MOORE INDUSTRIES WORLDWIDE

Vetting Smart Instruments for the Nuclear Industry

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. We provide products and services to Fortune 500 companies worldwide that 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
- Environmental and Pollution Monitoring

Moore Industries worked with the Control and Instrumentation Nuclear Industries Forum (CINIF, UK) on the conceptual development of the EMPHASIS assessment tool for “smart” instruments intended for use in nuclear safety-critical applications in the UK. The result was a common framework for determining suitability of these devices in nuclear powered facilities that was released in 2005. It provides a measure of “Production Excellence” which includes the entire scope of company, product development, and actual product in the assessment. The EMPHASIS assessment tool has subsequently been developed further and supported by Adelard LLP on behalf of CINIF.

Using the EMPHASIS tool, Moore Industries has achieved approval for four smart instruments (one at SIL 2) with a fifth instrument currently in the approval process.

Smart Instrument Assessment

Earlier designs for process control and safety systems typically used “good engineering practices and experience” as their guidelines. As safety awareness evolved, new standards also evolved. International standards such as IEC 61508/61511 require the use of more sophisticated guidelines for implementing safety. Compliance with IEC 61508 standards requires enormous documentation and a greater depth of analysis and testing. Unlike previous generation single-function analog circuits, software-based products such as those from Moore Industries are complex with their inherent programmable and flexible features.

Assessment and approval of smart instrumentation for nuclear applications uses the EMPHASIS tool, which asks in-depth questions based on the IEC 61508 standard. Each answer provides three links in the “Claim/Argument/Evidence” chain. The argument and evidence back up and justify the claims or provide mitigation when a requirement cannot be met or proven. In general, full compliance with IEC 61508 will significantly contribute toward the EMPHASIS assessment for Production Excellence.

Production Excellence is one of the two “legs” used to substantiate safety to the regulator. The second leg involves Independent Confidence Building Measures, where different and independent competent individuals or specialists use measurements and techniques such as Static Analysis or Statistical Testing to examine the device’s source code. This detailed analysis ensures that the product performs as claimed and designed.

Instruments that are fully compliant with IEC 61508 address systematic faults through 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 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.

Note: Some products claim compliance by a hardware failure analysis plus a “Proven in Use” argument. These products have no consideration for systematic faults introduced during the development process.

Initial EMPHASIS Assessment

Three of the four EMPHASIS-approved instruments from Moore Industries are older instruments that had not been designed and developed to IEC 61508. They were instead designed using an ISO9001-compliant process. The first instrument assessed in 2007 was a 535 process controller, which had more than 10 years proven in use and was also approved for use in U.S. nuclear applications. This assessment focused on original design documentation, current manufacturing and design processes, along with an independent hardware (FMEDA) and software analysis.

The hardware design is relatively straightforward and had been thoroughly tested under environmental and fault conditions and the warranty return data was able to support the FMEDA analysis. The software is more complex with many optional features. From a safety perspective, the source code required further examination and testing.

The assessors performed software analyses using both static and dynamic tools, QA.C and VectorCAST. These tools provide the required metrics – such as complexity metrics that measure code structure complexity and code coverage during testing (such as statement, condition or path coverage). Moore Industries previously used Lint for static analysis, which applies general rules as opposed to full MISRA compliance. No dynamic analysis had been used for unit testing, so this was a learning experience. In addition to the new tools, knowledge of the choice of metrics and thresholds was also gained.

Figure 1. *STA SIL 2 and SIL 3 Capable Programmable Current/ Voltage and RTD/Thermocouple Safety Trip Alarm*

IEC 61508 Compliant Process

Moore Industries decided that its first IEC 61508-compliant, independently certified safety product would be a Safety Trip Alarm (STA) (Figure 1). In the safety world this is called a single loop logic solver. The company has been providing single loop logic solvers for safety applications for many years and drew on this extensive

experience when developing a safety trip alarm designed from the ground up to IEC 61508 standards. A single loop logic solver monitors any process variable including temperature, pressure, level, flow, or position. 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.

