Office for Nuclear Regulation

Workshop on Scoping Safety Cases for Nuclear Robotics

Manchester Marriot Victoria & Albert Hotel, Manchester

12 April 2019

Office for Nuclear Regulation

- ONR is an independent statutory body. We are as far removed from Government as is possible. Government has no role in regulatory decision making.
- Formed in April 2014 when the Energy Act 2013 came into force.
- Formerly a Directorate of the Health & Safety Executive (HSE).
- Began as Nuclear Installations Inspectorate (NII) in 1960.
- ONR's Mission Statement is:

'to provide efficient and effective regulation of the nuclear industry, holding it to account on behalf of the public'

Office for Nuclear Regulation

ONR C&I RESEARCH ACTIVITIES – ENABLING INNOVATIVE TECHNOLOGIES

Office for Nuclear Regulation

OVERVIEW

- ONR has an active programme of research and cooperates with international regulators on safety and security issues of common concern, including associated research.

- Major element of C&I Research Portfolio is collaborative with nuclear industry through participation in the C&I Nuclear Industry Forum (CINIF) – currently over 20 separate initiatives/projects in progress.

- ONR also supports research through membership of other initiatives, such as RAIN Research Hub steering committee, as well as engaging in other BEIS-sponsored programmes.

ONR supports the use of innovative technologies that can benefit nuclear safety and security – these need to be demonstrably safe and secure through use of a "safety case"

Office for Nuclear Regulation

Safety Cases for Nuclear Robotics: ONR Perspective

Office for Nuclear Regulation

Definition of a Safety Case

‘A safety case is a logical and hierarchical set of documents that describes risk in terms of the hazards presented by the facility, site and modes of operation, including potential faults and accidents, and those reasonably practicable measures that need to be implemented to prevent or minimise harm. It takes account of experience from the past, is written in the present, and sets expectations and guidance for the processes that should operate in the future if the hazards are to be controlled successfully. The safety case clearly sets out the trail from safety claims through arguments to evidence.’

From ‘ONR Safety Assessment Principles for Nuclear Facilities. 2014 Edition Rev 0’

