Office for Nuclear Regulation

Workshop on Nuclear Robotics Safety & Security Cases

Sachas Hotel, Manchester

11 September 2018

Office for Nuclear Regulation

Safety Cases for Autonomous Systems: ONR Perspective

11 September 2018

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 independently regulates safety and security at 36 licensed nuclear sites in the UK.
- ✓ These include the existing fleet of operating civil reactors, fuel cycle facilities, waste management and decommissioning sites and the defence nuclear sector.
- ✓ ONR also regulates the design and construction of new nuclear facilities and the transport of nuclear and radioactive materials and works with international inspectorates to ensure that safeguards obligations for the UK are met. Also, regulates the nuclear supply chain.
- ✓ ONR cooperates with international regulators on safety and security issues of common concern, including associated research.

Office for Nuclear Regulation

- ✓ ONR independently regulates safety and security at 36 licensed nuclear sites in the UK.
- ✓ These include the existing fleet of operating civil reactors, fuel cycle facilities, waste management and decommissioning sites and the defence nuclear sector.
- ✓ ONR also regulates the design and construction of new nuclear facilities and the transport of nuclear and radioactive materials and works with international inspectorates to ensure that safeguards obligations for the UK are met. Also, regulates the nuclear supply chain.
- ✓ ONR cooperates with international regulators on safety and security issues of common concern, including associated research.

ONR's strategic aim is to be "an exemplary regulator that inspires respect, trust and confidence"
(seehttp://www.onr.org.uk/documents/2016/strategic-plan-2016-2020.pdf)

Office for Nuclear Regulation

ONR C&I RESEARCH ACTIVITIES – ENABLING INNOVATIVE TECHNOLOGIES

Office for Nuclear Regulation

OVERVIEW

- ✓ 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 is a full member of CINIF - key role in directing research to ensure focus is on areas that support regulation of technological developments.
- ✓ CINIF has introduced cyber security focussed research.
- ✓ 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 Case

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

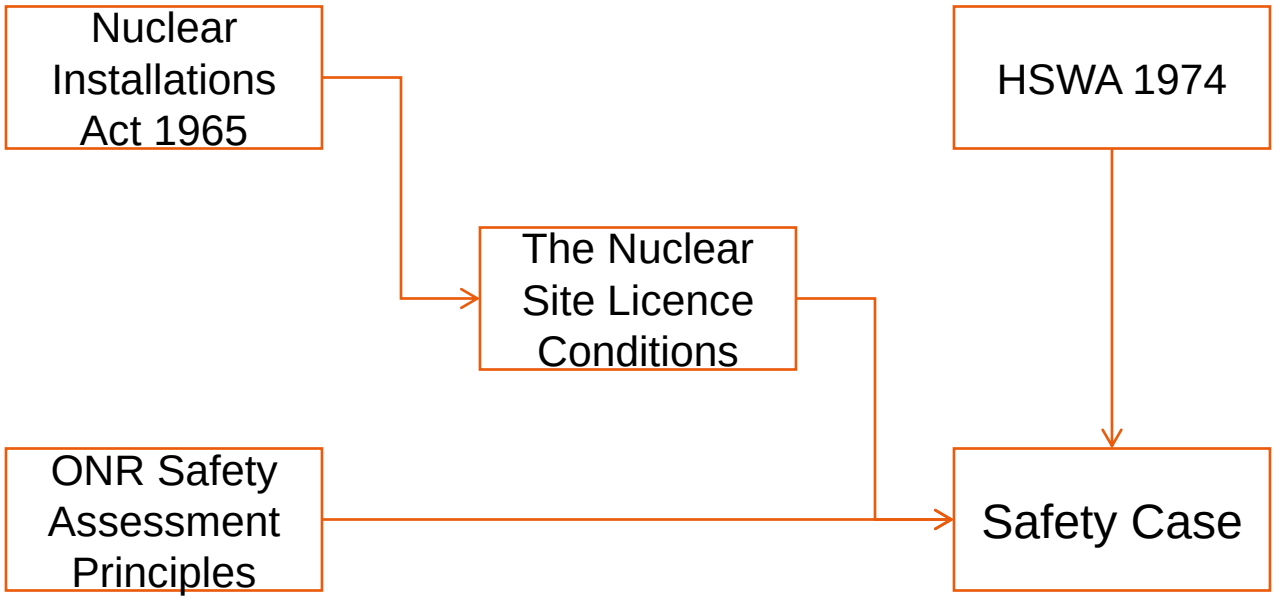
Purpose of a Safety Case

- 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.

From 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

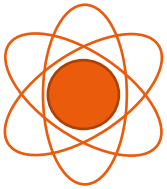


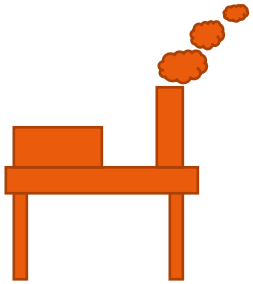
Office for Nuclear Regulation

Safety Cases Across UK Industries

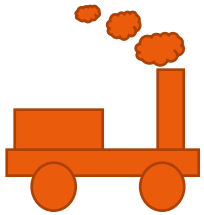
Civil

Nuclear





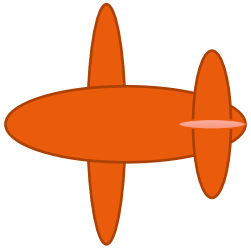
Offshore



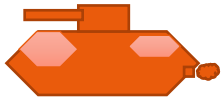
Railways

High Hazard/Chemical

Defence



Aerospace



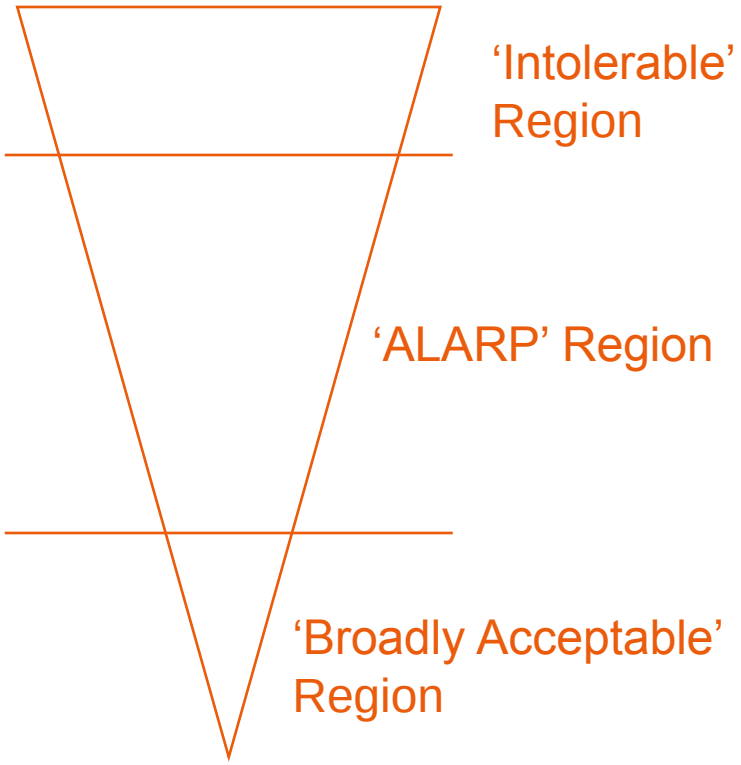
Land Systems

Naval

Nuclear

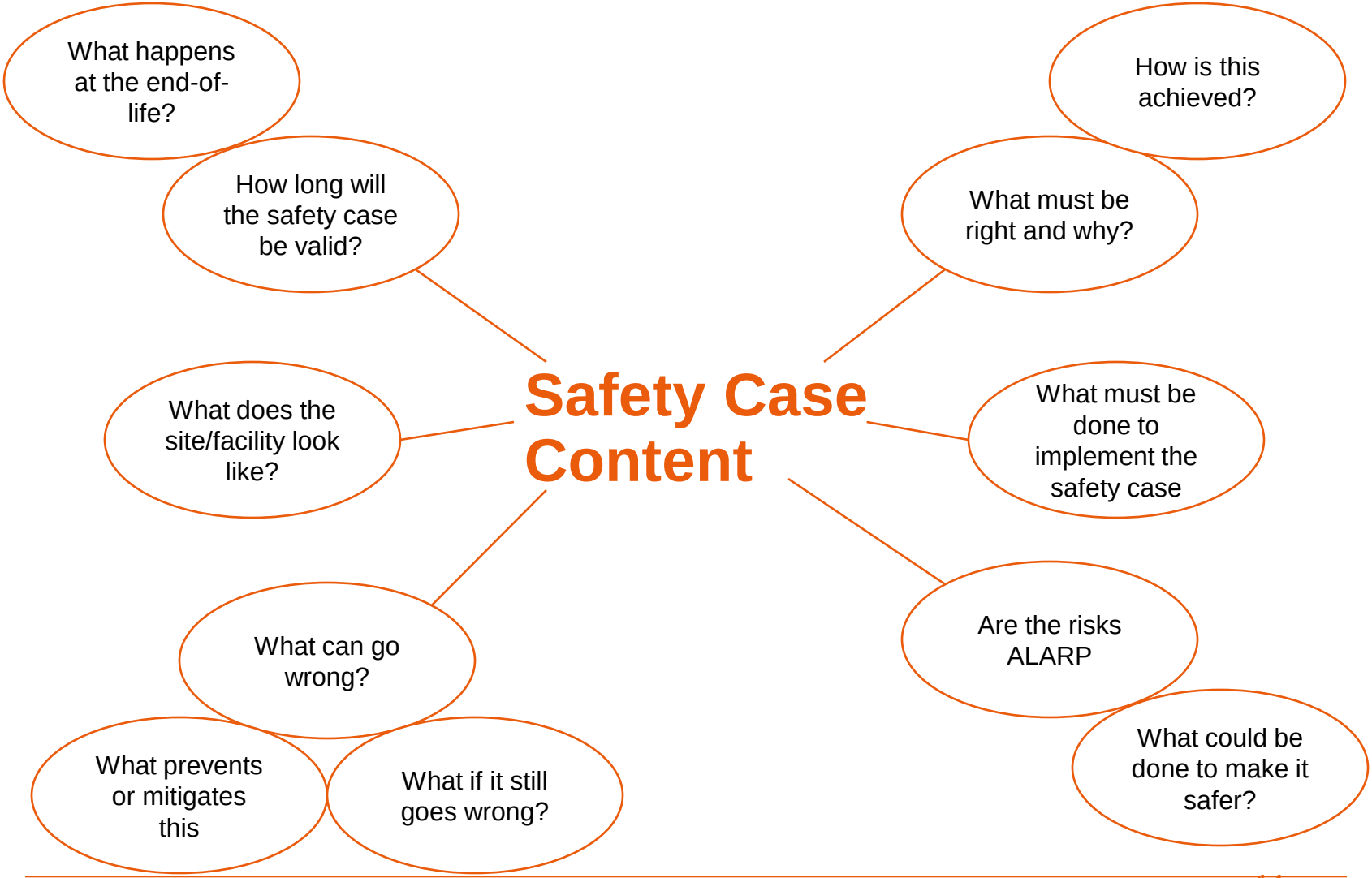
Office for Nuclear Regulation

ALARP



- Idea behind ALARP is 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.

