Failure Modes, Effects and Diagnostic Analysis

Project:
Fireye Flame Sensor Module
CE Flameswitch, model MBCE-110/230FR

Company:
Fireye
Derry, NH
USA

Contract Number: Q09/10-26
Report No.: FIR 09/10-26 R001
Version V1, Revision R2, December 13, 2010
Griff Francis
Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Fireye Flame Sensor Module. The CE Flameswitch, model MBCE-110/230FR uses flame rods to sense flame presence independently or as a component in a burner management system.

A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined.

For safety instrumented systems usage it is assumed that the MBCE-110/230FR Flame Sensor Module relay contacts are used as the safety output. The 4-20mA current loop is considered as non-interfering.

The MBCE-110/230FR Flame Sensor Module is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

The failure rates for the MBCE-110/230FR Flame Sensor Module are listed in Table 1.

Table 1 Failure rates MBCE-110/230FR Flame Sensor Module

<table>
<thead>
<tr>
<th>Failure Category</th>
<th>Failure Rate (FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Safe Detected</td>
<td>50.0</td>
</tr>
<tr>
<td>Fail Safe Undetected</td>
<td>80.0</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>245.1</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>8.0</td>
</tr>
<tr>
<td>Residual</td>
<td>89.4</td>
</tr>
<tr>
<td>Annunciation Undetected</td>
<td>21.4</td>
</tr>
</tbody>
</table>

¹ Type B device: “Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
Table 2 lists the interfering failure rates for the MBCE-110/230FR Flame Sensor Module according to IEC 61508.

Table 2 Failure rates according to IEC 61508

<table>
<thead>
<tr>
<th>Device</th>
<th>$\lambda_{SD}$</th>
<th>$\lambda_{SU}^2$</th>
<th>$\lambda_{DD}$</th>
<th>$\lambda_{DU}$</th>
<th>SFF$^3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBCE-110/230FR Flame Sensor Module</td>
<td>50 FIT</td>
<td>190.8 FIT</td>
<td>245.1 FIT</td>
<td>8.0 FIT</td>
<td>98.4%</td>
</tr>
</tbody>
</table>

A user of the MBCE-110/230FR Flame Sensor Module can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF). It is recommended that an engineering tool like the exida exSILentia® be used for this purpose. A full table of failure rates is presented in section 4.4 along with all assumptions.

---

$^2$ It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

$^3$ Safe Failure Fraction needs to be calculated on (sub)system level
Table of Contents

Management Summary ....................................................................................................... 2

1 Purpose and Scope ...................................................................................................... 5

2 Project Management .................................................................................................... 6

  2.1 exida ................................................................................................................................. 6

  2.2 Roles of the parties involved .......................................................................................... 6

  2.3 Standards and Literature used ..................................................................................... 6

  2.4 Reference documents ................................................................................................... 7

    2.4.1 Documentation provided by Fireye ........................................................................... 7

    2.4.2 Documentation generated by exida ......................................................................... 7

3 Product Description ...................................................................................................... 8

4 Failure Modes, Effects, and Diagnostic Analysis .......................................................... 9

  4.1 Failure Categories description ..................................................................................... 9

  4.2 Methodology – FMEDA, Failure Rates ....................................................................... 9

    4.2.1 FMEDA ....................................................................................................................... 9

    4.2.2 Failure Rates .............................................................................................................. 9

  4.3 Assumptions ................................................................................................................... 10

  4.4 Results ........................................................................................................................... 11

5 Using the FMEDA Results .......................................................................................... 13

  5.1 PFD_{AVG} Calculation MBCE-110/230FR Flame Sensor Module ................................ 13

6 Terms and Definitions ................................................................................................ 14

7 Status of the Document .............................................................................................. 15

  7.1 Liability .......................................................................................................................... 15

  7.2 Releases ........................................................................................................................... 15

  7.3 Future Enhancements .................................................................................................... 15

  7.4 Release Signatures ......................................................................................................... 16

Appendix A Lifetime of Critical Components .................................................................... 17

Appendix B Proof tests to reveal dangerous undetected faults .................................... 18
1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by exida according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration per IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by exida according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends Option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the MBCE-110/230FR Flame Sensor Module. From this, failure rates are calculated.

The information in this report can be used to evaluate whether a sensor subsystem meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.
2 Project Management

2.1 exida

exida is one of the world’s leading certification and knowledge companies specializing in automation system safety and availability with over 300 man years of cumulative experience in functional safety. Founded by several of the world’s top reliability and safety experts from assessment organizations and manufacturers, exida is a global company with offices around the world. exida offers product functional safety and security certification, training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. exida maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Fireye Manufacturer of the MBCE-110/230FR Flame Sensor Module

exida Performed the hardware assessment according to Option 1 (see Section 1)

Fireye contracted exida in November 2009 with the hardware assessment of the above-mentioned device.