Much of the design process of IEC 61508 was familiar to Moore Industries' design engineers. The major difference was the focus on specific techniques and measures and the rigor in documenting what was done and why.

In the concept/planning phase, the focus 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, personnel competence, 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.) This phase included the following activities:

- Product development plan (based on the V Lifecycle Model - see Figure 2)
- Selection of techniques and measures for the safety integrity level (SIL)
- System design to meet the required diagnostic coverage.

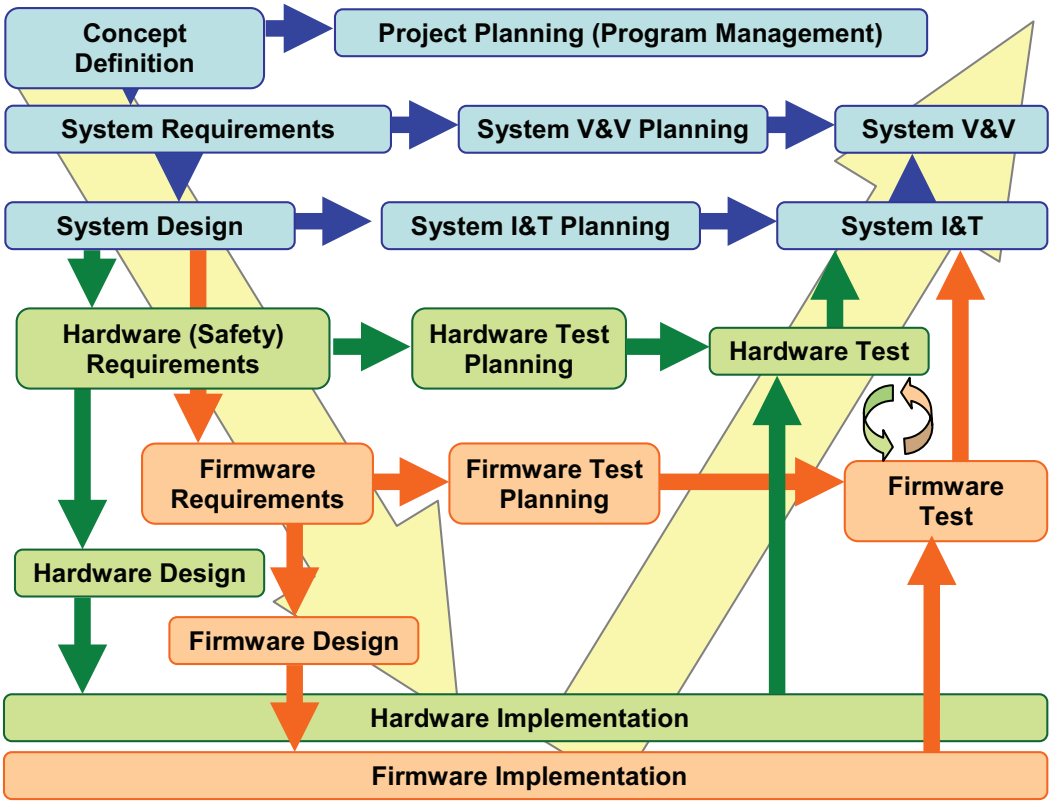

Figure 2. *Development Lifecycle "V model" for Functional Safety Product.*

Once the concept phase was complete, engineers started on the design, implementation and test phases.

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 (PFD_{AVG}). 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. Since this was the first in a series of safety products the company planned on developing, it was decided to maximize the investment in software by creating a library of re-usable software functions/modules. Selection of techniques and measures from the standard was guided by discussions during the first EMPHASIS assessment. The C coding standard and style guide were also reviewed and updated based on this experience.

To help meet the stringent safety requirements, Moore Industries' engineers used a number of tools including:

- Doxygen for automated document generation
- QA.C for static analysis
- VectorCAST for 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 developed by the company 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 previously performed tests after an issue has been identified and corrected. In addition, fault insertion testing was specified. This is a process where faults were deliberately initiated and the results witnessed 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.

