Rob Stockham looks at the latest method being employed by the UK nuclear industry to assess control systems in safety-related and safety-critical applications in power stations

emphasis on safety

IN THE NUCLEAR industry there are a growing number of 'smart' instruments on the market claiming to have Safety Integrity Level certification. But whereas the methods for dealing with random hardware failures had been well established, systematic flaws in the software are a real concern, especially when looking at the consequences in nuclear installations.

It is for this reason that an extensive safety-related assessment of a single-loop process controller has recently been completed by Moore Industries using the new rigorous Emphasis assessment method developed by the UK's nuclear industry.

The Moore Industries 535 process controller and the company itself were tested by Emphasis. This systematically asks questions and requires evidence to show compliance to the international functional safety standard IEC 61508, together with some extra requirements from the UK nuclear industry gained from their experience. Emphasis challenges the design and looks for 'gaps' in compliance ▶

'Many smart instruments claim to have SIL certification but regulators were becoming aware of the software/ firmware in these devices possibly introducing systematic failures'

Safety related modifications are strictly controlled and may require regulatory 'permission' from the UK nuclear regulator

◀ that need to be addressed. Additional 'compensating measures' may also be required to provide further evidence of confidence and suitability.

The specific version of the 535 controller being used in UK nuclear power plant improvements is of a 'mature design' and pre-dates IEC 61508 by some years. This made it likely that Emphasis would discover 'gaps' in its compliance.

Agreement was made on 'compensating measures', which together with the findings of the Emphasis assessment, are included in the safety case. A safety case and justification have to be completed by the nuclear site licensee before installation can proceed.

STRICT SAFETY CONTROL

Safety-related modifications are strictly controlled through a categorisation process and modifications may (depending on factors such as safety category and importance) require regulatory 'permission' from the UK nuclear regulator (Nuclear Installations Inspectorate) prior to implementation.

Most other industries do not need this type of specific prior permission.

As a nuclear licensee, British Energy needs to able to make a reasoned claim that an instrument has been subject to good practice in its production processes and requires the evidence to support that claim. The Emphasis tool helped British Energy's assessor in structuring the claim and identifying the associated evidence. British Energy was also very appreciative of Moore Industries' openness about the company's product and processes.

NUCLEAR INDUSTRY'S NEED FOR EMPHASIS

The nuclear industry is aware that there are a growing number of 'smart' instruments on the market and many claim to have certification to a Safety Integrity Level. However, going back to the late 1990s the regulators were becoming aware of the significance of software/firmware in these devices and the possibility of introducing 'systematic' failure of the device. The methods of dealing with random hardware failures had been well established, but systematic flaws in the software are a real concern, especially when looking at consequences in nuclear installations.

Certification and assessment companies with competence in functional safety have been working with end-users and vendors around the world and offer varying levels of assessment and 'certification'. This has been very valuable to engineers and designers in having confidence in selection.

However, there is no common framework for assessment for suitability of use of these devices in IEC61508 applications and this can lead to confusion in interpretation of what is a 'certified IEC61508 device'. Is it hardware assessment only? What about software? Are proven-in-use IEC61511 arguments used?

The situation is certainly improving and leading functional safety certifying bodies are consolidating on the fundamental requirements 'to meet certification to a SIL', but still the expertise and process they use is proprietary and not transparent to the nuclear industry.

For manufacturers themselves, there is a real challenge of risk and reward to consider when engaging with the nuclear industry on such a rigorous assessment program. The purchase order in real terms may be 'small' but the time and money to undertake an assessment has been onerous. In addition, what if something unpleasant is found in the process or product during the assessment?

EMPHASIS REDUCES THE PROBLEMS

Firstly, the assessment tool itself was part of a long and intensive research and development project undertaken by the UK Control & Instrumentation Nuclear Industry Forum (CINIF), which included nuclear licensees and oversight by the Nuclear Installations Inspectorate.

Secondly, Emphasis is a comprehensive, transparent and consistent questioning and evidence gathering 'tool', aiming to show (or otherwise) compliance with each part and clause of IEC61508.

Because Emphasis has a lifecycle approach and is 'phased' along the line of the IEC61508 standard (Part 1 – Functional Safety Management, Part 2 – Hardware and Part 3 – Software) the assessment can be segmented and managed. Also the questions are quite specific, reducing the amount of debate and ambiguity as to how they can be answered.

