International Conference
Nuclear Energy for New Europe 2005
Bled, Slovenia, September 5-8, 2005

Use of Modern Software - based Instrumentation In Safety Critical Systems

John Emmett
Moore Industries Europe Inc
United Kingdom
jemmett@mooreind.com

Bob Smith
Moore Industries Europe Inc
United Kingdom
prsmith@mooreind.com

ABSTRACT

Many Nuclear Power Plants are now ageing and in need of various degrees of refurbishment. Installed instrumentation usually uses out of date 'analogue' technology and is often no longer available in the market place. New technology instrumentation is generally un-qualified for nuclear use and specifically the new 'smart' technology contains 'firmware', (effectively 'soup' (Software of Uncertain Pedigree)) which must be assessed in accordance with relevant safety standards before it may be used in a safety application. Particular standards are IEC 61508 [1] and the British Energy (BE) PES (Programmable Electronic Systems) guidelines EPD/GEN/REP/0277/97. [2] This paper outlines a new instrument evaluation system, which has been developed in conjunction with the UK Nuclear Industry. The paper concludes with a discussion about on-line monitoring of Smart instrumentation in safety critical applications.

1 INTRODUCTION

The originators of this project recognised that the only way to procure instrumentation that complies fully with either IEC 61508 (parts 1, 2 & 3 implied) or the British Energy PES guidelines (or both) is to commission a bespoke design. This would result in the following:

- High development costs
- Very specialised product
- Very small production runs
- High individual component costs
- High cost support to ensure repair & maintenance facility
- Very high cost spares
- Statistically insignificant field data for confirmation of theoretical reliability data.

Despite all the effort put in to this type of contract it is still possible that some hidden failure to danger may be characteristic of the instrument finally produced. Software failures are 'systematic' in nature and it is rarely possible to implement a software test regime, which is 100% thorough. The inherent problem of small production quantities means that the potential failure mechanism may lie dormant for many years without discovery. The potential consequences of a dangerous process failure are significant to human life, the environment and the national and local economy.

The contrary problems of so called COTS (Commercial off the Shelf) instrumentation result in very large, statistically significant, quantities of instruments used in diverse environments. Hidden dangerous faults are more likely to be revealed due to the large population of field applications and therefore might be expected to surface in an application where the consequences are not critical and in a time scale, which is meaningful in the lifetime of a nuclear power station. Hence, the potential consequences might be mitigated. The use of high quality COTS devices might therefore offer no more risk than the specially produced instrument but this assertion is difficult to prove. The difficulty being the identification of suitable evidence to demonstrate that design and development was carried out with due diligence in order to minimise the possibility of a systematic error being 'designed in'.

The project was intended to research 'practical' guidelines that might be used to select and assess manufacturers of so-called 'smart' instrumentation and their products for use in safety critical applications. These guidelines would use the requirements established in IEC 61508 and the British Energy PES guidelines as the primary basis for the assessment. The assessment encompasses aspects of 'functional safety management', 'Hardware assessment' and 'software assessment'. The EMPHASIS of the project is on the availability and quality of evidence that can be offered in support of each phase of the assessment. It recognises that few suppliers are as yet complying with IEC61508 and fewer still understand the requirements of parts 1, 2 & 3 or the BE PES guidelines. Consequently, it is the intention to research the procedures that are being used by Moore Industries Inc., of Los Angeles as a typical example of a quality supplier of smart instruments. A mapping between the reference requirements and available evidence of compliance will be performed.

It is clear that there may be some considerable 'distance' between 'available' evidence and the 'requirement' of the reference standards. It is consequently essential that this project establish not only the requirements but also a clear understanding of the quality required of the available evidence. It is expected that "EMPHASIS" will establish appropriate guidelines and propose suitable 'generally available' evidence in support of compliance with key requirements.

2 EMPHASIS - EVALUATION OF MISSION IMPERATIVE, HIGH-INTEGRITY APPLICATIONS OF SMART INSTRUMENTS FOR SAFETY

An evaluation mechanism has been developed that facilitates the assessment of smart instruments against the requirements of IEC61508 parts 1, 2 and 3 and the BE PES Guidelines. The assessment uses an Excel spreadsheet-based questionnaire, which identifies 'practical' evidence that should be provided in support of claims and questionnaire answers. This 'mechanism' provides an 'approved' means with which available instrumentation may be compared and graded against the requirements of the standards referenced above and hence against each other so that an optimum 'safest' choice may be made. The assessment is evidence based so that the choice can be justified to the regulator.

