FMEDA report is available from the Mobrey Hydratect web page at Emerson.com/Mobrey. In the Documents section, there are SIL documents including the FMEDA report (and this safety manual).

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer using a PFD_{AVG} calculation 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 Hydratect system 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 Hydratect system. The failure rates 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 Mobrey Hydratect Steam/Water Detection System has met manufacturer design process requirements of Safety Integrity Level 3 (SIL 3). These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with the Hydratect system 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

The Hydratect system is classified as a type A device according to IEC 61508, and has a Hardware Fault Tolerance (HFT) of zero in single configuration and a Hardware Fault Tolerance of one in a redundant configuration.

Random Integrity for Type A device:
- Control units A, C, E: SIL 2 @ HFT=0 and SIL 3 @HFT=1

#### 3.5.3 Safety parameters

Table 3-1 and Table 3-2 on page 11 summarize the Mobrey Hydratect failure rates. For detailed failure rate information, including PFD_{AVG} and MTTR data, see the FMEDA report for the Mobrey Hydratect.

**Note**

The FMEDA report is available from the Mobrey Hydratect web page at Emerson.com/Mobrey. In the Documents section, there are SIL documents including the FMEDA report (and this safety manual).
3.6 Connection of the Mobrey Hydratect to the SIS logic solver

The Hydratect system should be connected to the safety-rated logic solver which is actively performing the safety function as well as automatic diagnostics (if any) designed to diagnose potentially dangerous failures within the Hydratect system. In some cases, it may also be connected directly to the final element.


Note
For all product information and documentation downloads, see the on-line Mobrey Hydratect web page at Emerson.com/Mobrey.
3.7 **General requirements**

- The system and function response time shall be less than the process safety time.
- The Hydratect system will change to its defined safe state in less than this time with relation to the specific hazard scenario.
- All SIS components, including the Hydratect system must be operational before process start-up.
- The user shall verify that the Hydratect system is suitable for use in safety applications by confirming the Hydratect system nameplate and model number are properly marked.
- Personnel performing maintenance and testing on the Hydratect system shall first be assessed as being competent to do so.
- Results from periodic proof tests shall be recorded and periodically reviewed.
- The Hydratect system shall not be operated beyond the useful lifetime as listed in the specification section of the product reference manual without undergoing overhaul or replacement.

---

**Note**
For all product information and documentation downloads, see the on-line Mobrey Hydratect web page at [Emerson.com/Mobrey](https://Emerson.com/Mobrey).
Section 4 Installation and Commissioning

4.1 Installation

The Mobrey Hydratect 2462 Steam/Water Detection System (“Hydratect system”) must be installed as described in the installation section of the Mobrey Hydratect Reference Manual. Check that environmental conditions do not exceed the ratings in the specification section.

The Hydratect system must be accessible for physical inspection.

4.2 Physical location and placement

The Hydratect system shall be accessible with sufficient room for cover removal and electrical connections, and allow for manual proof-testing to take place.

4.3 Electrical connections

Wiring should be adequately rated and not be susceptible to mechanical damage. Electrical conduit is commonly used to protect wiring.
4.4 Configuration

4.4.1 PCB jumper settings

The Hydratect system provides extensive configuration options, achieved using ‘jumpers’ on each electronics control unit channel. Each control unit channel features two relays to indicate status conditions (status relay) and two relays to indicate fault conditions (fault relay). The relay pairs are always actuated to the same position.

4.4.2 Steam-normal/water-normal setting

The steam-normal/water-normal setting determines the condition of the status relays when the channel electrode is in steam or water conditions. This setting must be set to the appropriate normal condition of the electrode.

4.4.3 Low/high-sensitivity setting

The low/high sensitivity setting determines the threshold for steam and water detection. This should only be changed to low sensitivity if operating temperatures below 200 °C are causing false switching.

4.4.4 Electrode-contamination setting

Electrode contamination should be enabled to detect fouling of the associated electrode.

4.4.5 Electrode-contamination sensitivity setting

The electrode-contamination should be set to high sensitivity, and only changed to low sensitivity when poor water quality causes erroneous tripping.

4.4.6 Electrode-type setting

The electrode-type setting must be set to “Series III”.

4.4.7 Status relay operation setting

The status relays can be configured to latch (until power cycling of the control unit channel) by using the status relay operation setting.

