SMART Instruments 2010

Robin Pearce


Date: 27/04/10 Mayfair Conference Centre, London, UK
Presentation Content

• What are the issues of using these instruments in safety applications in the nuclear sector?

• HSE/NII expectations and the joint European nuclear regulators position on SMARTs.

• What's been agreed in the UK nuclear sector - the 2 legged approach and the "Emphasis" methodology & Brief outline of the assessment process.

• Overview of Nuclear Industry licences forum. SMART Industry working group. (NISIWG)

• Our experiences of the reactions of instruments suppliers to assessment

• Questions
What are the issues of using these instruments in safety applications in the nuclear sector?

Definition: A SMART instrument meets the following criteria -

- That the main purpose of the instrument is to measure or directly control a single process variable.
- That despite using a microprocessor (or similar), it is a proprietary or ‘off the shelf’ instrument in common use.
- It may (or may not) include some flexibility in its use, due to parameters that are set by the vendor or user.
- That its life cycle includes the production of some generic firmware by the manufacturer and may include some particular configuration software or settings by the user.
- SMARTs are not restricted to measurements but also include actuators, valves, motor starters, UPS and other control instruments.
What are the issues of using these instruments in safety applications in the nuclear sector?

The nuclear Industry & the NII.

- Nuclear Industry intensely regulated.
- By the HSE’s Nuclear Safety Division (NII).
- Nuclear Sites are licensed.
- Consents to build/test/commission/operate/modify are required prior to each stage for each plant.
- Consent for continued operations required for each plant every 10 years.
- Safety cases including substantiation of the engineering (instrumentation) are required to justify consent being granted.
- Nuclear Industry is required to conduct research for the regulator.
- SMARTs seen as a safety issue by NII. Other industries don’t seem to be regulated on this issue.
What are the issues of using these instruments in safety applications in the nuclear sector?

- Difficulty of substantiation of the reliability of the on-board firmware.
- Potential for undetected systemic errors.
- Errors may lie dormant for years.
- Triggered by specific conditions, e.g. time, change/combination of input conditions, maintenance or calibration.
- SMART instruments can be physically indistinguishable from the conventional non-SMART. (i.e used in error)
- Common mode firmware (software) failure on different Instruments.
- Thus the safety system may fail on demand!
- Changes of instrument type, make, hardware, and firmware (software) version required to be substantiated prior to use.
Potential Failure Modes.

- Random and Systematic Hardware Failures
- Systematic Firmware Failures

Potential Failure Mechanisms
HSE/NII expectations and the joint European nuclear regulator’s position on SMARTs.

- There is currently no nuclear sector standard specifying the design documentation for smart sensors/actuators, nor even the issues that should be addressed.
- NII first raised the issue of use of SMART instruments in safety applications 10 years ago.
- NII Safety Assessment Principles & Technical Assessment Guide T/AST/046 - Issue 2. computer based safety systems have been used as a basis for discussions on substantiation of SMART instruments.
- Agreements reached in 2006 with the NII on a “2 legged ”graded to the SIL approach by the UK nuclear licences'.
- More recently in 2010: a revised common position statement of seven European nuclear regulators and authorised technical support organisations for the licensing of safety critical software for nuclear reactors was issued. This includes a section on SMART instruments based on the “2 legged ” approach.
- Note new build reactor vendors are addressing this issue. Instrument suppliers should take note of the pan European approach.
What's been agreed in the UK Nuclear sector?

The 2 legged approach and the "Emphasis" methodology..

Based on the NII Safety Assessment Principles (SAPs) “Two Legged Approach”

- Production Excellence (PE)
- Independent Confidence Building Measures (ICBM)
What's been agreed in the UK Nuclear sector?
The 2 legged approach and the "Emphasis" methodology.

- Production Excellence
  - Covers initial specification through to the finally commissioned system, comprising:
    - The thorough application of technical design practice consistent with current accepted standards. (IEC61508)
    - The implementation of an adequate quality assurance programme and plan in accordance with appropriate quality assurance standards
    - The application of a comprehensive testing programme formulated to check every system function

NII Technical Assessment Guide T/AST/046
What's been agreed in the UK Nuclear sector?
The 2 legged approach and the "Emphasis" methodology.

