Product Safety Case Study
Compliance Testing and Certification

MOORE INDUSTRIES WORLDWIDE

Background

Moore Industries-International, Inc. is a world leader in the design and manufacture of signal interface instruments for industrial process control, system integration, and factory automation.

Providing products and services to fortune 500 companies worldwide, the products of Moore Industries are used in industries such as: chemical and petrochemical; power generation and transmission; petroleum extraction, refining and transport; pulp and paper; food and beverage; mining and metal refining; pharmaceuticals and biotechnology; industrial machinery and equipment; water and wastewater; and environmental and pollution monitoring.

Moore Industries is an international company with direct sales offices in strategic worldwide locations including the United States of America, Australia, Belgium, the Netherlands, the People's Republic of China and the United Kingdom. These offices oversee an expansive network of independent representatives and agents serving every corner of the globe.

Challenge

Moore Industries believes it is of vital importance to have third-party SIS evaluation for plant safety provided by a company with global coverage and reputation. Earlier designs for process control and safety systems typically used "good engineering practices and experience" as their guidelines. As safety awareness evolved new standards started to evolve. International standards such as IEC 61508/61511 and U.S. born standards like ANSI/ISA84 require the use of more sophisticated guidelines for implementing safety. Unfortunately for manufacturers, compliance with IEC 61508 standards requires enormous documentation. In addition, more complex products require a greater depth of analysis. Software-based products such as those from Moore Industries are complex with their inherent programmable and flexible features unlike previous generation single function analog circuits.

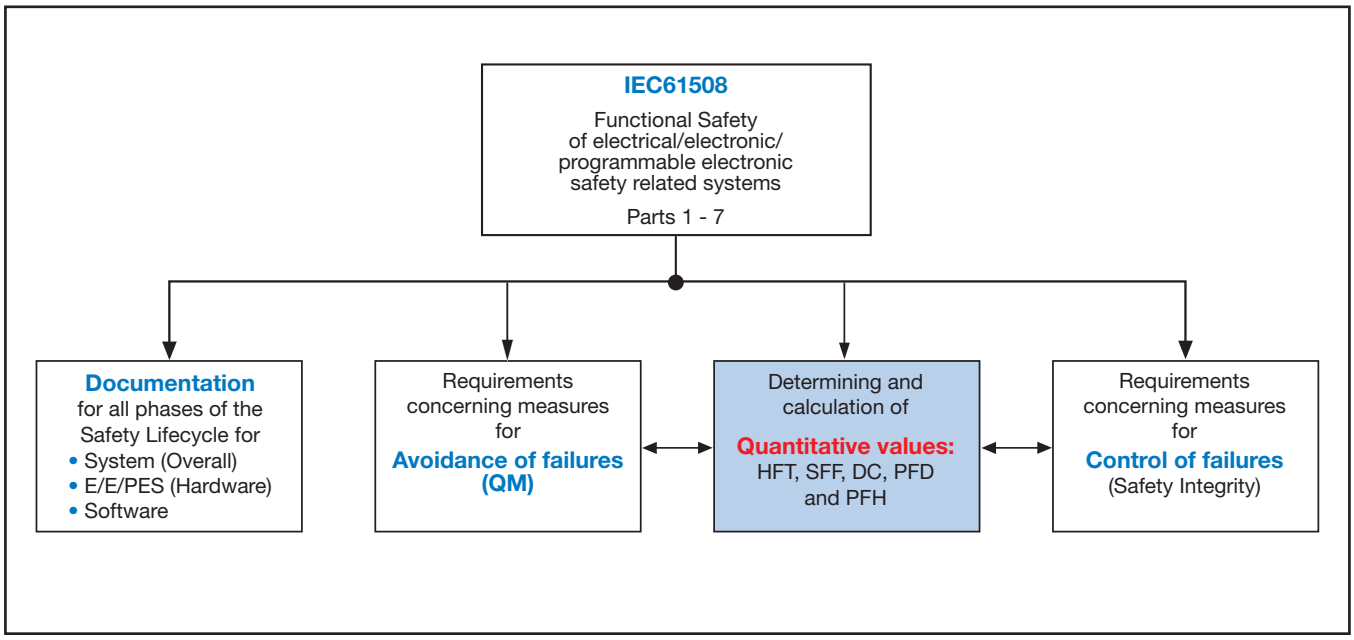

Figure 1: IEC 61508 product development requirements (from TÜVRheinland® gap analysis presentation)

Some companies are actively attempting to bypass the vital third party certification by proclaiming self certification to IEC 61508. This is not in the best interest of end users or the safety industry in general. Self certification is analogous as someone proclaiming compliance without third party testing on a hazardous area approval (such as Intrinsically-Safe).

Moore Industries has been working for many years with customers who require products for safety systems, including those compliant with worldwide safety standards such as ANSI/ISA 84 and IEC 61508/61511. To assist customers in determining if their instruments are appropriate for specific safety systems, Moore Industries has been providing Failure Modes, Effects and Diagnostic Analysis (FMEDA) reports for key products, and has been involved in the evolution of the IEC 61508 standard. As this standard has become more widely recognized and adopted by worldwide customers it was clear that end users were looking for products which had been designed to IEC 61508 from their initial concept. Customers are demanding not only compliance to the standards but verification from an independent third party agency such as TÜVRheinland®.