4.4.8 Configuration settings and output relays

The Hydratect system must be user-configured for an application so that the fault and status relays are closed in the safe or normal condition (see Table 4-1 and Table 4-2 on page 15).
**Table 4-1. Configuration Settings Affecting Output relays and Front Panel LEDs (Water-normal)**

<table>
<thead>
<tr>
<th>System state</th>
<th>Front panel LEDs</th>
<th>Output relays</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I</td>
<td>Steam</td>
</tr>
<tr>
<td>Electrode in water, no fault</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Electrode in steam, no fault</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Power supply loss</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Electrode contaminated or short-circuited</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection in electrode sense element is broken</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection in electrode ground is broken</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection to ground sense is broken - electrode in water</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection to ground sense is broken - electrode in steam</td>
<td>On</td>
<td>On</td>
</tr>
</tbody>
</table>

**Table 4-2. Configuration Settings Affecting Output relays and Front Panel LEDs (Steam-normal)**

<table>
<thead>
<tr>
<th>System state</th>
<th>Front panel LEDs</th>
<th>Output relays</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I</td>
<td>Steam</td>
</tr>
<tr>
<td>Electrode in steam, no fault</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Electrode in water, no fault</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Power supply loss</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Electrode contaminated or short-circuited</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection in electrode sense element is broken</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection in electrode ground is broken</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection to ground sense is broken - electrode in water</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Connection to ground sense is broken - electrode in steam</td>
<td>On</td>
<td>On</td>
</tr>
</tbody>
</table>
Section 5 Operation and 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. Undetected failures that prevent the SIF from performing its function are the main concern.

Periodic proof-tests shall take place at the frequency (or interval) defined by the 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 Appendix B: Proposed Comprehensive Proof-test Procedure.

Results from periodic proof tests shall be recorded and periodically reviewed.

5.2 Repair and replacement

Repair procedures in the Mobrey Hydratect Reference Manual must be followed.

5.3 Notification of failures

In case of malfunction of the system or SIF, the Hydratect system shall be put out of operation and the process shall be kept in a safe state by other measures.

Emerson™ must be informed when the Hydratect system is required to be replaced due to failure. The occurred failure shall be documented and reported to Emerson using the contact details on the back page of this functional safety manual. This is an important part of Emerson SIS management process.
Appendix A Specifications

A.1 General

In Table A-1, the safety response time for all control unit types is 10 seconds.

Table A-1. General Specifications

<table>
<thead>
<tr>
<th>Control unit type</th>
<th>Supply voltage</th>
<th>Relay ratings</th>
<th>Safety response time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single pole single throw relay outputs (option code A)</td>
<td>93.5 to 130 Vac 187 to 256 Vac</td>
<td>0.2A @ 125Vdc 8A @ 30Vdc 8A @ 250Vac (resistive load)</td>
<td>10 s minimum</td>
</tr>
<tr>
<td>Single pole single throw relay outputs (option code C)</td>
<td>20 to 60 Vdc</td>
<td>0.2A @ 125Vdc 8A @ 30Vdc 8A @ 250Vac (resistive load)</td>
<td>10 s minimum</td>
</tr>
<tr>
<td>Two pole changeover relay outputs (option code E)</td>
<td>93.5 to 130 Vac 187 to 256 Vac</td>
<td>0.25A @ 225Vdc 8A @ 250Vac (resistive load)</td>
<td>10 s minimum</td>
</tr>
</tbody>
</table>

A.2 Useful life

Based on general field failure data and manufacturers component data, a useful life period of approximately 10 years is expected for the Hydratect system at an ambient temperature of 55 °C. This decreases by a factor of two for every increase of 10 °C, and increases by a factor of two for every decrease of 10 °C.

A.3 Useful lifetime

According to the standard IEC 61508-2, a useful lifetime based on experience should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see FMEDA report), this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is therefore meaningless as the probability of failure significantly increases with time.

The useful lifetime is highly dependent on the subsystem itself and its operating conditions. Specifically, the equipment contains electrolytic capacitors which have a useful life which is highly dependent on ambient temperature (see Safety Data in the FMEDA report).

