THIS IS A SCHEDULE DRAWING.
THIS DRAWING SHALL NOT BE MODIFIED
WITHOUT THE CONSENT OF THE AUTHORIZED
PERSON AS DEFINED IN SOP-295.

REV.	ECN	AUTHOR	DATE
D	500000522174	R.E. PADILLA	05/16/2024
C	500000470279	C. LONGFIELD	12/05/2022
B	500000253187	K. LAMBACH	05/10/2017
A	500000206746	J. HASHMI	03/11/2016
NC	500000177959	J. HASHMI	05/18/2015

Notice

Contents

1 Introduction

The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of the standard.

This safety manual contains the required information to install and maintain a Safety Instrumented Function (SIF) utilizing the Reuter-Stokes Flame Tracker Dry (Part number RS-FS-9009-03-XXX or RS-FS-9010-03-XXX).

This manual provides the necessary requirements to enable the integration of the Reuter-Stokes Flame Tracker Dry (FTD 325) when showing compliance with the IEC 61508:2010 standard. The international standard IEC/EN 61508 has been widely accepted as the basis for the specification, design and operation of safety instrumented systems (SIS). It is assumed that the operator is familiar with the Reuter-Stokes FTD 325 and the use of the product in a hazardous environment. Failure to properly follow the instructions defined in the Flame Tracker Dry Operation and Maintenance Manual and this safety manual may adversely affect the Safety Integrity Level (SIL) capability of the product.

Failure rates for each failure mode/category, useful life, and proof test coverage are determined for FTD 325 and available in the Appendix A- Failure Modes, Effects, and Diagnostic Analysis (FMEDA) report. The information in the report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PD_{avg}) requirements and the architectural constraints/minimum hardware fault tolerance requirements per IEC 61508/IEC 61511. The analysis shows that the Flame Tacker 9009 has a Safe Failure Fraction >60% and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

2 Application & Installation

It is very important that the SIF designer read and understand the FTD 325 Operation and Maintenance Manual (FS-9009OM or FS-9010OM).

The product shall be maintained and operated per the instructions and within the parameters as defined in the appropriate operation and maintenance manual. If the sensor is used outside the application limits or not properly installed, the reliability data and predicted SIL capability becomes invalid.

The FTD 325 is not repairable. In the event of a failure, the sensor must be replaced.

Under no circumstances should the sensor be disassembled. A breach of the sensor will render it unusable and it must be replaced.

Approved cables shall be used for installation. Cable wiring should be adequately protected and not be susceptible to mechanical damage. Grounded electrical conduit is commonly used for protection and performance. Further information is available in the operation & maintenance manual.

After a change of configuration or preventive maintenance and prior to the commissioning of the product, the sensor shall be verified for proper operation.

The SIF designer must follow the FTD 325 Operation and Maintenance manual for product specifications and environmental limits. If the sensor is used outside the application limits or not properly installed, the reliability data and predicted SIL capability becomes invalid.

Failure due to operating the cool end over rated temperature (T_a > 140°C)

When operated above rated temperatures the circuit output is undefined. It may go high or low and could vary from sensor to sensor. Because the turbine does not directly monitor temperature at the flame tracker the turbine controller should monitor sensor outputs over a specified time to check for unexpected output shifts. If an unexpected output change occurs without a corresponding change in turbine output, the controller should assume the cool end is operating outside its rated temperatures and notify operation personnel. If there is any question whether the cool end was operated above 140°C it should be replaced.

3 Flame Tracker Dry 325 Versions

This document will refer to a complete sensor as shown in the Sensor Reference column of Table 1. Unless otherwise noted all comments refer equally to any possible configuration.

Table 1: Applicable sensors

Sensor Reference	Possible configurations
RS-FS-9009-XXX	RS-FS-9009-03, RS-FS-9009-03-25X, RS-FS-9009-03-126, RS-FS-9009-03-173
RS-FS-9010-03- XXX	RS-FS-9010-03, RS-FS-9010-03-25X, RS-FS-9010-03-126, RS-FS-9010-03-173

4 Documents

Table 2: Reference Documents

Document	Description
FS-9009OM	RS-FS-9009 Operation & Maintenance Manual
FS-9010OM	RS-FS-9010 Operation & Maintenance Manual
IEC 61508:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
BHR 19-11-139 R001	Failure Modes, Effects and Diagnostic Analysis (exida) RS-FS-9009-XXX and RS-FS-9010-03- XXX (Refer to Appendix A)

5 Abbreviations & Terms

FMEDA
Failure Modes, Effects and Diagnostics Analysis.

