Welcome

Nuclear Innovation Programme – safety & security

27th March 2019

SYSTEMS AND ENGINEERING TECHNOLOGY

FRAZER-NASH CONSULTANCY

Welcome and overview

James Cornish, Exploitation Manager, Frazer-Nash Consultancy

Objective

The purpose of this event is to disseminate initial results on a select number of projects to initiate a discussion with you.

As representatives from across industry and academia we need your help to ensure that future scope and outputs are tailored to maximise the potential for exploitation.

We welcome and encourage you to contribute feedback, both today and into the future.

© Frazer-Nash Consultancy Ltd. All rights reserved.

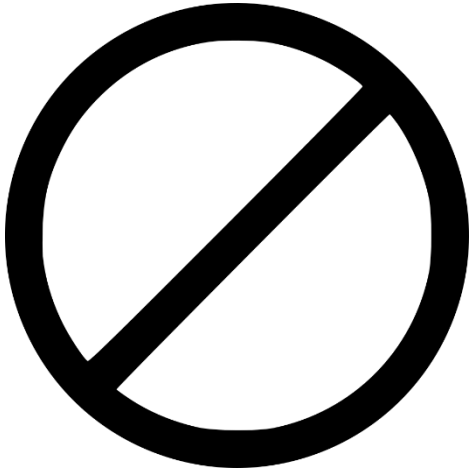
Programme

09:00	Arrival, registration and refreshments
09:40	Welcome and overview James Cornish, Frazer-Nash Consultancy
09:45	The nuclear innovation programme Paul Nevitt, Nuclear Innovation and Research Office
10:00	Introduction to the safety & security project David McNaught, Frazer-Nash Consultancy
10:15	ALARP approach for security & safety Adam Dolman, Rolls-Royce
10:45	Tea & coffee
11:00	Application of model based systems engineering in the UK nuclear sector Steven Fletcher, Frazer-Nash Consultancy
11:30	Advanced modular reactors: key note speech Richard Deakin, Department for Business, Energy & Industrial Strategy

11:45	Nuclear control & instrumentation supply chain roadmaps Ryan Gilhooley, Frazer-Nash Consultancy
12:00	Delivery model for centralised testing facility for C&I systems Simon White, Frazer-Nash Consultancy
12:30	Lunch
13:30	Advanced safety cases Allan Fairbairn, Frazer-Nash Consultancy
14:15	State-of-the-art review of CCF analysis in UK nuclear PSA David Watson, Jacobsen Analytics Ltd
14:45	Common categorisation and system classification methodologies and tools Mandy Roberts, Rolls Royce
15:15	Exploitation: how can we help? James Cornish, Frazer-Nash Consultancy
15:30	Discussion and networking session
16:00	Depart

© Frazer-Nash Consultancy Ltd. All rights reserved.

House Keeping



© Frazer-Nash Consultancy Ltd. All rights reserved.

The Nuclear Innovation Programme

Dr Paul Nevitt , NIRO

NUCLEAR INNOVATION AND RESEARCH OFFICE

The BEIS Nuclear Innovation Programme (NIP)

Dr Paul Nevitt

The future of Nuclear Safety and Security, a dissemination event for the Nuclear Innovation Programme

27th March 2019

"There has been some criticism of the prospective cost of the Hinkley project, but one aspect of the benefit that has not been emphasised often enough is that it restarts programme of civil nuclear power in this country and conversely the loss of much of the supply chain and the domestic skills in the civil nuclear sector was a set back which could have been avoided if we'd thought ahead.

*We need to have a supply chain that is active - engineers who understand the technology, PhDs and university departments specialised in it, welders, civil engineers, concrete pourers, and more… **We've had to restart our civil nuclear industry more or less from scratch, and doing so has bought us an opportunity to meet our climate targets over the longer-term at lowest cost.**"*

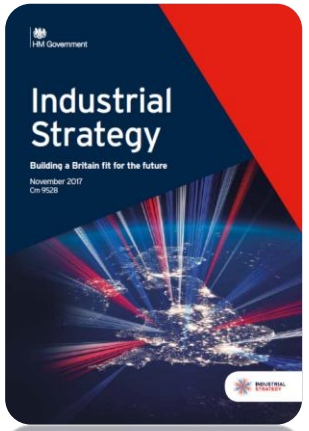
After the trilemma - 4 principles for the power sector
Delivered on: 15 November 2018
https://www.gov.uk/government/speeches/after-the-trilemma-4-principles-for-the-power-sector?utm_source=eea5cc55-3293-4796-987d-3c4cdd7ce724&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate

"Now, everyone in finance knows this - but when you hold an option, the next decision you face is whether to exercise it. ***If nuclear is sufficiently competitive, then it is worth, in my view, turning that option into a commitment.***

We recently announced a nuclear industry sector deal with its emphasis on the need to reduce the costs by 30% through increasing modularisation and advanced manufacturing."

After the trilemma - 4 principles for the power sector
Delivered on: 15 November 2018
https://www.gov.uk/government/speeches/after-the-trilemma-4-principles-for-the-power-sector?utm_source=eea5cc55-3293-4796-987d-3c4cdd7ce724&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate

Industrial Strategy – Productivity and Grand Challenges



Published Nov 2017

Raising productivity

Industrial Strategy is built on 5 foundations

5 foundations of productivity

- **Ideas** – the world's most innovative economy
- **People** – good jobs and greater earning power for all
- **Infrastructure** – a major upgrade to the UK's infrastructure
- **Business environment** – the best place to start and grow a business
- **Places** – prosperous communities across the UK

Grand challenges

We will set Grand Challenges to put the United Kingdom at the forefront of the industries of the future:

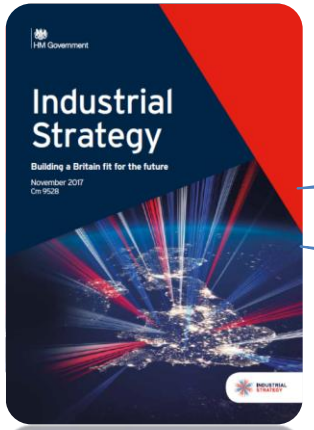
- **AI & Data Economy** – We will put the UK at the forefront of the artificial intelligence and data revolution
- **Clean Growth** – We will maximise the advantages for UK industry from the global shift to clean growth
- **Future of Mobility** – We will become a world leader in the way people, goods and services move
- **Ageing Society** – We will harness the power of innovation to help meet the needs of an ageing society

Sector Deals

Offshore wind

Rail

Life Sciences



Con

"The nuclear sector is integral to increasing productivity and driving growth across the country."

"Nuclear is a vital part of our energy mix, providing low-carbon power now and into the future"

Automotive

Creative industries

Nuclear

Sector Deals

between Government a

t d ry does y then z will result

- 8 Sector Deals to

Artificial Intelligence

Nuclear Sector Deal - targets

30% reduction in the cost of **new build** projects by 2030

40% **women** in nuclear by 2030

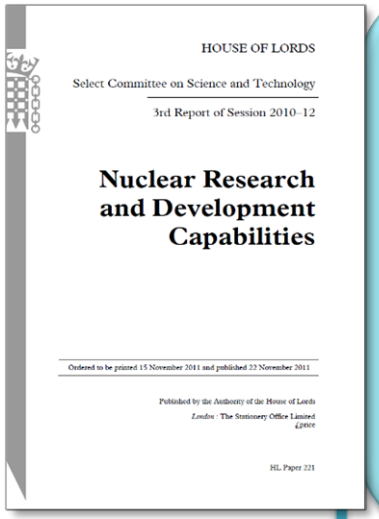
Innovation will be key to achieving each of these targets

Savings of 20% in the cost of **decommissioning** compared with current estimates by 2030

Up to £2bn domestic and international **contract wins** by 2030

NUCLEAR INNOVATION AND RESEARCH OFFICE

BEIS Nuclear Innovation Programme



HOUSE OF LORDS

Select Committee on Science and Technology

3rd Report of Session 2010–12

Nuclear Research and Development Capabilities

Ordered to be printed 15 November 2011 and published 22 November 2011

Published by the Authority of the House of Lords

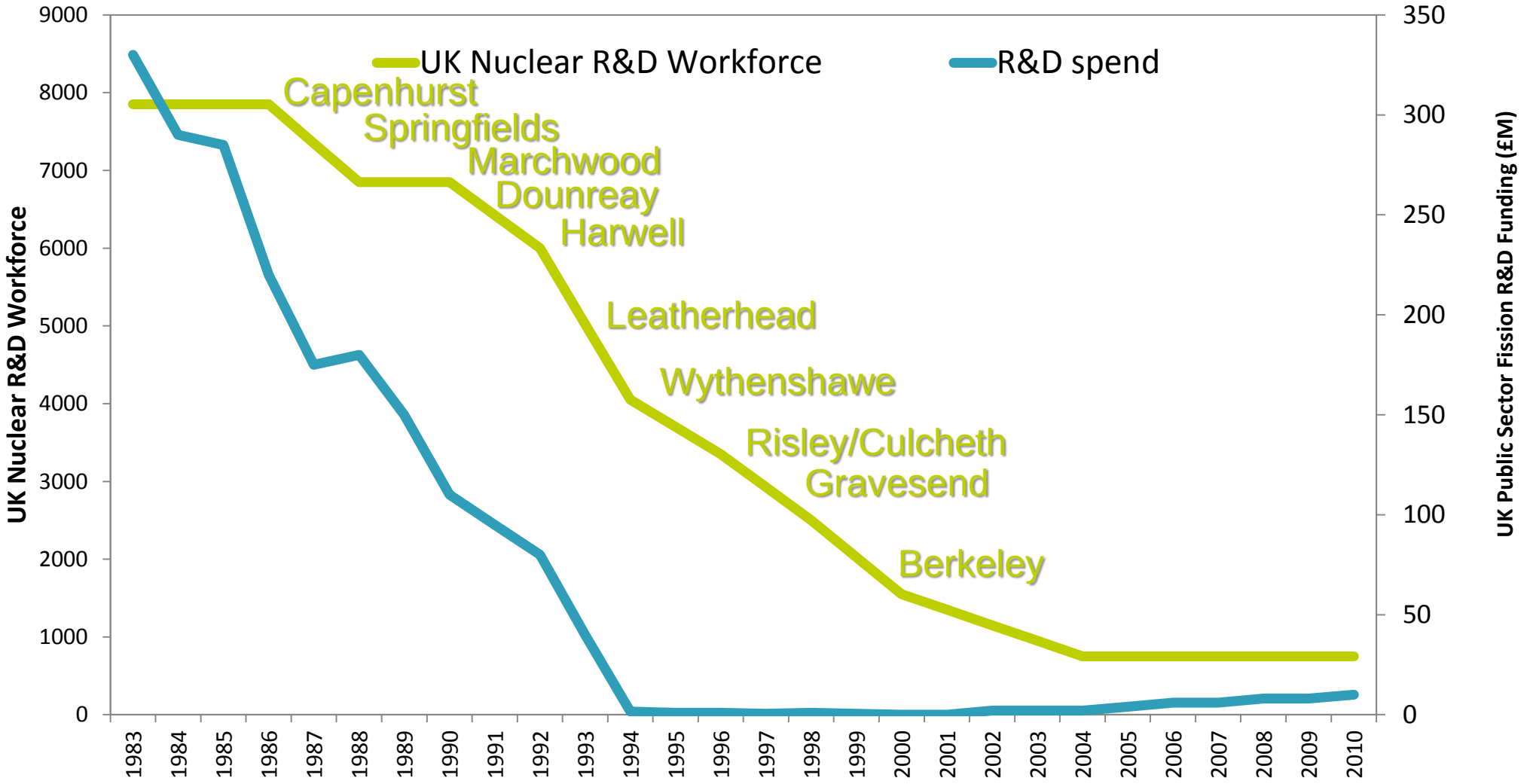
London : The Stationery Office Limited
£price

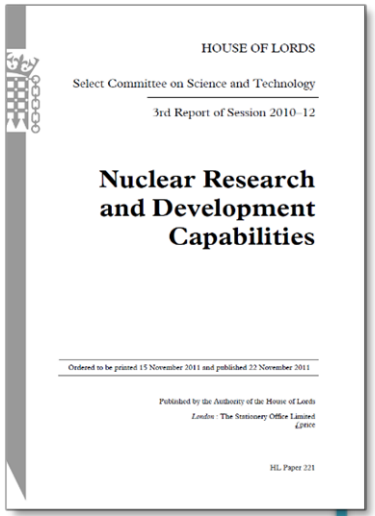
HL Paper 221

*"In a few years time there will be **crucial gaps in capabilities**"*

"The Government's view that the need for R&D capabilities and expertise in the future will be met without Government intervention is troublingly complacent."

2011	2012	2013


UK Nuclear R&D Workforce
R&D spend
Capenhurst
Springfields
Marchwood
Dounreay
Harwell
Leatherhead
Wythenshawe
Risley/Culcheth
Gravesend
Berkeley
UK Nuclear R&D Workforce
UK Public Sector Fission R&D Funding (£M)
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
350
300
250
200
150
100
50
0
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010



HOUSE OF LORDS

Select Committee on Science and Technology

3rd Report of Session 2010–12

Nuclear Research and Development Capabilities

Ordered to be printed 15 November 2011 and published 22 November 2011

Published by the Authority of the House of Lords

London : The Stationery Office Limited

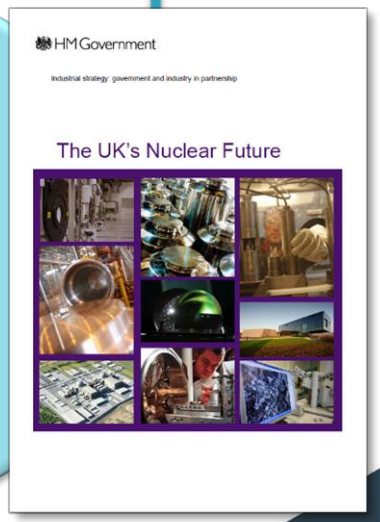
£price

HL Paper 221

2011 **2012** **2013**

*"A **vibrant UK nuclear industry** that is an area of economic and strategic national strength, providing the UK with a safe reliable and affordable supply of low-carbon electricity"*

*"…the Government will **set up a Nuclear Innovation Research Advisory Board** comprising of Government scientific advisors, academic experts, the Research Councils, TSB, NDA, and business leaders."*



nirab NUCLEAR INNOVATION AND RESEARCH ADVISORY BOARD

2014	2015	2016

Independent advisory board

Members appointed by ministerial invitation, drawn from academia, industry, research organisations and funding bodies.

Established by Government in January 2014 to:

Advise Ministers, Government Departments and Agencies on **priorities for UK nuclear R&D and innovation**

To support the **development of new R&D and innovation programmes** to underpin energy and industrial policy

To foster greater **cooperation and coordination** across the UK research and innovation landscape

To oversee the development of a **coordinated international engagement strategy**

Supported by NIRO (Nuclear Innovation and Research Office)

Context for NIRAB advice – long term aims

"… respected partner contributing to appropriate international research programmes…"

"…top table nuclear nation…"

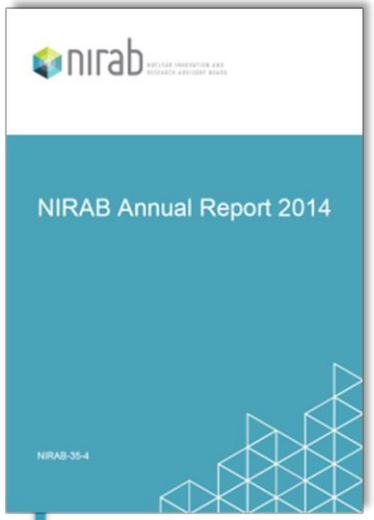
"… partner of choice in commercialising Gen III+, IV and SMR technologies…"

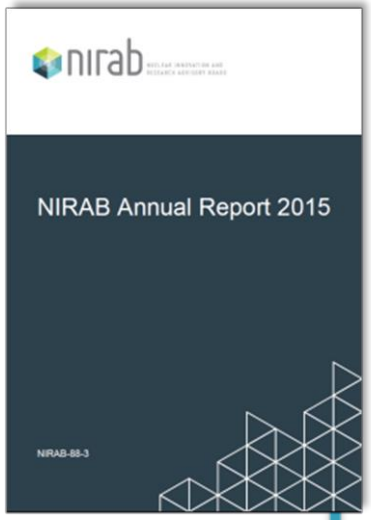
Context for NIRAB advice – Government policy drivers

Why is Government funding needed?

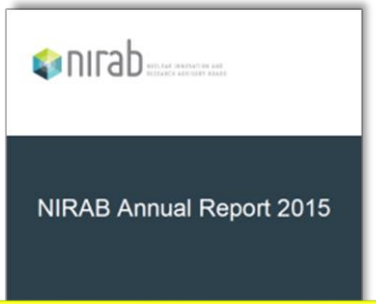
nirab

NUCLEAR INNOVATION AND RESEARCH ADVISORY BOARD





2014 **2015** **2016**



nirab

2014

Secretary of State for Business, Energy and Industrial Strategy
The Rt Hon Greg Clark MP

Department for Business, Energy & Industrial Strategy

15th September 2016

"Having thoroughly reviewed the proposal for Hinkley Point C, we will introduce a series of measures to enhance security and will ensure Hinkley cannot change hands without the Government's agreement. Consequently, we have decided to proceed with ***the first new nuclear power station for a generation****."*

"Britain needs to upgrade its supplies of energy, and we have always been clear that ***nuclear is an important part of ensuring our future low-carbon energy security****."*

Nuclear Innovation, 2016 - 2018

Department for Business, Energy & Industrial Strategy

3rd November 2016

*"****£20 million*** *will be provided to support* ***innovation in the civil nuclear sector across 5 major areas*** *from 2016-18,* ***building on the recommendations set out by the Nuclear Innovation Research Advisory Board NIRAB"***

*"****£60 million*** *to extend the capabili*
National Nuclear Users Facility *"*

nuclear technologies. This will include a competition to identify the best value small modular reactor design for the UK"

lear

of the
n,
which will generate a list of SMR developers that could deliver on the government's objectives"

NIRAB recommendations for research in 5 areas

Future Fuels	Making more efficient, safer fuels of the future
21st Century Nuclear Manufacture	Advanced materials and manufacturing - modular build in nuclear factories of the future.
Reactor design	Delivering the people, processes and tools to make the UK the partner of choice as the world designs SMRs and 4th generation nuclear power plants.
Recycling Fuel for Future Reactors	Cost effective technologies to deliver a

The BEIS Nuclear Innovation Programme

Advanced Nuclear Fuels	**Advanced Nuclear Manufacturing and Materials**
Digital Nuclear Reactor Design	**Nuclear Fuel Recycle and Waste Management**
Nuclear Safety and Security Engineering	**Nuclear Facilities and Strategic Toolkit**
AMR Feasibility and Development Study	

- An integrated £180m 5 year programme from 2017-21
- First phases commenced in early 2017 - £20m total over 1-2 years

Department for Business, Energy & Industrial Strategy

£505m Energy Innovation Programme

Aim: to accelerate the commercialisation of innovative cheap, clean, and reliable energy technologies by the mid 2020s and 2030s.