This assumption of a constant failure rate is based on the bath-tub curve. Therefore, it is obvious that the \( PFD_{AVG} \) calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

(1) Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.
It is the responsibility of the end-user to maintain and operate the Hydratect system according to the manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

For high-demand mode applications, the useful lifetime of the mechanical parts is limited by the number of cycles. The useful lifetime of the mechanical and electrical parts is greater than 100000 operations. When plant experience indicates a shorter useful lifetime than indicated, the number based on plant experience should be used.
Appendix B  Proposed Comprehensive Proof-test Procedure

B.1 Suggested comprehensive proof-test (water-normal)

According to Section 7.4.5.2 (f) of the standard IEC 61508-2, proof-tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof-testing.

The suggested comprehensive proof-tests consist of operation tests with the appropriate channel electrode removed from the plant pipework or manifold.

Procedure

1. Inspect the accessible parts of the electronics control unit and cabling for any damage, and the electrode inserts and covers for any leaks or damage.

2. Bypass the safety function and take appropriate action to avoid a false trip. With the system at ambient temperature and pressure, drain any fluid from the pipework and remove the electrode.

   Independent precautions must be taken to ensure that no hazard can result from this operation.

3. Verify the control unit jumpers are set for the required mode of operation.

4. To simulate the electrode in water, short the electrode tip to ground through a 120 kΩ resistor (when configured for high-sensitivity operation) or a 56 kΩ resistor (when configured for low-sensitivity operation).

   Due to the electrode being exposed to air, a steam indication is given. If the status-relay-operation setting is set to latched, the control unit must first be power cycled to set the status relay back to the energized position.
Appendix B: Proposed Comprehensive Proof-test Procedure
March 2017

5. Check the front panel LED states are as expected:
   - ! LED off
   - STEAM LED off
   - WATER LED on

6. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay energized

7. To simulate the electrode in steam, remove the resistor.

8. Check the front panel LED states are as expected:
   - ! LED off
   - STEAM LED on
   - WATER LED off

9. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay de-energized

10. To simulate electrode contamination detection (if enabled), short the electrode tip to ground through an 820 Ω resistor (for high sensitivity operation) or a 270 Ω resistor (for low sensitivity operation).

Due to the electrode being exposed to air, a steam indication will be given. If the status-relay-operation setting is set to latched, the control unit must first be power cycled to set the status relay back to the energized position.
11. Check the front panel LED states are as expected:

- ! LED on
- STEAM LED off
- WATER LED on

12. Check on the fault and status relays are as expected:

- a. Fault relay de-energized
- b. Status relay energized

13. Remove the resistor.

Check that the LEDs, and fault and status relays, have returned to their original states shown in steps 8 and 9.

14. Remove a knurled nut from the electrode and disconnect the white conductor.

Due to the electrode being exposed to air, a steam indication will be given. If the status-relay-operation setting is set to latched, the control unit must first be power cycled to set the status relay back to the energized position.

15. Check the front panel LED states are as expected:

- ! LED on
- STEAM LED off
- WATER LED on

16. Check the fault and status relays are as expected:

- a. Fault relay de-energized
- b. Status relay energized

17. Reconnect the white conductor.

Check the LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

18. Disconnect the black conductor (lead) from ground by removing the screw securing it to the manifold or, if using an insert, by removing the electrode cover base plate.

If the status-relay-operation setting is set to latched, the control unit must first be power cycled to set the status relay back to the energized position.

19. Check the front panel LED states are as expected:

- ! LED on
- STEAM LED on
- WATER LED off

20. Check the fault and status relays are as expected:

- a. Fault relay de-energized
- b. Status relay de-energized
21. Reconnect the black conductor (lead).

If the status-relay-operation setting is set to latched, the control unit must be power cycled to set the status relay back to the energized position.

Check the front panel LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

22. Replace and secure the electrode cover.

23. Remove the safety function bypass and otherwise restore normal operation.

B.2 Suggested comprehensive proof-test (steam-normal)

According to Section 7.4.5.2 (f) of the standard IEC 61508-2, proof-tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof-testing.

The suggested comprehensive proof-tests consist of operation tests with the appropriate channel electrode removed from the plant pipework or manifold.

**Procedure**

1. Inspect the accessible parts of the electronics control unit and cabling for any damage, and the electrode inserts and covers for any leaks or damage.

2. Bypass the safety function and take appropriate action to avoid a false trip. With the system at ambient temperature and pressure, drain any fluid from the pipework and remove the electrode.

Independent precautions must be taken to ensure that no hazard can result from this operation.