Solution Testimonial — SIL Certification with TÜVRheinland® — Experience of Developing a Functional Safety Product

Moore Industries decided that its first IEC 61508-compliant, independently certified safety product would be a safety trip alarm (STA), in the safety world, called a single loop logic solver. The company has been providing single loop logic solvers for safety applications for many years, and would draw on this extensive experience when developing a safety trip alarm designed from the ground up to IEC 61508. A single loop logic solver, monitors a temperature, pressure, level, flow, position or status variable. If the input exceeds a selected high or low trip point, one or multiple relay outputs warn of unwanted process conditions, provide emergency shutdown or provide on/off control, such as in a level control application. Users can realize many of the same advantages of larger and more expensive safety-certified PLCs at a fraction of the cost.

Instruments fully compliant with IEC 61508 address systematic faults by a full assessment of fault avoidance and fault control measures during hardware and software development. There are three main parts to IEC 61508 which specify these requirements. Part 1 addresses the overall functional safety management of the product. Part 2 covers the hardware requirements, including achievement of failure rates and diagnostic coverage as well as specific techniques and measures for avoidance of systematic failures. Part

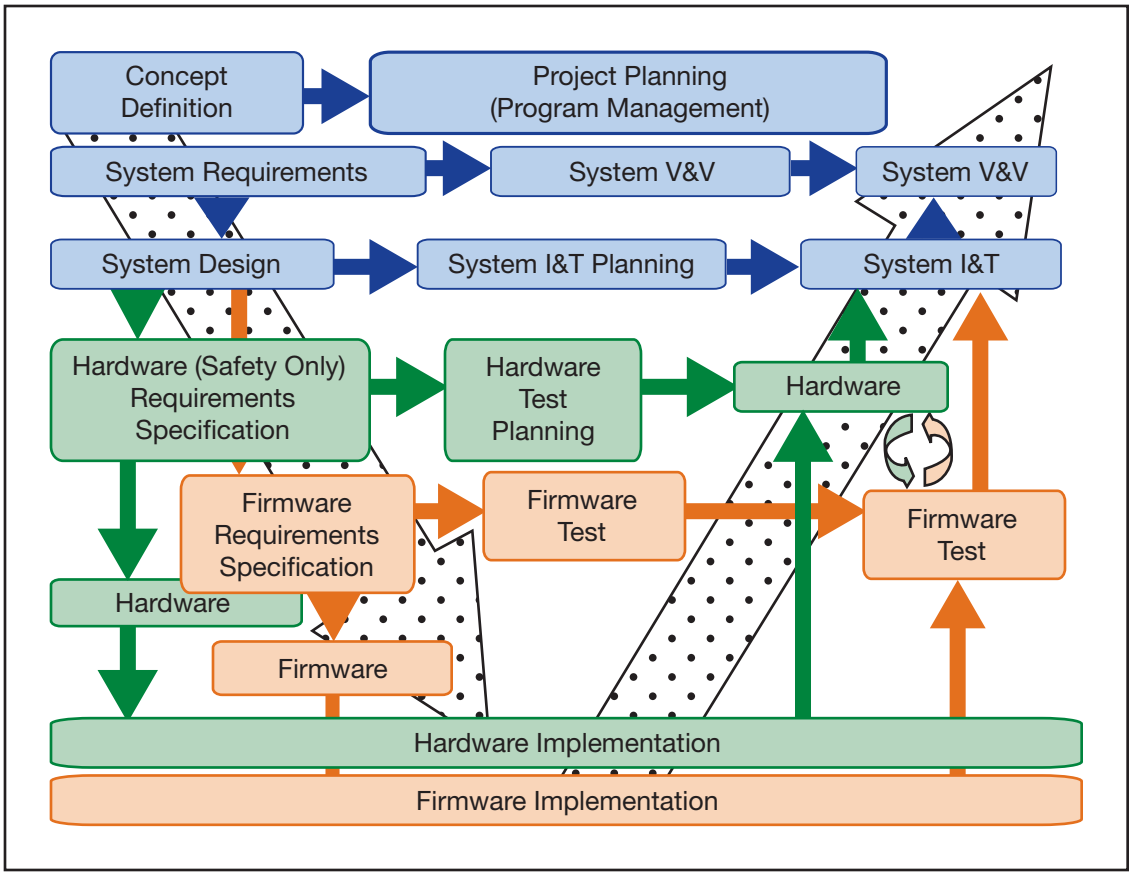

Figure 2: Development Lifecycle "V model" Functional Safety Product

3 covers the software requirements and is primarily focused on the process used when developing the software, including specific use of techniques, design and coding standards and analysis and testing techniques. Some products claim compliance by a hardware failure analysis plus a 'proven in use' argument. These have no consideration for systematic faults introduced during the development process. (See Figure 1).

