

IEC 61508 / IEC 61511
Failure Rate Data – Validity Insights
The need for Certified Data Sets

Bud Adler
Moore Industries International

There is not a chemical plant or refinery on the globe that does not have the need for insuring the functional safety of their process operations. International standards including IEC 61508 and IEC 61511 provide guidance on reaching safety integrity levels commensurate with the risks of operating the process. This guidance requires demonstrating competence in every phase of the safety life cycle from original design thru all of its years of operation until the system is retired from service.

Part of the lifecycle deals with verifying that the components of a Safety Instrumented Function (SIF) function together in accordance with the desired Safety Integrity Level (SIL). There are published methods of verifying that a SIL has been reached that require calculations of Probability of Failure on Demand (PFD). The equations that are provided in the standard require the design engineer to insert reliability data for each device. The concern is for using data that accurately represents the potential for a dangerous failure of each device. This fail dangerous data is part of a failure analysis performed on each device or can be based on having adequate long-term usage data for the device complete with detailed failure records.

Few plants have adequate data keeping of device failures to be able to make intelligent decisions on failure probability. A Failure Modes and Effects, Diagnostic Analysis (FMEDA) report is an alternative that has gained wide industry acceptance. The report contains all of the failure rate data required to do SIL verification calculations.

All FMEDA techniques are not the same. The basic procedure has evolved from MIL standard 1620A and is a rigorous mathematical analysis that manipulates data from a variety of component databases. Where there is room for interpretation, the testing engineer will typically do further testing and analysis. This may be by actual fault insertion into the device or by circuit simulation software like PSPICE. This technique adds significantly to the validity of the FMEDA. Unfortunately, not all FMEDAs are done by engineers with the same level of competence. Competent safety hardware engineers are more likely to perform a complete and accurate analysis than would a less experienced engineer.

A manufacturer that has accredited certification to IEC 61508 must go through a rigorous auditing process. SIRA is one of the premier agencies that conduct such audits according to the Conformity Assessment of Safety Systems (CASS) scheme. The assessment includes verification of Functional Safety Capability from management levels all the way throughout the company. The assessment also demands that detailed design,

manufacturing, testing and documentation policies are in place. A successful certification insures that the manufacturing company has the qualifications to design and build instrumentation devices in accordance with IEC 61508. As part of this certification, the manufacturer is capable of conducting a valid FMEDA.

Accordingly, the FMEDA report from such a vendor includes data that is certified to be in conformance with the intent and guidance of IEC 61508. The term “Certified Data Sets” has emerged to provide this distinction. FMEDA reports from other sources may carry some concern as to their validity. A prudent user would be wise to inquire as to the qualifications of the company with regard to its functional safety capabilities and engineers doing the FMEDA.

A user should expect to receive a complete FMEDA report with certified data sets, testing detail, product scope and functionality and references to its use in accordance with a product safety manual.

Certified Data Sets for any given component to be used in a safety related system provide far more open, meaningful and useable information, with far greater confidence than a ‘certified product certificate’. It is often the case, ‘product certificates’ are provided through closed investigation and assessment regimes, within unknown competencies, tools, techniques and procedures.

The liabilities of non-conformance with the guidelines of the standard may be significant. It is a wise design engineer that demands failure rate data from qualified and certified sources.