Office for Nuclear Regulation

4th MDEP Conference on New Reactor Design Activities
London, 12-13 September 2017

Digital Instrumentation and Control: Current and Emerging Technical Challenges in the U.K.

Stephen Wardle
Principal Inspector – Nuclear Safety

Office for Nuclear Regulation

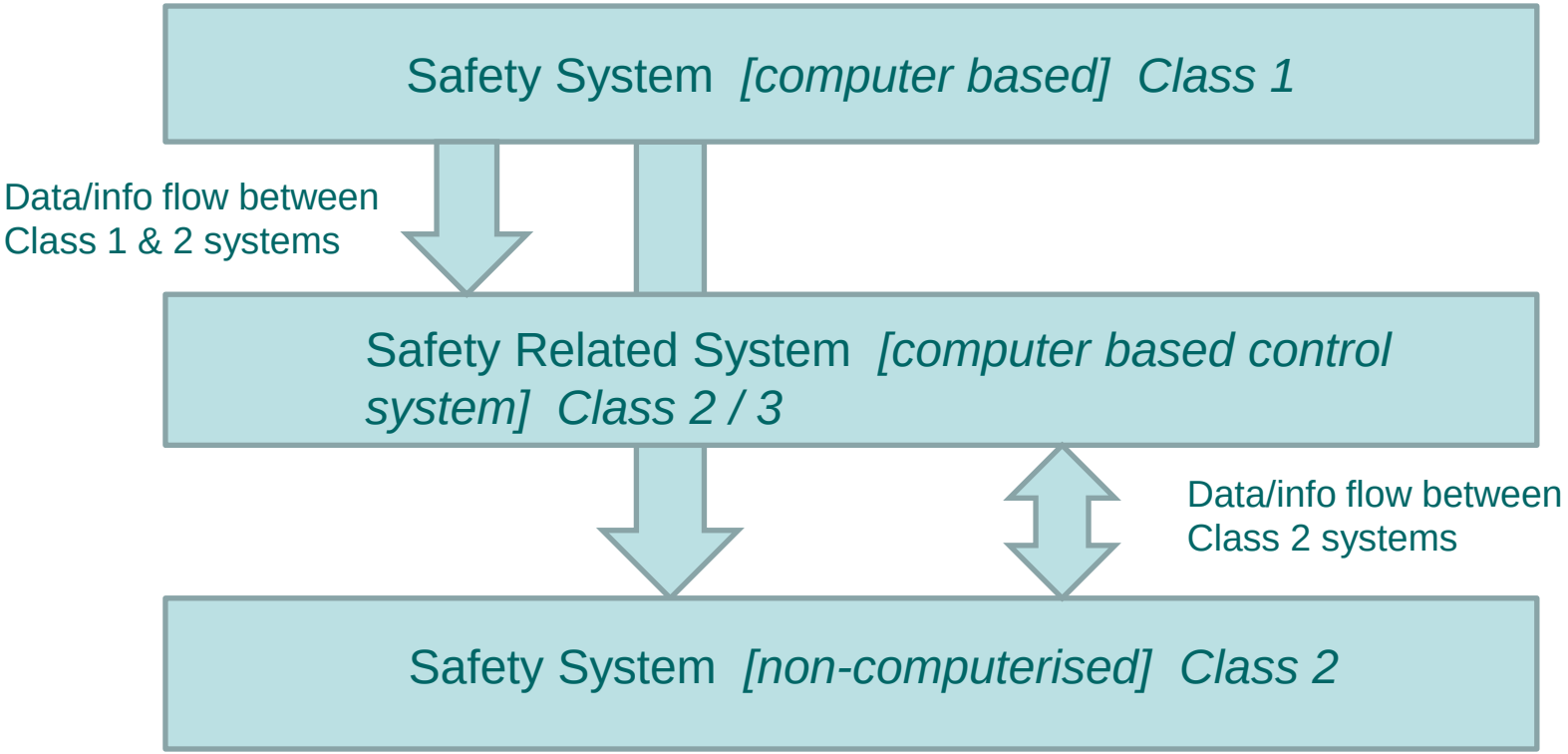
Digital Instrumentation and Control: Current and Emerging Technical Challenges in the U.K.