Office for Nuclear Regulation



Office for Nuclear Regulation

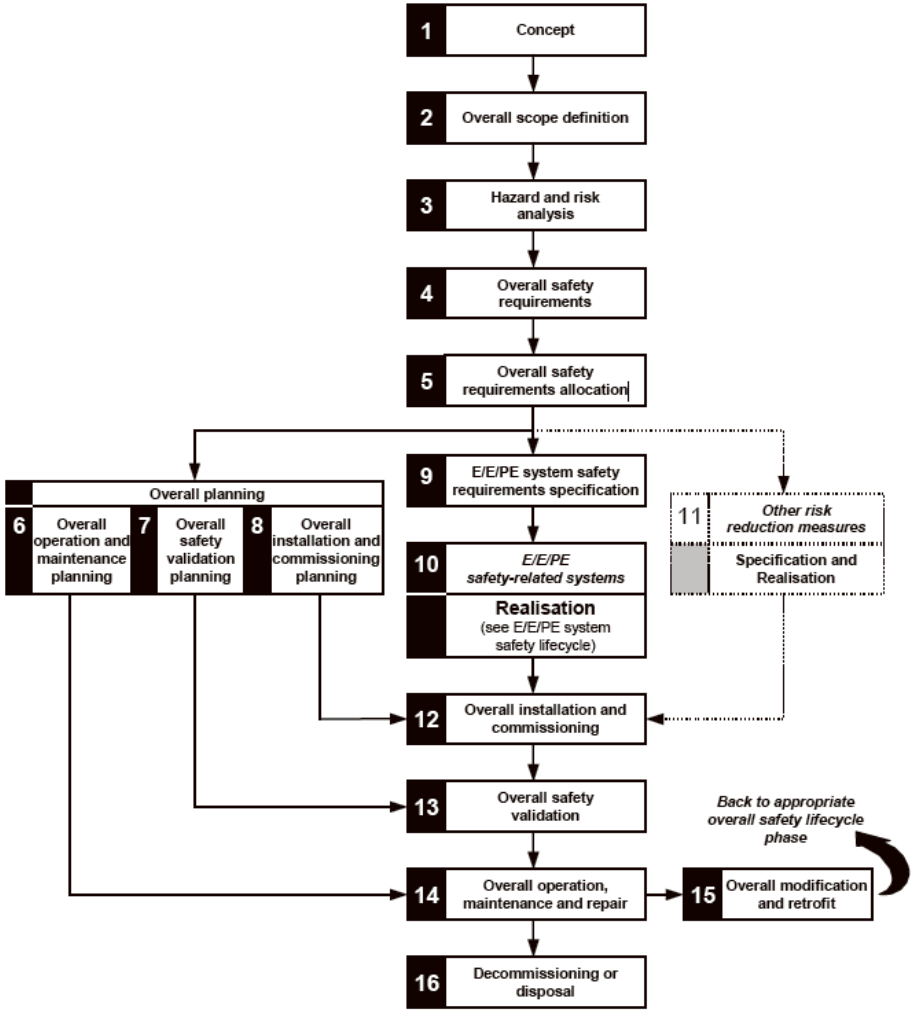
Context

- The documented safety case is not an end in itself. It forms an important part of how the licensee manages safety.
- 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 the system must and must not do

Office for Nuclear Regulation

Life Cycle

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



Office for Nuclear Regulation

The Security Case

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

Office for Nuclear Regulation

Summary

- Safety and Security Cases are a legal requirement
- They are required to show that a system/facility is safe and secure
- They are used in many industries