DC (Diagnostic Coverage)
The ratio of detected dangerous failures to the total number of dangerous failures (λ_{DD}/λ_D).

EUC (Equipment Under Control)
Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

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 that is not detected.

Functional Safety

Functional Safety is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes.

HFT (Hardware Fault Tolerance)
Count of faults which are tolerated by hardware without any dangerous failures (HFT + 1 can be dangerous)

λ_{dd}, λ_{du}, λ_{sd}, λ_{su}, λ_{d}, λ_{s}
Failure rates (Lambda) with respect to the safety function, where the first letter determines the kind of failure (s = safe, d = dangerous) and the second letter defines the detection (d = detected, u = undetected). $\lambda_d = \lambda_{du} + \lambda_{dd}$, $\lambda_s = \lambda_{su} + \lambda_{sd}$

LL (Lower Limit)
The sensor output current below which the external diagnostics detect a failure. This document assumes sensor output currents less than or equal to 3.0 mA meet this criterion.

Mode of Operation
Low demand mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or high demand mode where the safety function is only performed on demand, in order to transfer the EUC into a specified state, and where the frequency of demands is greater than one per year; or continuous mode where the safety function retains the EUC in a safe state as part of normal operation.

MTBF (Mean Time Between Failures)
A basic measure of reliability for repairable items. The mean number of life units during which all parts of the item perform within their specified limits, during a measurement interval under stated conditions.

MTTF (Mean Time to Failure)
A basic measure of reliability for non-repairable items. The total number of life units of an item population divided by the number of failures within that population, during a measurement interval under stated conditions.

MTTR (Mean Time to Restoration)
Expected time to achieve restoration.

PFD (Probability of Dangerous Failure on Demand)
Safety unavailability of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.

PFD_{avg} (Average Probability of Dangerous Failure on Demand)
Mean unavailability of an E/E/PE safety related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.

RS-FS-9009-03-XXX
Class I Div 2, Zone 2, hazardous area certification.

RS-FS-9010-03-XXX
Class I Div I, Zone 0, hazardous area certification.

SFF (Safe Failure Fraction)
Property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.
$SFF = 1 – \lambda_{du} / (\lambda_d + \lambda_s)$

SIF (Safety Instrumented Function)
Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

SIL (Safety Integrity Level)
Safety Integrity Level – a discrete level (one out of four) for specifying the safety integrity requirement of the safety instrumented functions to be allocated to the safety instrumented systems.

SIS (Safety Instrumented System)
A SIS system comprises one or more safety functions; for each of these safety functions there is a SIL requirement.

Type A element
"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2.

UL (Upper Limit)
The sensor output above which the external diagnostics detect a failure. This document assumes sensor output currents greater than or equal to 21.0 mA meet this criterion.

6 Safety Function

The FTD 325 function is to take UV light as input and provide a standard 4 – 20 mA signal output. The sensor uses optics and electronics to generate a 4 -20 mA signal that is passed to the control system. The standard instrument range is 4-20 mA.

7 Failure classification

It is assumed that the operator is familiar with the Reuter-Stokes FTD 325 and the general use of industrial products in a hazardous environment. It is very important that the SIF designer verifies the FTD 325 Operation and Maintenance Manual for product specifications and environmental limits. If the sensor is used outside the application limits or not properly installed, the reliability data and predicted SIL capability becomes invalid.

The following references are used in the definition of Safe and Dangerous:

1) The output of the sensor shall be at least 5.00 mA when exposed to the minimum photon flux defined as $1x10^{10}$ photons/inch^2/sec at a wavelength of 310 nm.
2) In the field, at gas turbine power plants, set points for Flame OFF and Flame On are defined in the control logic. For Mark VIx and later controllers these values are commonly 6.25% (5 mA) and 12.5% (6 mA), respectively. Mark Vx controllers may be different. The SIL designer shall specify specific turbine settings to ensure safety.