3. Verify the control unit jumpers are set for the required mode of operation.

4. To simulate the electrode in water, short the electrode tip to ground through a 120 kΩ resistor (when configured for high-sensitivity operation) or a 56 kΩ resistor (when configured for low-sensitivity).
5. Check the front panel LED states are as expected:

<table>
<thead>
<tr>
<th></th>
<th>LED off</th>
<th>LED off</th>
<th>LED on</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>STEAM</td>
<td>WATER</td>
<td></td>
</tr>
</tbody>
</table>

6. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay de-energized

7. To simulate the electrode in steam, remove the resistor.

   If the status-relay-operation setting is set to latched, the control unit must be power cycled to set the status relay back to the energized position.

8. Check the front panel LED states are as expected:

<table>
<thead>
<tr>
<th></th>
<th>LED off</th>
<th>LED on</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>STEAM</td>
<td>WATER</td>
</tr>
</tbody>
</table>

9. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay energized

10. To simulate electrode contamination detection (if enabled), short the electrode tip to ground through an 820 Ω resistor (for high sensitivity operation) or a 270 Ω resistor (for low sensitivity operation).

11. Check the front panel LED states are as expected:

<table>
<thead>
<tr>
<th></th>
<th>LED on</th>
<th>LED off</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>STEAM</td>
<td>WATER</td>
</tr>
</tbody>
</table>

12. Check on the fault and status relays are as expected:
   a. Fault relay de-energized
   b. Status relay de-energized
13. Remove the resistor.

If the status-relay-operation setting is set to latched, the control unit must first be power cycled to set the status relay back to the energized position.

Check that the LEDs, and fault and status relays, have returned to their original states shown in steps 8 and 9.

14. Remove a knurled nut from the electrode and disconnect the white conductor.

15. Check the front panel LED states are as expected:

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>LED on</td>
</tr>
<tr>
<td>STEAM</td>
<td>LED off</td>
</tr>
<tr>
<td>WATER</td>
<td>LED on</td>
</tr>
</tbody>
</table>

16. Check the fault and status relays are as expected:

a. Fault relay de-energized
b. Status relay de-energized

17. Reconnect the white conductor.

If the status-relay-operation setting is set to latched, the control unit must be power cycled to set the status relay back to the energized position.

Check the LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

18. Disconnect the black conductor (lead) from ground by removing the screw securing it to the manifold or, if using an insert, by removing the electrode cover base plate.

19. Check the front panel LED states are as expected:

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>LED on</td>
</tr>
<tr>
<td>STEAM</td>
<td>LED on</td>
</tr>
<tr>
<td>WATER</td>
<td>LED off</td>
</tr>
</tbody>
</table>

20. Check the fault and status relays are as expected:

a. Fault relay de-energized
b. Status relay energized

21. Reconnect the black conductor (lead).

Check the front panel LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

22. Replace and secure the electrode cover.

23. Remove the safety function bypass and otherwise restore normal operation.
B.3 Full proof-test coverage

Table B-1 shows the percentage coverage achieved using the full proof-test for the Hydratect systems with a SIL rating and operating in the water-normal mode.

<table>
<thead>
<tr>
<th>Control unit type</th>
<th>Proof-test coverage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, E</td>
<td>84</td>
</tr>
<tr>
<td>C</td>
<td>76</td>
</tr>
</tbody>
</table>

Table B-2 shows the percentage coverage achieved using the full proof-test for the Hydratect systems with a SIL rating and operating in the steam-normal mode.

<table>
<thead>
<tr>
<th>Control unit type</th>
<th>Proof-test coverage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, E</td>
<td>84</td>
</tr>
<tr>
<td>C</td>
<td>76</td>
</tr>
</tbody>
</table>

B.4 Impact on SIF and process

In order to achieve the product safe state, the electrode must be removed from the pipework whilst the proof-test is performed. The process cannot be allowed to operate whilst the proof-test is being conducted.

B.5 Duration of full proof-test

The full proof test takes several hours to perform with all safety measures being followed.

B.6 System elements tested

The full proof-test performs a complete test of the system elements. The electrode, measuring electronics, and output stage are all checked by virtue of changing of the electrode condition and observation of the output.

B.7 Tools and data required

Appropriate tooling is required to remove the electrode from the pipework.

270 Ω, 820 Ω, 56 kΩ, and 120 kΩ resistors are required to test all configuration settings.