Office for Nuclear Regulation

Principles of Safe Systems

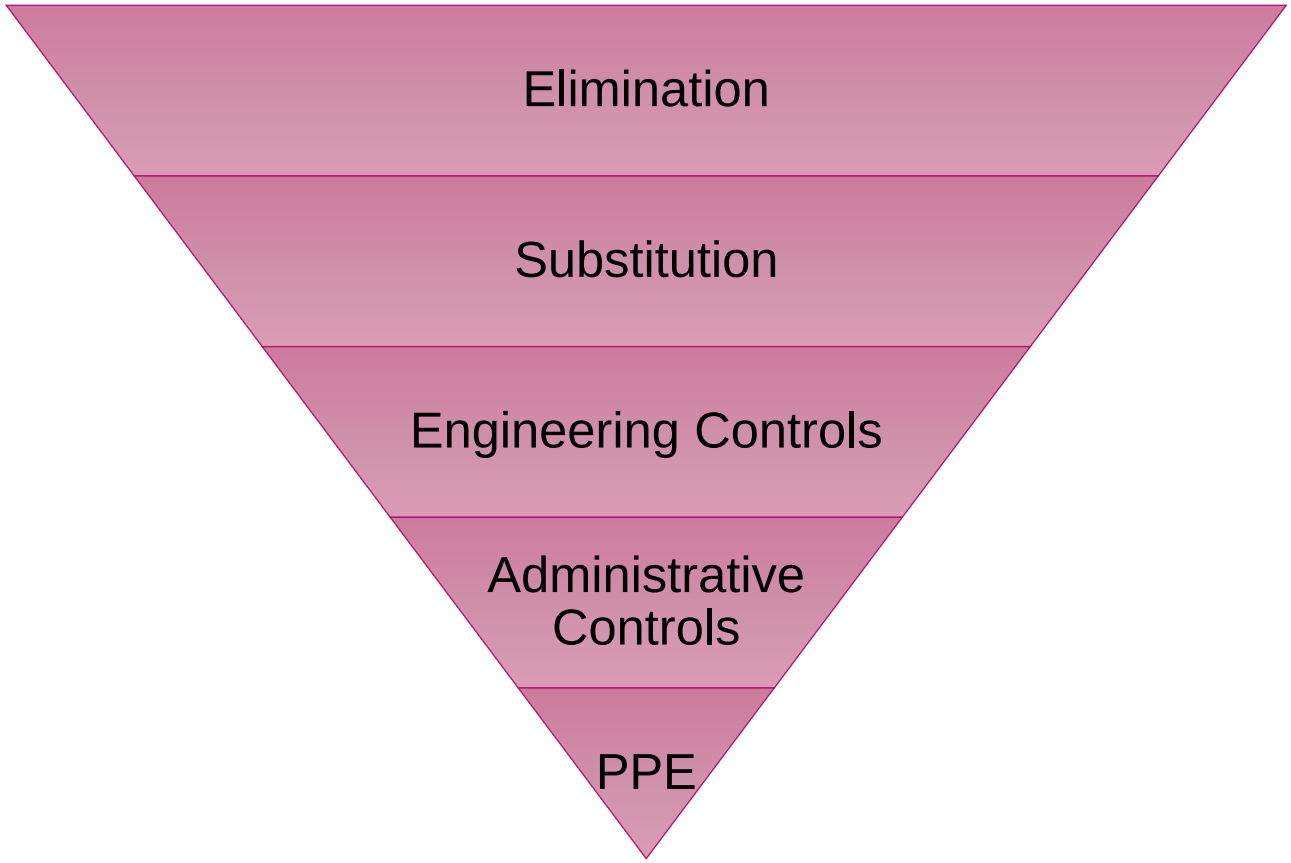
Office for Nuclear Regulation

Safe System Design

Hierarchy of Control Measures

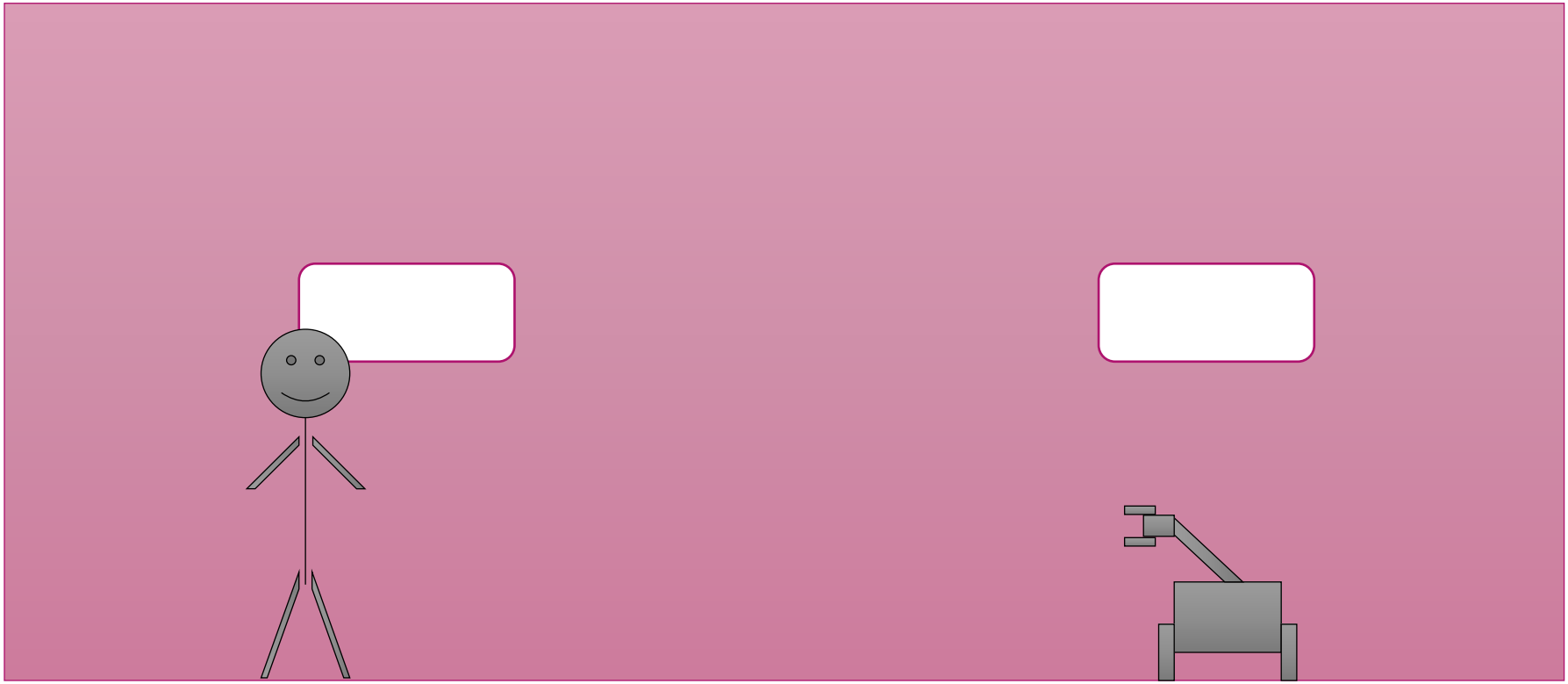
Office for Nuclear Regulation

Hierarchy of Control Measures



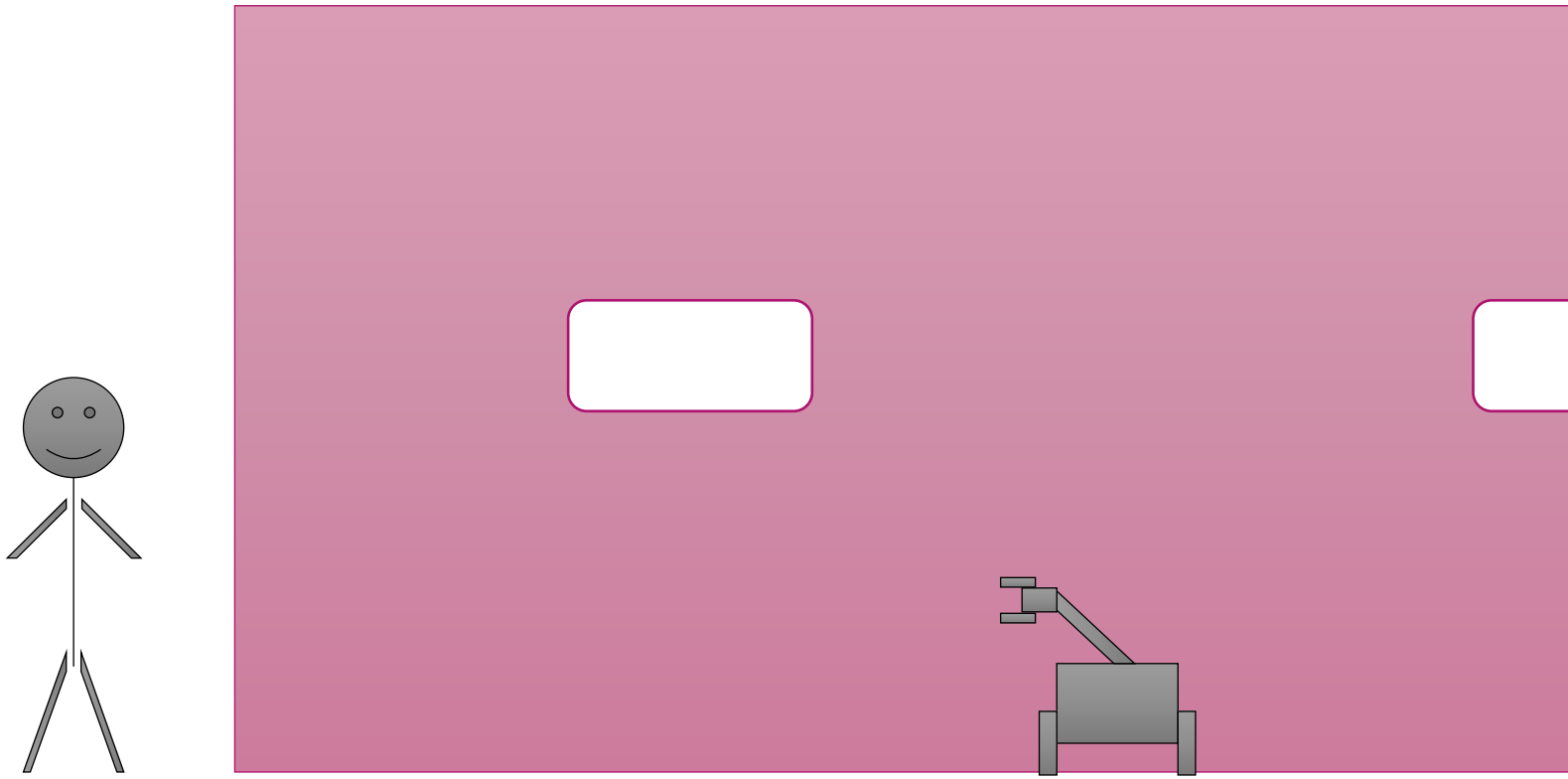
Office for Nuclear Regulation

Example



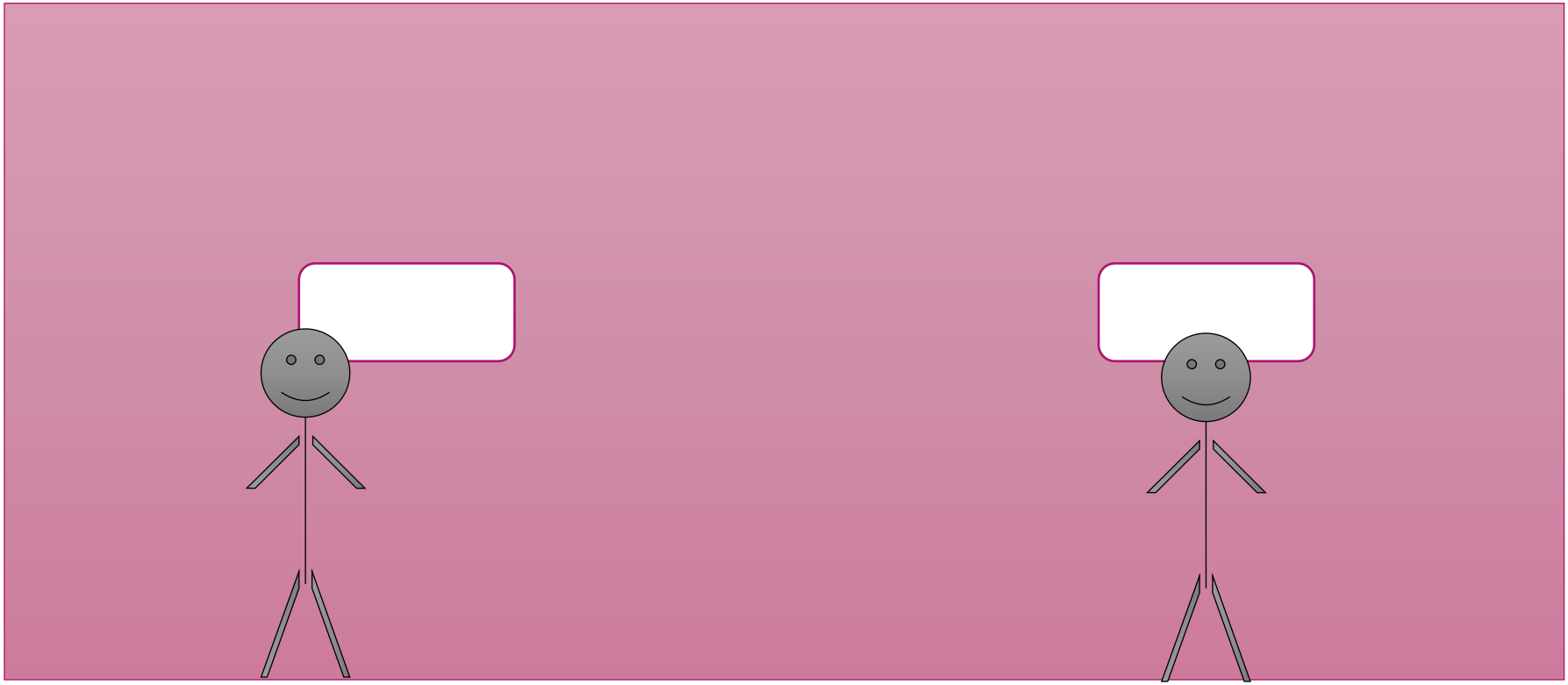
Office for Nuclear Regulation

Elimination/Avoidance



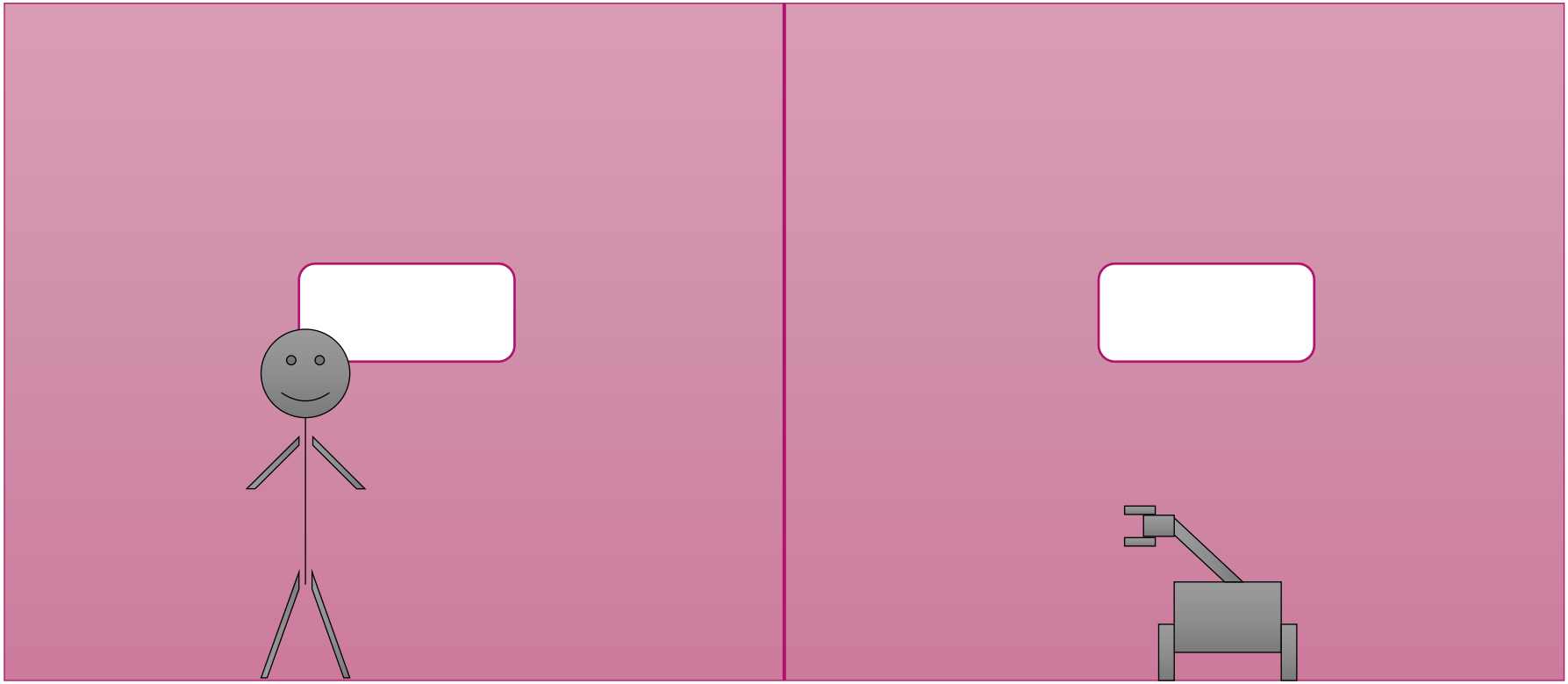
Office for Nuclear Regulation

Substitution



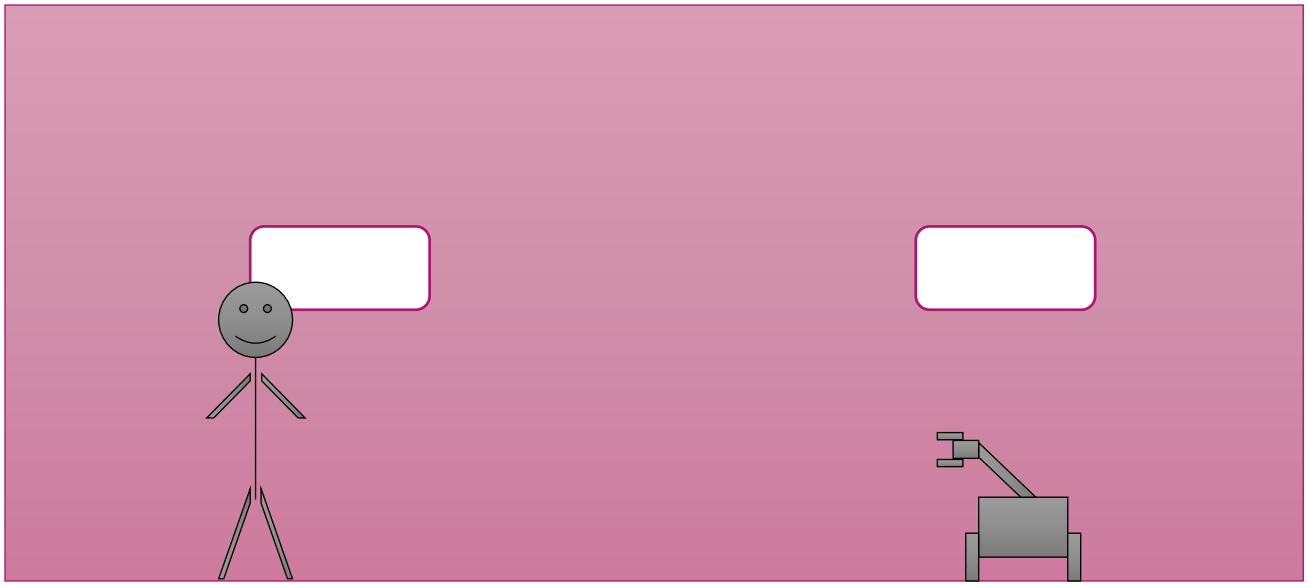
Office for Nuclear Regulation

Engineering Controls

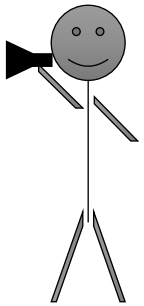


Office for Nuclear Regulation

Administrative Controls

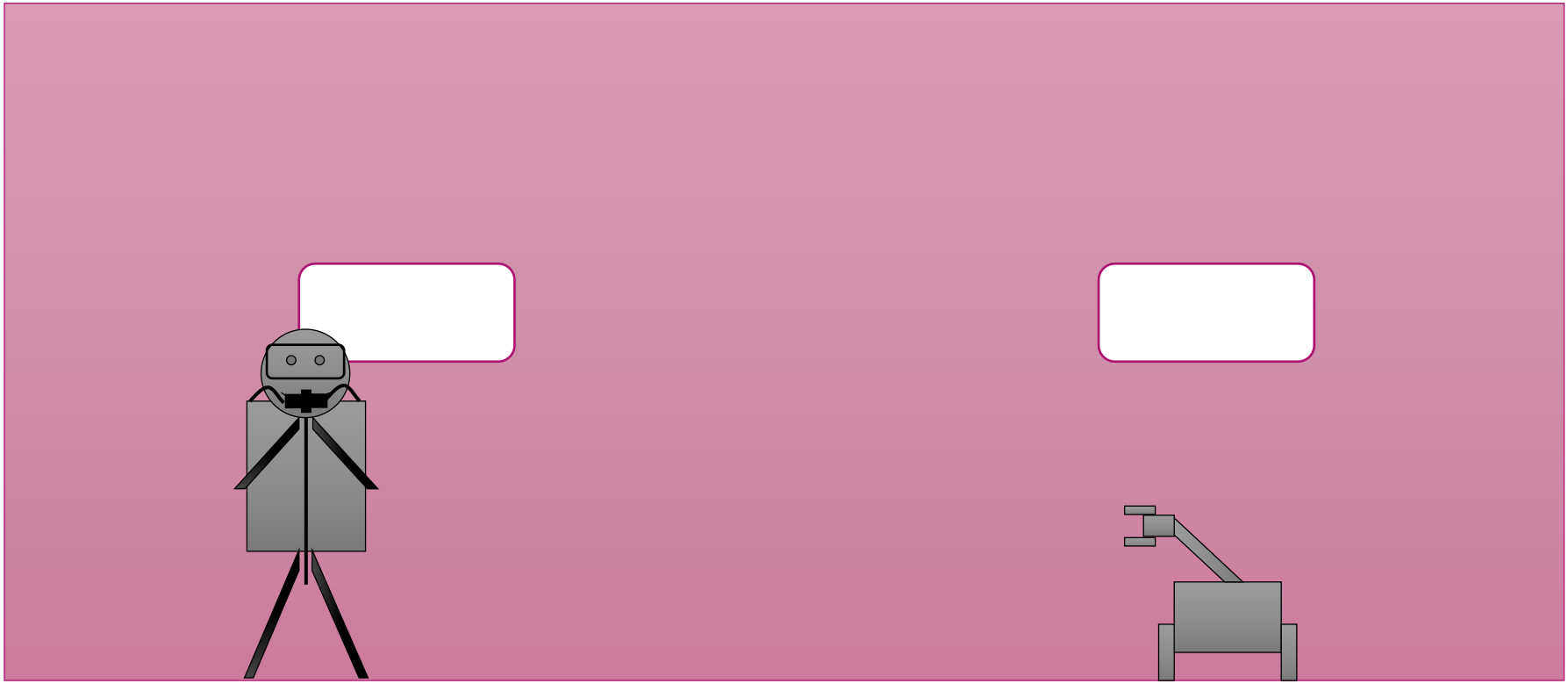


Don’t go near the robot!