£180m Nuclear
Driving down costs and building new UK supply chains and skills

£15m Renewables
Driving down the cost of low carbon electricity at scale

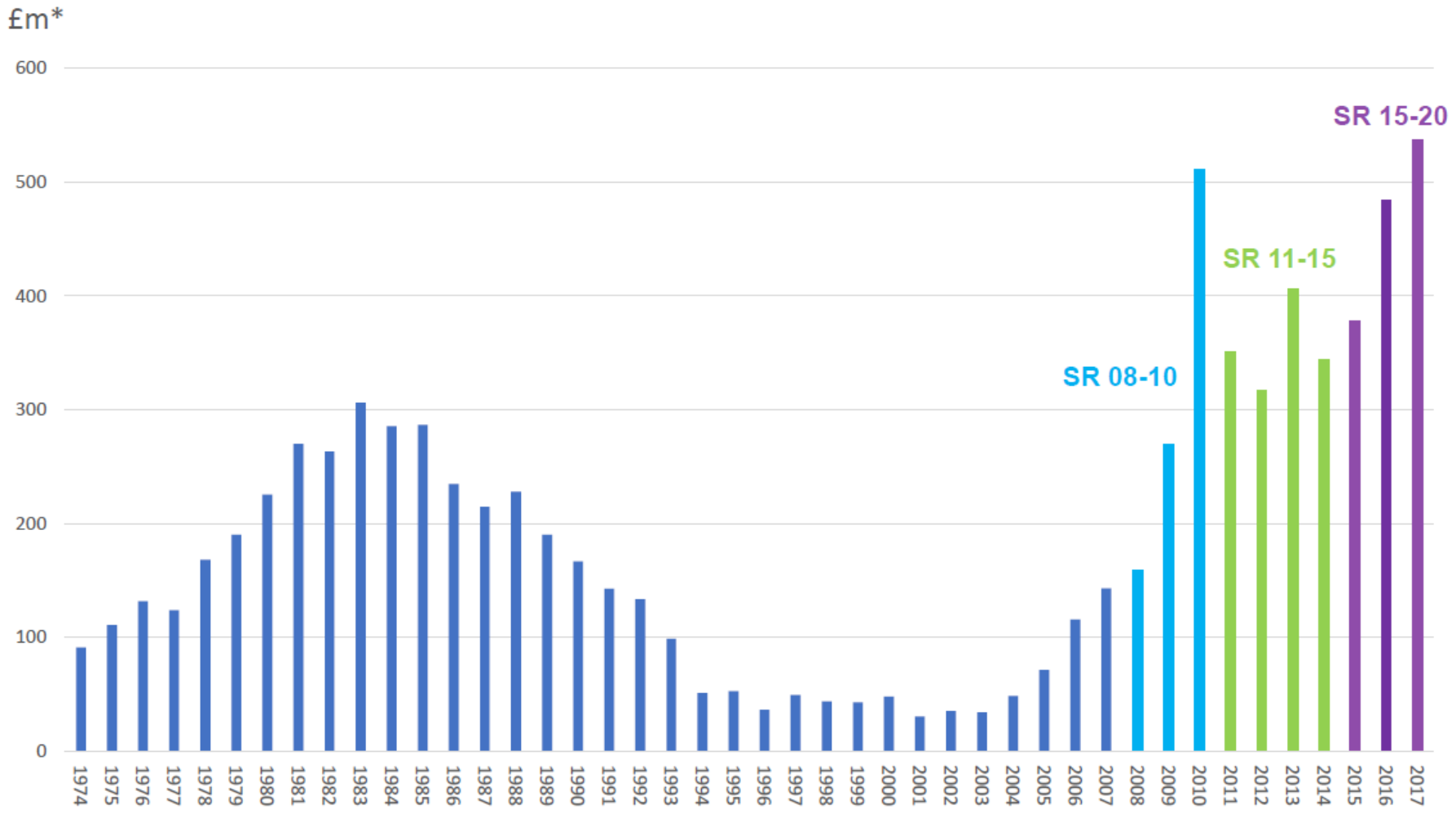
£100m CCS & Industry
Low carbon options for industry, lowering energy costs

£90m Built Environment
More cost effective energy efficiency and low carbon heating

£70m Smart Systems
Scaling up flexibility and looking for new storage options

£50m Cross Cutting Supporting disruptive innovations (particularly for SMEs), including using innovative finance.

UK Government spend on energy RD&D



Source: IEA; *nominal

Energy innovation: UK ecosystem

Energy-related Catapult network:
Large facilities & expertise to support SMEs on energy innovaiton

CATAPULT Energy Systems

CATAPULT High Value Manufacturing

CATAPULT Offshore Renewable Energy

EPSRC
Engineering and Physical Sciences Research Council

Support for blue-skies research, new discoveries and how to improve technologies

£40m+ Clean Growth Fund
Venture Capital fund to provide financing

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY
Delivering growth, prosperity, opportunity

Challenge Fund
Focussed funding to address specific energy challenges

Energy Innovation Programme
£505m portfolio to address policy options and accelerate technologies

What is the Nuclear Innovation Programme trying to achieve?

Support the sector in ensuring nuclear can contribute to **low carbon energy generation** and **economic growth** – Industrial Strategy and The Nuclear Sector Deal

Securing **essential capability** and a future pipeline of expertise

Developing **commercially exploitable** technologies

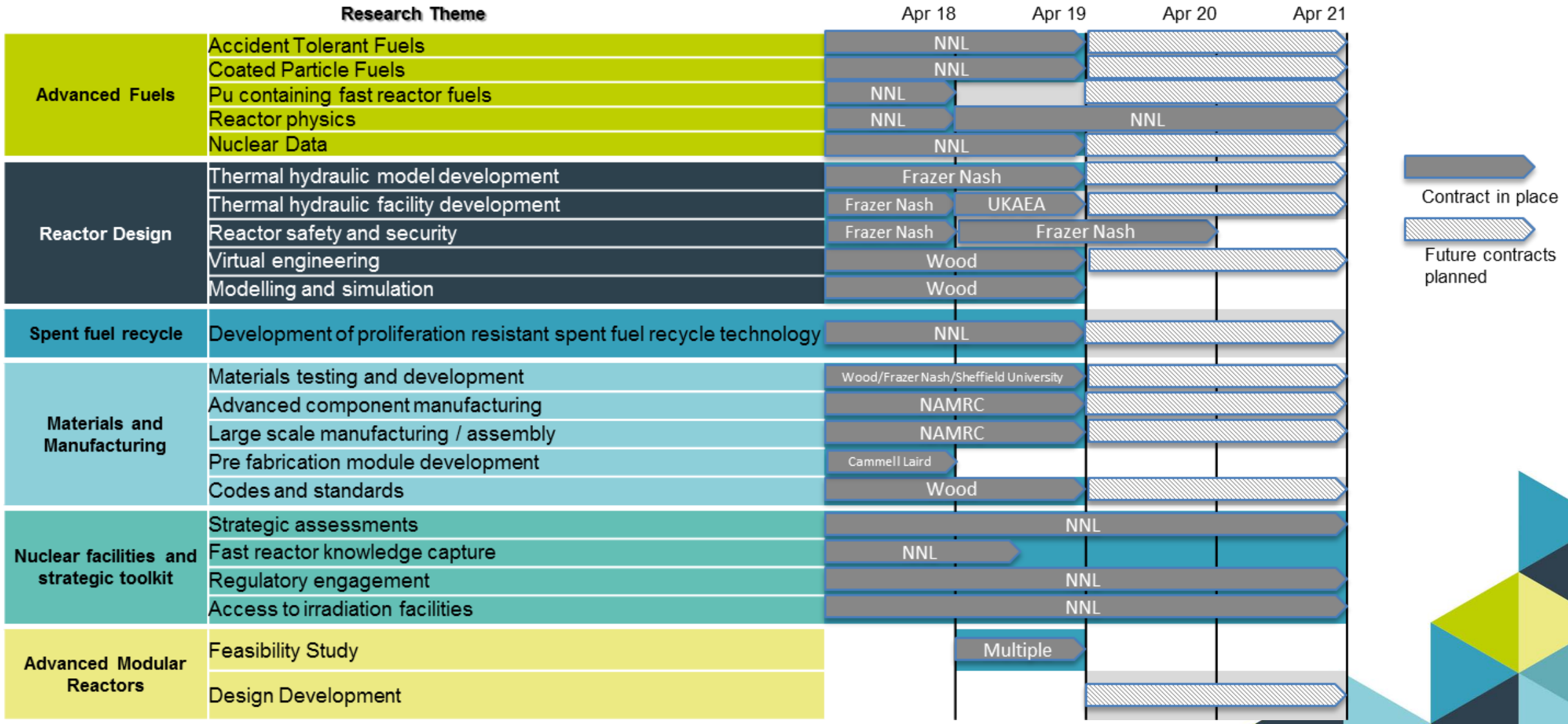
Leveraging private sector investment – research areas align with industry needs

Reducing costs of the nuclear lifecycle

Enable the UK to engage in national and **international collaborations**

BEIS Nuclear Innovation Programme

"BEIS expects to invest around £180 million in nuclear innovation between 2016 and 2021"



PEAK NDT

NATIONAL NUCLEAR LABORATORY

MetLase
A JOINT VENTURE BETWEEN ROLLS-ROYCE AND UNIPART

Advanced Manufacturing Research Centre
BOEING

University of BRISTOL

AFRC
ADVANCED FORMING RESEARCH CENTRE
UNIVERSITY OF STRATHCLYDE

NUCLEAR AMRC

The Welding Institute

FRAZER-NASH CONSULTANCY

UNIVERSITY of York

HITACHI

Imperial College London

CVE CAMBRIDGE VACUUM ENGINEERING

MANCHESTER 1824
The University of Manchester

ATKINS
Member of the SNC-Lavalin Group

wood.

UNIVERSITY OF CAMBRIDGE

UNIVERSITY OF SURREY

Manchester Metropolitan University

SHEFFIELD FORGEMASTERS INTERNATIONAL

IDM
integrated decision management

CAMMELL LAIRD

The University Of Sheffield.

Westinghouse

ADELARD

Lancaster University

UNIVERSITY OF LEICESTER

UNIVERSITY OF LIVERPOOL

Brunel University London

UNIVERSITY OF LEEDS

Science & Technology Facilities Council

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

UK Atomic Energy Authority

ARUP

Rolls-Royce

EDF ENERGY

NPL
National Physical Laboratory

AMR programme

- **Phase 1**: funding (up to £4 million) to undertake a series of feasibility studies for AMR designs.

ARC ADVANCED REACTOR CONCEPTS, LLC
Sodium cooled fast reactor

DBD
High temperature reactor

moltex energy safer, cheaper, nuclear
Molten Salt Reactor

Westinghouse
Lead cooled fast reactor

USNC ULTRA•SAFE•NUCLEAR
High temperature reactor

tokamak energy a faster way to fusion
Fusion Reactor

LeadCold
Lead cooled fast reactor

U BATTERY Local Modular Energy
High temperature reactor

- **Phase 2**: a share of up to £40 million could be available for selected projects from phase 1 to undertake development activities. Up to a further £5 million may also be made available to regulators to support this

Long term vision for Reactor Design

2020

UK **engaged in collaborative design projects** for new reactors (Generation IV and SMR), **building on its existing** and **growing design expertise**.

2030

Maturing R&D results in deployment of new plant with **significant UK design content and manufactured parts**.

2050

UK industry a significant partner in the global deployment of Gen III+, Gen IV and SMR technologies.

Long term vision for Reactor Design

2020

UK **engaged in collaborative design projects** for new reactors (Generation IV and SMR), **building on its existing** and **growing design expertise**.

2030

Maturing R&D results in deployment of new plant with **significant UK design content and manufactured parts**.

The programme is expected to deliver the following benefits:

- **enhanced designs**, **increased productivity** and a **step change** in the way that nuclear design, development and construction programmes are delivered
- **increased and widespread uptake** of modern digital engineering practices within the UK nuclear industry
- improved understanding and **safety of through life performance** of reactor components
- a greater **predictive modelling capability** and understanding of **passive safety arguments**

2050

UK industry a significant partner in the global deployment of Gen III+, Gen IV and SMR technologies.

Current challenges

- Advanced reactor design programmes are multinational and led by Governments or Government funded agencies
  - UK now re-joining as an active member of the Generation IV International Forum
- UK companies are not involved in current or future civil reactor design to any significant extent.
  - UK's historic expertise in advanced reactor design in danger of being lost
- Nuclear sector lagging behind other sectors in some key areas e.g.:
  - Best practice digital engineering and construction technologies currently not widely adopted in the nuclear sector.
  - Need to develop a framework for regulation of digital C&I systems

What can advanced reactor design R&D deliver?

- Cost reduction:
  - Embed state of the art digital engineering and design technology in the UK supply chain
- Economic growth:
  - Create jobs through engagement in international collaboration in advanced reactor projects including SMRs, securing high value design content
- Security of supply:
  - Knowledge base and high level skills supply pipeline that will enable the UK to operate and regulate future reactors
  - Generate information on advanced reactor options to inform future policy
- Improved Safety:
  - UK influence on future reactors, ensures that safety, security and decommissioning are key considerations at early design stage

Nuclear Innovation Programme future calls

- Launch the remainder share of the programme (>£100m) around the beginning of 2019, with work commencing in the next financial year.
- Five main areas of calls:
  - **Materials & Manufacture** (Linked to NSD)
  - **Reactor Design** (Virtual Engineering & Thermal Hydraulics models)
  - **Advanced Fuels** (ATF, CPF, Pu,etc)
  - **Recycle and Reprocess (**Aqueous & Pyro, linked to fuels)
  - **Thermal Hydraulics Facility –** UKAEA undertaking design scope. Managed procurements for facility commence next year.

For further information:

https://www.gov.uk/guidance/funding-for-nuclear-innovation

Innovation in the NSD

Nuclear Innovation Programme

- AMR feasibility and development study
- Thermal Hydraulics Facility

Ideas

To be the world's most innovative economy.

Government action to support nuclear

Developing and deploying advanced nuclear technologies

- We will provide up to £56m for R&D for advanced modular reactors
- Setting out a new framework to support the development and deployment of small modular reactors (SMRs) and the innovative technologies that support them

Nuclear Research & Development

- We are providing £86m for a National Fusion Technology Platform at Culham in Oxfordshire
- We will work in partnership with the Welsh Government to develop a £40m thermal hydraulics facility in the north of Wales as part of the Nuclear Innovation Programme developing and deploying advanced nuclear technologies

Sector action to support nuclear

Developing and deploying advanced nuclear technologies

- Bring forward technically and commercially viable propositions that would lead to deployment of new reactors that would be investable and cost competitive in the energy system

Innovation in the NSD

Business Environment

To be the best place to start and grow a business.

Government action to support nuclear

Advanced manufacturing and construction programme

- We will provide up to £20m to demonstrate how advanced manufacturing and construction can increase UK competitiveness and reduce costs in a range of products and services across the sector, such as:
  - digital engineering execution and assurance
  - modular and advanced construction

Winning new business

- We will provide up to £10m for a new national supply chain and productivity improvement programme, including for regional applications of the programme

Sector action to support nuclear

Advanced manufacturing and construction programme

- Make a £12m initial commitment to demonstrate and embed new advanced capabilities in the UK supply chain, leading to increased contract wins and scope in export markets
- Leverage further funding (e.g. from local and International sources) to support the creation or extension of current research infrastructure to demonstrate new construction, qualification, control & instrumentation and modular build techniques
- The industry will continue to develop ideas for research & commercialisation of innovation proposals, including through bids to the Industrial Strategy Challenge Fund

Winning new business

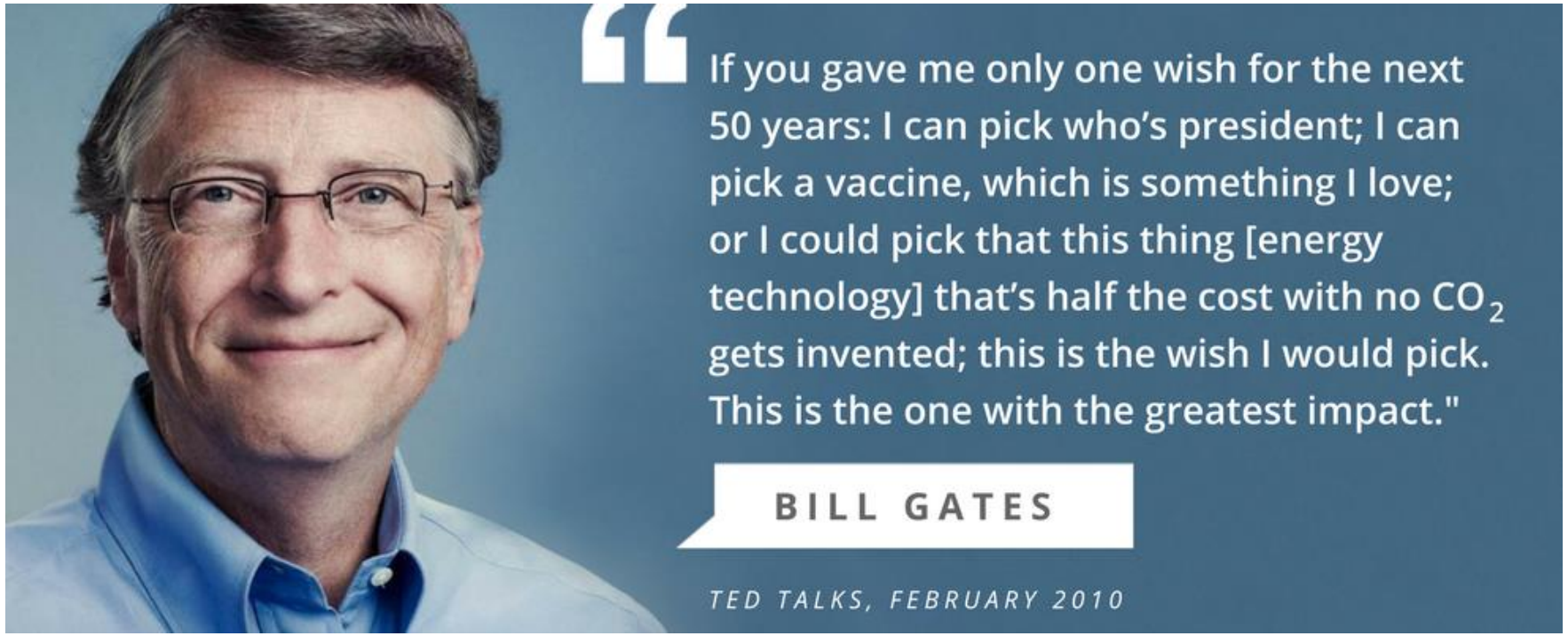
- Provide £20m (£10m funding and £10m contribution-in-kind) for a national supply chain and productivity improvement programme
- Deliver a programme that:
  - increases market competition
  - identifies growth opportunities
  - strengthens UK competitiveness (e.g. by embedding advanced manufacturing techniques)

Nuclear Innovation Programme

- Advanced materials and manufacturing

Industrial Strategy Challenge Fund

- Nuclear proposal related to SMRs under consideration



"*Nuclear is ideal for dealing with climate change, because it is the only carbon-free, scalable energy source that's available 24 hours a day*."
Bill Gates, December 2018
https://www.gatesnotes.com/About-Bill-Gates/Year-in-Review-2018

Introduction to the safety & security project

David McNaught, Project Manager, Frazer-Nash Consultancy

Nuclear Innovation Programme – Safety and Security Aims

"The purpose of the programme is to undertake R&D activities whose outputs can be exploited by the UK nuclear industry to enhance both safety and security performance, while reducing new reactor development and operational costs."

