IET Nuclear Safety

March 2013

Plan Design Enable

Agenda

1. The need for Computer Based Systems Important to Safety
2. Overview regulatory context
3. Focus on high-SIL software issues
   – Basis of Safety Case
   – Hardware Platforms
   – Lessons from civil nuclear
   – Good software development practice
   – Good software V&V practice
   – Timescale and Cost issues

Safety-Critical Systems in UK Nuclear

Plan Design Enable

Advantages

ATKINS

Computer based C&I systems offer advantages over traditional hardware systems

- Better accuracy
- Self test features
- More complex functionality
- Smaller footprint
- Software does not age

Disadvantages

ATKINS

- Difficult to test and analyse – can't interpolate results in the same way as analog systems
- Difficult to quantify reliability claims
- Software is increasingly pervasive (firmware, RTOS, etc) and access to information may be limited

Regulatory Context

ATKINS

- UK Nuclear sites are regulated by the Office for Nuclear Regulation, includes Nuclear Power Plants, Sellafield, nuclear powered submarines and AWE.
- Regulator has a strong influence, but only in a reviewing context.
- Safety Assessment Principles and Technical Assessment Guidelines
  - ESS.27 – computer based systems important to safety
  - TAG046 - computer based systems
- Common approach to regulator assessment across all sectors

System Design Principles

ATKINS

- It is good practice to isolate and minimise the safety functionality in the system:
  - Isolate safety functionality from non-safety functionality
  - Do not mix SILs on the same processor
  - Be cautious about locating subsystems on the same network
  - Be cautious about independence arguments as a mechanism for reducing SIL
  - “Non-interference” arguments need to be robust
  - Benefits in terms of simpler safety systems, improved reliability, less contentious safety case
- Safety analysis needs to consider whole system:
  - Not just application
  - “Smart Instruments” and I/O cards containing firmware

Hardware design

- 1990s - Bespoke hardware
  - e.g the Westinghouse Eagle series hardware used for the Sizewell B PPS (based on standard Intel microprocessors).
  - Commercial PLCs
  - Redundant designs used to mitigate hardware reliability issues
- 2000s - Pre-qualified hardware (e.g. PLCs)
  - TUV Certificated (e.g. 61508 SIL x) platforms available from suppliers but need to be used with caution. SIL 3 seems to be highest integrity for systems containing software
  - Smart Sensors increasingly an issue
- 2010s – Best Practice
  - Consider use of dedicated safety related hardware platforms (e.g. Areva's Teleperm XS),
  - Redundant designs probably needed for high-SIL systems
  - High-SIL systems should not be on the same network as lower SIL systems, or should have "data diodes"
  - Lots of talk about FPGAs but little use in nuclear

Safety Argumentation

ATKINS

- ONRs Safety Assessment Principles and Technical Assessment Guideline mandate a “two-leg” safety argument:
  - **Production Excellence.** Covers the development of the computer system by the supplier. Essentially, a process compliant with a suitable standard (IEC 61508, IEC 60880, IEEE 1012), with a robust QA system will be satisfactory.
  - **Independent Confidence Building Measures.** Independent and thorough ‘reasonably practicable’ assessment of the system’s fitness for purpose.

    Must be performed by an independent third-party

    Preferably using diverse techniques

    Performed **after** production excellence, applied to the delivered product after the manufacturer’s V&V is complete
- The approach used on Sizewell B Primary Protection System created a strong precedent

Good Software Design Principles

- Classic V life cycle is preferable. Use Agile methods with caution
- Requirements Capture and Design
  - Meaningful levels of abstraction
  - Gradual refinement of the requirements into design
  - Use of mathematical / logic design techniques or a structured design approach such as UML is preferable to natural language specifications
- Good implementation practice
  - Use a good programming language (Ada)
  - Use of a “safe” subset (e.g. MISRA C)
  - Take advice from standards on suitable techniques , e.g. IEC 61508 part 3 or IEC 60880 Annex B
  - Use a Certified compiler (usually certified for avionics, but credible with ONR)
  - Avoid complex designs and obscure programming techniques – multi-tasking, interrupts , pointers

Example V&V Techniques

ATKINS

Dynamic (Production Excellence)

- Unit Testing with Structural coverage,
- Factory Acceptance Testing
- Commissioning Tests
- Extensive pre-operational test “in situ”
- Degree of rigour increases with SIL (c.f. 61508)

Static (Independent Confidence Building)

- Functional Analysis
- Integrity Checking
- Compiler Validation (at SIL 3)
- Statistically significant testing

Independent Confidence Building Measures

- Functional Static Analysis
  - Comparison of specification and code.
  - More formality added with increasing integrity claims
  - Ought to be tool supported by a Formal Static Analysis tool , e.g. MALPAS

- Integrity Checking
  - Analysis to ensure an absence of run-time errors
  - Example, no divide by zero errors
  - Again, needs to be tool supported

Independent Confidence Building Measures

- Compiler Validation
  - Analysis to ensure that the compilation tools have not introduced any bugs
  - The executable code is disassembled, and the disassembled code formally compared with the source code for semantic equivalence
  - Approach was developed by EDF Energy as part of the Sizewell B independent confidence building, and is proposed for use on New Build
  - Only required at the highest integrity level
- Statistical Testing
  - Black box test approach
  - If a certain number of independent tests are performed with zero errors, then the results can support the integrity level claim at a certain confidence level.
  - For example, 50,000 tests support a 10^{-4} pfd claim at 99% confidence level

Timescales / Opportunities

ATKINS

- The ONR requirement to perform production excellence and independent confidence building sequentially adds delay to the programme, which can be significant, particularly for large, high SIL systems.
- Early engagement with the regulator is highly beneficial – agree major design issues, work programme and safety case plan prior to implementation.
- Exploiting CINIF research is encouraged, likely to gain favour with ONR
- Development of site Programmable Electronic Systems (PES) Guidelines can be a means to document basic software development and V&V principles & form the basis of a broad agreement with the ONR.

Supportability issues

ATKINS

Software systems may have very long lifetimes (e.g. over 20 years)

There are a number of challenges:

- Knowledge retention
- Retention of code and documentation (e.g. obsolete word processing systems, micro fiche etc.)
- Support platforms (e.g. development system, test rigs)
- Hardware obsolescence, including operating system for PC based systems
- Long-term Support
- Installation of modifications for on-line systems

ATKINS

Thank you for listening

Any questions?