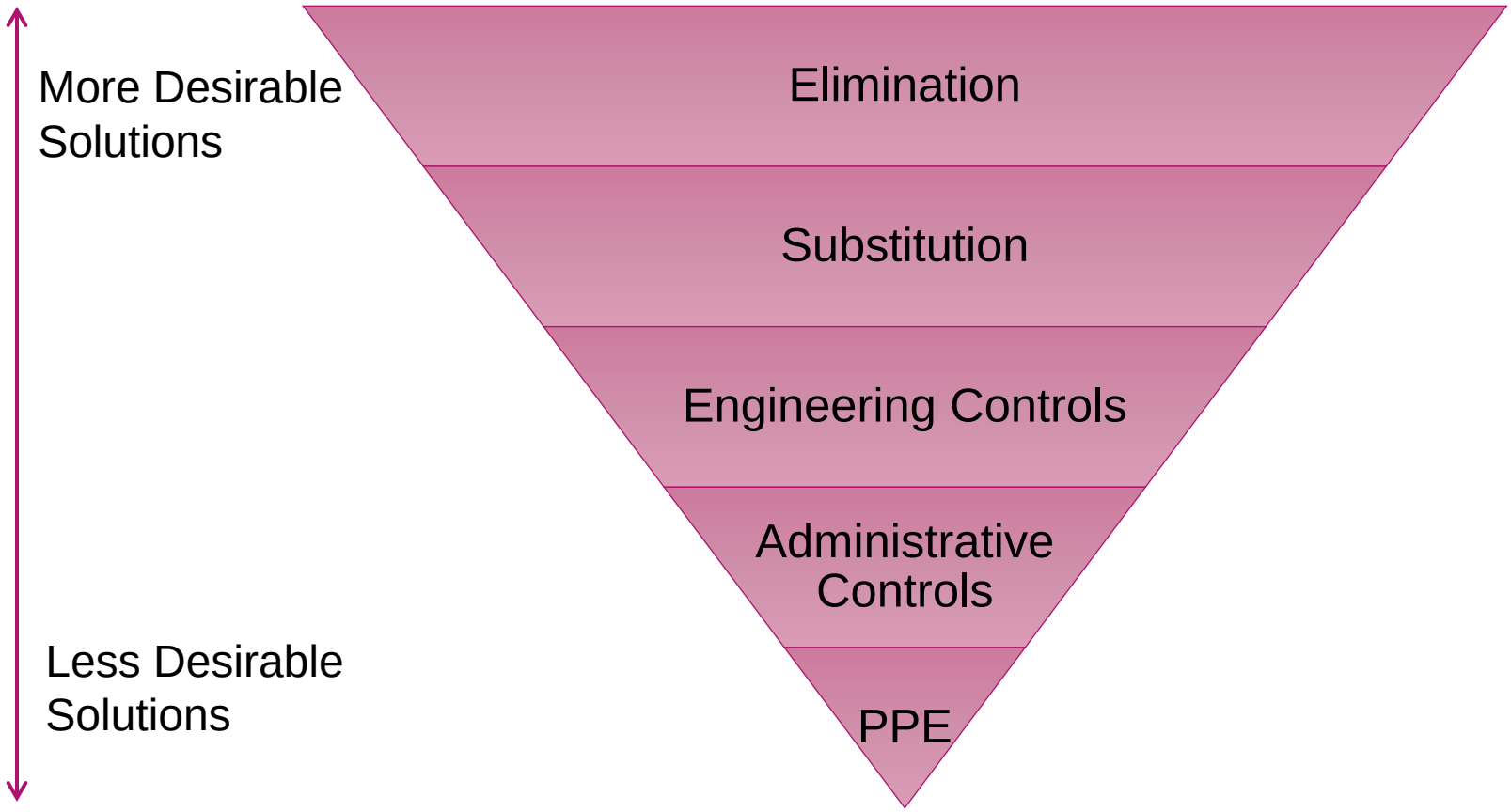
Office for Nuclear Regulation

Personal Protective Equipment



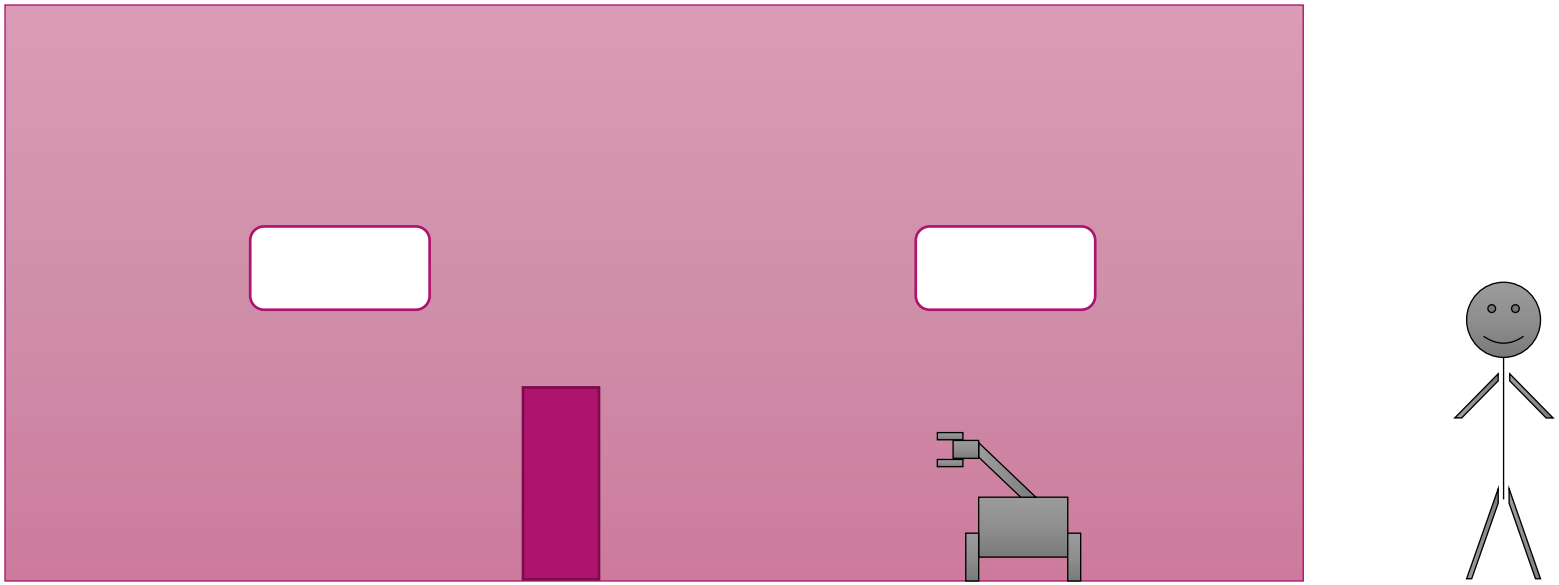
Office for Nuclear Regulation

Hierarchy of Control Measures



Office for Nuclear Regulation

Engineering Controls



Office for Nuclear Regulation

Safe System Design

Separation of Control and Protection

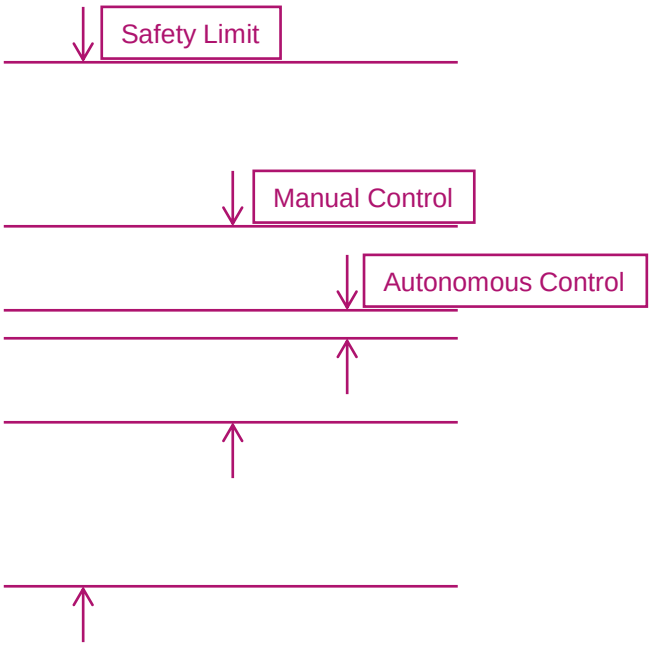
Office for Nuclear Regulation

Separation of Control and Protection

- In the design of complex control of a system, it is expected to separate the control and protection systems
- This prevents the failure of one system affecting the other
- This may be difficult in a robotic system, so design may have to get creative

Office for Nuclear Regulation

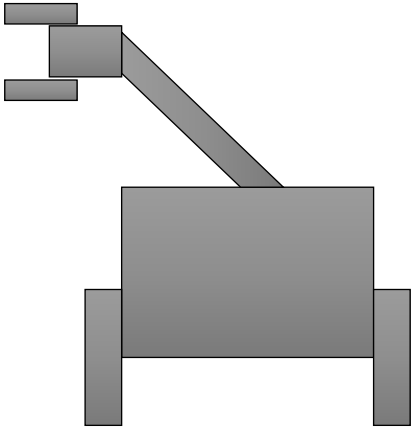
Functional Separation of Control and Protection

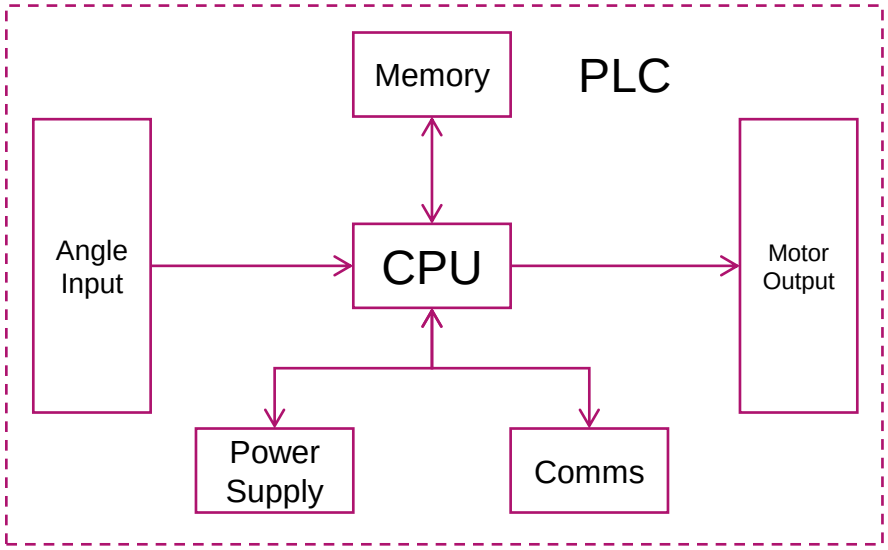


- The autonomous control is primarily designed for optimisation
- Manual control is some systems – but not all
- ‘Safety limit’ the protection systems take over

Office for Nuclear Regulation

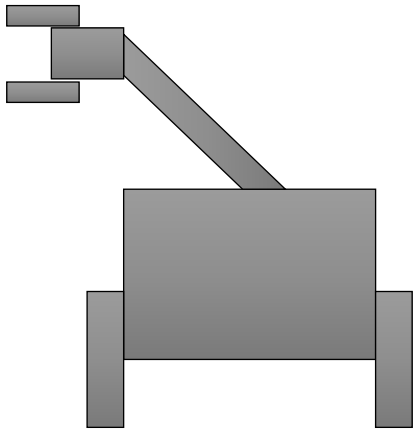
Systematic Separation of Control and Protection