The date, time and name of the operator that performed the proof-test, the response time, and result of the proof-test will be documented for maintaining the proof-test history of the device for PFD_{AVC} calculations.
B.8 Personal safety concerns

As stated in the section Impact on SIF and process, the process must not be allowed to run during the proof-test procedure.
Appendix C Proposed Partial Proof-test Procedure

Suggested partial proof-test (water-normal) ........................................... page 29
Suggested partial proof-test (steam-normal) ........................................... page 32
Partial proof-test coverage ................................................................. page 34
Impact on SIF and process ............................................................... page 35
Duration of partial proof-test .......................................................... page 35
System elements tested ................................................................. page 35
Tools and data required ................................................................. page 35
Personal safety concerns ............................................................... page 35

C.1 Suggested partial proof-test (water-normal)

According to Section 7.4.5.2 (f) of the standard IEC 61508-2, proof-tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof-testing.

The suggested partial proof-tests consists of Hydratect system operation tests on-site.

Procedure

Note
This test requires the electrode to be in its normal state (e.g. immersed in water).

1. Inspect the accessible parts of the control unit and cabling for any damage, and the electrode inserts and covers for any leaks or damage.

2. Bypass the safety function and take appropriate action to avoid a false trip.

   ! Independent precautions must be taken to ensure that no hazard can result from this operation.

3. Verify the control unit jumpers are set for the required mode of operation.

4. Check the front panel LED states are as expected:
   
   ! LED off
STEAM   LED off
WATER   LED on

5. Check the fault and status relays are as expected:
   
   a. Fault relay energized
   b. Status relay energized
6. To simulate the electrode in steam:
   a. Remove the white and red conductors.
   b. Place a 10 MΩ resistor in series with the electrode sense element terminal and conductors.

7. Check the front panel LED states are as expected:
   ! LED off
   STEAM LED on
   WATER LED off

8. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay de-energized

9. To simulate electrode contamination detection (if enabled), short the electrode tip to ground through an 820 Ω resistor (for High Sensitivity operation) or a 270 Ω resistor (for Low Sensitivity operation).

   Due to the electrode being exposed to steam conditions, a steam indication will be given. If the status-relay-operation setting is set to latched, the control unit must first be power cycled to set the status relay back to the energized position.

10. Check the front panel LED states are as expected:
    ! LED on
    STEAM LED off
    WATER LED on
11. Check on the fault and status relays are as expected:
   a. Fault relay de-energized
   b. Status relay energized

12. Remove the resistor.

   Check that the LEDs, and fault and status relays, have returned to their original states
   shown in steps 4 and 5.

13. Remove a knurled nut from the electrode and disconnect the white conductor.

14. Check the front panel LED states are as expected:

   ! LED on
   STEAM LED off
   WATER LED on

15. Check the fault and status relays are as expected:
   a. Fault relay de-energized
   b. Status relay energized

16. Reconnect the white conductor.

   Check the LEDs, and fault and status relays, have returned to their original states as shown
   in steps 4 and 5.

17. Disconnect the black conductor (lead) from ground by removing the screw securing it to
    the manifold or, if using an insert, by removing the electrode cover base plate.

18. Check the front panel LED states are as expected:

   ! LED on
   STEAM LED on
   WATER LED off

19. Check the fault and status relays are as expected:
   a. Fault relay de-energized
   b. Status relay de-energized

20. Reconnect the black conductor (lead).

   If the status-relay-operation setting is set to latched, the control unit must be power cycled
   to set the status relay back to the energized position.

   Check the front panel LEDs, and fault and status relays, have returned to their original states
   as shown in steps 4 and 5.

21. Replace and secure the electrode cover.

22. Remove the safety function bypass and otherwise restore normal operation.
C.2 Suggested partial proof-test (steam-normal)

According to Section 7.4.5.2 (f) of the standard IEC 61508-2, proof-tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof-testing.

The suggested partial proof-tests consists of Hydratect system operation tests on-site.

Procedure

Note
This test requires the electrode to be in its normal state (e.g. immersed in steam).

1. Inspect the accessible parts of the Control Unit and cabling for any damage, and the electrode inserts and covers for any leaks or damage.

2. Bypass the safety function and take appropriate action to avoid a false trip.

⚠️ Independent precautions must be taken to ensure that no hazard can result from this operation.

3. Verify the control unit jumpers are set for the required mode of operation.

4. To simulate the electrode in water, remove the electrode cover and short the electrode sense element terminal to ground through a 120 kΩ resistor (when configured for High Sensitivity operation) or a 56 kΩ resistor (when configured for Low Sensitivity operation).