- I&C architecture design
- Commercial Off-The-Shelf Software (COTS)
- Justification of smart devices
- Development of coherent safety cases

I&C Architecture Design

- Categorisation of safety functions
- Classification of systems
- Simplicity, separation and segregation
  - Perceived move towards more integrated systems
- Common cause failures
- Interconnections between systems of different safety classes
- Fault propagation through the architecture
- Support systems e.g. power supplies, HVAC
- Security by design (defence in depth for security and safety)

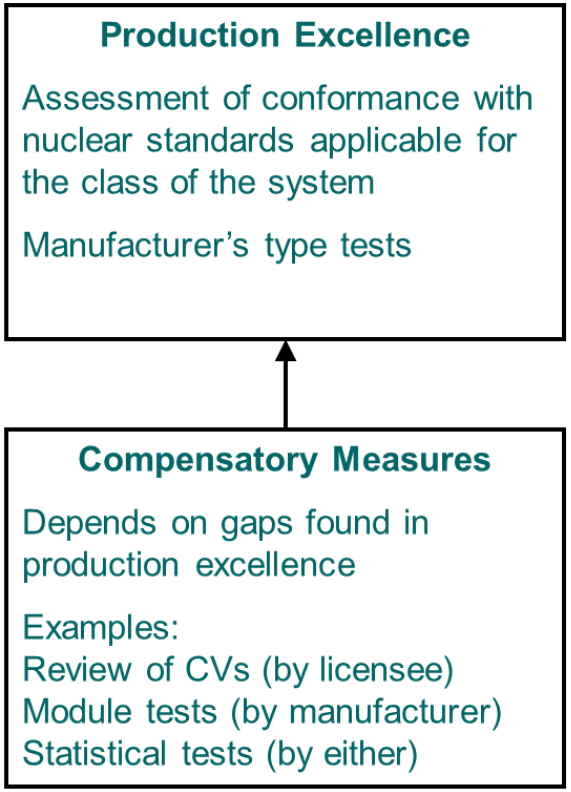
Safety System Platform Level Architecture



Commercial Off-The-Shelf Software (COTS)

- Use of COTS in Digital I&C systems important to safety
  - Control and Protection system platforms
  - Smart devices
- Depth of COTS
  - Embedded devices e.g. FPGAs
  - Embedded software e.g. operating systems
  - Tools e.g. compilers
- Typically not developed for nuclear safety applications
- Access to evidence is the key
  - Manufacturers IPR
  - Certification

The Two-Legged Approach – NS-TAST-GD-046



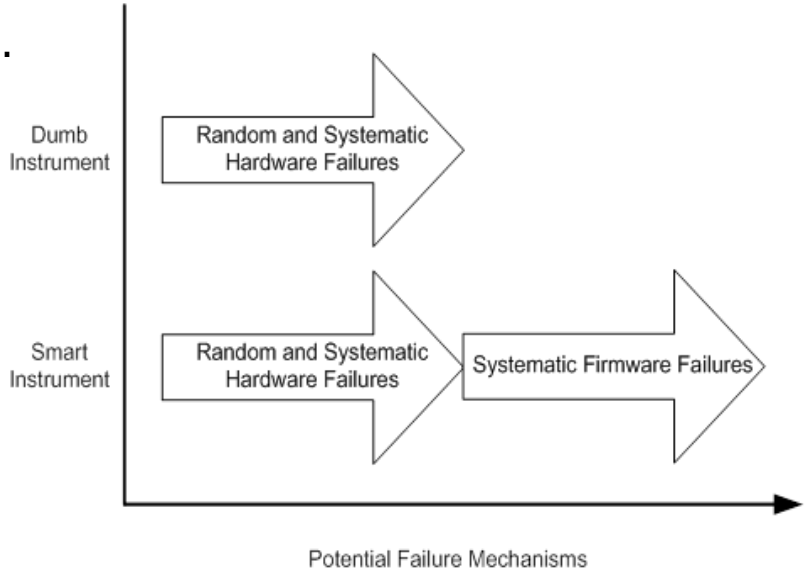
Independent Confidence Building Measures

