Certification of Compliance for SIL Safety Applications

1st December 2011

Certification of Compliance for 45UV5 Flame Scanners and 25SU3 and 25SU5 Flame Safeguard family used in SIL Safety Applications

Fireye Controls and Safety Testing - A critical part of certifications and agency testing (eg TUV, DVGW, DIN, CE) is extensive analysis to verify that the products are fail-safe as defined in clause 9 (Protection against internal faults) of EN298.EN 298, clause 9 states the system shall be fail-safe. It further defines that the system must be fail-safe with any 2 concurrent hardware and/or software faults. Verifying that capability required several months of detailed failure mode testing and analysis, involving design engineers and test technicians.

The general procedure is as follows:

(1) One by one, a fault is asserted in every component and software module in the product. With that fault asserted, the product must immediately either a) de-energize the flame relay or b) continue to operate in compliance with all applicable standards.
(2) If, in response to the fault asserted in (1) above, the product responds as described in b) above, then, one by one, while maintaining the first fault, a second fault must be asserted in every component and software module in the product. With two faults now asserted, the product must immediately either a) de-energize the flame relay or b) continue to operate in compliance with all applicable standards.

The Fireye controls listed passed rigorous test and analysis and each has been certified by TUV (arguably the most demanding agency in the world) as meeting the requirements of EN298.

MTBF and use with SIL classifications - MTBF, Failure Mode Analysis, SIL calculation information

In order to make a SIL calculation for probability of failure on demand average (PFDavg), we need to specify the dangerous failure rate of the product. The dangerous failure rate of the products are the failure rate of the times that they will see or indicate flame when there is not flame, i.e. fail to trip on loss or lack of flame. Total numbers can be used but two other parameters are required. First is the percent safe failures and the second is the dangerous diagnostic coverage (that percent of the diagnostics that will detect dangerous failures from the over all dangerous failure modes.)

Proof testing for these devices are undertaken to reveal dangerous faults that may be undetected by diagnostic tests (according to section 7.4.3.2.2 f of IEC 61508-2). It is

necessary to record how dangerous undetected faults which have been noted during FMEDA can be detected during proof testing. The overview above provides some details of the type of proof testing as it applies to the design verification testing (DVT) carried out by the numerous independent test agencies. Each individual agency provides detailed analysis, testing and test reports to the product vendor to ensure final compliance. As the dangerous undetected failure rates of these products is low and in addition the solid state nature of the controls have many years of proven in use documentation and well identified failure modes, the use of specific proof tests is limited to those recommended in the product technical bulletin. This is namely a proof test where the loss of flame is simulated and the operation of the flame relay is observed. This will assist in the detection of more than 90% of dangerous undetected failures. The use of a pre-start permissive in BMS logic to monitor the flame relay condition prior to start up is an industry recommended practice. With regards to installation, it is assumed for these calculations that the installation is completed correctly and tested at startup.

45UV5 FLAME SCANNER FAMILY NUMBERS

Current Failure rate = 0.053 failure per year = 6.05E-06 per hour
MTBF (dem) = 1/failure rate = 18.86 years

Overall failure rate	= 6.05E-06 hr
Assumed Safe failure %	= 40%
Safe Failure Rate	= 2.44E-06hr
Dangerous failure rate w/o diagnostics	= 3.63E-06 hr
Dangerous Diagnostic Coverage	= 98.8
Dangerous failure rate w/ diagnostics	= 4.36-08 hr

Probability of failure on demand can be calculated from the above.

The calculation used is

$$PFDavg \sim \tfrac{1}{2} \lambda_u T_i = \frac{T_i}{2 \times MTBFFTD}$$

PFDavg = Average Probability Failure on Demand,
?u = Unrevealed Failure Rate (per year),
Ti = Test interval in years between the life testing of the protective function,
MTBF(FTD) = Mean Time Between Failure (Fail To Danger) [yr]

The unknown is the Ti - This would typically be defined by the customer's specific needs or to meet a particular safety level. In general the more frequent the test interval the better the

PFD and therefore the higher the SIL level that can be accommodated with the product. Using the calculations above, assuming (Ti = 2 years) the product has a PFD of 3.81 x 10-4

This would mean the product would exceed the requirements for use in a SIL 2 category.

25SU3, 25SU5 FLAME SAFEGUARD FAMILY NUMBERS

Failure rate = 0.016 failure per year = 1.83E-06 per hour
MTBF (dem) = 1/failure rate = 62.5 years

Overall failure rate	= 1.83E-06 hr
Assumed Safe failure %	= 50%
Safe Failure Rate	= 9.13E-07hr
Dangerous failure rate w/o diagnostics	= 9.13E-07hr
Dangerous Diagnostic Coverage	= 97.2
Dangerous failure rate w/ diagnostics	= 2.56-08 hr

Probability of failure on demand can be calculated from the above.

Using the calculations above, assuming (Ti = 2 years) the product has a PFD of 2.24 x 10-4
This would mean the product would exceed the requirements for use in a SIL 2 category.

Regards

John Devine
Vice President Sales and Marketing
Fireye Inc.