3 THREE PHASES

The assessment covers the following three phases which follow IEC61508 parts 1, 2 and 3:

Phase 1 Pre-qualification, investigates the top level Functional Safety Management Issues which could lead to rejection on vendor non-compliance.

Phase 2 Investigates the hardware procedures and capabilities which might also lead to rejection on vendor non compliance.

Phase 3 Investigates the software and other in depth issues to obtain a final EMPHASIS rating for the instrument.

4 CURRENT "EMPHASIS" PROJECT STATUS

Phase 3 is due for completion at the end of September 2005. The project completion is due by the end of the year. The UK nuclear industry is planning to beta test the tool later this year.

5 ON-LINE INSTRUMENTATION HEALTH MONITORING USING HART®

5.1 HART® Background

Fisher Rosemount Corporation originally developed HART® (Highway Addressable Remote Transducer). All rights have now been transferred to the HART® Communication Foundation. It is now a de-facto open standard used by most leading instrument manufacturers. A digital signal is superimposed on the analogue 4-20mA signal pair. This same pair of wires powers the remote transmitter. The latest estimate is 15,000,000 installed devices world-wide [3]

HART® normally operates as a "maser-slave" protocol. A HART master such as a DCS or HART loop monitor instrument sends requests to a HART slave, (the field device) which responds with digital data. HART is commonly used for on-line configuration of field devices.

5.2 Field Device Diagnostics

Every HART® compatible field device will return valuable diagnostic information every time a HART Master polls the device (Typically 2 times per second). The HART standard specifies a "Field Device Status Byte" which will indicate the following standardised faults:

- Primary Variable Out of Limits
- Non-Primary Variable Out of Limits
- Analogue Output Saturated
- Analogue Output Fixed (In loop test mode)
- More Status Available
- Cold Start
- Configuration Changed
- Field Device Malfunction

A simple HART Loop Monitor connected transparently across (in parallel with) the loop can continuously monitor these status bits and automatically alarm if there are any problems with the measurement. This on-line monitoring will increase the measurement confidence factor. The monitor can also access up to 4 variables from a multivariable transmitter (e.g. Mass Flow Transmitter). These variables can be "Broken out" and repeated as separate 4-20mA signals back to the control room although only one pair of wires needs to be cabled to the field.

As HART signals communicate directly with the Microcontroller in the field device, it bypasses the Digital to Analogue (D/A) circuit. The HART loop monitor can convert the digital signal directly to a standard RS485 digital serial signal thus eliminating the field device D/A errors

5.3 Device Specific Alarms

The HART® protocol allows for "Device Specific Alarms" to be designed and monitored remotely. These can, for example, indicate a failed back-up sensor in a dual input Temperature Transmitter. There is no point having a back-up sensor if you don't know it has failed! Another application is the advance warning of a pH electrode failure.

6 Safety related accuracy issues

"A Dangerous failure is a failure that results in an error of more than 2% of span and leaves the output within an active scale"[4].
Measurement accuracy is paramount in safety related systems. On-line HART monitoring will increase Diagnostic Coverage and reveal dangerous undetected faults. Safety Integrity Level (SIL) calculations are based on Probability of Failure on Demand (PFD) and Safe Failure Fraction (SFF)

On-line HART monitoring can be used with ESD valves and Partial Stroke Valve Testing to extend proof test intervals. The Device Specific Alarms from latest SMART valve positioners can detect a "Suck Valve" before it is called upon to close in an emergency

ACKNOWLEDGMENTS

The authors acknowledge the valuable input from the UK nuclear industry.

REFERENCES

[1] International Electrotechnical Commission, "Functional Safety of Electrical, Electronic, and Programmable Electronic Safety Related Systems", IEC 61508, Parts 1 to 7, 1998 to 2000
[2] British Energy Generation Ltd, "Guidelines for Using Programmable Electronic Systems in Nuclear Safety and Nuclear Safety-Related Applications", EPD/GEN/REP/0277/97 Issue 2.
[3] HART Communication Foundation: www.hartcomm.org
[4] Exida: www.exida.com