Office for Nuclear Regulation

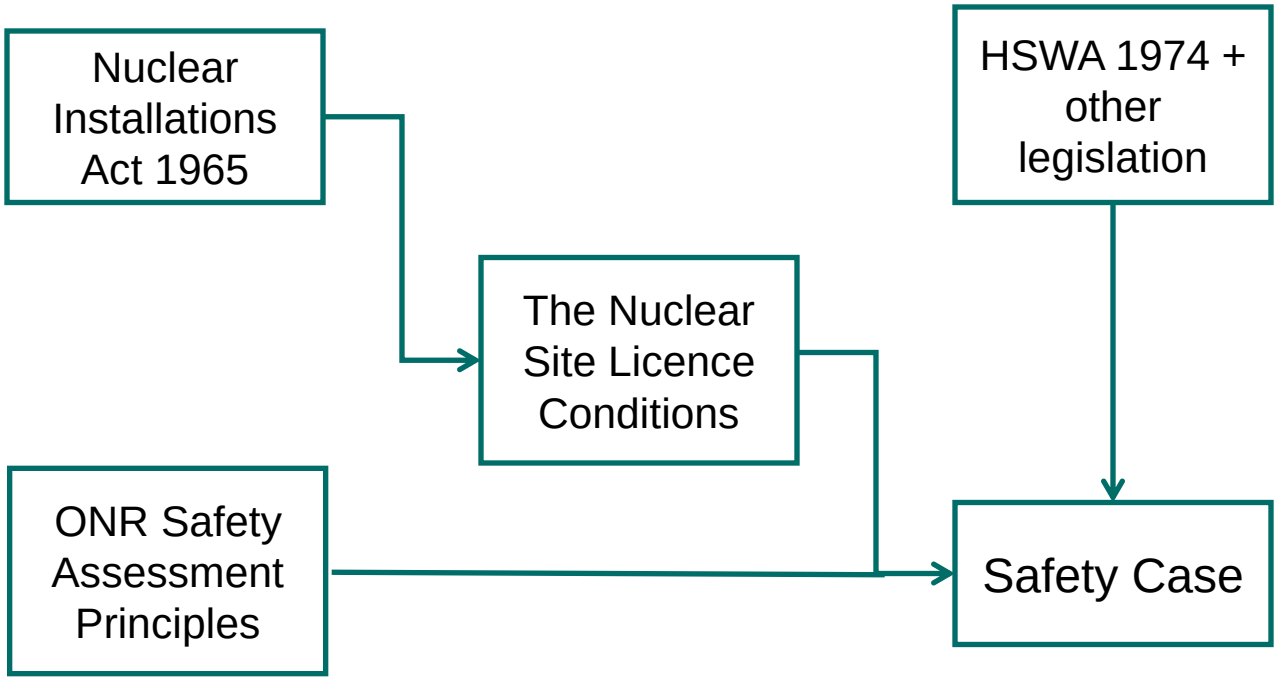
Purpose of a Safety Case

- The primary purpose of a safety case is to provide the licensee with the information required to enable safe management of the facility or activity in question.
- A safety case should communicate a clear and comprehensive argument that a facility can be operated or that an activity can be undertaken safely.
- A safety case should demonstrate that the associated risk and hazards have been assessed, appropriate limits and conditions have been defined, and adequate safety measures have been identified and put in place.
- It is essential that the safety case documentation is clear and logically structured so that the information is easily accessible to those who need to use it. This includes designers, operations and maintenance staff, technical personnel and managers who are accountable for safety.

See also ONR Technical Assessment Guide 'The Purpose, Scope, and Content of Safety Cases' NS-TAST-GD-051 Rev 4.

Office for Nuclear Regulation

Why? Relationship to Licence and Legislation



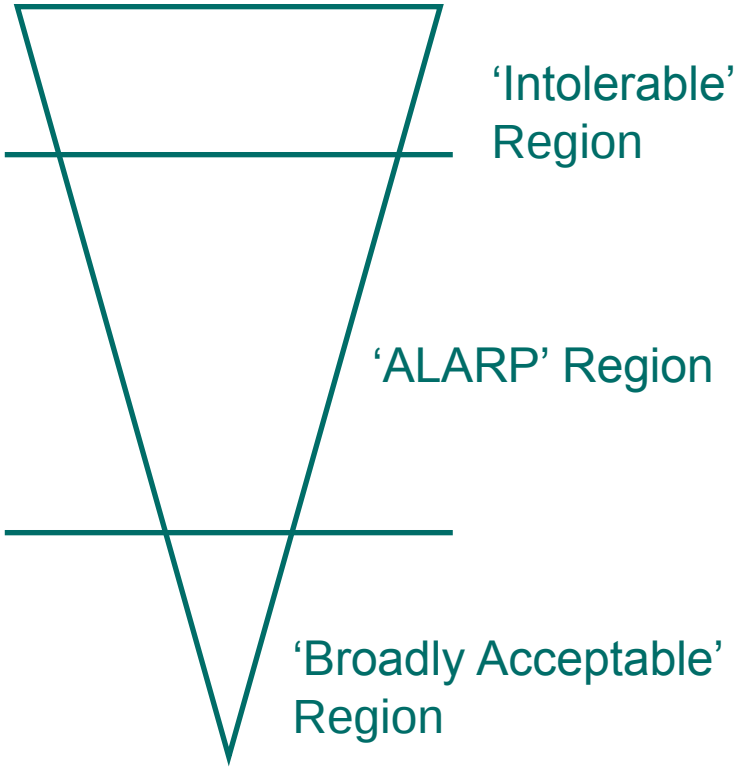
Office for Nuclear Regulation

Context

- The documented safety case is not an end in itself. It forms an important part of how the licensee manages safety of plant/facility.
- The requirements of the safety case need to be implemented and managed effectively to deliver safety.
- Fundamental to the safety case are the principles, standards, and criteria which the licensee intends to maintain. At a minimum, these must meet statutory requirements and show that risks to individuals will be acceptably low and ALARP.
- What a system must and must not do.