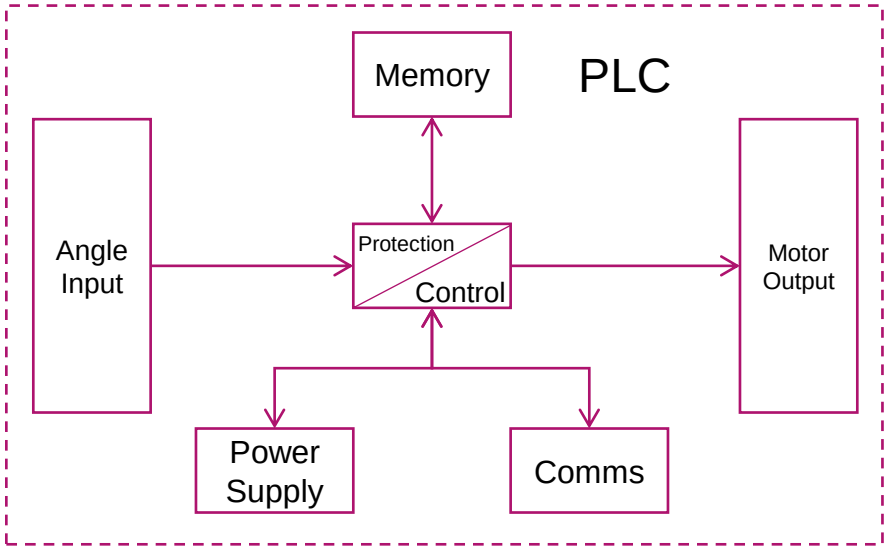




Office for Nuclear Regulation

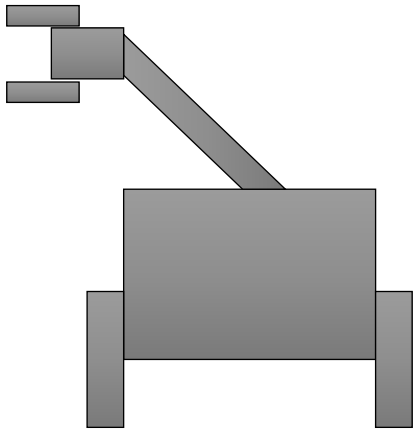
Systematic Separation of Control and Protection

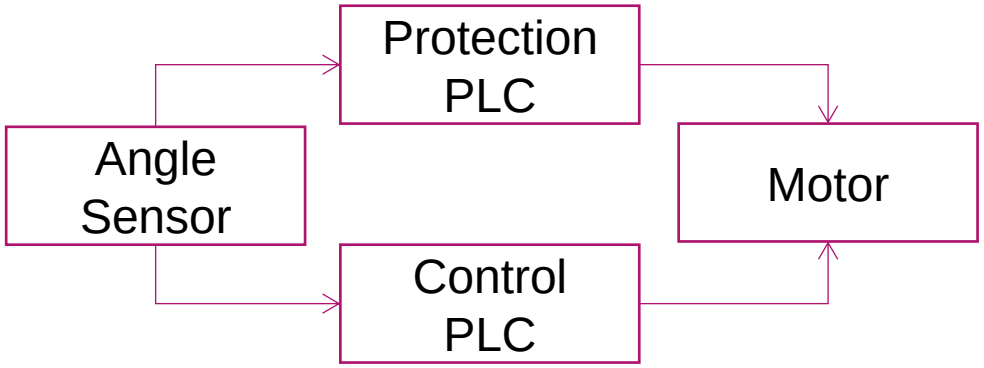




Office for Nuclear Regulation

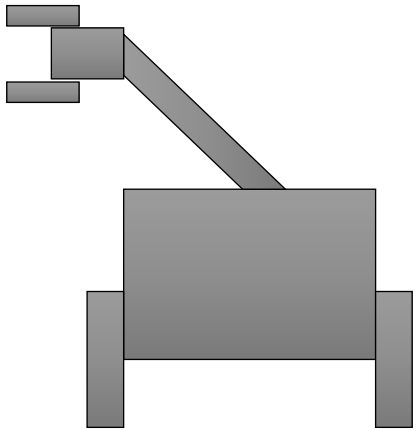
Systematic Separation of Control and Protection

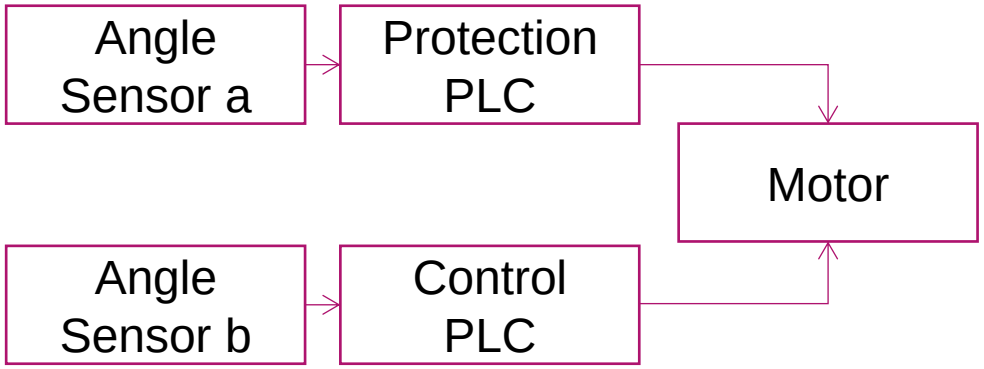




Office for Nuclear Regulation

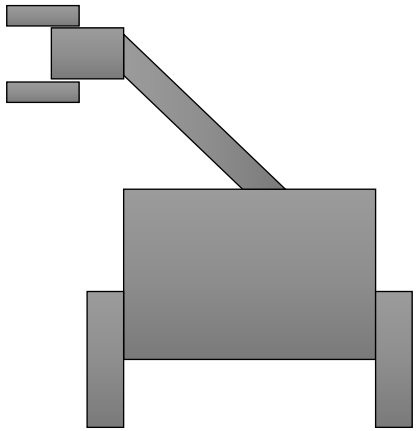
Systematic Separation of Control and Protection

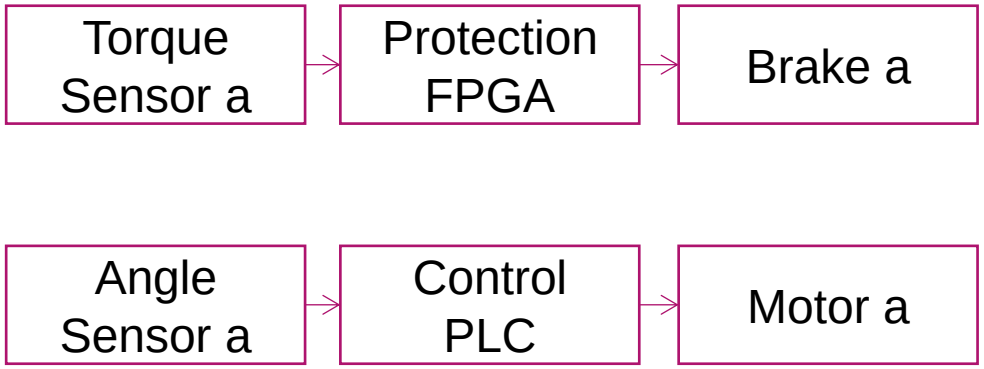




Office for Nuclear Regulation

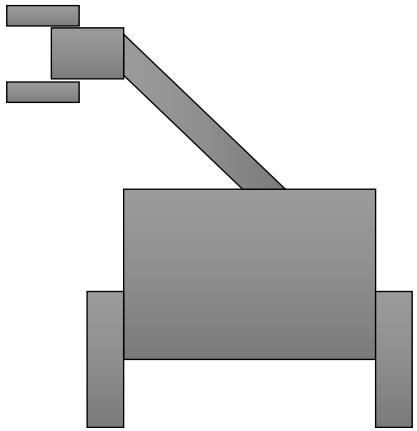
Systematic Separation of Control and Protection

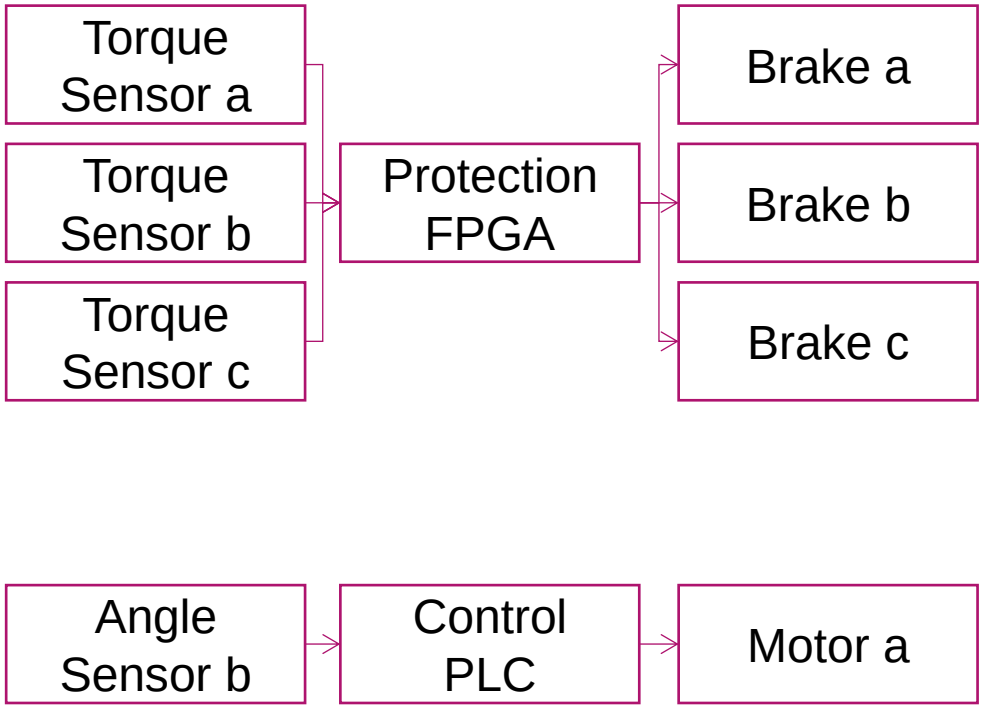




Office for Nuclear Regulation

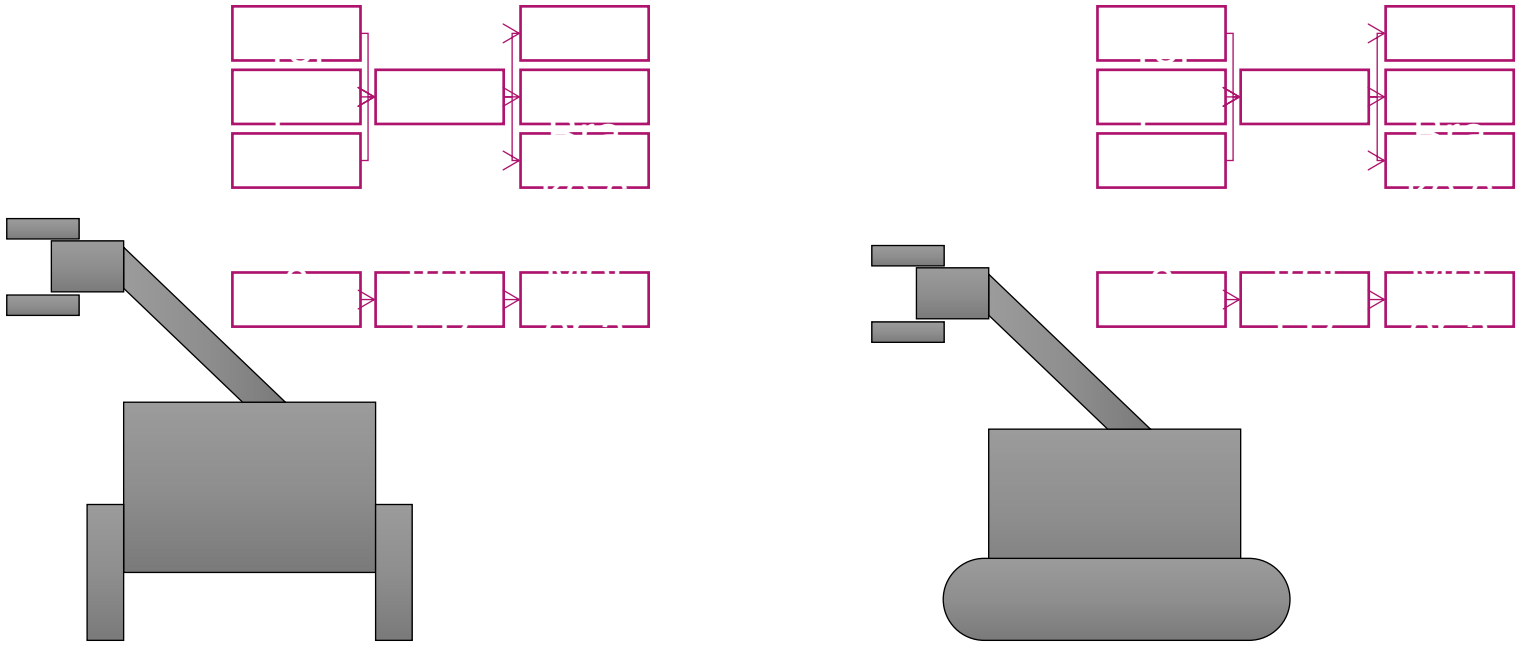
Systematic Separation of Control and Protection