Implementing lessons learned from the 1st EMPHASIS assessment, Moore Industries was able to achieve SIL3 systematic capability for the STA when audited by TÜV Rheinland® (and subsequently exida®). The STA Safety Trip Alarm is now certified to IEC 61508 for single use in Safety Instrumented Systems (SIS) up to SIL2 and systematic capability of SIL 3. This allows the STA to be used in a redundant architecture (1oo2, 2oo3, etc.) up to SIL 3.

STA EMPHASIS Assessment

The STA was the first instrument to have been designed and certified to IEC 61508, which made the EMPHASIS assessment more straightforward. Due to the additional rigor applied to the interpretation of the standard, the STA was assessed to have a SIL 2 capability for UK nuclear use.

Figure 3. *STA-EMP Unit with EMPHASIS Label.*

Items addressed to meet the nuclear requirements included:

- Documenting a strategy for tool use and validation
- Documentation of boundary value analysis, equivalence classes and input partitioning for software module testing
- Traceability matrix from Requirements to Verification and Validation (V&V) testing
- A special EMPHASIS build to include labelled terminals and specified firmware version

Additional items for future projects include:

- Recording decisions made and their rationale during the design process
- Greater use of structured design methods such as UML, data flow diagrams, sequence diagrams
- Use of checklists for verification
- Avalanche/stress testing

Next EMPHASIS Project: STZ

The STZ Safety Series Dual Input Smart HART® Temperature Transmitter is in the final stages of development.

Figure 4. *STZ HP Version with Integral Display.*

Based on our experience of IEC 61508 and EMPHASIS assessments, we invested in Polarion, a requirements management tool which provides traceability of requirements to design and V&V testing. It also provides a single repository for design documents and configuration management.

A preliminary EMPHASIS assessment a few months ago was very positive and provided confidence that Moore Industries knows what needs to be done to successfully complete the product development and the assessment process.

Conclusion

Assessment of smart instruments for use in the UK Nuclear industry is a rigorous process and requires thorough documentation and a greater depth of analysis and testing in the product development process. Moore Industries' early experience with EMPHASIS provided an insight into the process, tools and techniques required for both IEC 61508 and the UK Nuclear industry.

From day one, we took an open and collaborative approach to each audit and found that the auditors respond well to this. Each subsequent assessment has provided additional help with interpreting the standards and selecting the appropriate techniques and tools. This has resulted in an improved development process and products for safety applications.

References

IEC 61508:2010 Parts 1 to 7 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

QA.C Static Analysis Tool by PRQA Programming Research:
http://www.programmingresearch.com/products/qac

VectorCAST Unit test by Vector Software: http://www.vectorcast.com

Doxygen tool for generating documentation from annotated C sources:
http://www.stack.nl/~dimitri/doxygen/index.html

Polarion Application Lifecycle Management (ALM) Tool for requirements management:
http://www.polarion.com

Useful Links

Moore Industries Website	http://www.miinet.com
Functional Safety Poster	http://www.miinet.com/SafetySeries
The STA Data Sheet	http://www.miinet.com/InterfaceSolutionDownloadCenter/PopularProducts.aspx
IEC Functional Safety Website	http://www.iec.ch/functionalsafety/

MOORE INDUSTRIES

United States • info@miinet.com
Tel: (818) 894-7111 • FAX: (818) 891-2816
Australia • sales@mooreind.com.au
Tel: (02) 8536-7200 • FAX: (02) 9525-7296

www.miinet.com

BeNeLux • info@mooreind.eu
Tel: 03/448.10.18 • FAX: 03/440.17.97

China • sales@mooreind.sh.cn
Tel: 86-21-62491499 • FAX: 86-21-62490635
United Kingdom • sales@mooreind.com
Tel: 01293 514488 • FAX: 01293 536852