Office for Nuclear Regulation

ALARP



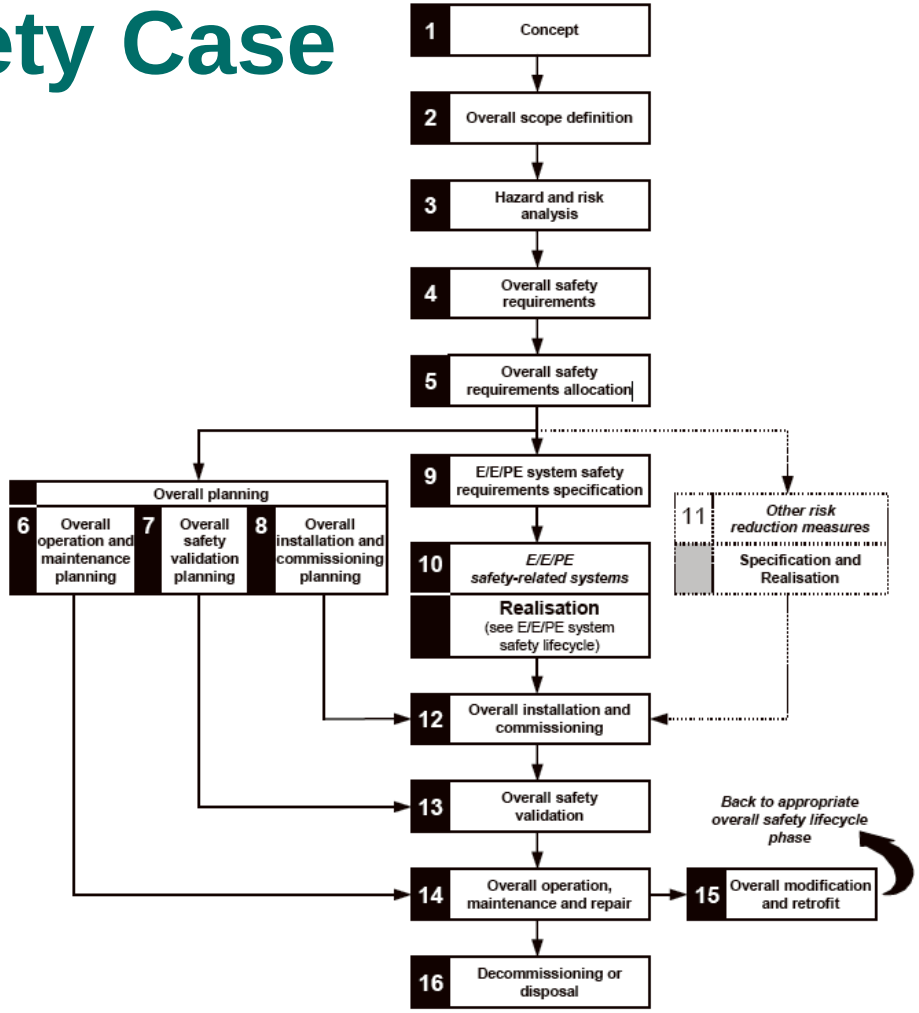
- ALARP is a legal construct that the 'cost' of a risk reduction measure must be grossly disproportionate to the reduction in risk for the risk to be considered 'ALARP'
- Practically this is not done through an explicit comparison of cost and benefits but by applying established relevant good practice (RGP) and standards.

See also NS-TAST-GD-005 "Guidance on the Demonstration of ALARP"