2.3 Standards and Literature used

The services delivered by exida were performed based on the following standards / literature.

|-------|------------------|--------------------------------------------------------------------------------------|
2.4 Reference documents

2.4.1 Documentation provided by Fireye

<table>
<thead>
<tr>
<th>[D1]</th>
<th>75-5687-R3.pdf</th>
<th>Schematic, CE Flameswitch, Drawing No. 75-5687, Rev. 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D2]</td>
<td>127-3541-R4.pdf</td>
<td>Parts List for 61-7177-1 Board CE Flameswitch, Drawing No. 127-3541, Rev. 4</td>
</tr>
</tbody>
</table>

2.4.2 Documentation generated by *exida*

<table>
<thead>
<tr>
<th>[R1]</th>
<th>Fireye Flame Sensor Module Common.efm</th>
<th>Failure Modes, Effects, and Diagnostic Analysis – MBCE-230FR Flame Sensor Module</th>
</tr>
</thead>
</table>
3 Product Description

The MBCE-110/230FR Flame Sensor Module provides LED indication and electrical outputs that signal the user regarding flame presence in a combustion chamber. The electrical outputs consist of normally open and normally closed relay contacts (safety critical) and a 4-20mA current loop (non-interfering) for flame signal strength. The module uses Fireye flame rods to sense flame presence using the ionization principal. It may be used independently or as a component in a burner management system.

The MBCE-110/230FR Flame Sensor Module for interference purposes is classified as a Type B\(^4\) device according to IEC 61508, having a hardware fault tolerance of 0.

Figure 1 provides an overview of the MBCE-110/230FR Flame Sensor Module and the boundary of the FMEDA.

---

\(^4\) Type B device: “Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Fireye and is documented in [D1] through [D3].

4.1 Failure Categories description

In order to judge the failure behavior of the MBCE-110/230FR Flame Sensor Module, the following definitions for the failure of the device were considered.

- **Fail Dangerous**: Failure that interferes with the safety function of the PLC or Burner Management System.
- **Fail Safe**: Failure that causes a false relay contact open
- **Fail Dangerous Detected**: Dangerous failure that is detected by automatic internal diagnostics
- **Fail Dangerous Undetected**: Dangerous failure that is not detected by automatic internal diagnostics
- **Fail Safe Detected**: Safe failure that is detected by automatic internal diagnostics
- **Fail Safe Undetected**: Safe failure that is not detected by automatic internal diagnostics
- **Residual**: Failure of a component that is part of the safety function but has no impact on proper operation of the safety function
- **Annunciation**: Failure of a component that will impact automatic diagnostics

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by exida in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook [N2] which was derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match exida Profile 1, see Table 3. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.
Table 3 exida Environmental Profiles

<table>
<thead>
<tr>
<th>EXIDA ENVIRONMENTAL PROFILE</th>
<th>GENERAL DESCRIPTION</th>
<th>PROFILE PER IEC 60654-1</th>
<th>AMBIENT TEMPERATURE [°C</th>
<th>TEMP CYCLE [°C / 365 DAYS]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cabinet Mounted Equipment</td>
<td>Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings</td>
<td>B2</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>2 Low Power/Mechanical Field Products</td>
<td>Mechanical / low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings</td>
<td>C3</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>3 General Field Equipment</td>
<td>General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings</td>
<td>C3</td>
<td>25</td>
<td>45</td>
</tr>
<tr>
<td>4 Unprotected Mechanical Field Products</td>
<td>Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation.</td>
<td>D1</td>
<td>25</td>
<td>30</td>
</tr>
</tbody>
</table>

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however, should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the MBCE-110/230FR Flame Sensor Module.

- Only a single component failure will fail the entire MBCE-110/230FR Flame Sensor Module
- Failure rates are constant, wear-out mechanisms are not included
- Propagation of failures is not relevant
• All components and failure modes that are not potentially interfering and cannot influence the safety function of the connected sub-device (feedback immune) are excluded.

• The stress levels are average for an industrial environment and can be compared to the exida Profile 1 with temperature limits within the manufacturer’s rating. Other environmental characteristics are assumed to be within manufacturer’s rating.

• Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics.

• The device is installed per manufacturer’s instructions.

• External power supply failure rates are not included.

4.4 Results

Using reliability data extracted from the exida Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the MBCE-110/230FR Flame Sensor Module FMEDA.

The failure rates for the MBCE-110/230FR Flame Sensor Module are listed in Table 4.

Table 4 Failure rates MBCE-110/230FR Flame Sensor Module

<table>
<thead>
<tr>
<th>Failure Category</th>
<th>Failure Rate (FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Safe Detected</td>
<td>50.0</td>
</tr>
<tr>
<td>Fail Safe Undetected</td>
<td>80.0</td>
</tr>
<tr>
<td>Fail Dangerous Detected</td>
<td>245.1</td>
</tr>
<tr>
<td>Fail Dangerous Undetected</td>
<td>8.0</td>
</tr>
<tr>
<td>Residual</td>
<td>89.4</td>
</tr>
<tr>
<td>Annunciation Undetected</td>
<td>21.4</td>
</tr>
</tbody>
</table>

These failure rates are valid for the useful lifetime of the product, see Appendix A.