Independent Confidence Building Measures

- An independent and thorough ‘reasonably practicable’ assessment of the Safety Systems’ ‘fitness for purpose’ comprising the following elements:
  
  - Complete and preferably diverse, checking of the finally validated system by a team which is independent of the system’s suppliers
  
  - Independently assessed testing, covering the full scope of test activities (e.g. verification, validation, commissioning and dynamic testing) including traceability of tests to specification and confirmation that the specification is met

NII Technical Assessment Guide T/AST/046
What's been agreed in the UK Nuclear sector?
The 2 legged approach and the "Emphasis" methodology.

• Basic Justification
  – Those techniques and measures which are considered to be the basic requirements for a safety justification graded to the SIL (SIL1-3)
  – Includes both Production Excellence and Independent Confidence Building Measures

• Compensating Activities
  – Where gaps are found in the Production Excellence arguments these are the techniques used to plug those gaps
  – May be undertaken by the manufacturer or others
What's been agreed in the UK Nuclear sector - the 2 legged approach and the "Emphasis" methodology.

**Smart Instrument Substantiation Framework**

**Production Excellence**
- EMPHASIS Assessment
  - Part 1
  - Part 2
  - Part 3
- Type Testing

**Compensating Activities**
- Depends upon gaps found in Production Excellence
  - e.g.
  - Review of CVs (by Licensee)
  - Module Tests (by Manufacturer)
  - Statistical Tests (by either)
  - etc.

**Independent Confidence Building Measures**
- Select From:
  - EIMT Records
  - Proof Test Records
  - Commissioning Tests
  - Hardware Reliability Analysis
  - Certification
  - Supplier Pedigree
  - Review of suppliers standards and procedures
  - Functional Safety Assessment
  - Review of Tools
  - Prior Use
  - Static Analysis
  - Dynamic Analysis
  - Statistical Testing
  - Others...
• EMPHASIS originated from a nuclear research project designed to develop guidelines for the assessment of smart instruments
• Feedback from suppliers on previous approaches were:
  – Cumbersome
  – Took too long to complete
  – Inconsistent questions
  – Different approaches to the same task from licensees
• EMPHASIS is intended to provide a streamlined, consistent approach to the assessment of smart instruments for the U.K. Nuclear Industry
• EMPHASIS uses a Microsoft® Excel® base to ensure wide accessibility
• The tool has been subject to extensive validation
• Based on IEC 61508.
• EMPHASIS consists of three interactive Excel Worksheets
• Part 1
  – Pre-qualification, investigates the top level Functional Safety Management Issues which could lead to rejection on vendor non compliance
• Part 2
  – Investigates the hardware procedures and capabilities which might also lead to rejection on vendor non compliance.
• Part 3
  – Investigates the software and other in-depth issues to obtain a final ‘EMPHASIS’ rating for the instrument.
U.K. Stakeholders

- Nuclear Industry Smart Instruments Steering Group (NISIWG)
Nuclear Industry Smart Instruments Steering Group (NISIWG)

Purpose

- To provide a forum for UK nuclear site licensees to address the use of SMART instruments in nuclear safety applications.
- To agree a common methodologies to be jointly adopted by the UK nuclear site licensees for the assessment of SMART instruments in safety applications in the nuclear industry.
- To plan and jointly undertake SMART instrument assessment activities to minimise costs to individual licensees.
- To provide a single body for the UK nuclear site licensees that the NII can interface to agree a single assessment methodology for SMART instruments.
- To provide a single UK nuclear industry body which the instrument suppliers can interface and consult on assessment methodologies.
Our experiences of instruments suppliers reactions to assessment.

- Initial resistance.
- Supplier’s concern over IPR and potential undermining of their safety claims.
- Additional cost to the supplier was a concern.
- The experience of being assessed has given the suppliers confidence that it is an advantage to them. Has increased market penetration.
- Many suppliers now actively seeking assessments to be undertaken.
ANY QUESTIONS?