Health and Safety
Executive

Regulatory Information Conference

NOVEL/COMPLEX SYSTEMS

WHAT TO DO WHEN THINGS GET DIFFICULT

Bob Jennings

March 10, 2010

My Presentation will cover

- Examples sort of Systems, Structures or Components we are considering.
- Brief introduction to the UK legal framework relevant to this topic.
- Role of our Safety Assessment Principles in Novel Systems.
- Outline of the approach.
- A specific example on the quantification of system reliability for embedded software based Safety Related I&C.
- Concluding Remarks

Examples

- EPR
  - Core Catcher;
  - Complex I&C.
- AP1000
  - Modular Construction;
  - SQUIB valves;
  - In-vessel retention.

Legal and Regulatory Framework

- Our legal requirements come from our Licence Conditions - LC 14 on Safety Documentation and LC 23 on Operating Rules (Tech Specs).
- The UK has no formal regulations on technical matters such as I&C, mechanical engineering, PSA e.t.c.
- We make technical judgements on the adequacy of a licensee's Safety Documentation by assessing it against our Safety Assessment Principles which have no formal status in the UK's legal system.

SAFETY ASSESSMENT PRINCIPLES.

- Our Safety Assessment Principles (SAPs) are technology neutral and are used to make regulatory judgements on the adequacy of a licensee's safety case for all Nuclear Facilities in the UK.
- They are designed to cope with changing technologies by describing a strategy we would expect a licensee to follow for Novel and/or Complex systems.

SAFETY ASSESSMENT PRINCIPLES.

- Our Safety Assessment Principles (SAPs) are a mixture of deterministic requirements and numerical targets on the frequency of radiological consequences. The 1992 SAPs linked the achievement of the numerical targets to the probabilistic requirements. If the numerical targets could not be readily demonstrated SAP 70 was invoked.
- Numerical targets are demonstrated using L1, L2 and L3 PSAs.

BACKGROUND 1992 SAP 70

- SAP 70 was the entry point into what was called our Special Case Procedure. It stated that "Where a structure, system or component forms a principal means of ensuring nuclear safety and it is not practicable to demonstrate the accident frequency principles are satisfied in the event of its failure, the plant may only be accepted after the application of a special case procedure agreed as an alternative demonstration."
- The above was used in our assessment of the Sizewell B Primary Protections System.

BACKGROUND 2006 SAPs

- The 2006 SAPs take a slightly different approach. Under ERL.1 (Engineering Principles: reliability claims) it states that; “The reliability of any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods”.

BACKGROUND ERL.1

- Paragraphs 176 and 177 explain that reliability should be demonstrated by suitable analysis and data. Where this is unavailable the demonstration has to be on a case by case basis. Although the words are not used this demonstration is essentially a Special Case Procedure as previously required under the 1992 SAPs.

BACKGROUND to PARA. 177

Paragraph 177 requires:

a) a comprehensive examination of all the relevant scientific and technical issues;

b) a review of precedents set under comparable circumstances in the past;

c) an independent third-party assessment in addition to the normal independent verification and validation employed on designs which are neither novel nor complex;

d) periodic review of further developments in technical information, precedent and best practice.

Where is this process used

- Novel system – no generic ‘type’ qualification.
- Complex systems.
- Purpose designed – no track record.
- No means of guaranteeing reliability during production - for example the complexity and novelty of the system making it difficult to establish good fault avoidance principles.
- No simple means of measuring the reliability after production due to poor availability of data.
- Hence many uncertainties.

Overall Approach

- Establish the Safety Significance of the System, Structure or Component (SSC).
- For SSC's of safety significance justifying their safety performance through the two independent means:
  - Production Excellence;
  - Independent Confidence Building Measures.

Safety Significance

- Establish the Safety Significance of Novel and Complex Systems.
  - Generally this been the easiest part of the problem.
  - For example the AP1000 Stage 4 SQUIB valves the consequences of either spurious operation or failure-on-demand is bounded by standard transient analysis.
  - Less obvious for the highly interconnected EPR I&C system where establishing the safety significance of complex interconnectivity was a challenge although the PRA design base accident analysis did help.

Safety Justification

- Production excellence – Establish high build quality.
- Independent review of quality – Independent Confidence Building Measures performed by an organisation independent of the SSC vendor.
- The following slides demonstrates the approach taken in the UK to Novel Embedded Digital Devices examples of which would include:
  - Diesel Governors, Protection Relays for Class 1E power circuits; sophisticated motor control systems etc.

Quantification of the Numerical Targets for Embedded Digital Devices

- These are safety related sensors, actuators and embedded controllers employing complex microprocessor based hardware operating software that can contain much more than 200000 lines of code.
- Often developed to non-safety standards and the design information is covered by strict commercial confidentiality clauses.
- Standards call for a *White Box* approach, these devices are often *Black Box* or at best *Murky Grey*.

Production Excellence

- Use IEC61513 e.t.c. as a framework for the safety justification.
- Use modern probing techniques such as reverse engineering, perturbation analysis e.t.c. to reveal the inner architecture of the Smart device.
- Use the architecture of the whole safety system to establish fault tolerance – sub-system diversity using a much simpler embedded device (good example on the EPR of the emergency diesel generators with the SBOs).
- Use the powerful tool Emphasis to probe the manufacturer of the embedded to get key information about their approach to all aspects of the system lifecycle falling short of them giving away the full design details of the device.
- Analysis of available evidence of proven-in-use if there is comprehensive field data.

Independent Confidence Building Measures

Although many of the measures are of a similar nature to those applied during production, their purpose is quite different. Flaws are expected during production, and are corrected in the normal course of events. Flaws found during confidence building, although corrected, would seriously undermine confidence, and thus reduce the reliability claim allowable for the embedded device. **Significant loss of confidence would lead to a rejection of the embedded device.**

Independent Confidence Building Measures

- Independent high quality review – through manual inspection of the evidence gathered by the licensee.

- Statistical testing – 46000 demands from operational profile = 10^{-4} pfd for zero observed failures (99% conf).

$$\frac{\ln(1-\alpha)}{\ln(1-pfd)}$$

- Where information is made available from the manufacturer do sample Static Software analysis – control flow analysis, data flow analysis, information flow analysis, semantic analysis, compliance analysis.

Conclusions

I have tried to illustrate the process we ask the licensee to consider using to make up for the lack of information to satisfy the risk based numerical targets used in the UK.

An earlier version of this process was successfully applied to the Sizewell B primary protection system and emergent issues on the Magnox Reactor Steel Pressure Vessels in the late eighties and early nineties of the last century.

It has also been used to successfully rule out a safety related gamma monitor from a safety related role due to revealing inherent weaknesses.