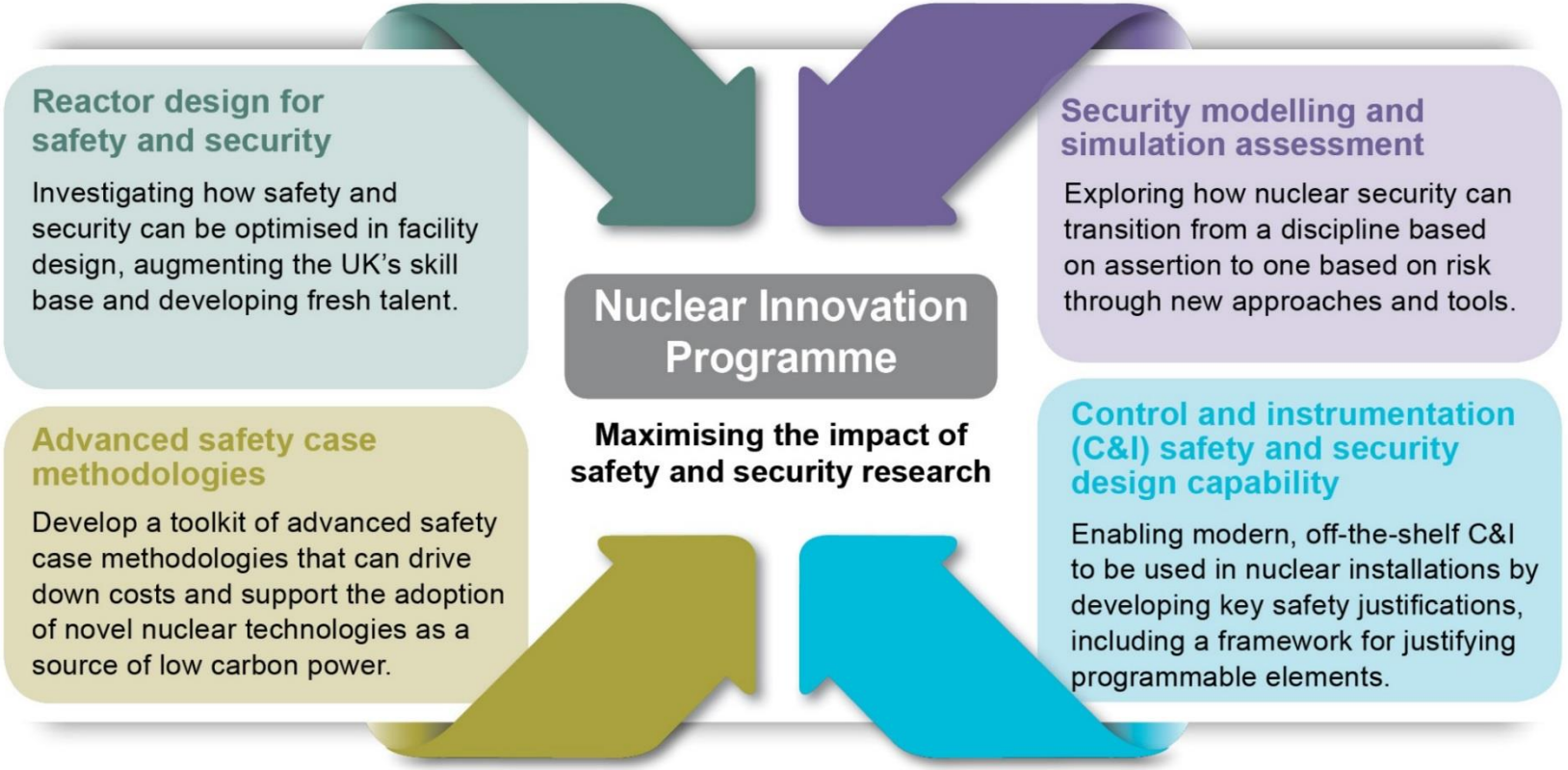
20 sector defining Research and Development (R&D) projects delivered before March 2020 which will:

- Enhance technical **skills** allowing the UK to remain an intelligent customer of foreign technology.
- Result in novel **intellectual property** that can be exploited by the wider nuclear industry;
- Drive a **competitive edge for the UK** through efficiencies in the design and operation of new and existing nuclear reactors through advances in the optimisation of safety, security and safeguards;
- Produce **long-term exploitation** plans, maximising opportunities for UK business to support and commercialise future nuclear technologies.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Nuclear Innovation Programme – Safety and Security Roles and Responsibilities

- The “Advanced Safety Case Methodologies” workstream constitutes 4 projects.
- The “Security Modelling and Simulation Assessment Methodologies” workstream constitutes 3 projects.
- The “Reactor Design for Safety, Security and Safeguards” workstream constitutes 6 projects.
- The “Control and Instrumentation Safety and Security Design Capability” workstream constitutes 7 projects.



© Frazer-Nash Consultancy Ltd. All rights reserved.

Project Representation

Security modelling and simulation assessment

C&I safety and security design capability

- Supply chain roadmaps
- Delivery Model for centralised testing facilities

Reactor design for safety and security

- ALARP for Security
- Application of MBSE
- Common categorisation methods and tools

Advanced safety case methodologies

- Advanced safety cases
- CCF analysis in UK PSA

© Frazer-Nash Consultancy Ltd. All rights reserved.

Project Partners

Workstream 2 - Advanced Safety Case Methodologies	Workstream 3 - Security Modelling and Simulation	Workstream 4 - Design for Safety, Security and Safeguards	Workstream 5 - C&I Safety and Security Design Capability
Jacobsen analytics ENGINEERING RISK SOLUTIONS Lancaster University	Rolls Royce National Nuclear Laboratory	Rolls Royce National Nuclear Laboratory Lancaster University EDF ENERGY context	University of Bristol Rolls Royce Lancaster University

© Frazer-Nash Consultancy Ltd. All rights reserved.

A Common ALARP Approach Between Safety and Security

Adam Dolman, Topic Lead, Rolls Royce (Civil Nuclear UK)

A Common ALARP Approach Between Safety and Security

Reactor Design: Safety & Security Research & Development Dissemination Workshop

Adam Dolman, Security Consultant, Rolls Royce (Civil Nuclear UK)

27 March 2019

This information is provided by Rolls-Royce in good faith based upon the latest information available to it; no warranty or representation is given; no contractual or other binding commitment is implied.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Contents

1. Impact of ALARP for Security
2. Project Overview
3. Key Stakeholders
4. Literature Review
5. Measuring the Effectiveness of the system
6. Outline Methodology
7. Utilising the same tools as safety
8. Integrated approach
9. Challenges and Opportunities

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Utilisation of Strategies to Support Cost Saving

Department for Business, Energy & Industrial Strategy

New nuclear power in UK would be the world's most costly, says report

UK eyes rethink after high cost of nuclear plant

How to stop nuclear costing the earth

High costs and renewables challenge the case for nuclear power

Economic risks of atomic plants threaten their place in future energy mix

Business

Cost of Hinkley Point nuclear plant climbs another £1.5bn to over £20bn, as project faces further delay

There is a genuine need to look at all areas of a plant to reduce the through life cost. Security is an area that should not be overlooked.

© 2019 Rolls-Royce
Private – Rolls-Royce Proprietary Information
No Export License Required – Not Listed

Anticipated benefits

Impact of ALARP for Security

- World-Leading British technology
- Multiple applications -> Value-for-money:
  - Nuclear industry
    - Offers a means of standardising an approach whilst still allowing flexibility in design.
  - Non-nuclear applications
    - can be used in other areas of critical national infrastructure.
  - Exportable process
    - Potential for use globally by regulators seeking to adopt the same of approach as the SyAPs.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Research to determine what was possible

Objective of Project

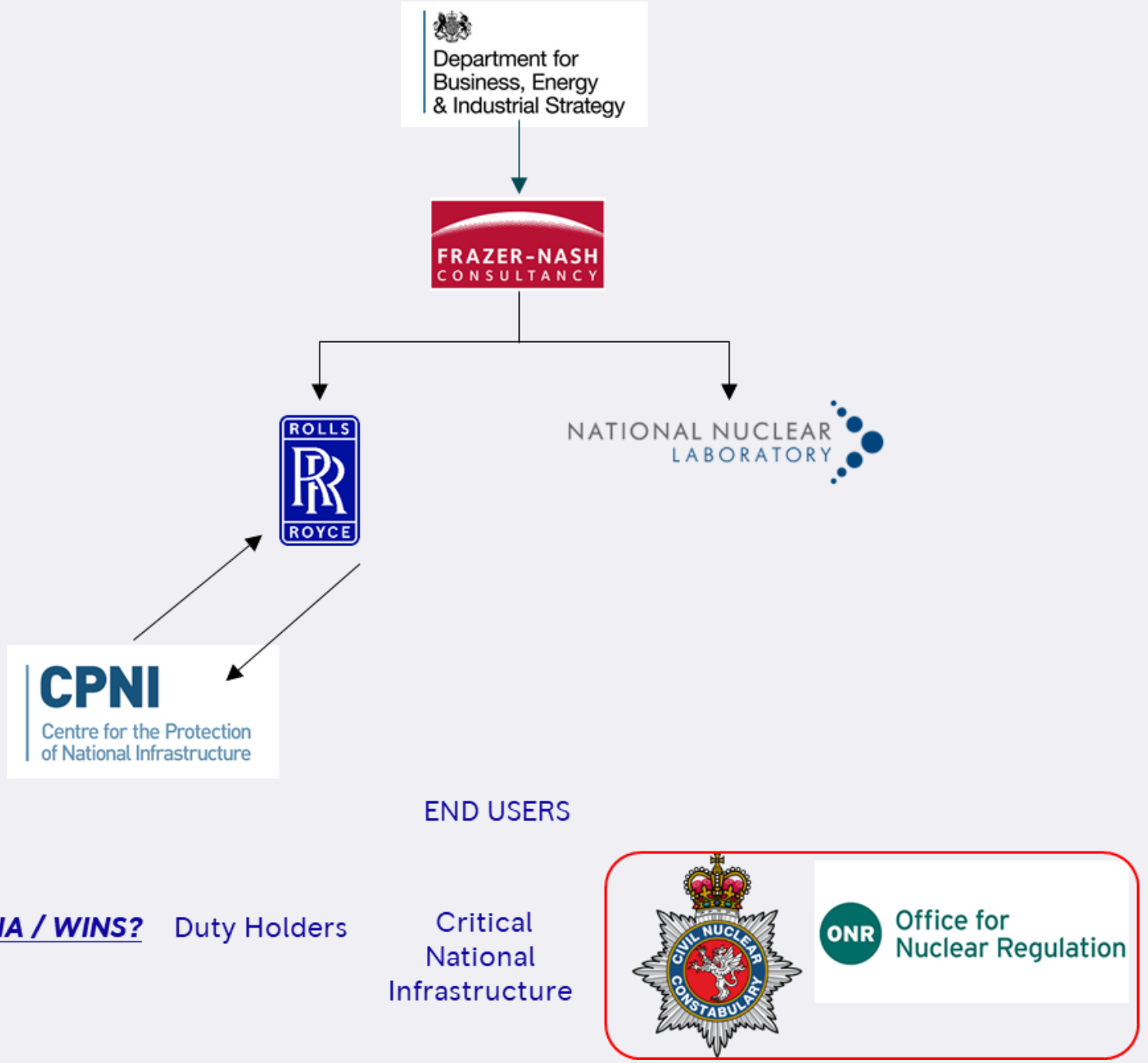
- To develop a common ALARP approach for Safety and Security
  - Task 1 – Literature review and feasibility report.
  - Task 2 – Outline Methodology report.

- The scope of task 2 was to:

"Conduct research to establish the feasibility of using the ALARP methodology as a route for demonstrating security compliance in civil nuclear installations. Use a combination of best practice drawn from existing research, and novel approaches where necessary, to synthesise a workable approach".

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Key Stakeholders / end users



© 2019 Rolls-Royce
Private – Rolls-Royce Proprietary Information
No Export License Required – Not Listed

Summary of Key Findings

- A fully worked example of an ALARP for security solution could not be found.
- There was evidence suggesting that some of the elements comprising an ALARP assessment were being used.
- Across the board, it was felt that trying to quantify the threat was too difficult and could not be achieved with any accuracy.
- Probabilistic methods of calculating security threats were presented but no evidence of a worked example was found.
- Several modelling and simulation tools were compared at a high level.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Measuring the effectiveness of a security system

Definition of system requirements

- Quantification of threat likelihood is considered unfeasible.
  - The DBT looks at threat capability and not threat likelihood.
- Measuring the effectiveness of the security system is a more viable approach.
- It is suggested that we focus on the detect and respond elements of a physical security system.
- Make an deterministic assessment regarding the amount of delay afforded based on the products selected.
- Develop functional security requirements to define expectations.
- Measure the quality of the system.
  - i.e. we don't just want to know if something works we want to know it works.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Outline Methodology Report

A common approach

- An outline methodology report has been created which suggests an approach to carrying out an ALARP for Security Assessment.
- This approach includes:
  - Utilising Safety IE frequency to define IEMO frequency target.
  - Utilisation of Event and Fault Trees to represent system likelihood success.
  - Distribution curves to as a means of determining a confidence security measure performance.
  - Utilising Modelling and Simulation tools to verify system

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Utilisation of Shared Tools and Processes

- The methodology proposes utilising Event and Fault Trees to enable probabilistic assessment.
  - This allows for Security to Model the safety systems ability to mitigate against an IEMO.
  - Enabling more informed design decisions to achieve the greatest
  - Ensures accurate modelling and simulation to support design

ADOPTING A COMMON APPROACH MAY EASE REGULATION.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

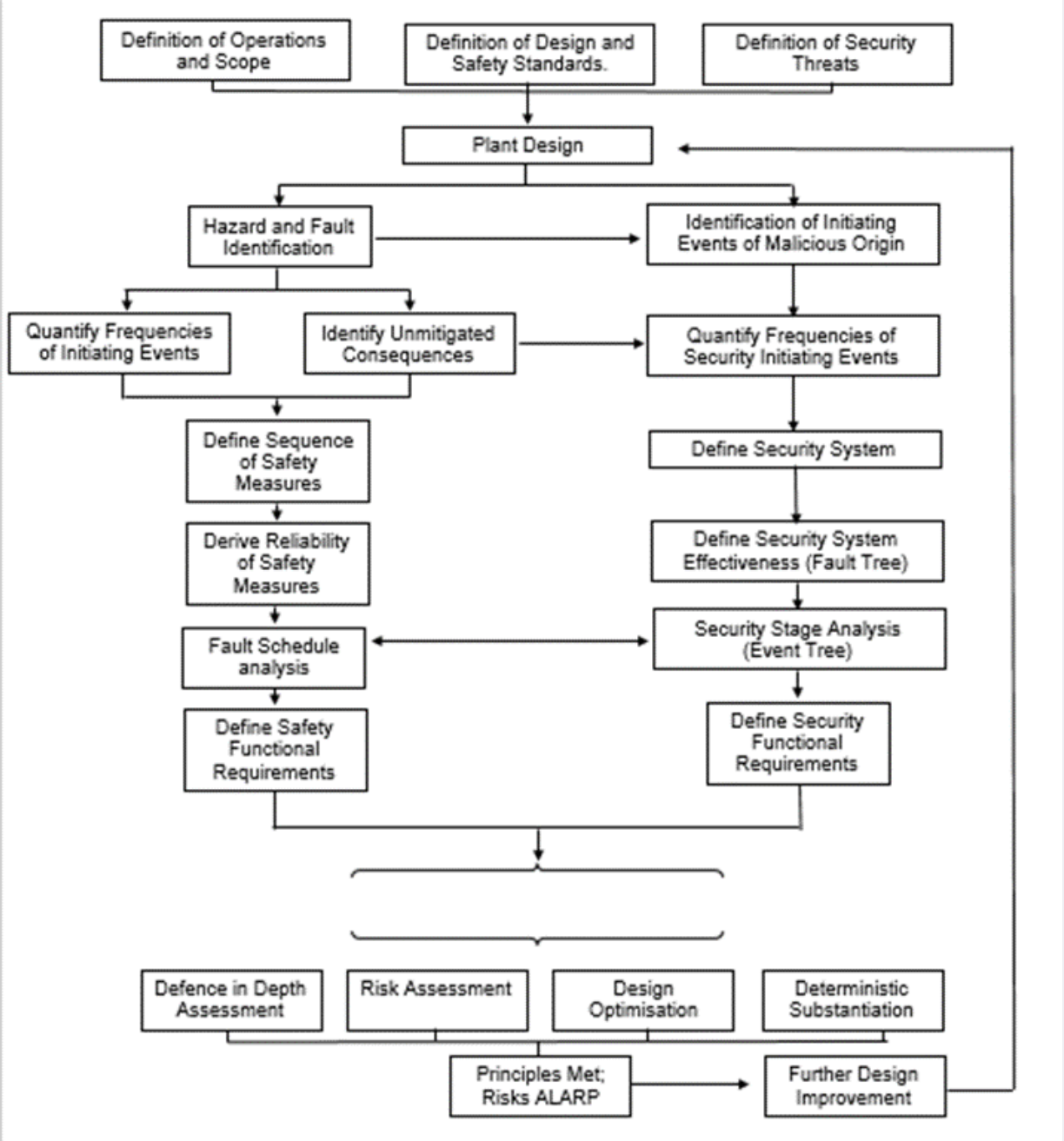
Outline
Methodology
Report

Unique Integrated Approach to Security and Threat Assessments

- Credible data to drive probabilistic assessments
- Using common methods to analyse security threats.
  - Treatment of IEMOs as external hazards.
  - Taking a SINS approach to security management.
- Utilise a common baseline with safety.
  - This allows Security to make claims against safety systems.
- Allows informed design optimisation.
- Win-win for all
  - How to measure success?