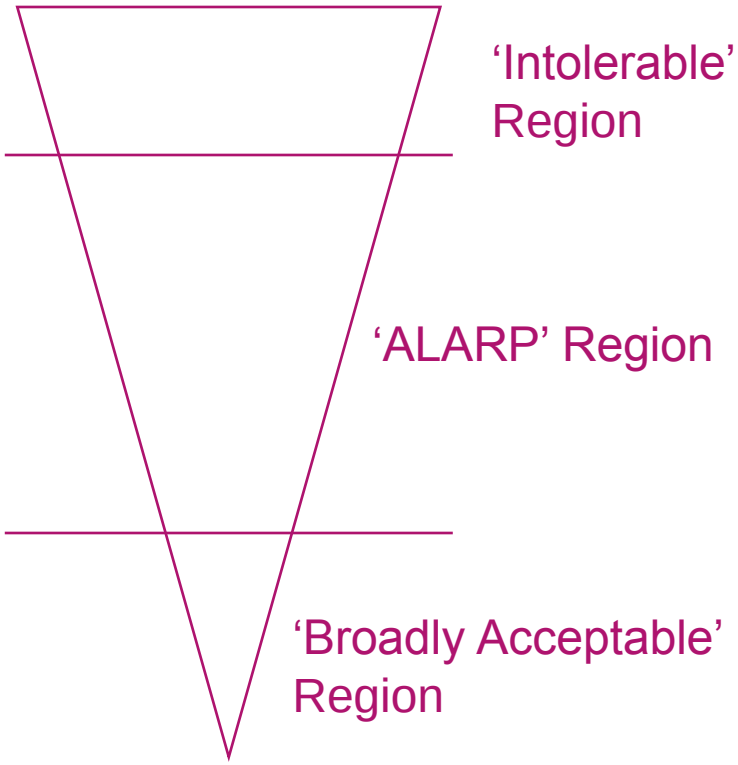
Office for Nuclear Regulation

Systematic Separation of Control and Protection



Office for Nuclear Regulation

ALARP always applies



- When has the risk been reduced to ALARP?
- Important to know what the next step is, then you can argue that it is not practicable.

Office for Nuclear Regulation

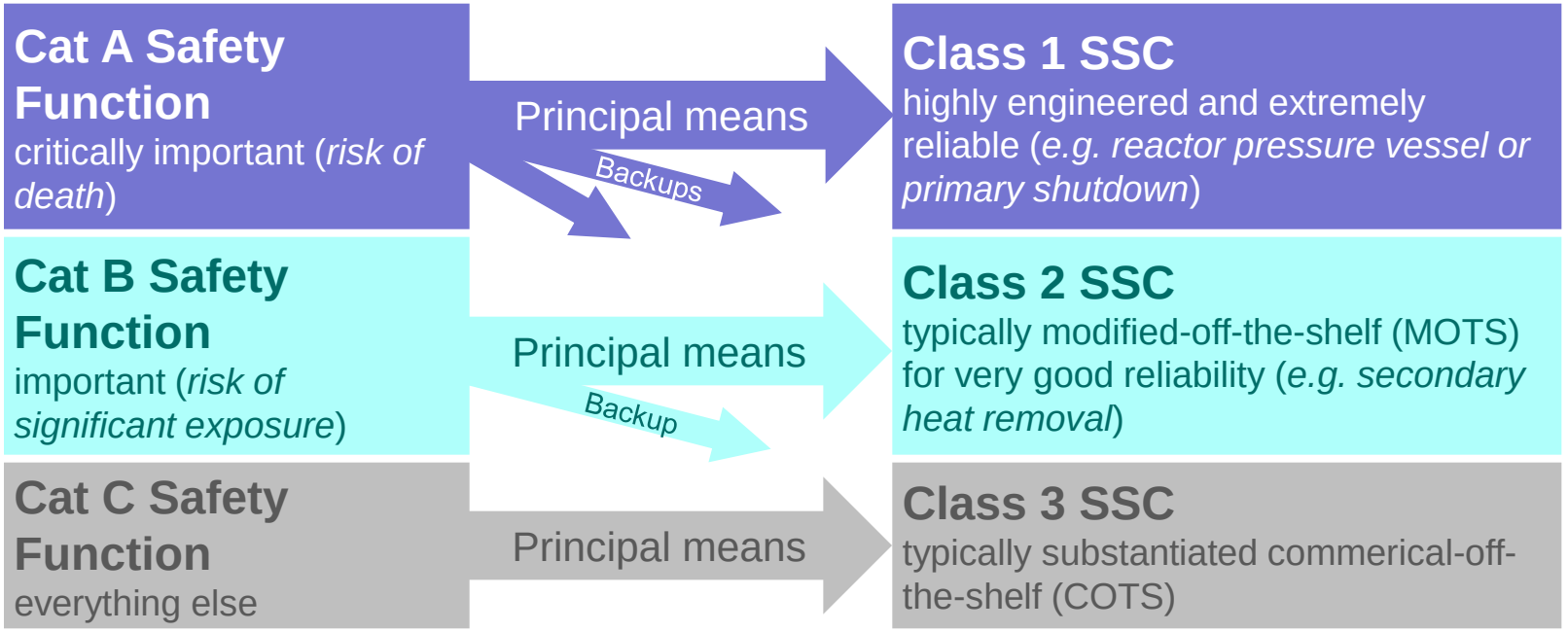
Safety Case Principles

Categorisation of safety functions and Classification of structures, systems and components

Office for Nuclear Regulation

In a nutshell…

- Cat and class arrangements are a systematic “short-cut” to the right quality of an SSC based on its safety significance…



Office for Nuclear Regulation

Key Principles – Defence in Depth

Defence in Depth (SAP EKP.3)

- Provision of multiple independent barriers to fault progression for potentially significant faults…
  - multiple barriers spanning prevention, protection and mitigation
  - independence between barriers
  - focus on early intervention in the fault sequence
  - later barriers should not take credit for earlier ones

- Cat & Class arrangements need to…
  - apply to various different types of nuclear safety barriers
  - support independence between prevention, protection and mitigation
  - support the hierarchy in prevention, protection and mitigation

Office for Nuclear Regulation

Key Principles – Safety Categorisation

Safety Categorisation (SAP ECS.1)

- Safety functions, both during normal operation and in the event of a fault or accident, should be identified and categorised based on their significance
  - safety functions include prevention, protection and mitigation (usually better to identify separate functions in each area – more later)
  - safety functions should be categorised based on their significance (more later on what factors should be included)
  - safety functions themselves are separate to their delivery

- Cat & Class arrangements need to…
  - systematically identify safety functions
  - categorise safety functions according to their importance

Office for Nuclear Regulation

Key Principles – Safety Classification

Safety Classification of SSCs (SAP ECS.2)

- The SSC needed to the deliver the safety functions should be identified and classified based on their significance
  - SSC cover both the normal duty systems and those provided for safety
  - cover all elements needed to fully deliver the safety function
  - SSC should be classified based on their significance (more later on what factors should be included)

- Cat & Class arrangements need to…
  - systematically identify which SSC deliver the safety functions
  - classify the SSC according to their importance

Office for Nuclear Regulation

Key Principles – Codes & Standards

Codes and Standards (SAP ECS.3)

- SSC should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards
  - this should be commensurate with the SSC Class
  - although SSC Class is fundamentally linked to the reliability (pfd) this is not the only aspect – SSC class informs the whole span of activities associated with the plant

- Cat & Class arrangements need to…
  - inform the depth of substantiation associated with SSCs commensurate with their class
  - link to arrangements to ensure that due priority is given to safety

Office for Nuclear Regulation

Identification of safety functions

- A safety function is something that is needed in the interests of nuclear safety e.g. control reactivity (high level) or provide a heat sink for a heat transfer system (more detailed)
- A safety case should identify the safety functions that are needed in the interests of nuclear safety both during normal operation and following a fault or accident
  - Should cover prevention, protection and mitigation (i.e. all levels of defence-in-depth)
  - Should be largely independent from the engineering

Office for Nuclear Regulation

Categorisation of safety functions

- The identified safety functions should be categorised based on their significance to nuclear safety, using a methodical approach
- Safety functions should be categorised based on:
  - consequences of failing to deliver the function
  - likelihood of calling upon the function
  - extent to which the function is required to prevent, protect or mitigate
- ONR SAPs suggest a scheme:
  - Category A – any function that plays a principal role in ensuring nuclear safety.
  - Category B – any function that makes a significant contribution to nuclear safety.
  - Category C – any other safety function contributing to nuclear safety.

Office for Nuclear Regulation

Classification of SSC

- The SSC delivering each safety function should be identified
  - functions are normally delivered by ‘safety measures’ (SSC + people & procedures) but TAG-094 and this presentation focus on just the physical SSC
  - SSC can be at any level of resolution as appropriate – from an entire 4-train post-trip cooling system down to a single bolt
- Importantly (but not exclusively) is that classification informs the reliability
  - for an SSC delivering a normal duty safety function, this means the likelihood in terms of a failure frequency per annum
  - for an SSC called upon to deliver a safety function in response a fault of accident, this means the probability of failure on demand

Office for Nuclear Regulation

SSC Classification – initial class

		Prominence of the SSC in the delivery of the safety function		
		Principal means	Significant means	Other means
Safety function category	Cat A	Class 1	Class 2	Class 3
	Cat B	Class 2	Class 3	
	Cat C	Class 3		

Office for Nuclear Regulation

Classes and reliability

SSC class	Failure frequency per annum	Probability of failure on demand (pfd)
Class 1	10^{-3} to 10^{-5}	10^{-3} to 10^{-5}
Class 2	10^{-2} to 10^{-3}	10^{-2} to 10^{-3}
Class 3	10^{-1} to 10^{-2}	10^{-1} to 10^{-2}

e.g. primary reactor shutdown system, PWR pressure vessel

e.g. backup reactor cooling or secondary shutdown

e.g. hand and foot monitors on leaving a controlled area, emergency lighting, …

Office for Nuclear Regulation

Computer Based Safety Systems

Expectations for justification

Office for Nuclear Regulation

Key SAPs – ESS.27

Computer-based safety systems (ESS.27)

- Where system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design.

- The safety demonstration should adopt a 'multi-legged' approach, comprising
  - 'Production Excellence' – a demonstration of excellence in all aspects of production from initial specification through to the finally commissioned system.
  - 'Independent Confidence Building' – an independent and thorough assessment of the system's fitness for purpose

Office for Nuclear Regulation

Production Excellence

- Thorough application of technical design practice consistent with current accepted standards
- Implementation of a modern standards quality management system
- Application of a comprehensive testing programme that checks every system function, including:
  - Verification of all phases of the system production process
  - Validation of the integrated system against its specification
  - Dynamic testing, to demonstrate that the system is functioning as intended

Office for Nuclear Regulation

Independent Confidence Building

- Complete, and preferably diverse, checking of the finally validated production software by a team that is **independent of the system suppliers**
  - Independent product checking that provides a searching analysis of the final system, including application of static analysis
  - Independent checking of the production process, such as adequacy of the specification, compliance with the design specification, methods and standards
- Independent assessment of the comprehensive testing programme (eg verification, validation, commissioning and dynamic testing – including statistical testing), including traceability of tests back to specification

Office for Nuclear Regulation

Safety Case Structure

Claims, Arguments, Evidence

Office for Nuclear Regulation

Claims, Arguments, Evidence

Claim

What do I need to demonstrate?

Sub-claims

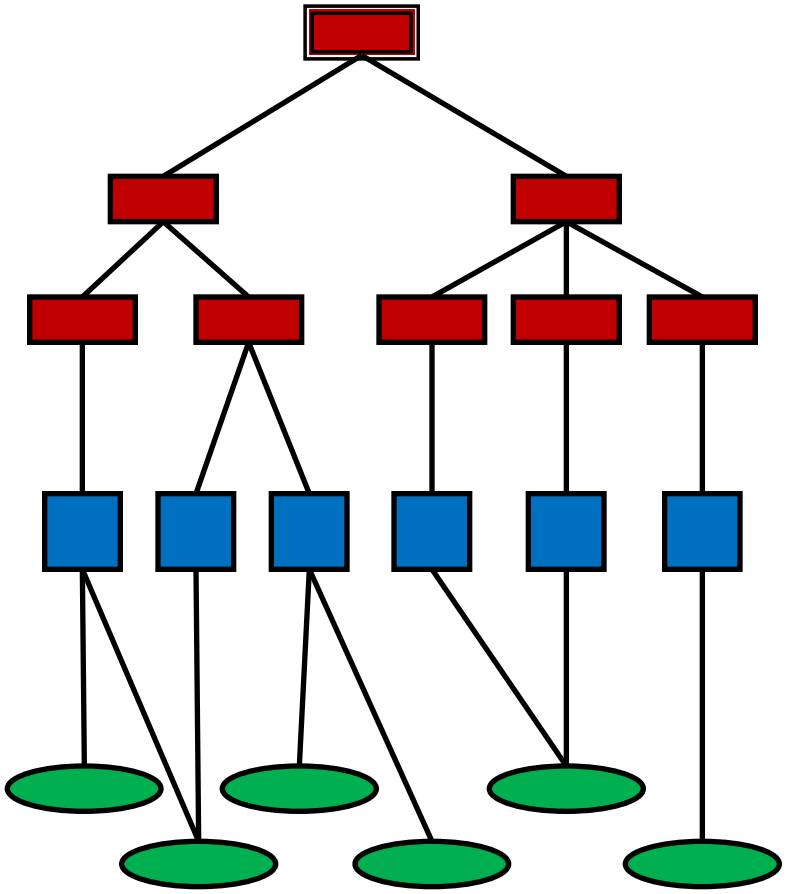
What does my claim depend on?