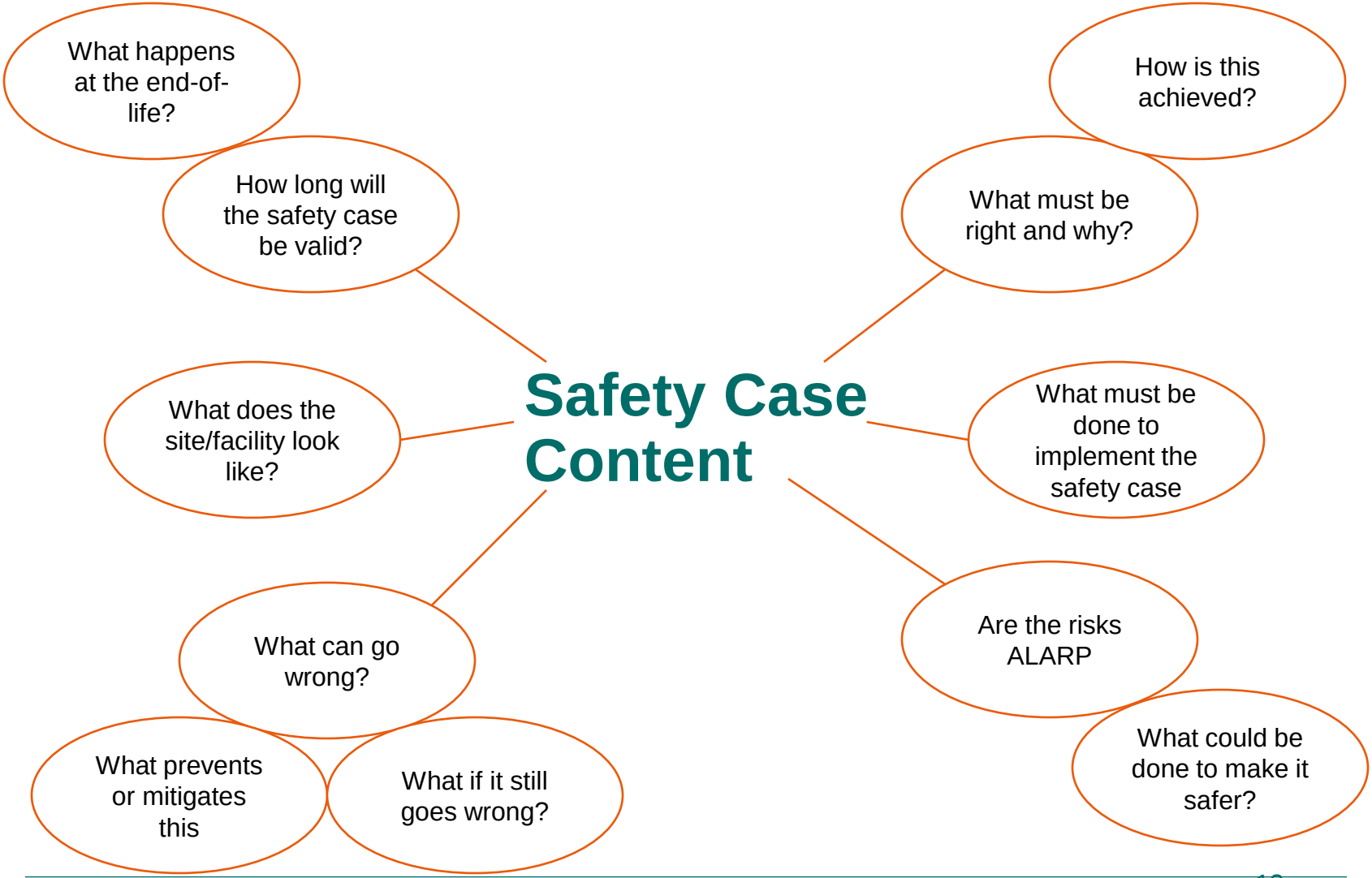
Office for Nuclear Regulation

Life Cycle & Safety Case

- Early design
- Pre-Installation
- Pre-operation
- Operation
- Post Operation
- Decommissioning
- Post-Decommissioning



Office for Nuclear Regulation



Office for Nuclear Regulation

The Security Case

- Security cases are similar to safety cases but from a security perspective.
- In the realm of robotics, autonomy, AI et al this should include both cyber security.
- ‘Air gaps’ are rarely as fool proof as imagined, robot require maintenance, software updates etc…

Office for Nuclear Regulation

Workshop on Scoping Safety Cases for Nuclear Robotics

Manchester Marriot Victoria & Albert Hotel, Manchester

12 April 2019