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Process Map



© 2019 Rolls-Royce
Private – Rolls-Royce Proprietary Information
No Export License Required – Not Listed

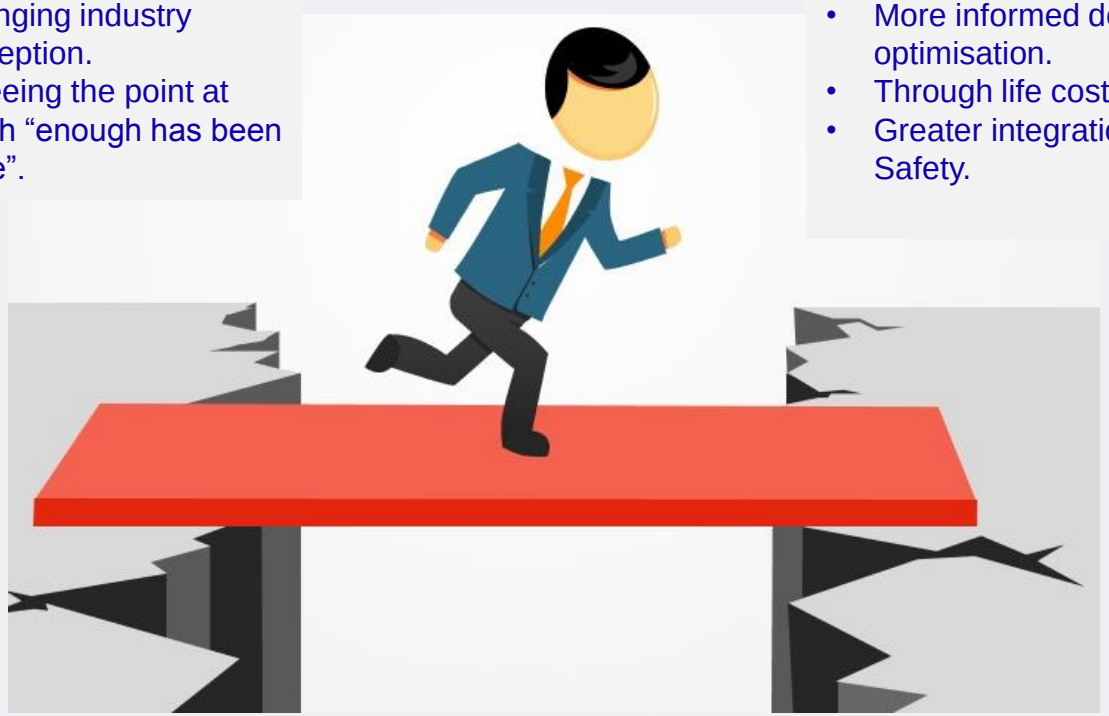
Challenges and Opportunities

Challenges

- Gathering “real world” data.
- Changing industry perception.
- Agreeing the point at which “enough has been done”.

Opportunities

- Greater understanding of residual risk.
- More informed design optimisation.
- Through life cost saving.
- Greater integration with Safety.



© 2019 Rolls-Royce
Private – Rolls-Royce Proprietary Information
No Export License Required – Not Listed

Interested in how our we can help you integrate our research outputs into your organisation?

For design and operation

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

For regulatory acceptance

We recognise that regulatory acceptance is a key milestone in the adoption of new techniques. The project team welcomes your guidance and knowledge to steer our research to ensure it is aligned with the UK's regulatory regime. We seek to engage with the regulator to provide early insight into proposed methodologies that we hope will form part of future submissions.

For educators

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget.
We're looking to engage with undergraduate and post-graduate students and provide material for your teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped for the UK's nuclear future.

© 2019 Rolls-Royce
Private – Rolls-Royce Proprietary Information
No Export License Required – Not Listed

FRAZER-NASH CONSULTANCY

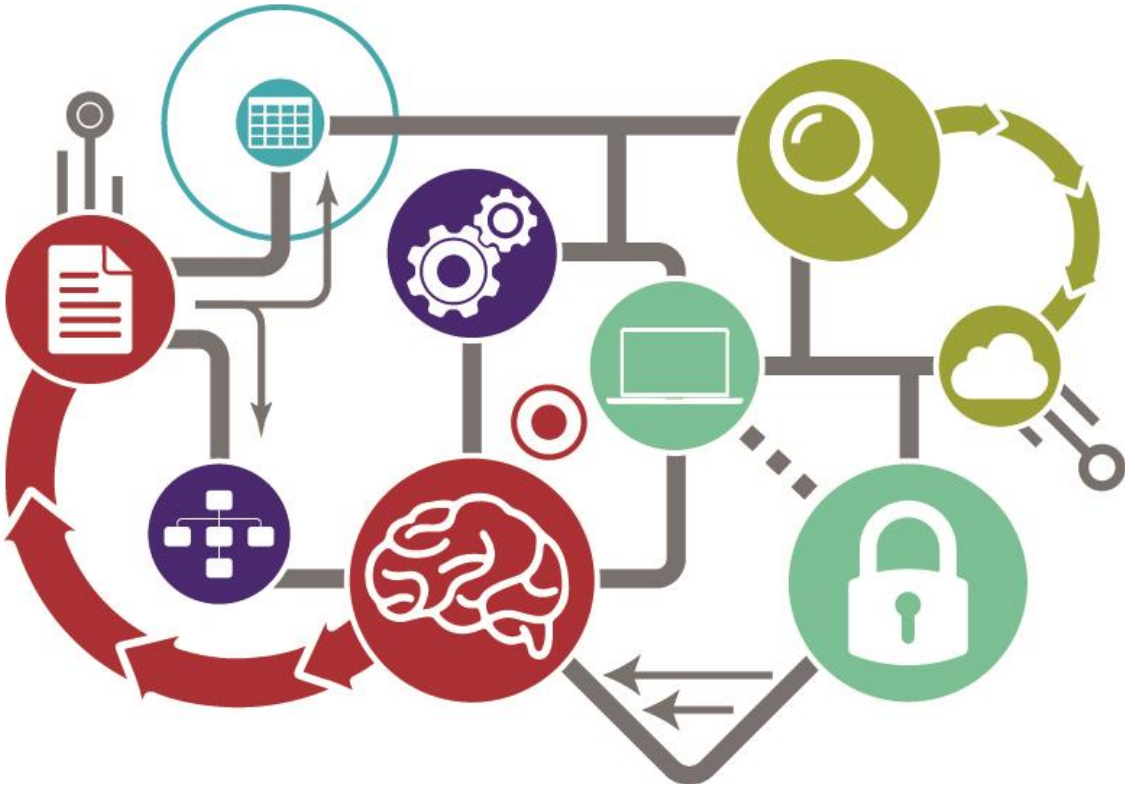
Tea & Coffee Break

Application of Model-Based Systems Engineering (MBSE) in the UK Nuclear Sector

Steven Fletcher, Topic Lead, Frazer-Nash Consultancy

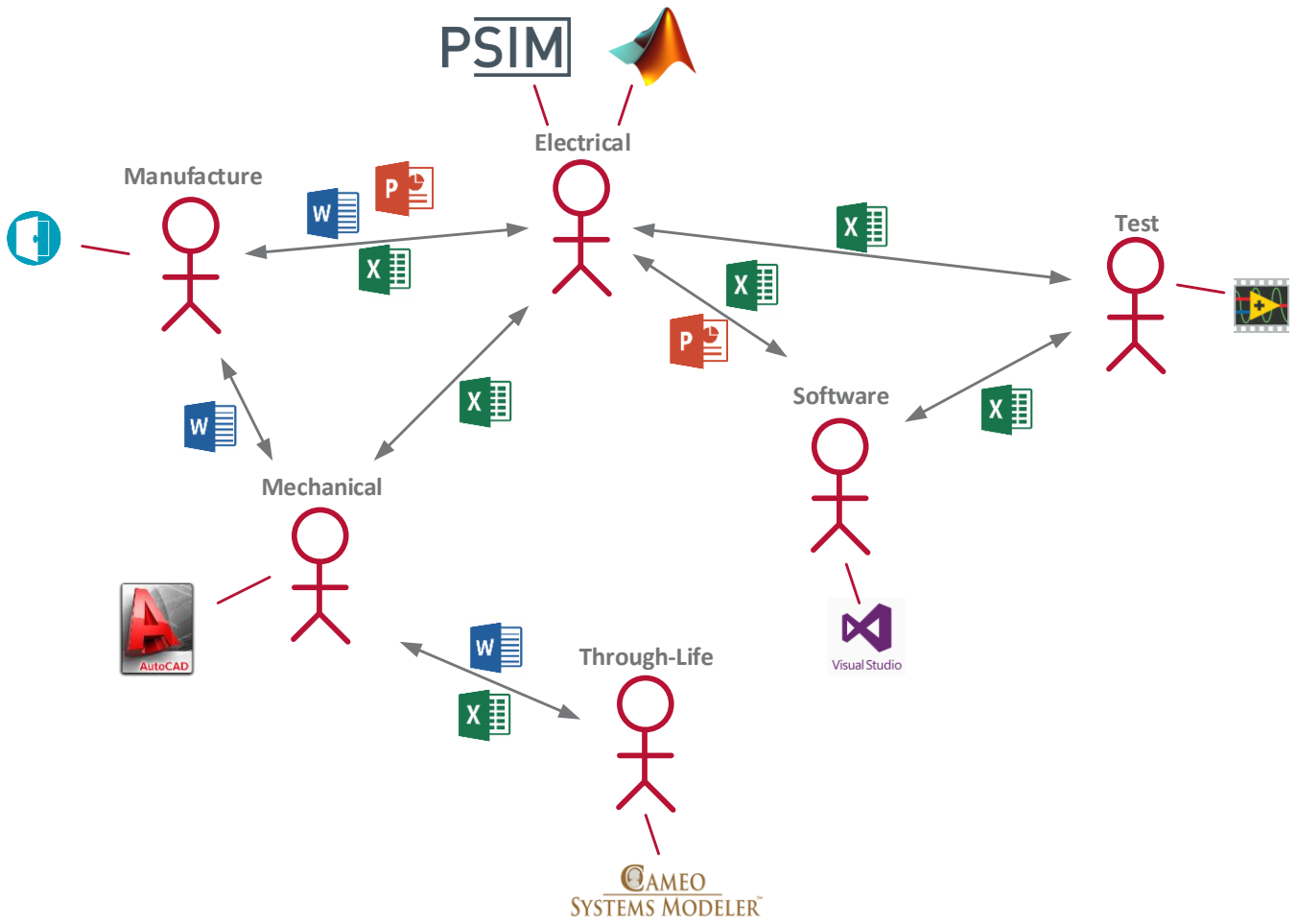
Overview

- What is MBSE?
- Project overview
- State of the art review
- UK ABWR case study
- Next steps



© Frazer-Nash Consultancy Ltd. All rights reserved.

Modelling in Traditional Systems Engineering



- ‘Document based’ systems engineering
  - Individual domains use models to support decisions but systems engineering activities are not ‘model-based’.
- Standalone models related via:
  - Static Documents
    - Interface documents
    - Requirements documents
    - Design documents
  - ‘Corporate Level’ lifecycle documents
    - Reporting
    - Design guides
  - Formal review
  - Informal communications
    - Whiteboard diagrams, Emails, Chat & scribbles

© Frazer-Nash Consultancy Ltd. All rights reserved.

What is MBSE?

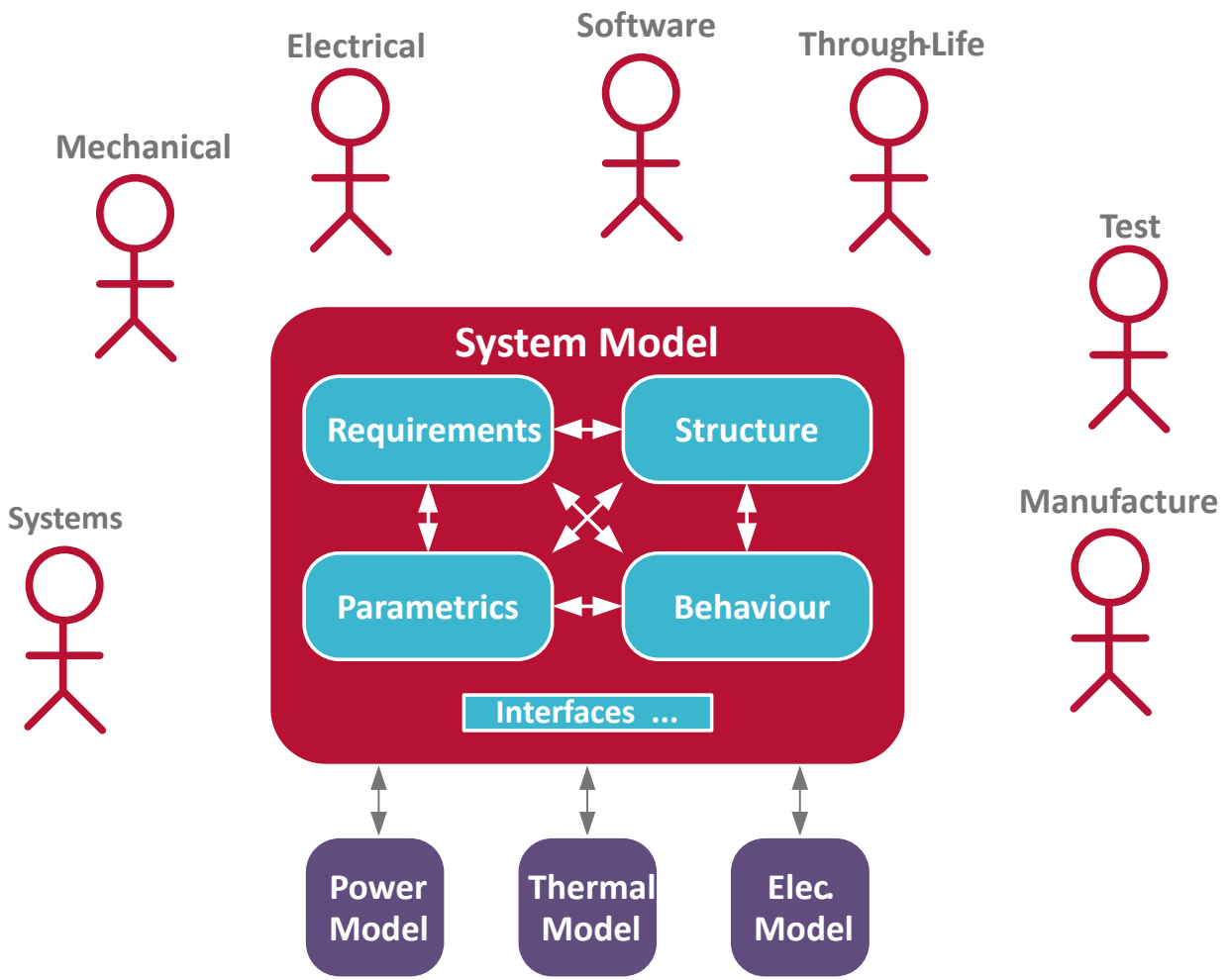
‘The <u>formalised</u> application of modelling to support system requirements, design, analysis, verification, and validation activities from concept to decommissioning’.

INCOSE SE Vision 2020 (INCOSE-TP-2004-004-02, Sep 2007)

- Models may be structural, behavioural, physical, electrical, parametric…
- …tied together by a <u>system model</u>, shared by all disciplines, with multiple ‘views’ as required

© Frazer-Nash Consultancy Ltd. All rights reserved.

What is MBSE?