Argument

Why is the evidence sufficient to demonstrate the sub-claim

Evidence

Where to find the evidence



Office for Nuclear Regulation

ONR's expectations

- ONR safety assessment principle SC.2
  - "The trail from claims through argument to evidence should be clear."
- ONR technical assessment guide 51 on safety cases
  - "The safety case clearly sets out the trail from safety claims through arguments to evidence."
- Chief nuclear inspector before the Parliamentary Select Committee on Energy and Climate Change
  - "examine the claims, examine the arguments… and seek evidence that backed up those claims"

Office for Nuclear Regulation

CAE – a hypothetical example

NOTE: This is a simplified example for illustrative purposes. As such it is not fully representative of the scenario on which it is based, nor has it been optimised to meet specific needs

Office for Nuclear Regulation

The scenario

- Retrieval of intermediate level waste from a legacy silo
- Retrievals carried out with a bespoke crane system, manually operated from above the silo
  - On-board PLC based system to control movement of the crane
- Main hazard to be protected against is the accumulation and sudden release of significant quantities of hydrogen
  - This could result in an ignition event that could result in a breach of waste containment

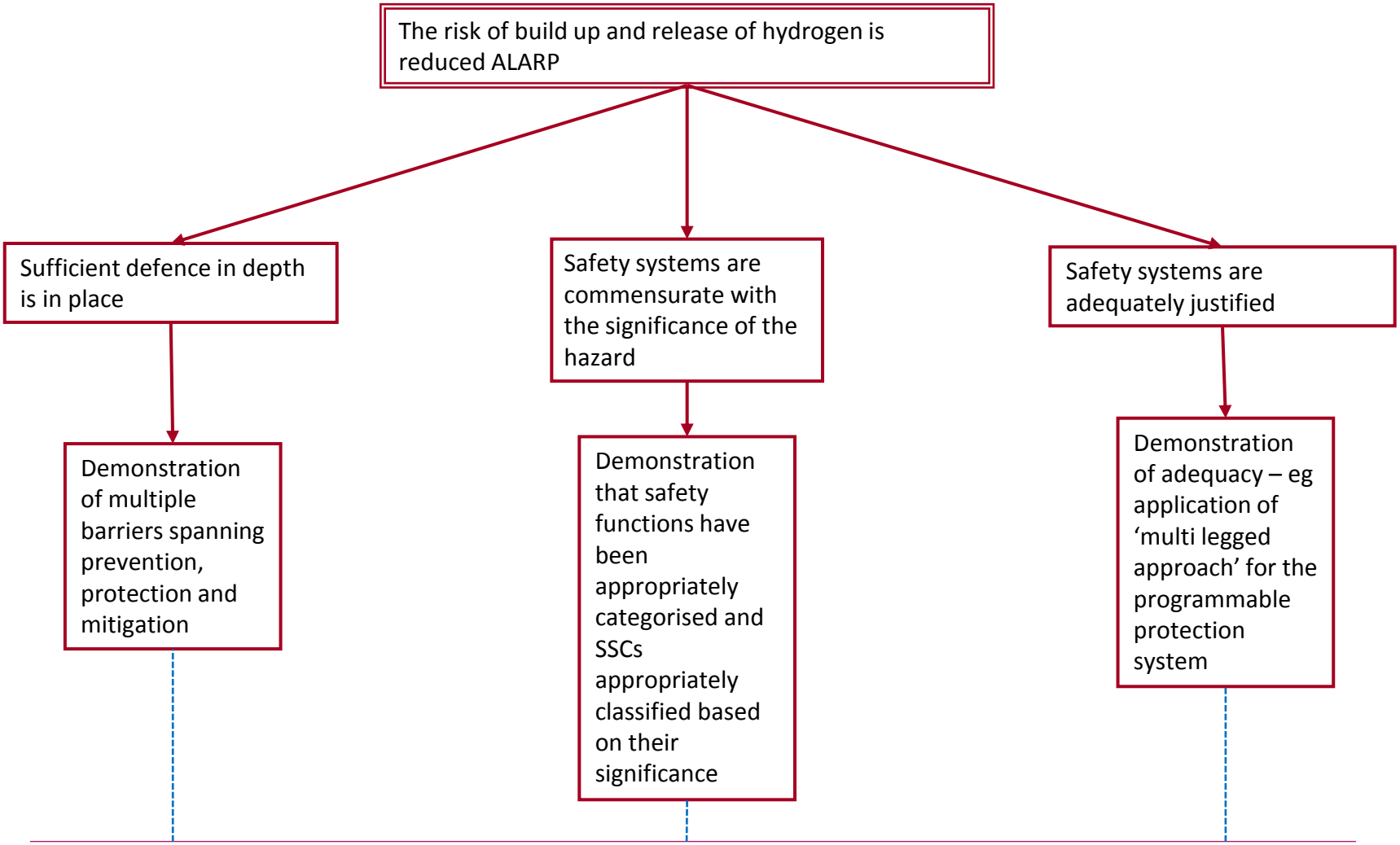
Office for Nuclear Regulation

The scenario (cont)

- A number of measures are in place to protect against the hazard:
  - Passive ventilation of the silo to prevent over-pressurisation
  - Injection of argon into the silo to provide an inert atmosphere during retrievals
  - A C&I system to limit the depth to which the crane grab can be deployed, to prevent digging of craters
    - This is a programmable system comprising COTS devices

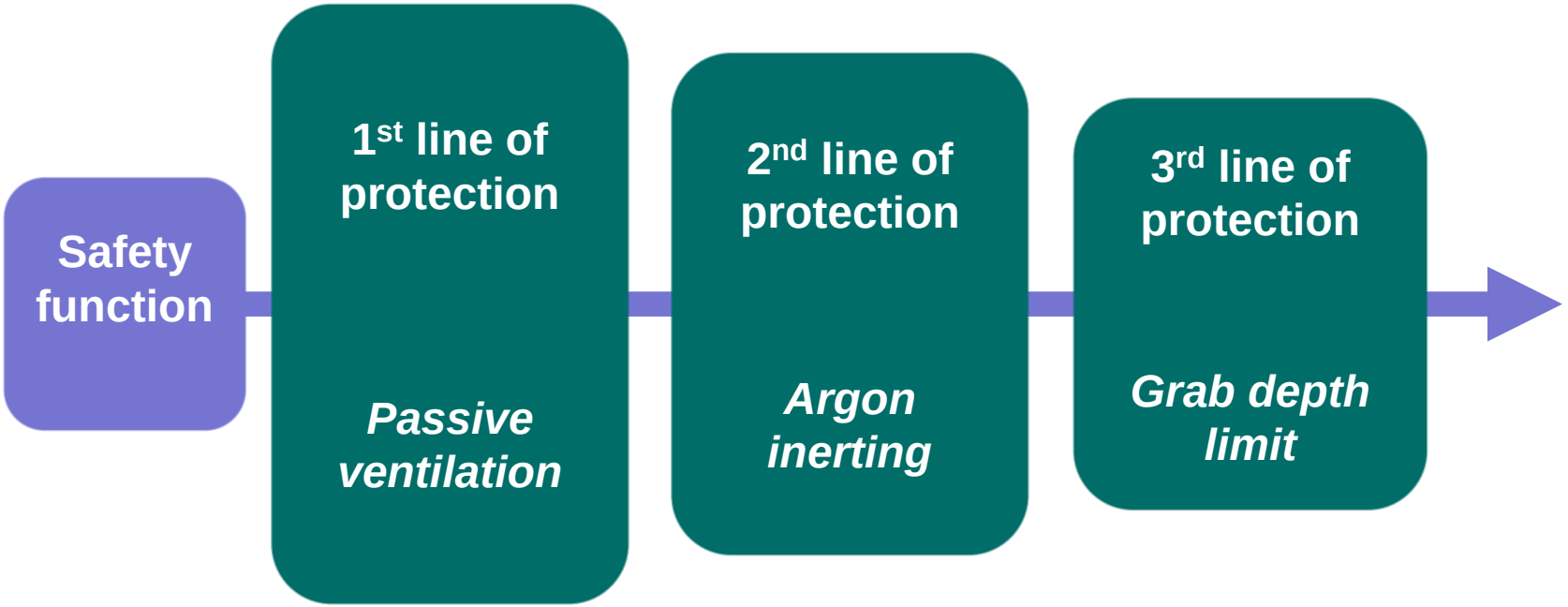
Office for Nuclear Regulation

Hypothetical CAE structure



Office for Nuclear Regulation

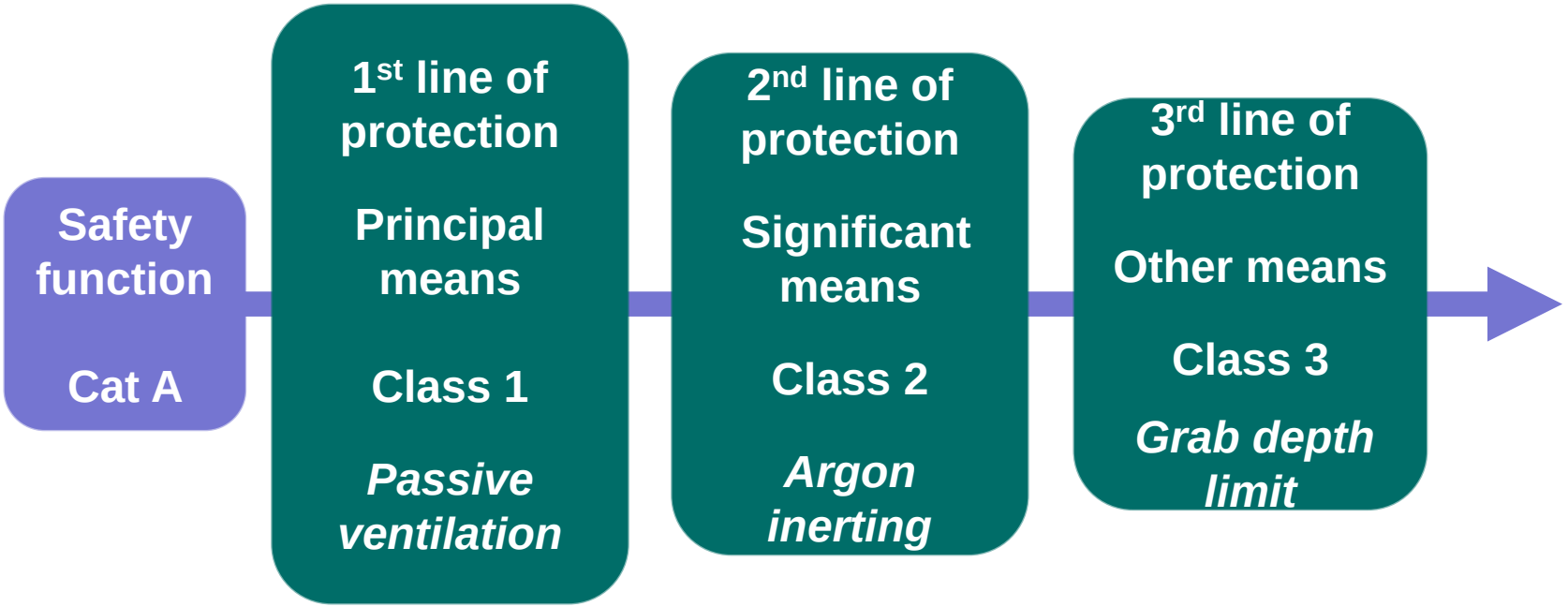
Sufficient defence in depth



- Three lines of protection exist to protect against the fault
- Three lines are independent of one another