5. Check the front panel LED states are as expected:

<table>
<thead>
<tr>
<th>LED</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>!L E D off</td>
<td>STEAM LED off</td>
</tr>
<tr>
<td>WATER LED on</td>
<td></td>
</tr>
</tbody>
</table>

6. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay de-energized
7. To check system operation in steam, remove the resistor.
   If the status-relay-operation setting is set to latched, the control unit must be power cycled to set the status relay back to the energized position.

8. Check the front panel LED states are as expected:
   - LED off
   - STEAM LED on
   - WATER LED off

9. Check the fault and status relays are as expected:
   a. Fault relay energized
   b. Status relay energized

10. To simulate electrode contamination detection (if enabled), short the electrode sense element terminal to ground through an 820 Ω resistor (for high sensitivity operation) or a 270 Ω resistor (for low sensitivity operation).

11. Check the front panel LED states are as expected:
    - LED on
    - STEAM LED off
    - WATER LED on

12. Check the fault and status relays are as expected:
    a. Fault relay de-energized
    b. Status relay de-energized

13. Remove the resistor.
    If the status-relay-operation setting is set to latched, the control unit must be power cycled to set the status relay back to the energized position.
    Check that the LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

14. Remove a knurled nut from the electrode and disconnect the white conductor.
15. Check the front panel LED states are as expected:

  !    LED on
STEAM LED off
WATER LED on

16. Check the fault and status relays are as expected:

a. Fault relay de-energized
b. Status relay de-energized

17. Reconnect the white conductor.

   If the status-relay-operation setting is set to latched, the control unit must be power cycled to set the status relay back to the energized position.

   Check that the LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

18. Disconnect the black conductor (lead) from ground by removing the screw securing it to the manifold or, if using an insert, by removing the electrode cover base plate.

19. Check the front panel LED states are as expected:

  !    LED on
STEAM LED on
WATER LED off

20. Check the fault and status relays are as expected:

a. Fault relay de-energized
b. Status relay energized

21. Reconnect the black conductor (lead).

   Check the front panel LEDs, and fault and status relays, have returned to their original states as shown in steps 8 and 9.

22. Replace and secure the electrode cover.

23. Remove the safety function bypass and otherwise restore normal operation.

C.3 Partial proof-test coverage

Table C-1 on page 35 shows the percentage coverage achieved using the partial proof-test for the Hydratect systems with a SIL rating and operating in the water-normal mode.

Table C-2 on page 35 shows the percentage coverage achieved using the partial proof-test for the Hydratect systems with a SIL rating and operating in the steam-normal mode.
### Appendix C: Proposed Partial Proof-test Procedure

March 2017

#### C.4 Impact on SIF and process

In order to achieve the product safe state, the electrode condition must be altered using resistors. Precautions must be taken to ensure actual demand for the safe state does not occur during the partial proof-test.

#### C.5 Duration of partial proof-test

The full proof test takes several hours to perform with all safety measures being followed.

#### C.6 System elements tested

The partial proof-test tests the wiring and control unit elements of the system. The measuring electronics and output stage are all checked by virtue of changing the electrode condition and observation of the output.

#### C.7 Tools and data required

Appropriate tooling is required to remove the electrode from the pipework.

270Ω, 820Ω, 56kΩ, 120kΩ, and 10MΩ resistors are required to test all configuration settings.

The date, time and name of the operator that performed the proof-test, the response time, and result of the proof-test will be documented for maintaining the proof-test history of the device for PFD<sub>AFC</sub> calculations.

#### C.8 Personal safety concerns

As stated in the section Impact on SIF and process, the process must not be allowed to run during the proof-test procedure.

---

### Table C-1. Partial Proof-test Coverage Percentage (Water-normal)

<table>
<thead>
<tr>
<th>Control unit type</th>
<th>Proof-test coverage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, E</td>
<td>74</td>
</tr>
<tr>
<td>C</td>
<td>72</td>
</tr>
</tbody>
</table>

### Table C-2. Partial Proof-test Coverage Percentage (Steam-normal)

<table>
<thead>
<tr>
<th>Control unit type</th>
<th>Proof-test coverage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, E</td>
<td>74</td>
</tr>
<tr>
<td>C</td>
<td>71</td>
</tr>
</tbody>
</table>