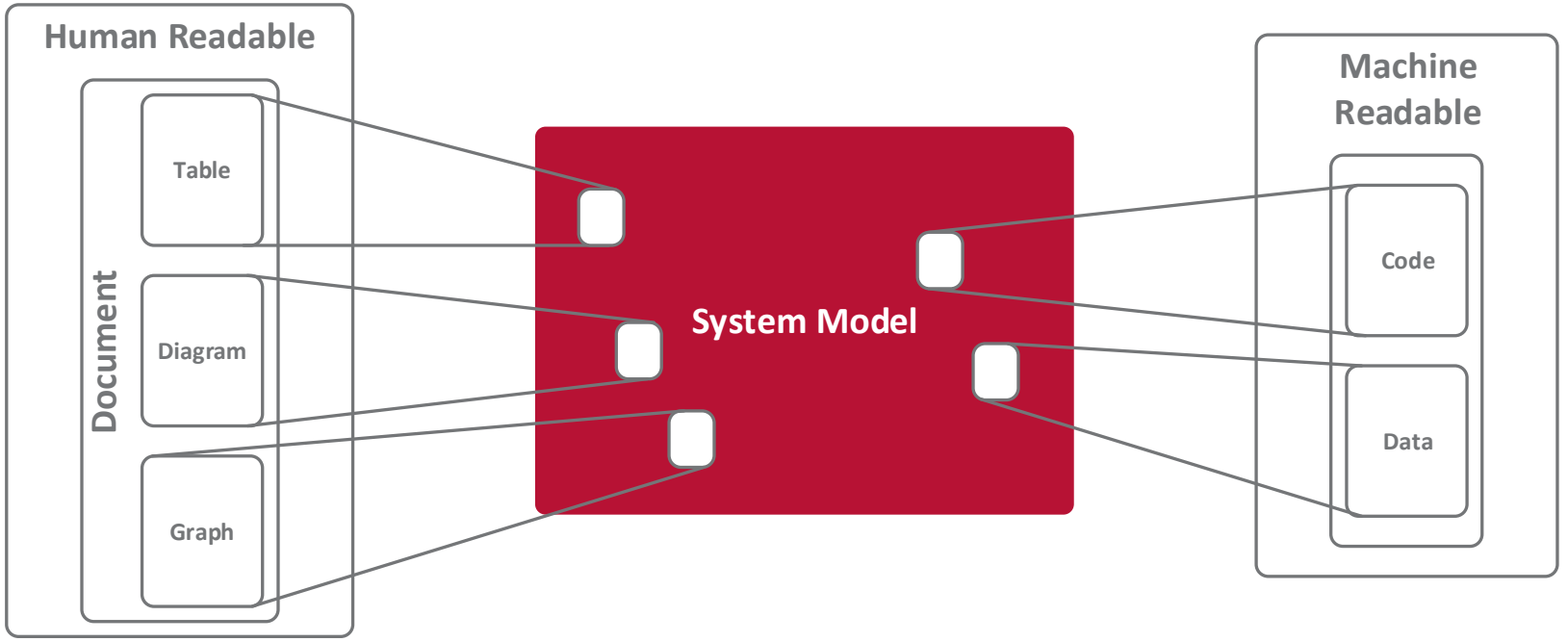


- Model the systems engineering activities
  - All of the same models and ‘work’ remains, but is tied together by a system model
- Integrated models related via:
  - Multiple views of coherent and consistent information, without ambiguity
  - More efficient and effective information exchange between parties
  - Better traceability ‘for free’
  - Information and data accessible by all parties
  - Formal system model, for example **SysML** / UML

© Frazer-Nash Consultancy Ltd. All rights reserved.

What is MBSE?

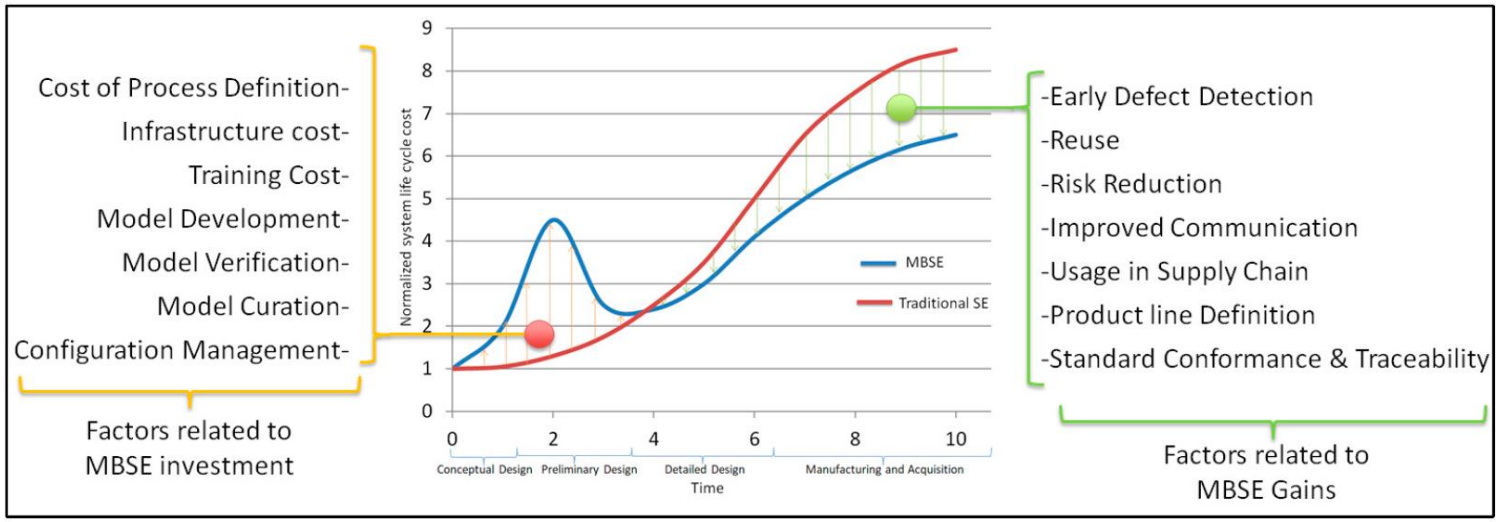
- MBSE is all about getting the ‘right info’ to the ‘right people’ as effectively and efficiently as possible.
- ‘Right people’ may be other models or simulations….
- MBSE provides a centralised source of information throughout the lifecycle of a system



© Frazer-Nash Consultancy Ltd. All rights reserved.

MBSE Benefits

- Allows for articulation of ‘traditional’ information but:
  - More consistent, maintainable, traceable and verifiable
- This supports:
  - Better management of complexity (especially ‘whole system’ considerations)
  - Reduced ambiguity in system design (supporting early detection of design defects)
  - More time on engineering design and less on document management
    - Automate the low-value add activities
- The model doesn’t do the hard work for you – it is a tool to allow for better and more informed decision making



MBSE should enable long term whole system development cost reduction – an effect which scales with system complexity and longevity

Source: Madni, Purohit, “Economic Analysis of Model-Based Systems Engineering” Available from: https://www.mdpi.com/2079-8954/7/1/12

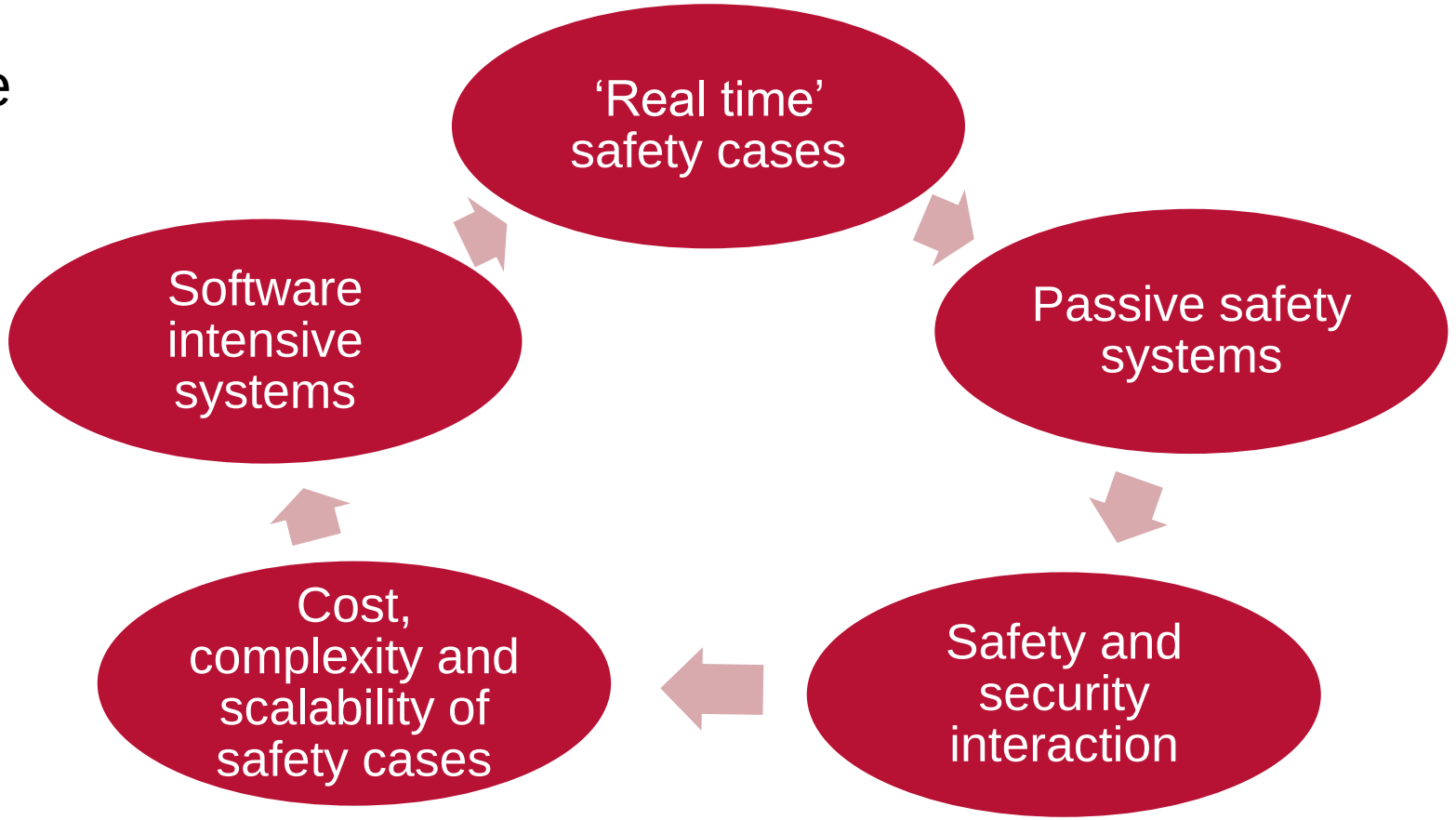
© Frazer-Nash Consultancy Ltd. All rights reserved.

Project overview

Application of Model-Based Systems Engineering (MBSE) in the UK Nuclear Sector

- We are working to demonstrate the usage of an MBSE approach to the conducting, capturing, and presenting of safety cases for a UK civil nuclear programme

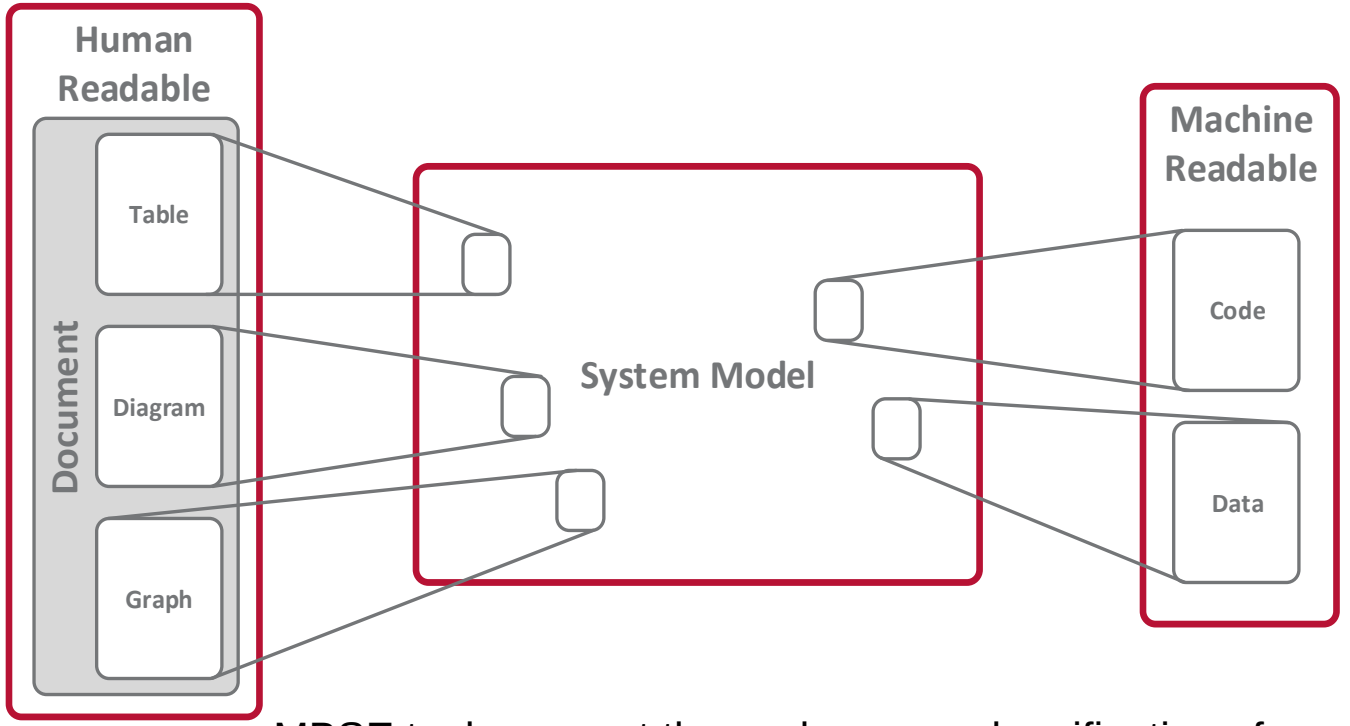
- This is in the context of wider nuclear sector challenges



© Frazer-Nash Consultancy Ltd. All rights reserved.

Specific modelling aims and challenges

- To effectively support process improvement MBSE models should provide
  - A means of tracking the impact of requirement or design changes on the system as a whole;
  - A way of articulating safety cases in a format which is visual and easier to understand;
  - A tool for recording the traceability; and,
  - A means of verifying large volumes of design information (e.g. between design model and specs).



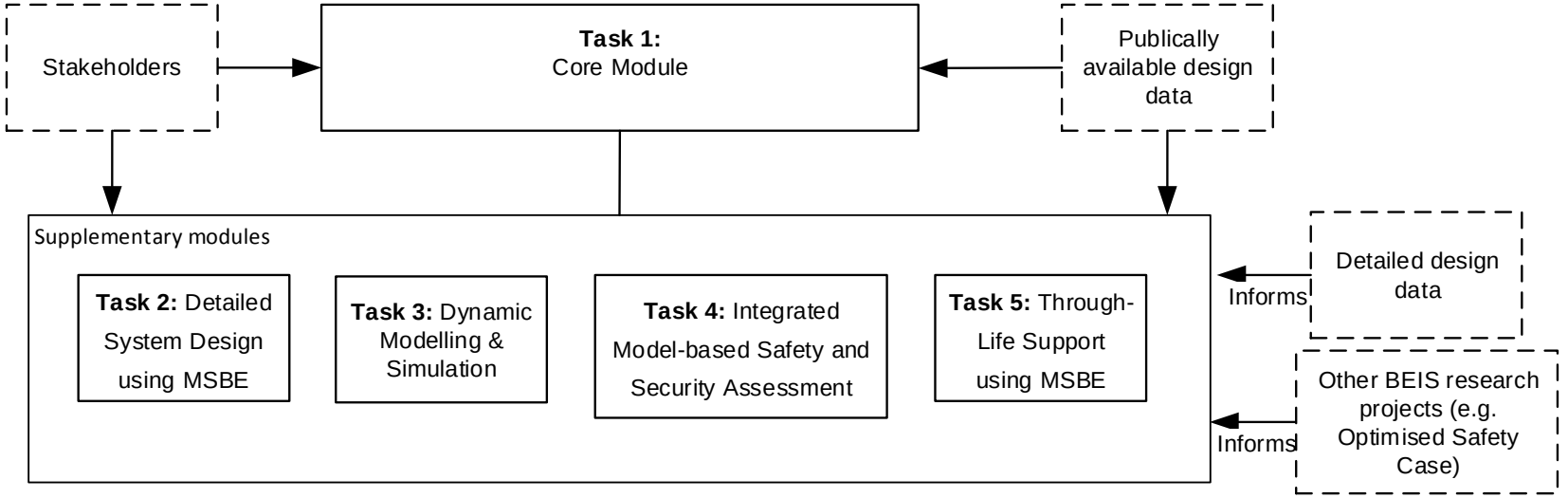
MBSE tools support the exchange and verification of information from multiple formats

Integration between design, other models (e.g. evidence) and the safety case will be a key differentiator from existing safety case software

© Frazer-Nash Consultancy Ltd. All rights reserved.

Research Project Structure

- This research project shall be split into a number of tasks as follows:
  - A ‘Core’ module that shall see the construction of a SysML model of top level design data and information from across a complex civil nuclear reactor design programme;
    - Includes a state of the art review of the use of MBSE
  - A number of ‘Supplementary’ modules that shall demonstrate specific techniques and approaches, using more detailed design data, that hook into the core model



© Frazer-Nash Consultancy Ltd. All rights reserved.

State of the art review

Review aims

Main aim:

- Identify the current capability of MBSE methodologies and tools to support the needs of the nuclear sector

- Questions included:
  - Where have tools been used in the nuclear sector to date?
  - How are tools being used in other sectors?
  - What capabilities do the tools have for representing safety information?

- Findings detailed in report titled “Application of MBSE in the Nuclear Sector - State of the art review”, FNC 57280/48483R Issue 1

© Frazer-Nash Consultancy Ltd. All rights reserved.

Where have tools been used in the nuclear sector to date?