Office for Nuclear Regulation

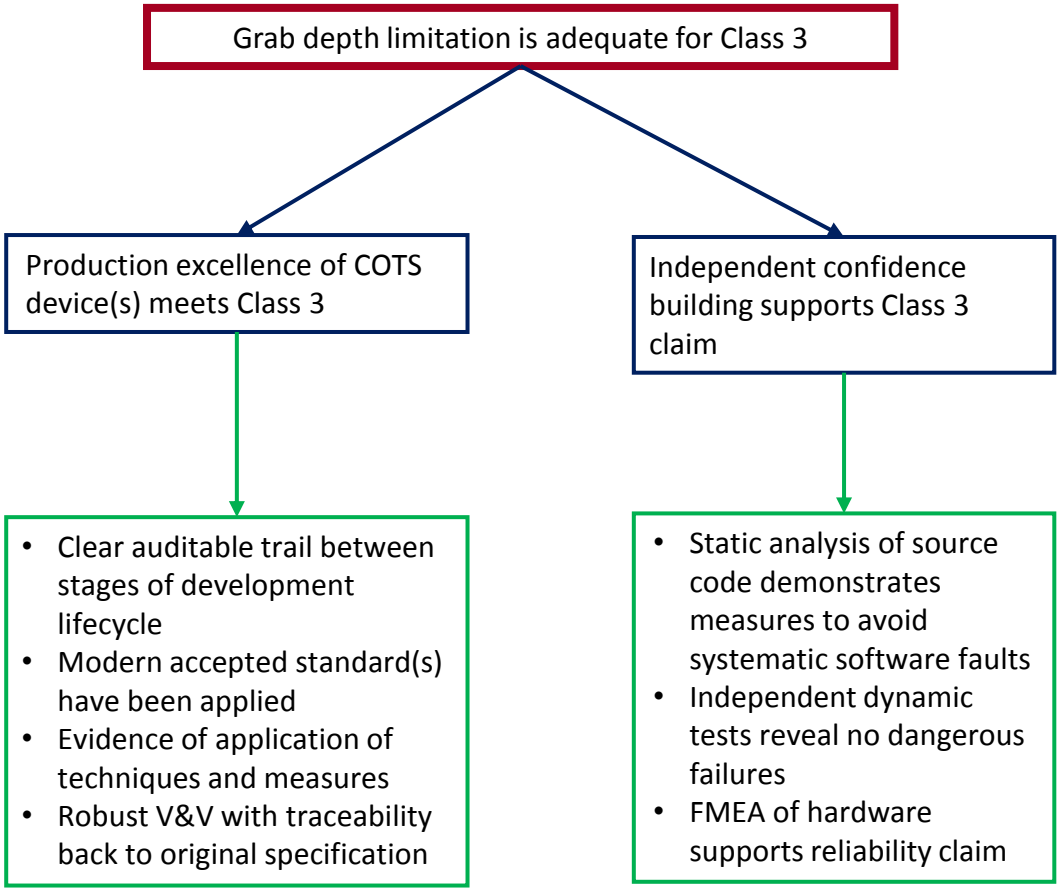
Categorisation and classification



- Function plays a principal role in ensuring nuclear safety – hence Cat A
- Principal means should be Class 1 – passive ventilation – most reliable
- Significant means are therefore Class 2 – argon inerting
- Other supporting means are Class 3 – grab height depth limit (programmable, most complex)

Office for Nuclear Regulation

Demonstration of adequacy



Office for Nuclear Regulation

Safety Case Shortcomings & Traps

Haddon-Cave Report

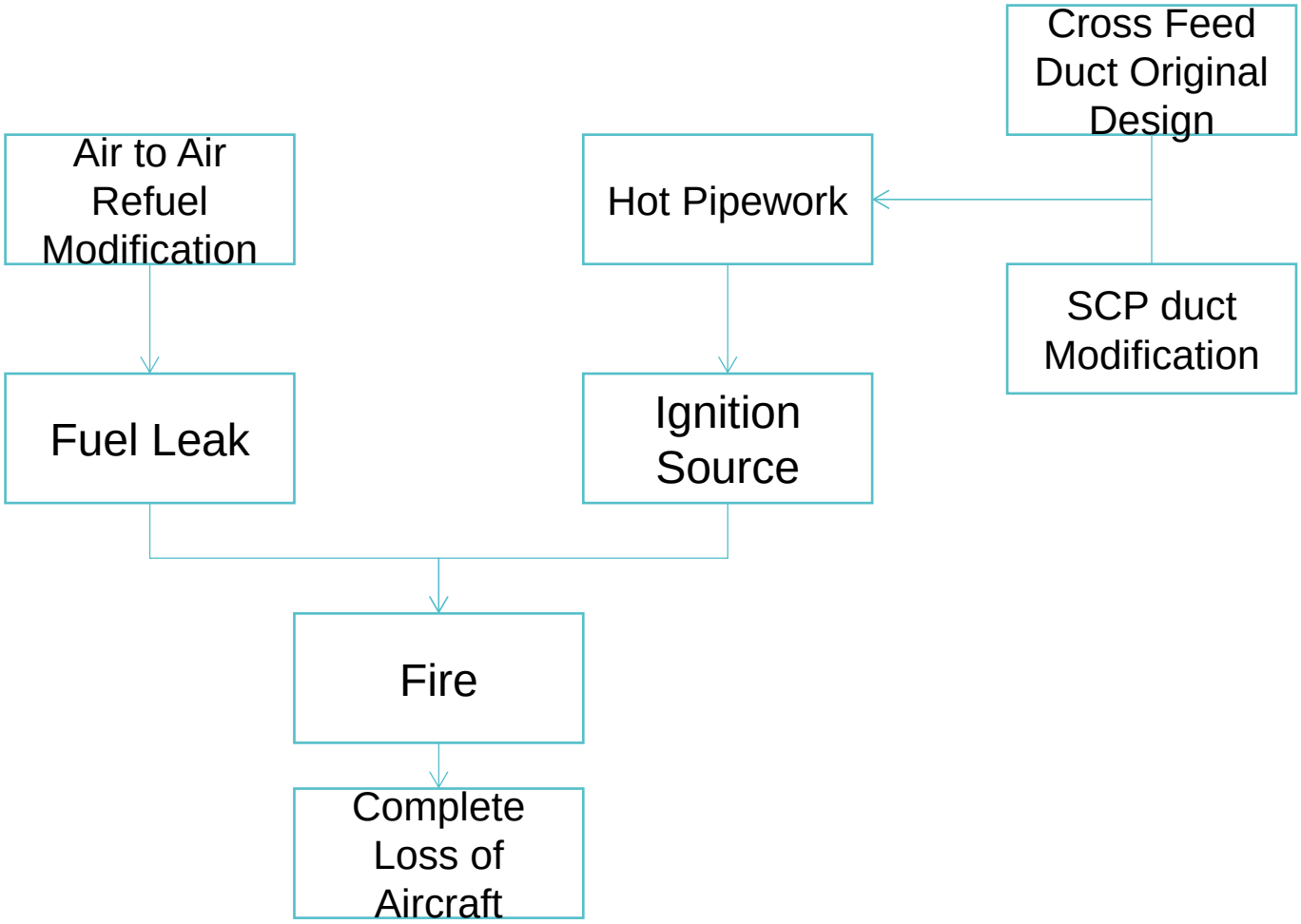
Office for Nuclear Regulation

Nimrod Crash

- RAF Nimrod XV230 crashed over Afghanistan in 2006
- Deaths of 14 servicemen
- Independent review chaired by Charles Haddon-Cave QC

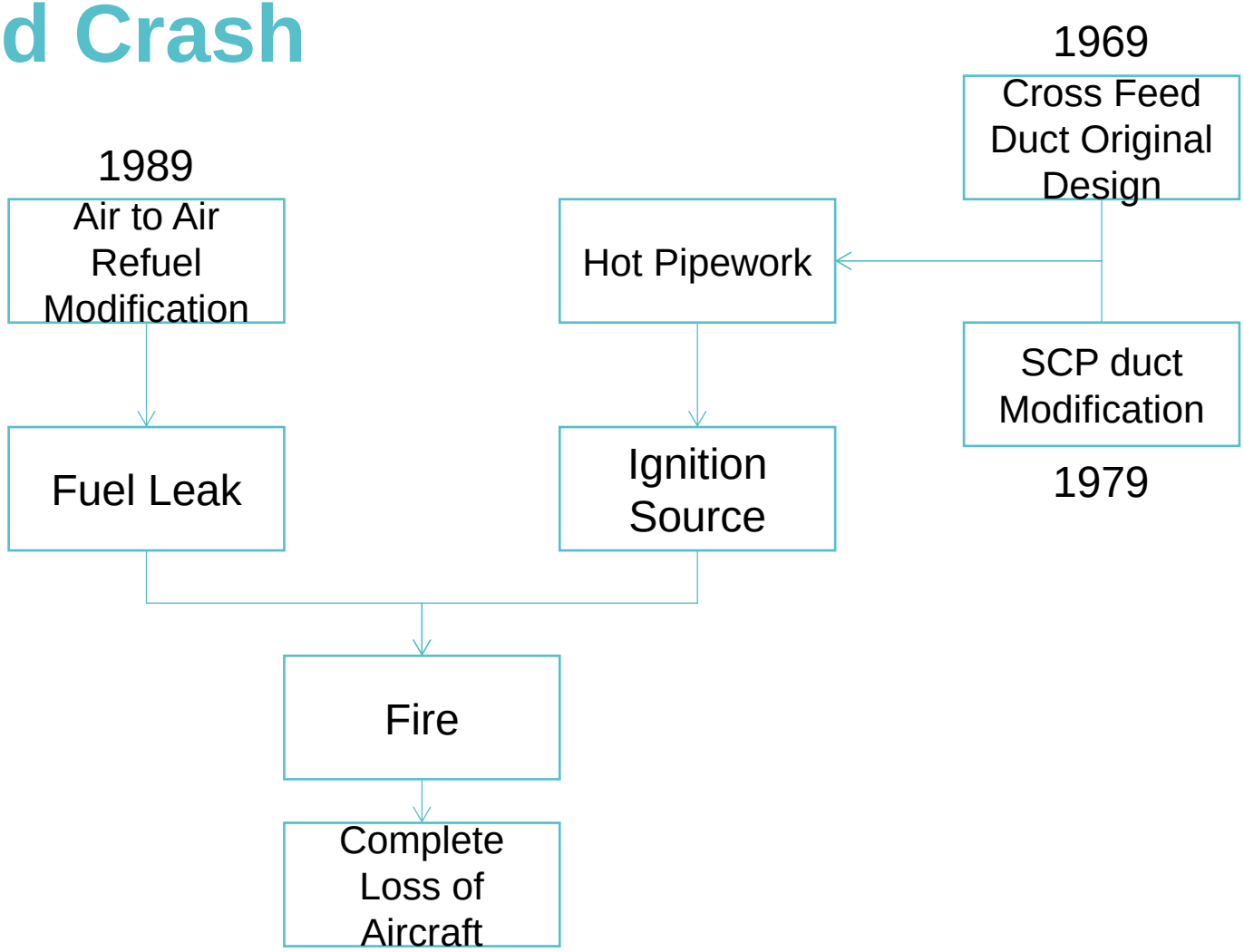
Office for Nuclear Regulation

Nimrod Crash



Office for Nuclear Regulation

Nimrod Crash



Office for Nuclear Regulation

Key Failings Identified

- Failure of the original designers to comply with the safety standards at the time. Proximity of fuel pipes to potential ignition sources and fuel pooling ability
- Failure of Nimrod subsequent safety cases to identify and remedy these hazards
- Poor maintenance policies and procedures
- Competence of staff to conduct safety case
- Cutbacks, lack of resources, and poor leadership

Office for Nuclear Regulation

Shortcomings

1. Bureaucratic Length
2. Obscure Language
3. Wood-for-the-trees
4. Archaeology
5. Routine Outsourcing
6. Lack of operator input
7. Disproportionate
8. Ignoring age issues
9. Compliance only
10. Audits
11. Self-fulfilling prophesies
12. Not living Documents

Office for Nuclear Regulation

Traps

1. The ‘Apologetic Safety Case’
2. The Document-Centric View
3. The Approximation to the Truth
4. Prescriptive Safety Cases
5. Safety Case Shelf-Ware
6. Imbalance of skills

Office for Nuclear Regulation

Conclusions

Office for Nuclear Regulation

Conclusion

- We are supportive of this work, and see how robotic systems could reduce risk to workers arising from nuclear activities
- Any robotic system would have to be demonstrably safe
- There is a framework available to do this.

Office for Nuclear Regulation

Standards and Resources

- IEC 61508 Functional Safety of Electronic Systems (and 61513 for nuclear specific applications)
- ONR Safety Assessment Principles http://www.onr.org.uk/saps/saps2014.pdf
- ONR Technical Assessment Guides http://www.onr.org.uk/operational/tech_asst_guides/index.htm

Office for Nuclear Regulation

Questions?