Dependent on the class, a justified selection 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

Smart Devices

- Particular class of COTS
- Ubiquitous – instruments, power supplies, drives, electrical fault relays etc.
- Safety justification issues as for COTS
- Standards and CINIF research informing UK relevant good practice
- Willingness of manufacturers to cooperate
- Nuclear market small – limited incentive for manufacturers
- Time and effort involved



Safety Cases for Computer-based Safety Systems

- The UK regulatory expectation is that Licensees submit:
  - A pre-construction safety report (PCSR) for the plant
  - Basis of safety case reports (BSCs) for each of the principal I&C systems
- A claims-arguments-evidence approach to the safety justification of I&C systems is encouraged
- The sort of questions that have been raised include:
  - What does a safety demonstration contain?
  - What is claim-based reasoning?
  - When is the case complete?

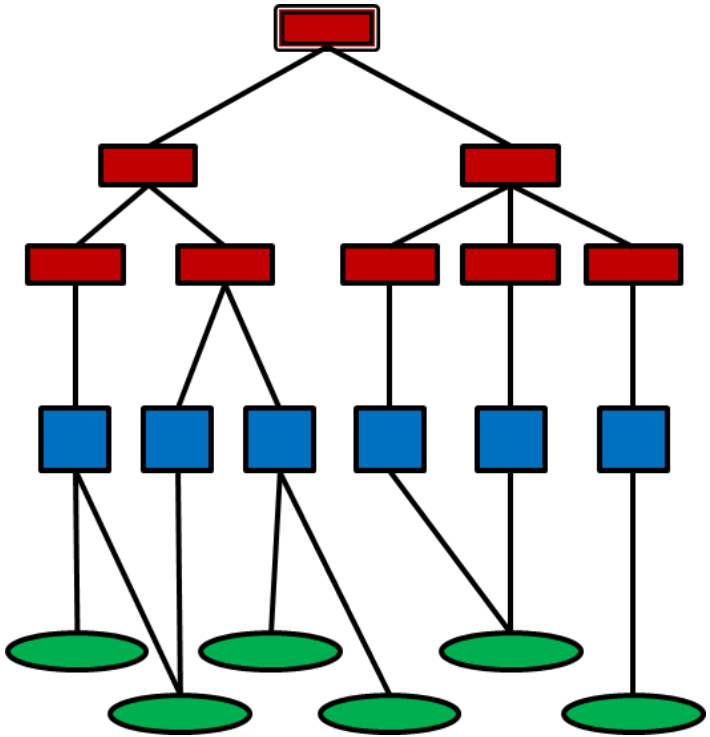
Safety Cases for Computer-based Safety Systems

Claim
What do I need to demonstrate?

Sub-claims
What does my claim depend on?

Argument
Why the evidence is sufficient to demonstrate the sub-claim

Evidence
Where to find the evidence



Applicable MDEP DICWG Common Positions

- MDEP DICWG Common Position 09 - Safety Design Principles and Supporting Information For The Overall I&C Architecture
- MDEP DICWG Common Position 08 - The Impact of Cyber Security Features on Digital I&C Safety Systems
- MDEP DICWG draft Common Position 14 - The Qualification of I&C Platforms For Use In Important To Safety Applications
- MDEP DICWG Common Position 07 – The Selection and Use of Industrial Digital Devices of Limited Functionality

Thank You