Table 5 lists the failure rates for the MBCE-110/230FR Flame Sensor Module according to IEC 61508. However as the MBCE-110/230FR Flame Sensor Module is only one part of a (sub)system, the SFF should be calculated for the entire sensor / logic / final element combination. The Safe Failure Fraction is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formulas for SFF: 

\[ SFF = 1 - \frac{\lambda_{DU}}{\lambda_{TOTAL}} \]
Table 5 Failure rates according to IEC 61508

<table>
<thead>
<tr>
<th>Device</th>
<th>$\lambda_{SD}$</th>
<th>$\lambda_{SU}^5$</th>
<th>$\lambda_{DD}$</th>
<th>$\lambda_{DU}$</th>
<th>SFF$^6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBCE-110/230FR Flame Sensor Module</td>
<td>50 FIT</td>
<td>190.8 FIT</td>
<td>245.1 FIT</td>
<td>8.0 FIT</td>
<td>98.4%</td>
</tr>
</tbody>
</table>

The architectural constraint type for the MBCE-110/230FR Flame Sensor Module is B. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

$^5$ It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

$^6$ Safe Failure Fraction needs to be calculated on (sub)system level.
5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

For use of the MBCE-110/230FR Flame Sensor Module on a connected sub-device that is part of a SIF, the Dangerous Undetected failure rates for the MBCE-110/230FR Flame Sensor Module are added to failure rates for the associated connected sub-device prior to the SFF or PFD$_{AVG}$ calculations for the Safety Instrumented Function (SIF).

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The results must be considered in combination with PFD$_{AVG}$ values of all other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a SIL.

5.1 PFD$_{AVG}$ Calculation MBCE-110/230FR Flame Sensor Module

An average Probability of Failure on Demand (PFD$_{AVG}$) calculation is performed for a single (1oo1) MBCE-110/230FR Flame Sensor Module. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. For the proof tests, a proof test coverage of 78% has been assumed, see Appendix B.

The resulting PFD$_{AVG}$ values for a variety of proof test intervals are displayed in Figure 2. As shown in the graph the PFD$_{AVG}$ value for a single MBCE-110/230FR Flame Sensor Module, with a proof test interval of 1 year equals 1.11E-04.

![Figure 2 PFD$_{AVG}(t)$ MBCE-110/230FR Flame Sensor Module](image)

For SIL 2 applications, the PFD$_{AVG}$ value needs to be $\geq 10^{-3}$ and $< 10^{-2}$. This means that for a SIL 2 application, the PFD$_{AVG}$ for a 1-year Proof Test Interval of the MBCE-110/230FR Flame Sensor Module is approximately equal to 1.1% of the range.

These results must be considered in combination with PFD$_{AVG}$ values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).
### 6 Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIT</td>
<td>Failure In Time (1x10-9 failures per hour)</td>
</tr>
<tr>
<td>FMEADA</td>
<td>Failure Mode Effect and Diagnostic Analysis</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>Low demand mode</td>
<td>Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>PFD$_{AVG}$</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SIS</td>
<td>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).</td>
</tr>
<tr>
<td>Type A component</td>
<td>“Non-Complex” component (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2</td>
</tr>
<tr>
<td>Type B component</td>
<td>“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2</td>
</tr>
</tbody>
</table>
7  Status of the Document

7.1  Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. exida accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, exida is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an exida FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2  Releases

Version: V1
Revision: R2

Version History: V0, R1: Draft; December 7, 2009
V1, R1: Edited per review, December 11, 2009
V1, R2: Added 110/230V transformer

Author(s): Griff Francis
Review: V0, R1: William Goble, exida
V1, R2: William Goble, exida

Release Status: Released

7.3  Future Enhancements

At request of client.
7.4 Release Signatures

Dr. William M. Goble, Principal Partner

Griff Francis, Safety Engineer
Appendix A  Lifetime of Critical Components

According to section 7.4.7.4 of 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 section 4.2.2) 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.

This assumption of a constant failure rate is based on the bathtub 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.

Table 6 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 6 Useful lifetime of components contributing to dangerous undetected failure rate

<table>
<thead>
<tr>
<th>Component</th>
<th>Useful Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aluminum Aqueous Electrolytic Capacitors, C1 and C4</td>
<td>Approx. 90,000 hours</td>
</tr>
</tbody>
</table>

It is the responsibility of the end user to maintain and operate the MBCE-110/230FR Flame Sensor Module per manufacturer’s instructions. Furthermore regular inspection should show that all components are clean and free from damage.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

---

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.
Appendix B  Proof tests to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic 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 simple suggested proof test can be performed with the MBCE-110/230FR Flame Sensor Module without need for removal from the process. This test will detect 78% of possible DU interfering failures in the MBCE-110/230FR Flame Sensor Module. This test technique should be added to the transmitter test if not already included in that test.

Table 7 Proof Test

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Bypass the safety function and take appropriate action to avoid a false trip.</td>
</tr>
<tr>
<td>2.</td>
<td>Manually verify relay deenergizes with no flame.</td>
</tr>
<tr>
<td>3.</td>
<td>Manually verify relay energizes with the flame.</td>
</tr>
<tr>
<td>4.</td>
<td>Remove the bypass and otherwise restore normal operation</td>
</tr>
</tbody>
</table>