- Two notable applications to date in the nuclear sector:

1. Finnish research project (part of SAFIR2014) assessing MBSE for requirements management and system design

2. Use of MBSE to support deployment of safety critical software development for plant modernisation activities.

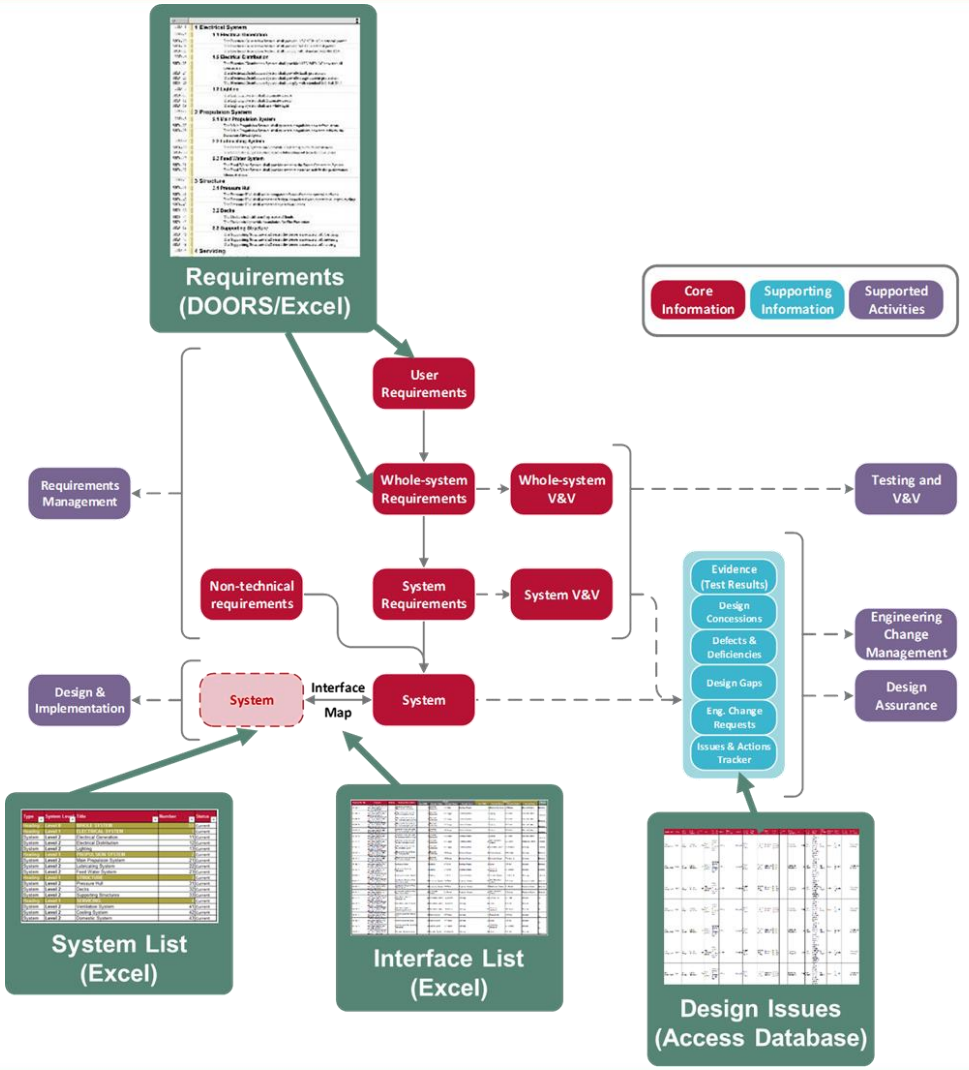
This project is pitched in the gap between these areas - a real-world demonstration of how MBSE can support the nuclear sector

© Frazer-Nash Consultancy Ltd. All rights reserved.

How are tools being used in other sectors?

- There are two main ways the MBSE tools could be deployed in support of the NPP design. These are:

  1. Support NPP development mid-programme – i.e. how can MBSE be used to better organise, understand and analyse current information sets;
  2. MBSE tools can be used to support whole system design and development – i.e. using the tools to design new systems and the associated safety case.

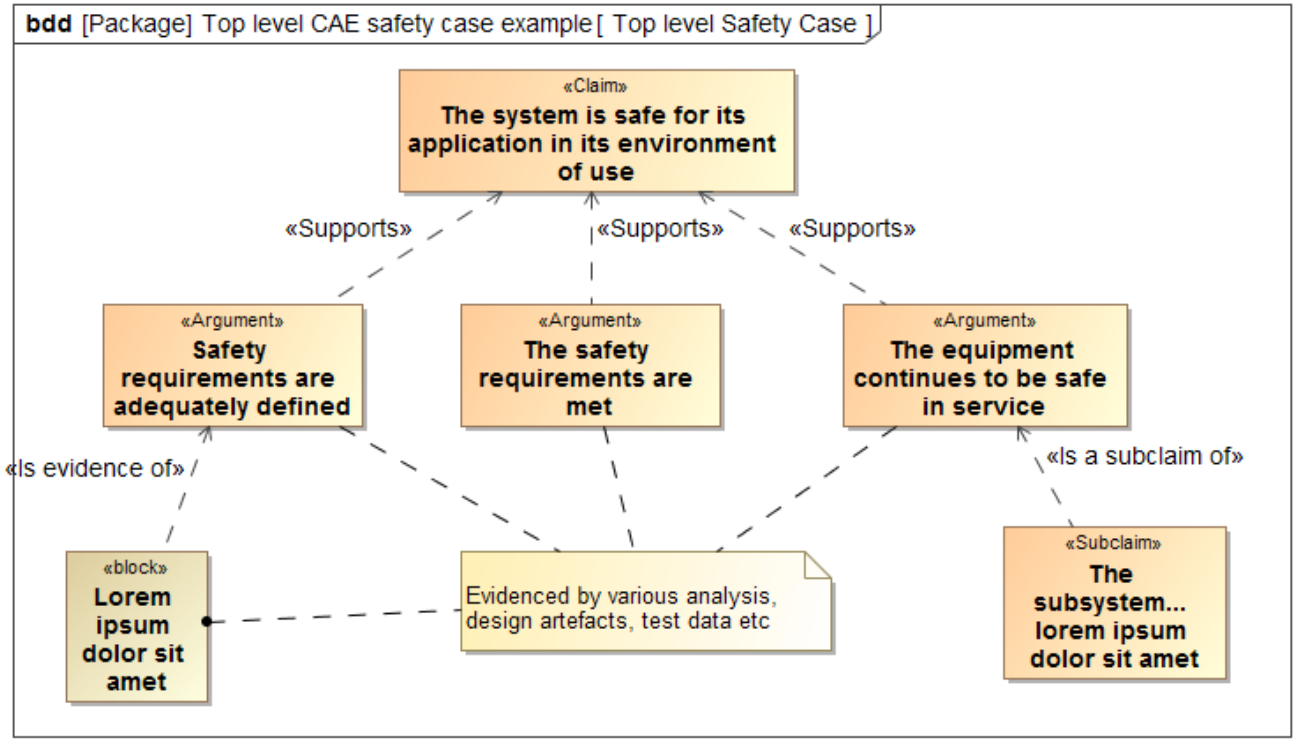


© Frazer-Nash Consultancy Ltd. All rights reserved.

What capabilities do the tools have for representing safety information?

- The structured/hierarchical safety case approach lends itself well to an MBSE approach:
  - Decomposition of safety functions from higher level to lower level
  - Linkage between arguments and design artefacts
  - Formal notation simple to recreate in tools SysML tools

- Integration of safety analysis into SysML is a recognised weakness across multiple domains
  - Some examples of fault tree generation, FMEA analysis from MBSE tools
  - The value of integrating safety analysis is still being explored

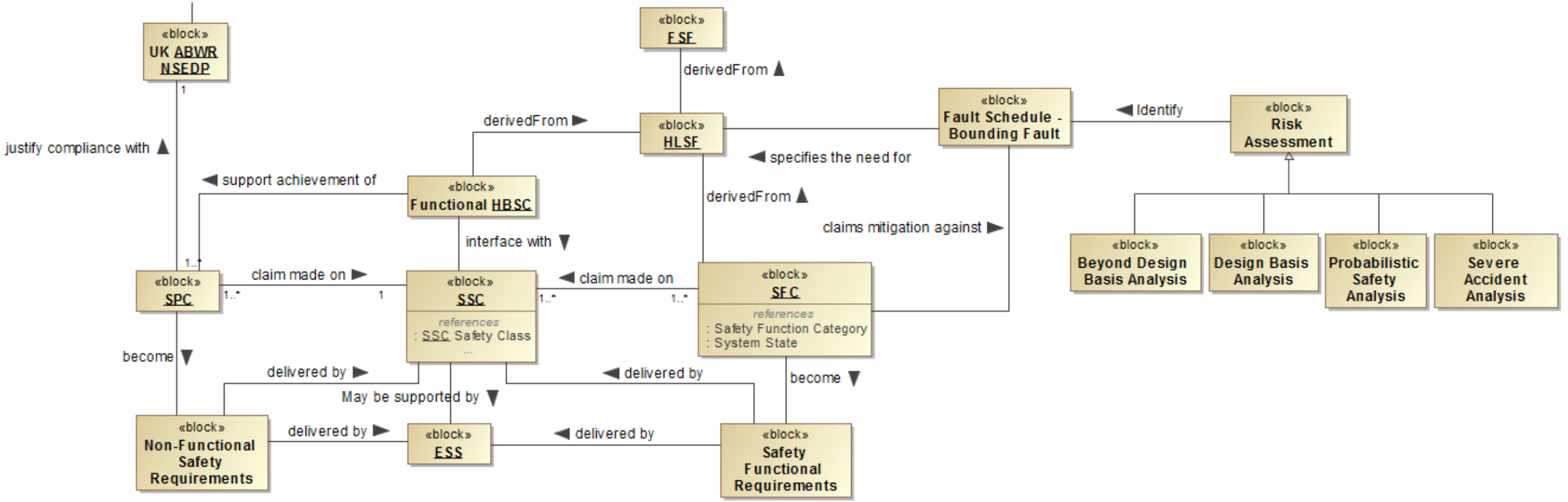


Example SysML representation of a Claims Argument Evidence Structure

© Frazer-Nash Consultancy Ltd. All rights reserved.

Generic Design Assessment using MBSE – UK ABWR Pre-Construction Safety Report Case Study

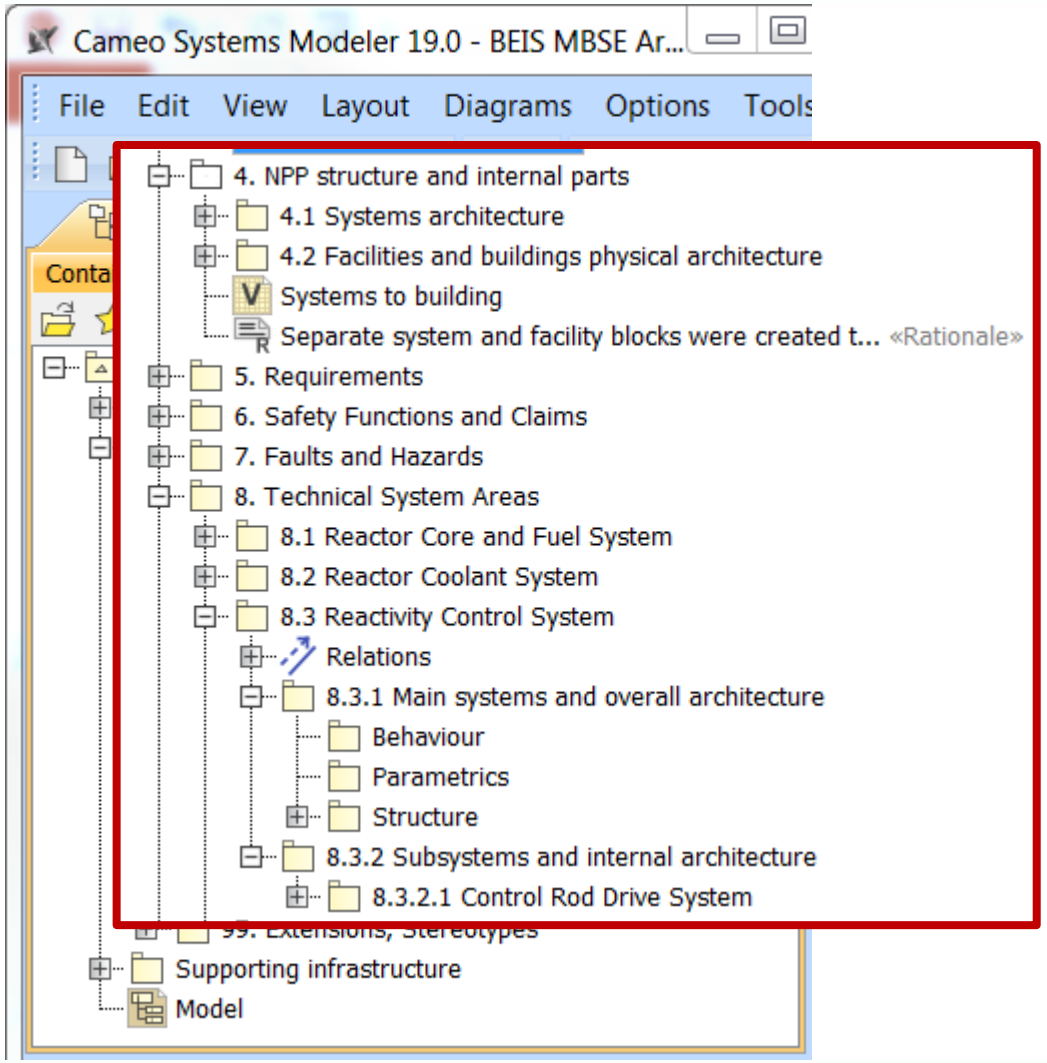
UK ABWR Safety case ontology



Example ontology for the key elements that comprise the Hitachi UK ABWR GDA safety case

© Frazer-Nash Consultancy Ltd. All rights reserved.

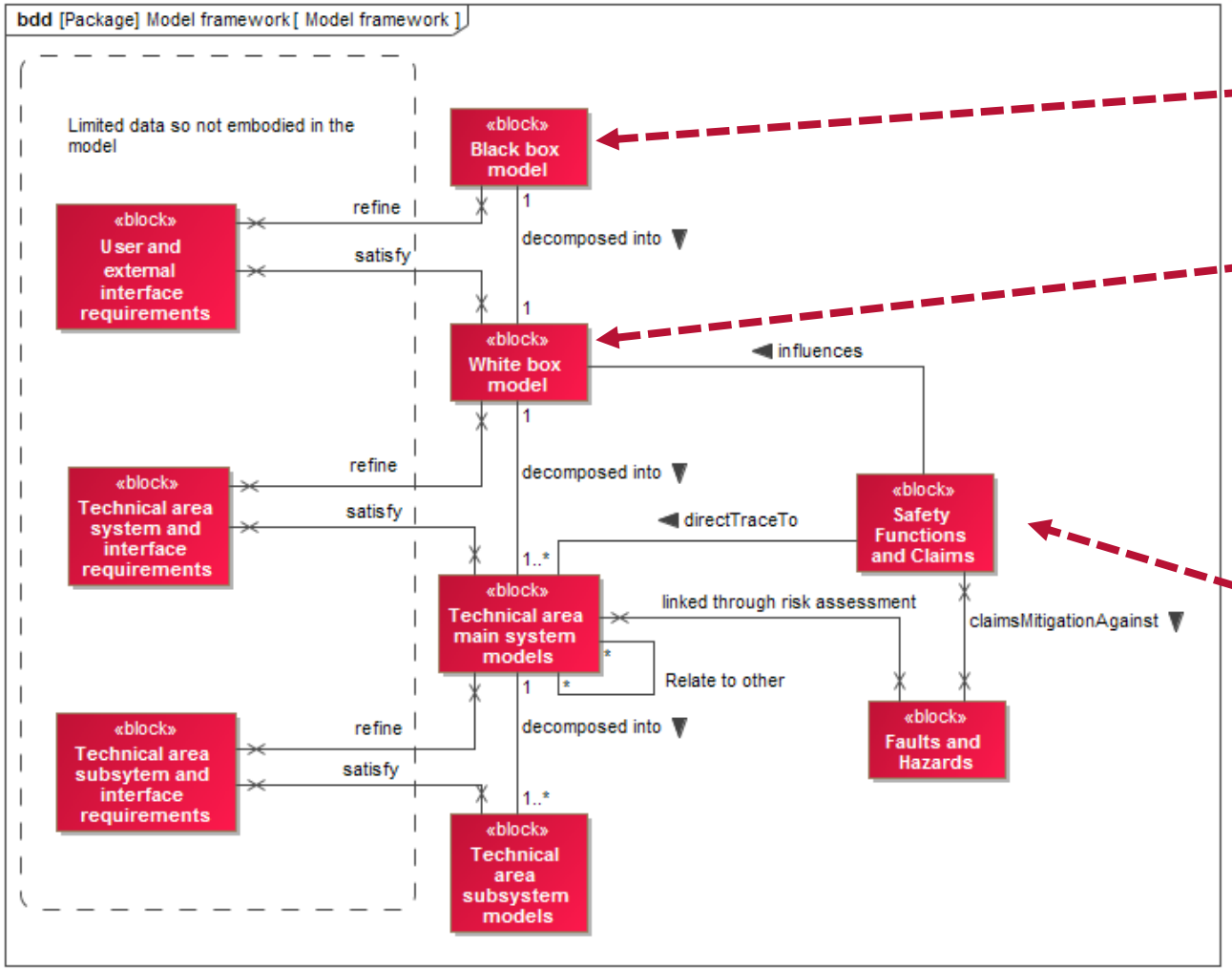
NPP model



- All information contained within the model browser
  - Different views are created to articulate information differently
- A relational database of connected items, inc:
  - Requirements to system design
  - Safety Functional Claims to System design
  - Fault Schedule to Safety Functional Claims
- Ultimately, by using a centralised source of information, the entirety of the design can be understood
- The model currently identifies types of information across most systems and expands on one specific subsystem

© Frazer-Nash Consultancy Ltd. All rights reserved.