Safe Failures

Safe Failures are defined as when a fault condition causes a sensor output below 4 mA anytime or below 5 mA when flame is present.

Dangerous Failures

Dangerous Failures are defined as when a fault condition causes a sensor output above 5 mA while no flame is present.

Safe Detected and Dangerous Detected Failures

Safe Detected and Dangerous Detected are failures detected by either software or personnel. The flame sensor RS-FS-9009 or RS-FS-9010 is not capable of detecting a failure unless it is part of an alarm/monitor/control system.

7.1 Definition of State(s) without External Diagnostic Control Logic

In this scenario, the turbine control system cannot detect any failure of the flame sensor. Therefore, all failures (safe or dangerous) are undetected.

7.2 Definition of State(s) with External Diagnostic Control Logic Containing Only LL

In this scenario, the turbine control system is configured to detect current below lower limit (LL). Current above upper Limit (UL) is not identified as a fault. Refer to section 5 for definitions of these values.

Current below LL alarm is considered Safe Detected. Failures which result in current above LL are undetected.

7.3 Definition of State(s) with External Diagnostic Control Logic Containing Both LL and UL

In this scenario, the turbine control system is configured to detect current below lower limit (LL) and above upper Limit (UL) as faults. Refer to section 5 for definitions of these values.

The LL alarm is considered Safe Detected.

The UL alarm is considered Dangerous Detected. Failures which result in current above 5mA and below UL remain Dangerous Undetected.

8 Proof Tests

Proof tests are to be performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition. Per section 7.4.3.2.2 (f) of the standard IEC 61508-2, proof-tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means 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 proof test can be performed either Off-Line or On-Line. For proof test coverage, it is assumed that external diagnostics are used. If the sensor fails to meet the functional check requirements as defined in either Off-Line or On-Line proof tests it must be removed from service.

8.1 Proof Test Off-Line

For the Off-Line proof test, the sensor should be disassembled from the machinery. The sensor shall remain connected to the wiring and the GT Control System can be used to check for performance. The following tests shall be performed:

1. Inspect the sensor assembly for any visual defects including but not limited to the connector i/o pins, the housing, NPT threads and the UV window. Clean the UV window as part of the preventive maintenance procedure defined in the operation and maintenance manual.
2. Perform Sensor Checkout, per the Sensor Checkout section of the appropriate O&M manual.

The proof test coverage of the Off-Line test is 90% in the field. Additional tests in factory with controlled equipment and instrumentation can exceed 90% proof test coverage. The sensor proof test is defined in the Operation and Maintenance Manual. It is recommended that this proof test be conducted at major scheduled maintenance intervals.

8.2 Proof Test On-Line

The On-Line proof test can be performed without the disassembly from the machinery. In this case, the GT Control System is powered but the machine is cool. There is no flame present and there are no light (dark) conditions. The following tests shall be performed:

1. Under no light conditions the sensor output should be between 3.7 mA and 4.1 mA. Performance can be verified using control software when the machine is idle (cool and no flame present).

This test is described in the Operation & Maintenance manual. The proof test coverage of the On-Line test is approximately 81% in the field. The on-line proof test coverage assesses Fail Dangerous Undetected. The on-line proof test does not monitor the output from a UV light source allowing only partial flame sensor function testing.

9 Failure Rates from FMEDA

Failure rate data from Table 3 could be utilized by the customer to calculate the average Probability of Failure on Demand (PFDavg). It is imperative to verify the assumptions and Architecture Constraints for each application listed in Section 4.2 of the FMEDA report.

Table 3 : Failure rates for the FTD325 with a Site Safety Index (SSI) of 2 (good site maintenance practices).

Failure Category	Failure Rate (FIT)
	Profile 3
Fail Safe Undetected (λ_{su})	2,199
Fail Dangerous Detected (λ_{dd})	168
Fail Detected (detected by internal diagnostics)	0
Fail High (detected by logic solver)	20
Fail Low (detected by logic solver)	148
Fail Dangerous Undetected (λ_{du})	351
No Effect	16

Customer Support Center

Reuter-Stokes
8499 Darrow Road
Twinsburg, OH, 44087 USA

Tel: +1-330-425-3755

www.bakerhughes.com