In reality the assessment can seem initially daunting, but once you have the right people in the room it can be progressed at a fair pace. Any such assessments are not entered into lightly and need the buy-in of senior management to allocate resource, but by the time the auditor and vendor sit down together they both have a good understanding of expectations in terms of business opportu-

CORBIS

The 535 process controller was of an older design from a time before IEC 61508

nity and level of openness and co-operation needed to complete the initial Q&A sessions. This can take upto a day or a day-and-a-half.

Evidence can then be collected in the following days and weeks, but initial impression from the results of the Emphasis Q&As will give a very good feel for whether 'compliance' can be achieved to the required standard and integrity levels.

Being open is crucial to the success of the assessment and commercial confidentiality agreements need to be in place. Considering the rigor with which Emphasis examines all aspects of the company, product development and the actual product, it would be surprising if some non-compliance were not found.

Non-compliances, if they are found, can be reviewed and corrected, with agreement. The process is a partnership that has been designed to succeed, not fail.

The UK nuclear industry intends to use Emphasis to collect, collate and measure data supplied as part of the 'Manufacturing Excellence' leg of a two-legged approach to building the required safety cases. Compensating measures may be used where specific gaps are identified by Emphasis.

The second leg – 'independent confidence building' – is not undertaken by the manufacturer. This involves the development of additional application-specific evidence and justification; however, the manufacturer maybe required to give access to hardware and software.

The nuclear industry benefits by having a standardised and regular system approach whereby auditors from different nuclear companies can quickly assess different vendors in a more open and consistent manner.

The manufacturer benefits by the application of a consistent approach from the nuclear industry and this may reduce the number of audit requests on them for the same device.

For Moore Industries this has been a very positive experience. The 535 process controller chosen was of an older design from a time way before IEC61508 and, since Emphasis tests the compliance to IEC 61508, the assessment was certainly a challenge.

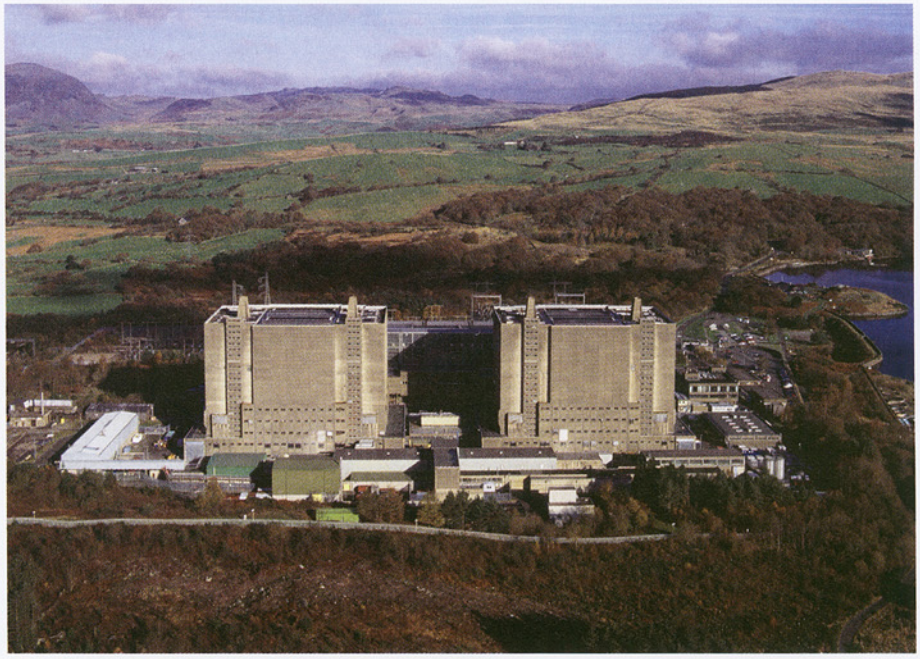
We found that the instrument with the required compensating measures easily made it into the SIL1 category. Senior managers and engineers became very involved with the assessment and we actually learned to apply new tools and techniques for development and testing.

This has taken commitment from our senior managers and engineers, but we have found positive benefits of being involved in Emphasis from the very beginning. For some of the giant instrument vendor companies such focus could be an issue, but for us the customer relationship and service to the industry is worthwhile.

In addition, the Emphasis exercise helped us in preparing for third party certification by TÜV for a forthcoming SIL2 product and lessons learnt will continue to be built into new product development programs.

Moore Industries looks forward to further assessments by the nuclear industry on our instruments in the future. ■

■ Rob Stockham is Moore Industries-Europe's general manager



The UK nuclear industry intends to use Emphasis to collect, collate and measure data to help build safety cases