Model structure



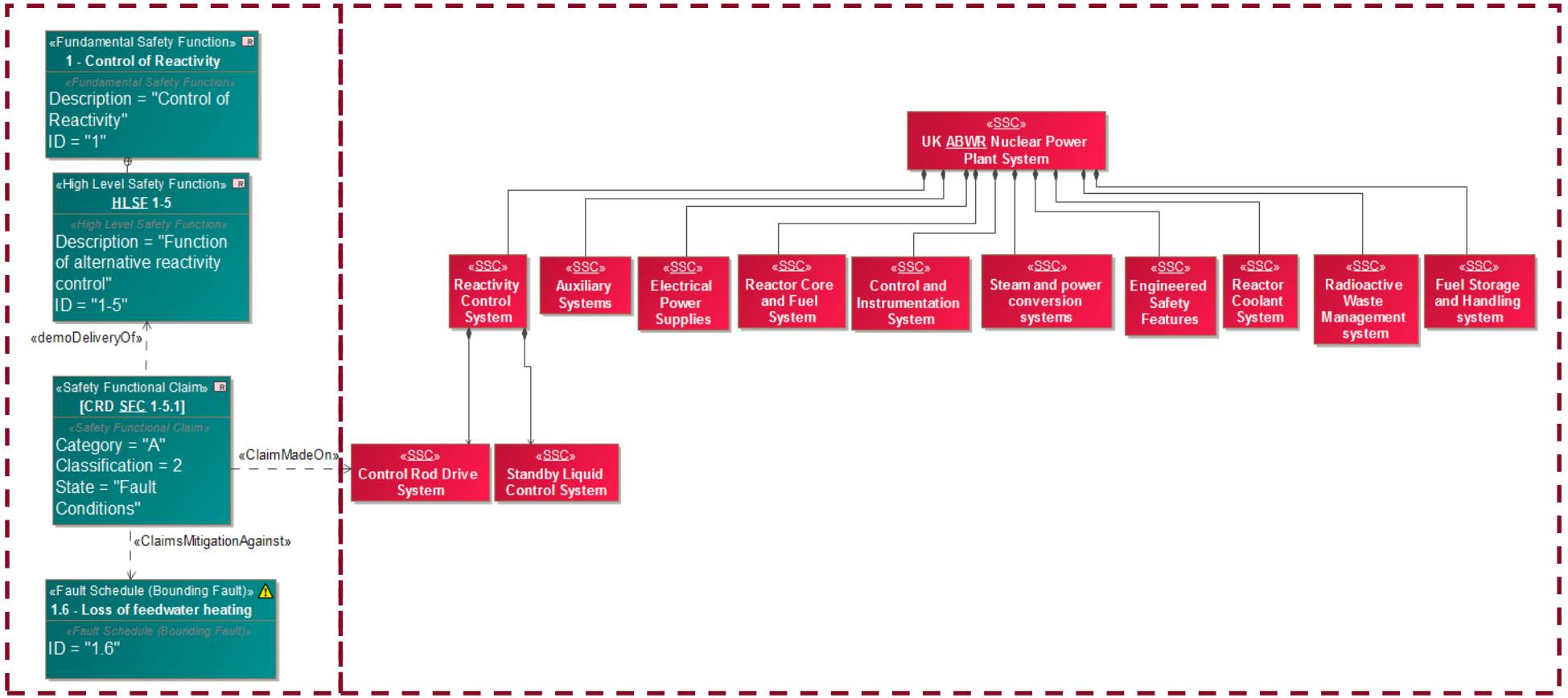
- Black Box model
  - Looks externally – stakeholders, use cases and NPP system interfaces
- White box model
  - The main systems which make up the NPP and purpose
- Technical Area models
  - Expand on the main systems
  - Define the roles and functions which contribute to safe operation
  - <u>Claims are linked at this level</u>
- Continue an iterative process of defining black box (external) and white box (internal) models with increasing levels of detail

© Frazer-Nash Consultancy Ltd. All rights reserved.

Model hierarchies

Safety function, claim and fault hierarchy

Design hierarchy

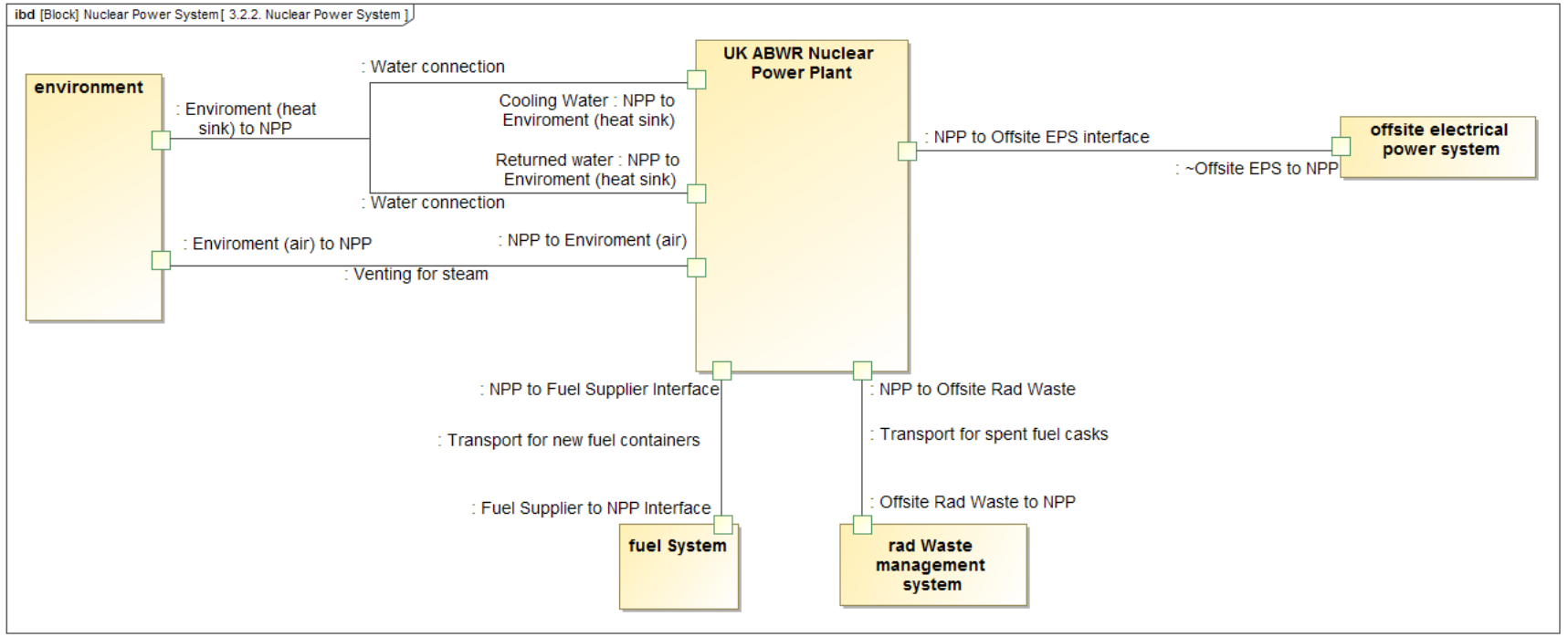


- All relationships created and stored within the model
- Once established these are simple to trace

Information based on Hitachi GDA documentation

© Frazer-Nash Consultancy Ltd. All rights reserved.

System architecture



Whole system internal block diagram

- The internal block diagram helps illustrate architecture and interfaces
- Connectors and ports can be defined in the model to understand requirements and constraints
- Parametric relationships can be defined to understand trade-offs

© Frazer-Nash Consultancy Ltd. All rights reserved.

Model Traceability

Legend
demoDeliveryOf

	CRD [6. Safety Fu	[CRD SFC 1-1.1]	[CRD SFC 1-1.2]	[CRD SFC 1-1.3]	[CRD SFC 1-3.1]	[CRD SFC 1-4.1]	[CRD SFC 1-4.2]	[CRD SFC 1-5.1]	[CRD SFC 1-5.2]	[CRD SFC 1-5.3]	[CRD SFC 1-7.1]	[CRD SFC 2-3.1]	[CRD SFC 4-1.1]	[CRD SFC 4-4.1]	[CRD SFC 4-7.1]	[CRD SFC 5-20.1]	[CRD SFC 5-20.2]
6.1 Fundamental and High Level		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1 - Control of Reactivity		1	1	1	1	1	1	1	1	1	1						
HLSF 1-1	3	↗	↗	↗													
HLSF 1-2																	
HLSF 1-3	1				↗												
HLSF 1-4	2					↗	↗										
HLSF 1-5	3							↗	↗	↗							
HLSF 1-6																	
HLSF 1-7	1										↗						
HLSF 1-8																	
HLSF 1-9																	
HLSF 1-10																	
2 - Fuel Cooling												1					
3 - Long term heat removal																	
4 - Confinement/Containment													1	1	1		
5 - Others																1	1

Safety Functional Claims

Bounding Faults

Legend
ClaimsMitigationAgai...

	Common Caus	11.1 - Loss of	11.2 - Inadver	11.3 - Inadver	11.4 - ADS inc	11.5 - MSIV ir	11.8 - M/C po	11.9 - D/C po	11.11 - Loss c	11.12 - Loss c	External Hazai	18.1 - Loss of	18.2 - 10-3/y	18.3 - DB eart	17.1 - Interna	17.2 - Interna	17.3 - Interna	17.4 - Interna	17.5 - Interna	17.6 - Turbine	Isolation Event	Loss of Coolar	No corresponding	Non-Isolation f	Reactor Fault
CRD [6. Safety Functio		1	1	1	1	1	1	1	1			2	2	1		2	2	2	2	1	1			14		
[CRD SFC 1-1.1]	1																							↗		
[CRD SFC 1-1.2]	1																							↗		
[CRD SFC 1-1.3]	1																							↗		
[CRD SFC 1-3.1]	49	6	↗	↗	↗			↗	↗	↗		3	↗	↗	↗	6	↗	↗	↗	↗	↗	↗	7	12		14	1
[CRD SFC 1-4.1]	1																							↗		
[CRD SFC 1-4.2]	1																							↗		
[CRD SFC 1-5.1]	25	2				↗	↗					2	↗	↗		4	↗	↗	↗	↗			6	2		9	
[CRD SFC 1-5.2]	1																							↗		
[CRD SFC 1-5.3]	1																							↗		
[CRD SFC 1-7.1]	1																							↗		
[CRD SFC 2-3.1]	1																							↗		
[CRD SFC 4-1.1]	1																							↗		
[CRD SFC 4-4.1]	1																							↗		
[CRD SFC 4-7.1]	1																							↗		
[CRD SFC 5-20.1]	1																							↗		
[CRD SFC 5-20.2]	1																							↗		

High level safety functions

Safety Functional Claims

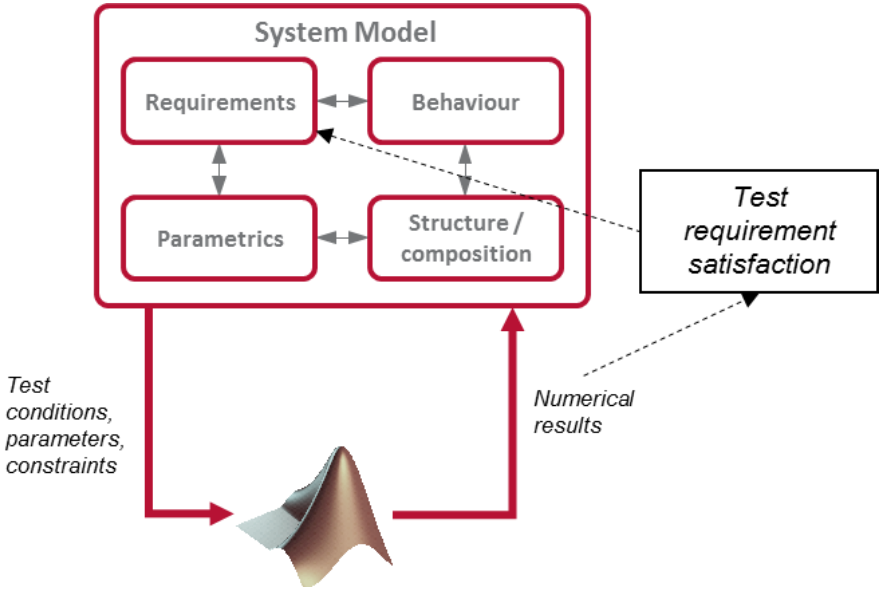
© Frazer-Nash Consultancy Ltd. All rights reserved.

Outputs and Next steps

Next steps

- Kicked off Dynamic Modelling & Simulation task
  - Where MBSE models can play a useful role?
    - e.g. What system codes and sub-channel codes could they interface?
  - How can safety related modelling can be coordinated using MBSE tools?
  - Linking up with the Project FORTE - Nuclear Thermal Hydraulics Research & Development
  - Linking up with the Virtual Engineering Phase 2 project

- Engaging with the INCOSE community about how to support the Nuclear sector
  - Opportunity for the outputs of this project to shape future standards and tool development

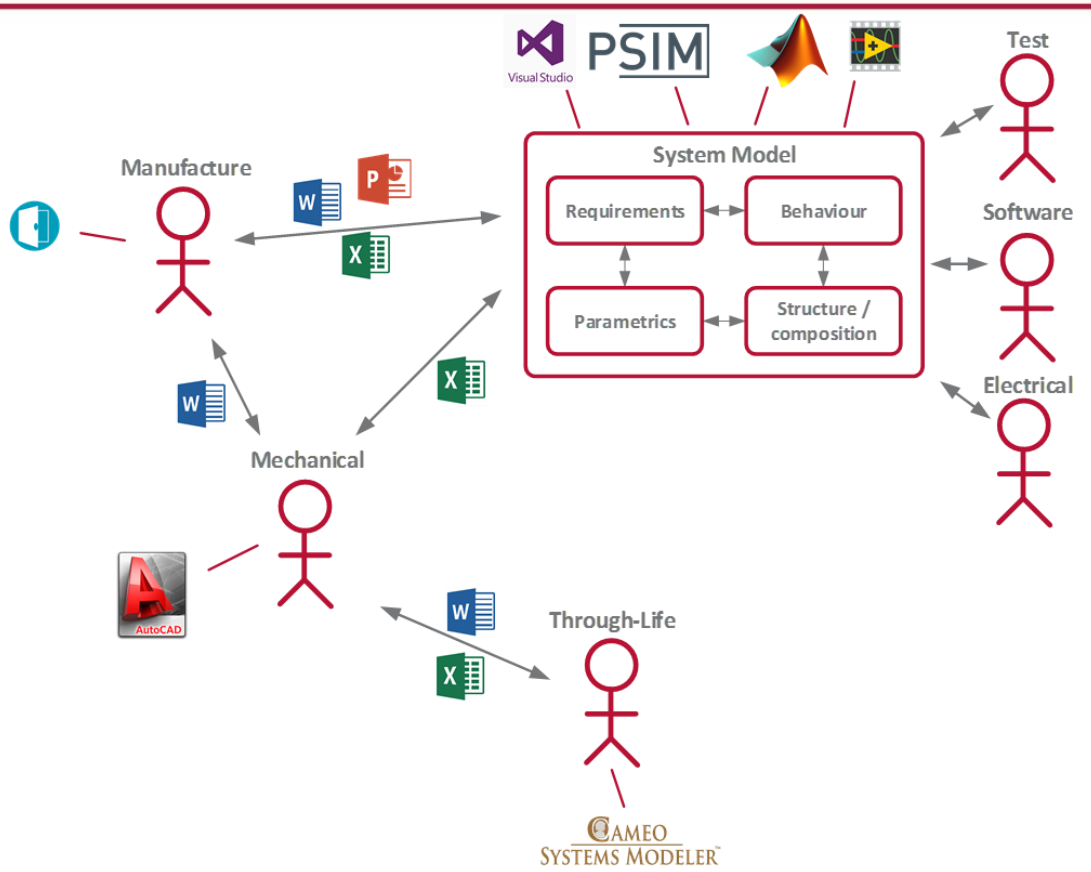


© Frazer-Nash Consultancy Ltd. All rights reserved.

Project Outputs

- The project cuts across a number of technical applications of MBSE – the end goal is to understand where and how it could be best used
  - This will be demonstrated through a series of case studies
  - Multiple opportunities for academic outputs

- Skills and development
  - 4 staff trained up in safety case development methodologies (inc. a year in industry student)
  - Promoting MBSE tools and methodologies within nuclear safety teams within Frazer-Nash
    - Safety case practitioners can see the value



A phased and pragmatic introduction of MBSE has been shown to be most effective in other sectors

© Frazer-Nash Consultancy Ltd. All rights reserved.

FRAZER-NASH CONSULTANCY

Interested in how our we can help you integrate our research outputs into your organisation?

For design and operation

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

For regulatory acceptance

We recognise that regulatory acceptance is a key milestone in the adoption of new technologies. The design of this project and how it is delivered capitalises on the delivery partners' decades of experience in supporting regulatory activities. This experience is embedded in the project's outputs that are available to you.

For educators

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget. The project team seek to engage with undergraduate and post-graduate students and provide material for teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped with for the UK’s nuclear future.

Advanced modular reactors

Richard Deakin, Department for Business, Energy & Industrial Strategy

Small Nuclear
UK Policy Perspectives

Rich Deakin
Head of innovation
Advanced Nuclear technologies

INDUSTRIAL STRATEGY

UK Nuclear Landscape

- Powering homes and businesses for over 60 years
- 20% of the UK's electricity needs
- 40% of UK low-carbon electricity
- Low-carbon, secure and reliable base-load power
- Reduction in UK's CO2 emissions
- Diversifying local economies.

Department for Business, Energy & Industrial Strategy

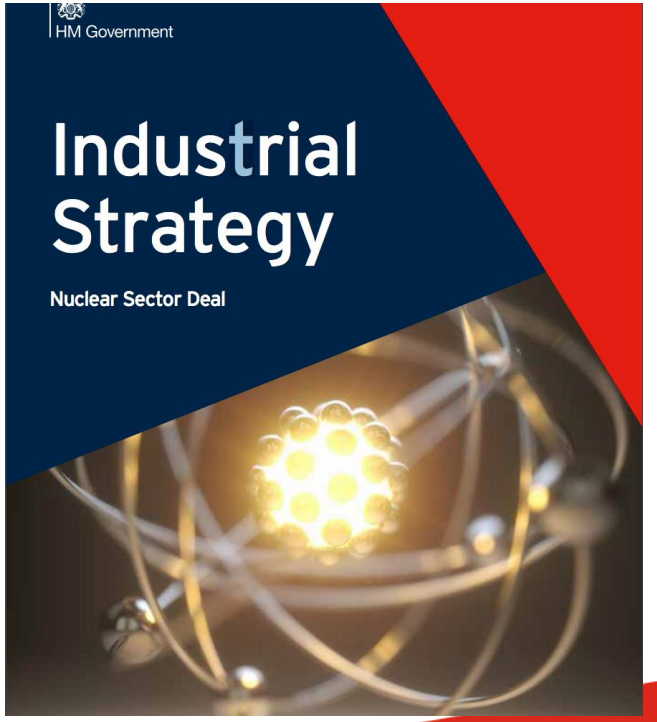
INDUSTRIAL STRATEGY

New Nuclear: Sustainability

- Nuclear has an important role to play in the UK's energy future as we transition to the low carbon economy
- Emphasis on value for money for consumers and taxpayers
- Feasibility of a Regulated Asset Base (RAB) funding model currently being explored
- Sustainable funding mechanisms are key.

