Office for Nuclear Regulation

Workshop on Verification and Regulatory Issues for Remote Robotic Inspection January 2021

- a view from the nuclear sector

Dr Andrew White
Principal Control & Instrumentation Specialist
Electrical, Control and Instrumentation (E,C&I) group
Office for Nuclear Regulation (ONR)

What does ONR do?

ONR regulates activities involving nuclear materials in the civil sector.

ONR's purposes cover:

- Nuclear safety
- Non-nuclear health and safety on a UK nuclear site
- Nuclear security
- Nuclear safeguards (accounting of nuclear materials)
- Nuclear transportation

Nuclear site licence holders are licensees and have certain legal obligations set out in 36 license conditions

Differences in international approaches to health and safety regulation

- The Health and Safety legislation in most countries is **prescriptive:**
  - Relying on **compliance** with Standards,
  - Type **certification**, and
  - is **rule** based

  This may mean the best solutions are not identified for a given problem and can result in a 'tick box' approach.

- UK Health and Safety regulation is **goal setting:**
  - Objective is to reduce risk So Far As Is Reasonably Practicable (SFAIRP) = reduce risk **As Low As Reasonably Practicable** (**ALARP**)
  - Requires a number of options to be evaluated to determine best one.
  - Also expect conformance with **Relevant Good Practice (RGP)** e.g. **International Standards** and other approaches that have been shown to be **Reasonably Practicable**.
  - When to stop? – When the cost of applying improvements is Grossly Disproportionate to the benefits.

How does ONR regulate (1)?

- ONR expects adequate safety to be **demonstrated** through a **safety case**, covering all aspects of the system, **before deployment.**
- The safety case covers all aspects of the system that could affect safety or security, such as:
  - Fault studies (what can go wrong)
  - Mechanical engineering
  - Structural engineering
  - Human factors
  - Electrical engineering
  - Controls and Instrumentation
  - etc.
- The safety case is normally structured in a Claims, Arguments, Evidence form.
- The safety case is **NOT** for the regulator, but is intended for the licensee to **demonstrate to itself** that adequate safety has been achieved.
- The risk of the activity **remains that of the licensee**.

How does ONR regulate (2)?

- ONR sets **high-level goals** that should be achieved rather than forcing licensees to take a particular approach.
- The high level goals are described in:
  - ONR's safety assessment principles (SAPs) www.onr.org.uk/saps/saps2014.pdf
  - ONR's security assessment principles (SyAPs) http://www.onr.org.uk/syaps/index.htm
  - Technical Assessment Guides (TAGs) www.onr.org.uk/operational/tech_asst_guides/index.htm

- ONR expects the demonstration to be primarily **deterministic**, supported by **probabilistic** arguments and evidence

Development of computer based systems

ONR expects computer system **development and verification** to be based on a safety lifecycle, such as that described in the international standard IEC 61508 “Functional safety of electrical electronic programmable electronic safety-related systems”

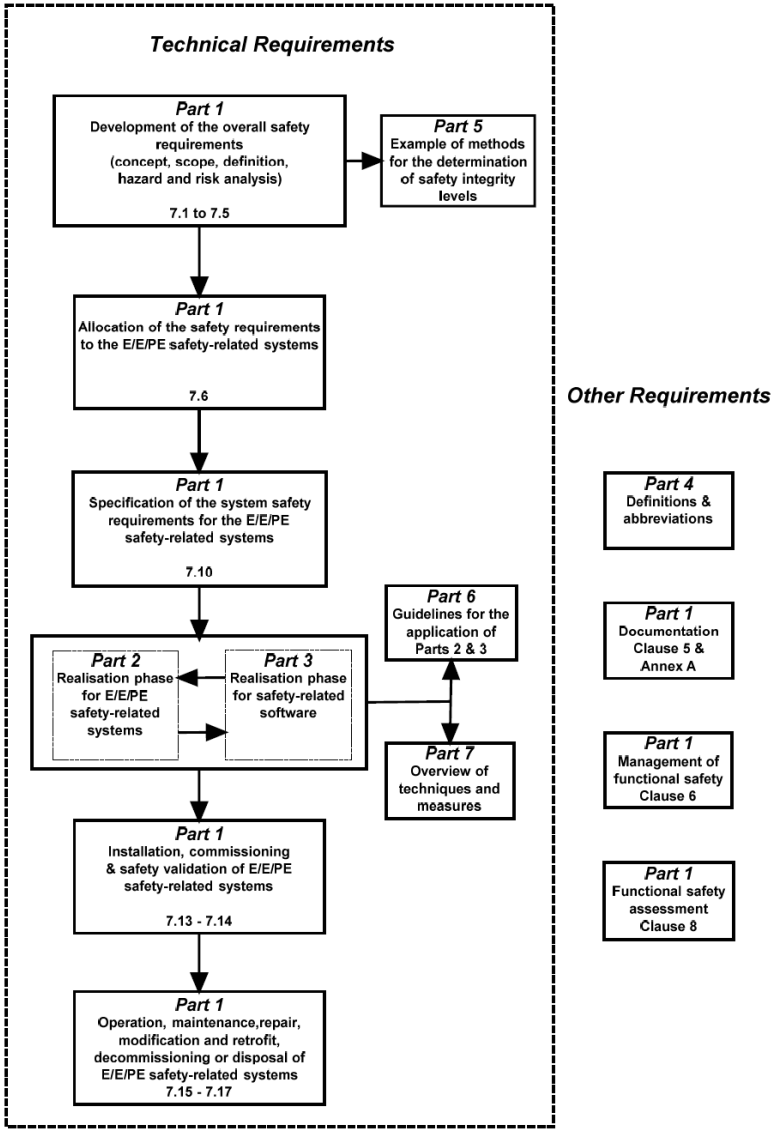

Figure 1 – Overall framework of the IEC 61508 series

Office for Nuclear Regulation

How does this relate to the verification of robotic systems?

All of the system should be considered, (e.g. mechanical, electrical, software, human factors, etc.) in the safety case.

For computer based systems, ONR's expectation is that there would be a **two legged safety argument** comprising a:

- Demonstration of sound software development processes and verification techniques (**Production Excellence** (PE))
- Proof that the development processes have been successful **(Independent confidence building measures** (ICBMs))

Example of how to go about verifying robotic systems (1)

Before you start, think about how you will verify your robotic system, and document this so everyone has a common understanding:

- Consider all the hazards:
  - arising from the environment (and changes in the environment)
  - caused by the robot
- How can these hazards be avoided, managed, or changed into hazards that are easier to deal with?
- Identify/develop what specific features of the robot are used to deal with each hazard, and how.
- What hazards cannot be dealt with? These may have to be limitations or conditions of use.

Example of how to go about verifying robotic systems (2)

- For any system containing software a demonstration of adequate safety is **difficult to show through testing alone**. This is because software systems are **vulnerable to changes** in input conditions and **can be in one of very many internal states**.
- **Analysis is almost always** a much more powerful and cost-effective way of demonstrating a system is adequately safe than **testing** (although testing is still necessary).
- **Simplicity** is always preferred over **complexity**, commensurate with getting the job done.

Examples:

- Use mechanical limits to prevent a robot straying
- Ensure that the amount of energy available to and stored in a robot is limited so it can do no harm.

Questions?