At the outset of STA Safety Trip Alarm product development, Moore Industries was looking for a trusted third-party certifying agency with a very solid reputation in the safety industry to assess our instrument. They selected TÜVRheinland® as one of the most respected agencies in safety. Moore Industries also wanted to benefit from their experience and partnered with TÜVRheinland® from the initial concept through the entire design and development process.

To understand the scope of the project, design engineers from Moore Industries had a two day meeting with the safety experts at TÜVRheinland® to discuss the proposed development and the requirements of IEC 61508. Moore Industries provided TÜVRheinland® with some initial project documentation (product proposal, product development plan, preliminary design and FMEDA analysis), and during the meeting TÜVRheinland® outlined the requirements and identified the 'gaps' that needed to be addressed. Moore Industries' process is already ISO9001 compliant, so a lot of the design process of IEC 61508 was familiar to the company's design engineers. The major difference was the focus on specific techniques and measures, and the rigor in documenting why as well as what was done.

In the concept/planning phase, the emphasis was placed on ensuring that the development plan, product concept and design methodology would result in a product which would address all the requirements of IEC 61508. This specifically addressed:

- Management of functional safety (project organization and responsibilities, development lifecycle, tools, and documentation).
- Avoidance of systematic failures (design of system architecture, hardware and software modules including techniques and measures).
- Control of operational failures (techniques and measures for control of random hardware, environmental or operational failures).

The system requirements were designed with functional safety in mind (fail-safe relays, dedicated fault relay, system diagnostics, etc.). During this phase Moore Industries worked closely with TÜVRheinland® to agree on the development plan (based on the V lifecycle model - see Figure 2), the selection of techniques and measures for the safety integrity level (SIL) and the system design to meet the required diagnostic coverage. Once the concept phase was complete and approved by TÜVRheinland®, Moore Industries' engineers started on the design, implementation and test phases, categorized by TÜVRheinland® as the main approval phase.

At the beginning of this phase there were a number of recently-assigned engineers on the project team, and TÜVRheinland® held a training class at Moore Industries' world headquarters, located outside of Los Angeles, CA. This helped accelerate the learning curve of the engineers and raised the awareness and knowledge of IEC 61508 in other groups in the company including quality, sales and customer support.

The hardware design was based on a previous alarm trip design, so design engineers had the benefit of using tried and tested components. The additional safety requirements added some redundancy and diagnostic circuitry (e.g. clock monitors, voltage detection.) The final design was subject to an FMEDA analysis to calculate the Safety Failure Fraction (SFF) and Probability of Failure on Demand (PFDAVG). Even though this was an area Moore Industries has considerable experience in, they worked very closely with TÜV to agree on the underlying assumptions, methodology and formatting of the FMEDA report, and TÜVRheinland® validated all calculations. This analysis also identified requirements for the software to provide increased diagnostic coverage.

Part 3 of IEC 61508 defines the requirements for software including use of techniques and measures to meet specific SIL ratings. TÜVRheinland® helped interpret these requirements with a set of software and coding guidelines, as well as a discussion of selecting the appropriate techniques. Since this would be the first in a series of safety products the company has planned, it was decided to maximize the investment in software by creating a library of re-usable software functions/modules. To help meet the stringent safety requirements, Moore Industries engineers used a number of tools including automated document generation, static analysis and module test. Use of these tools helped in the development of well documented, clean, structured and verified software code which could be released for integration testing with confidence.

Integration and V&V (Verification and Validation) testing also made use of an automated test tool which the company had developed in house over a number of years. With this tool, design engineers were able to run more complete regression testing whenever issues were found. Regression testing is repeating

tests already performed once an issue has been identified and corrected. During the main approval phase, updates were provided to TÜVRheinland® to ensure the product development was always on the right track. In addition, fault insertion testing was agreed upon. This is a process where faults were deliberately initiated and the results witnessed by TÜVRheinland® as part of the final verification.

Project management, documentation and configuration control were also essential disciplines that had to be maintained throughout this product development. One of the last steps in the approval process was a site visit by TÜVRheinland® to audit Moore Industries' Functional Safety Management process and witness fault insertion testing on the product. Final design, test and user documentation was then submitted to TÜVRheinland® for their inspection.

Working with TÜVRheinland® throughout the project enabled Moore Industries' design engineers to demonstrate compliance. A certificate was issued shortly after the audit. The company's STA Safety Trip Alarm is now certified to IEC 61508 for single use in Safety Instrumented Systems (SIS) up to SIL2 and the firmware development process is suitable for a SIL 3 system. This allows the STA to be used in a redundant architecture (1oo2, 2oo3, etc.) up to SIL 3.

Solution Results

The stringent steps required to pass an assessment by TÜVRheinland® equal a greater level of safety assurance. This reinforces the value of specifying products that have gone through the TÜVRheinland® assessment process and not self certified.

Moore Industries chose TÜVRheinland® as a source for international safety approval due to the company's strong quality reputation and recognition as a globally accepted certifying body.

TÜVRheinland®
Precisely Right.

1-TUV-RHEINLAND
(1-888-743-4652)
Int'l +1 203-426-0888
www.us.tuv.com

MOORE INDUSTRIES
WORLDWIDE

1-800-999-2900
Int'l +1 818-894-7111
www.miinet.com