Embedded digital technology in plant equipment

International Task Force on Safety Critical Software – Consensus and UK perspective

Mark Bowell
Office for Nuclear Regulation, UK

US NRC RIC, 12 March 2014

International Task Force on Safety Critical Software

- Licensing of safety critical software for nuclear reactors –
  Common position of a group of international nuclear regulators and authorised technical support organisations
- Belgium, Canada, Finland, Germany, Spain, Sweden, UK
- US NRC NUREG/IA
- More detailed presentation in RIC session on "Safety critical software – International perspectives"

Context

- Inclusion of embedded digital technology is a relentless commercial trend
- Increased functionality (signal processing, communications, diagnostics)
  - and complexity
- Can move critical processing to more hazardous environments
- Increased risk of common cause failure
- A type of pre-existing software
  - closer relationship to supplier
  - difficulties in access to design documentation
  - usually not nuclear-specific
  - hidden changes

Common positions (1)

- Clearly identify:
  make
  model
  application
  software versions
- Demonstrate fitness for purpose
- Safety class – essential part of system
  - specify the properties required
- Identify failure modes
- Analyse common cause failure

Common positions (2)

- Compare production to an applicable safety standard
  - address deficiencies by compensating activities or arguments
    - manufacturer rework
    - static and dynamic testing
    - restrict functionality
- Confidence building independent of the supplier
  - commissioning tests
  - static analysis
  - analysis of operating experience
  - statistical testing

Common positions (3)

- For safety systems:
  same assessment of final product as for new software
  - may involve reverse engineering
  - alternatively use additional compensating evidence
- Document safe envelopes and limits for acceptable use
  - functionality
  - maintenance
  - environment

UK perspective

Production Excellence

Compliance with IEC 61508 using EMPHASIS assessment tool

Manufacturer's type tests

Compensatory activities

Depends on gaps found in production excellence

Examples:
Review of CVs (by licensee)
Module tests (by manufacturer)
Statistical tests (by either)

Independent confidence building measures

Select from:

Examination, inspection, maintenance and test records
Proof test records
Commissioning tests
Hardware reliability analysis
Prior use
Certification
Supplier pedigree
Review of supplier's standards and procedures
Functional safety assessment
Review of tools
Static analysis
Dynamic analysis
Statistical testing

Office for Nuclear Regulation
An agency of HSE

7

Requirements for Class 1 smart devices (10^{-4})

- Class determined according to IEC 61226
  - IAEA terminology: safety systems
- Claimed probability of failure on demand of 10^{-4}
- Production excellence
  - Emphasis assessment with Class 1 10^{-4} techniques
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Instrument type tests
  - Examination, inspection, maintenance and test records
  - Proof test records
  - Commissioning tests
  - Hardware reliability analysis
  - Prior use
  - Supplier pedigree
  - Independent certification
  - Independent review of supplier's standards and procedures
  - Independent functional safety assessment
  - Independent review of tools
  - Static analysis
  - Dynamic analysis
  - Statistical testing

Office for Nuclear Regulation
An agency of HSE

8

Requirements for Class 1 smart devices (10^{-3})

- Class determined according to IEC 61226 (IAEA terminology: safety systems)
- Claimed probability of failure on demand of 10^{-3}; ***source code available***
- Production excellence
  - Emphasis assessment with Class 1 10^{-3} techniques
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Instrument type tests
  - Examination, inspection, maintenance and test records
  - Proof test records
  - Commissioning tests
  - Hardware reliability analysis
  - Prior use
  - Supplier pedigree
  - Static analysis
  - Dynamic analysis
  - Statistical testing
- Independent confidence building measures should consider
  - Certification
  - Review of supplier's standards and procedures
  - Functional safety assessment
  - Review of tools

Office for Nuclear Regulation
An agency of HSE

9

Requirements for Class 1 smart devices (10^{-3})

- Class determined according to IEC 61226 (IAEA terminology: safety systems)
- Claimed probability of failure on demand of 10^{-3}; ***source code unavailable***
- Production excellence
  - Emphasis assessment with Class 1 10^{-3} techniques
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Instrument type tests
  - Examination, inspection, maintenance and test records
  - Proof test records
  - Commissioning tests
  - Hardware reliability analysis
  - Prior use
  - Supplier pedigree
  - Statistical testing
- Independent confidence building measures should consider
  - Certification
  - Review of supplier's standards and procedures
  - Functional safety assessment
  - Review of tools

Office for Nuclear Regulation
An agency of HSE

Requirements for Class 2 smart devices

- Class determined according to IEC 61226 (IAEA terminology: safety-related systems)
- Claimed probability of failure on demand of 10^{-2}
- Production excellence
  - Emphasis assessment with Class 2 techniques
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Instrument type tests
  - Examination, inspection, maintenance and test records
  - Proof test records
  - Commissioning tests
  - Hardware reliability analysis
  - Prior use
  - Supplier pedigree
- Independent confidence building measures should consider
  - Dynamic analysis
  - Static analysis
  - Statistical testing
  - Certification
  - Review of supplier's standards and procedures
  - Functional safety assessment
  - Review of tools

Office for Nuclear Regulation
An agency of HSE

Requirements for Class 3 smart devices

- Class determined according to IEC 61226 (IAEA terminology: safety-related systems)
- Claimed probability of failure on demand 10^{-1} or less
- Production excellence
  - Demonstrated good commercial quality
  - Compensatory measures as required to address shortfalls
- Independent confidence building measures shall include
  - Examination, inspection, maintenance and test records
  - Commissioning tests
- Independent confidence building measures should consider
  - Prior use
  - Supplier pedigree

Office for Nuclear Regulation
An agency of HSE