The UK Nuclear Sector Deal

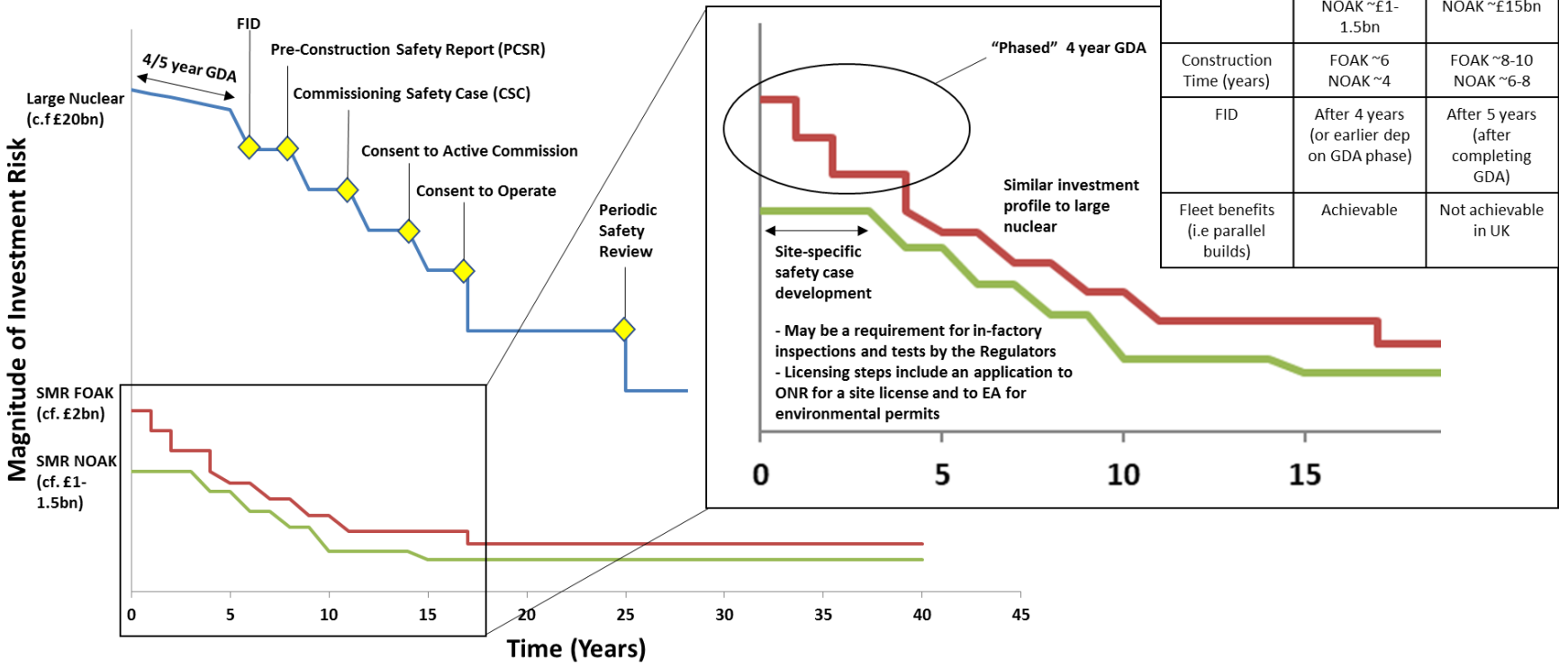
- UK Industrial Strategy published on 27 November 2017
- Right support from the government can help meet the **Clean Growth Grand Challenge**
- Nuclear Sector Deal signals fresh pace and ambition for SMRs
- Shared commitment from Government and Industry
- Working to create a fertile environment for Advanced Nuclear Technologies



Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

What makes Small Nuclear Different?



	SMR	Large Project
Capital Cost (£)	FOAK ~ £2bn NOAK ~£1-1.5bn	FOAK ~£20bn NOAK ~£15bn
Construction Time (years)	FOAK ~6 NOAK ~4	FOAK ~8-10 NOAK ~6-8
FID	After 4 years (or earlier dep on GDA phase)	After 5 years (after completing GDA)
Fleet benefits (i.e parallel builds)	Achievable	Not achievable in UK

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

The SMR & AMR Framework

Regulatory Readiness

Up to £12m to build capability and capacity

GDA Optimisation for small and advanced reactors

Vendor engagement

Finance

Consideration of recommendations from the **Expert Finance Working Group**.

Siting & Land Access

Role of HMG in enabling sites

Process to be announced soon

International Engagement

UK re-joining GIF

Participation in Nuclear Innovation: Clean Energy (NICE) Future

Bilateral cooperation e.g UK-Poland IGC

Supply Chain Development

£32m for Advanced Manufacturing & Construction Programme

Process to be announced soon

Research & the AMR Competition

Underpinning “need-case” for small nuclear

Up to £44m for Advanced Modular Reactor (AMR) Programme

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

UK Nuclear Landscape
AMR Project and Regulator Cpabillity

- Advanced Modular Reactor (AMR) Feasibility & Development project
- Phase 1 – Funding (up to £4m) to undertake a series of feasibility studies for AMR designs.
- Phase 2 – Subject to further HMG approval, up to £40m may be available for successful selected designs from Phase 1 to undertake applied R&D.

- Parallel project to provide funding to the Nuclear Regulators to increase regulatory capability for modular reactors
- Phase 1 – £7m
- Potential Phase 2 - £5m

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

Financing Small Nuclear

Department f
Business, Ene
& Industrial S

Expert Finance Working Group

Expert group brought together from financial sector, industry, academia and Government

Organisations came forward throughout the process to present commercial/ financing models

Process identified opportunities to integrate financial and nuclear sectors

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

Expert Finance Working Group

- The Group has identified several market conditions which if in place could attract private finance to support small nuclear technologies coming forward as commercially viable propositions.

- The Group issued a series of recommendations that it believes could enable the UK to become a vibrant market place for small and advanced reactor technologies.

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

EFGW recommendations

1. Government should enable small nuclear sector through **clear policy and a market framework**, rather than down-selecting technologies.
2. Government should work with **stakeholders from the energy, nuclear and finance sectors** to develop common understanding of risks associated with small nuclear projects; thereby removing perceived risks acting as barriers to investment and enabling a level playing field with other low carbon energy projects.
3. For technologies capable of being commercially deployed by 2030, Government should **focus resources on bringing FOAK projects to market**. Government should only provide support and grants to enhance UK's existing capability and/or in exchange for Intellectual Property (IP) and other rights investors would expect.

EFGW recommendations

4. Government should establish an **advanced manufacturing supply chain initiative** (as it did with offshore wind) to bring forward existing and new manufacturing capability in the UK and to challenge the market on the requirement for nuclear specific items, particularly Balance of Plant (BOP), thereby reducing the costs of nuclear and the perceived risks associated with it.
5. Government should work with the Office for Nuclear Regulation (ONR) and the Environment Agency (EA) to review regulatory processes to develop an **optimised and flexible approach and through the Generic Design Assessment (GDA)** process allow the market to down-select technologies.
6. Government should **make sites available** to FOAK small nuclear projects and should consider maintaining the UK's existing nuclear licensee capability to de-risk the licensee role for small nuclear projects.

EFGW recommendations

7. For technologies capable of being commercially deployed by 2030, HMG should focus resources on bringing FOAK projects to market by reducing capital costs and sharing risks through:
   - assisting with financing of small nuclear through **new infrastructure fund** (seed funded by HMG) and/or direct equity and/or Government guarantees;
   - assisting with financing of small nuclear projects through **funding support mechanisms** such as Contract for Difference (CfD)/Power Purchase Agreement (PPA) or potentially a Regulated Asset Base (RAB) model, while maintaining supply chain plans required for larger low carbon projects.

For NOAK projects market should be self-sustaining, having learnt lessons of previous large nuclear plant and the small nuclear projects.

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

Next Steps – Energy White Paper

Later this year an Energy White Paper is expected to set out:

- A new approach to financing new nuclear.
- The role SMRs have to play in the energy mix of the future.
- Outcomes of AMR R&D and next steps.
- Further development of the SMR & AMR framework.

Department for Business, Energy & Industrial Strategy

INDUSTRIAL STRATEGY

Thank you for listening

INDUSTRIAL STRATEGY

Nuclear control & instrumentation supply chain roadmaps

Ryan Gilhooley, Topic Lead, Frazer-Nash Consultancy

Project Aim

- Collate and analyse / investigate current C&I vendor technologies and research in order to develop an idea of what the future trends of nuclear C&I are for both existing and future reactor systems.
- To investigate the hazards, faults, mitigations and general safety concerns, which may arise due to the adoption of such new technologies.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Project Description

- Research project based around two questionnaires:
  - **Vendor specific**
    - Looking at technology types currently being produced
    - What will the next generation of technology be?
    - Challenges of implementing new technologies
  - **Licensee specific**
    - Current technology C&I being used
    - Obsolescence issues with current technology
    - Strategies for mitigating obsolescence

© Frazer-Nash Consultancy Ltd. All rights reserved.

Smart Instrumentation

- SMART Instrument is defined using the following criteria:
  - Contains a microprocessor
  - Controls or measures a process variable/ provide actuation
  - Commercial off the shelf (COTS)/ not designed to nuclear standards
  - Has software/ firmware
  - Can be configured by user

© Frazer-Nash Consultancy Ltd. All rights reserved.

FPGA

- What is an FPGA?
- Field Programmable Gate Array
  - Semiconductor device containing programmable logic blocks.
  - Programmed/ configured using Hardware Descriptive Language (HDL) either by manufacturer or ‘in field’ by user.
- Benefits to nuclear
  - Less ‘complex’ than comparable microprocessor equipment.
  - Easier to test and qualify
  - Can provide diversity options.

© Xilinx

© Frazer-Nash Consultancy Ltd. All rights reserved.

FPGA Technology Currently in Use

- UK-ABWR
  - The Class 1 Safety System Logic Control (SSLC) system was designed using FPGA technology in order to meet the latest control capability requirements, whilst also being suitably diverse in technology from other control systems.
- AP1000
  - Advanced Logic System (ALS).This design utilises digital instrumentation and control and automation which is enabled in part with FPGA technology. In the US design variant under construction, the Computer Interface Module (CIM) utilises FPGA technology and is rated as Class 1E.
- Also used in small scale applications for legacy replacement, sensors and actuators
- Hidden devices in use?

© Frazer-Nash Consultancy Ltd. All rights reserved.

Future Use of FPGA

- The use of FPGA for HMI is a relatively new concept. In early 2019, NuScale Power and Ultra Electronics Energy (Ultra) unveiled a:

  "*new safety display and indication system using field programmable gate array (FPGA) technology that represents the first application of FPGA technology for real time display and monitoring in the U.S. commercial nuclear industry.* "
  (NuScale, 2019)

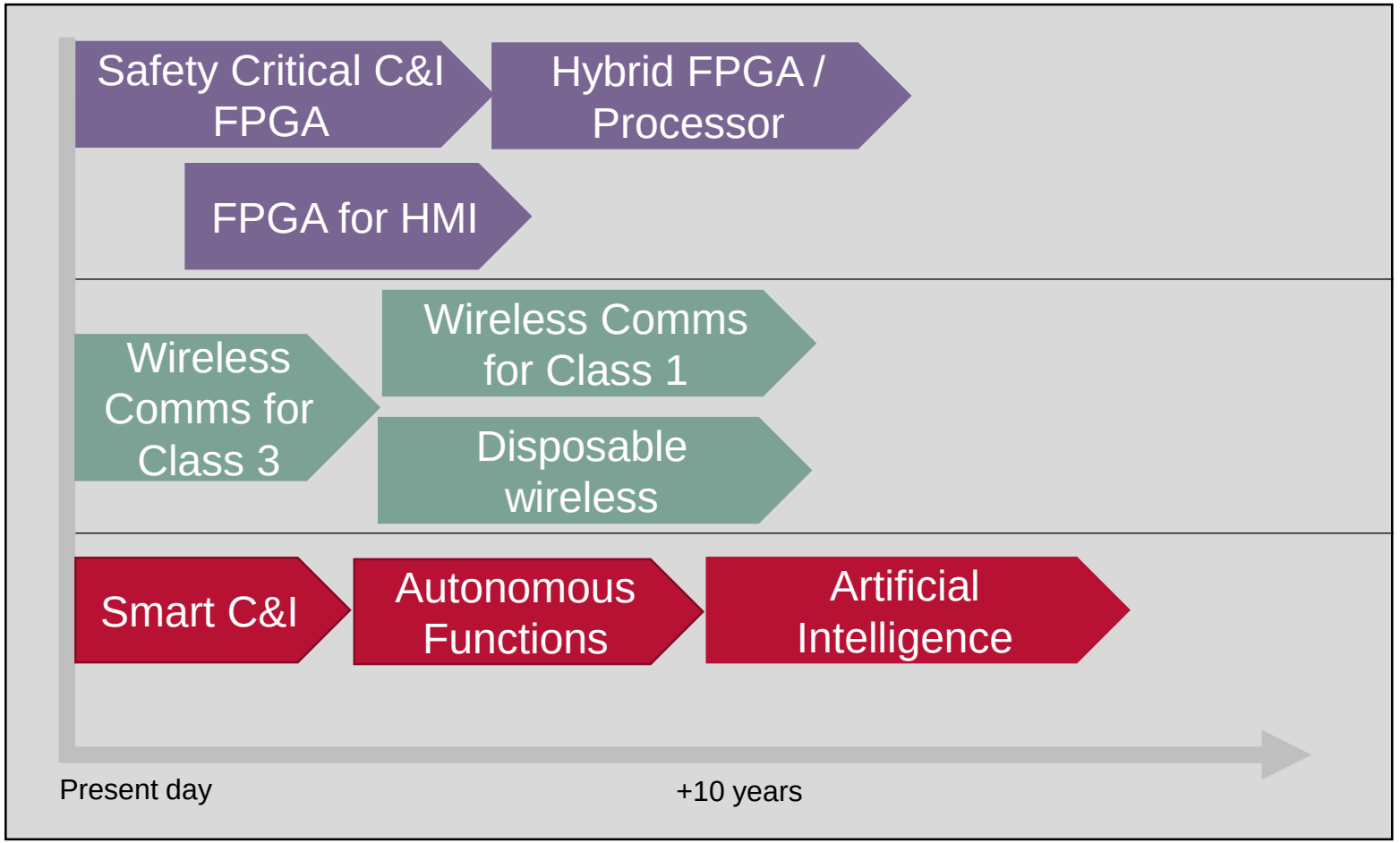
© Frazer-Nash Consultancy Ltd. All rights reserved.

Small Modular Reactor (SMR)

- Focus on simple design, utilising passive systems and inherent characteristics for reactor control.
- Use of COTS equipment where possible.
- Wireless instrumentation, that can be ‘disposable’ with spent fuel.

© Frazer-Nash Consultancy Ltd. All rights reserved.

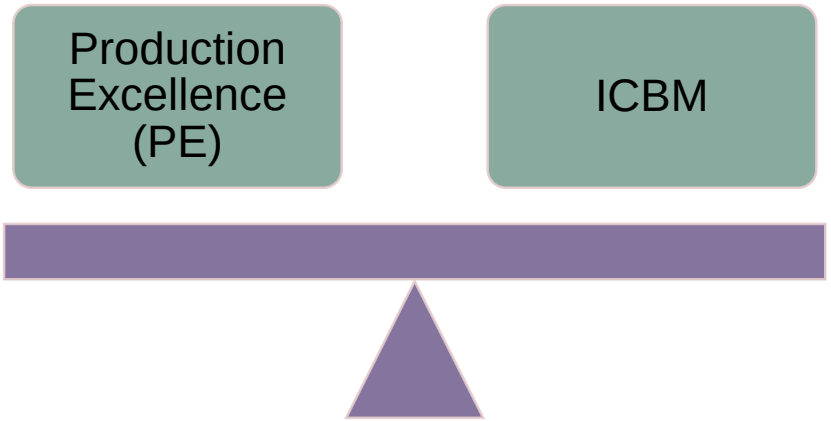
Technology Timeline (production ready)



© Frazer-Nash Consultancy Ltd. All rights reserved.

Challenges of Implementing New Tech

Qualification of Smart Devices & Computer Bases Systems Important to Safety (CBSIS)



Two legged approach to qualifying smart/ complex devices for use in nuclear.

PE

- Involves investigation into who designed the product
- Project lifecycle and process
- Use of software tools
- Design process, V&V, testing etc.
- **EMPHASIS -** Process for qualifying smart instrumentation

ICBM

- Statistical testing
- FMEA

© Frazer-Nash Consultancy Ltd. All rights reserved.

Initial Findings

- Wireless safety instrumentation and communication crucial for SMR
- FPGA based HMI and C&I continued usage
  - Limited manufacturing base is a risk
- Instrumentation with increased processing power
  - Devices performing more diagnostic and analytic functions locally.
  - Local processing comes with the benefit of reducing networking and bandwidth requirements
- Looking forward and possible future research
  - AI enabled FPGA, ways to control/ bound learning
  - Wireless comms in nuclear Class 1 – regulation
  - Qualification of ‘unused’ logic and memory

© Frazer-Nash Consultancy Ltd. All rights reserved.

Interested in how our we can help you integrate our research outputs into your organisation?

For operation and design

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

For regulatory acceptance

We recognise that regulatory acceptance is a key milestone in the adoption of new techniques. The project team welcomes your guidance and knowledge to steer our research to ensure it is aligned with the UK's regulatory regime. We seek to engage with the regulator to provide early insight into proposed methodologies that we hope will form part of future submissions.

For educators

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget. We're looking to engage with undergraduate and post-graduate students and provide material for your teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped for the UK's nuclear future.

Delivery model for centralised testing facility for C&I systems

Simon White, Workstream and Topic Lead, Frazer-Nash Consultancy

Project Aims and Scope

A test facility for C&I integrity testing, [to incorporate a virtual reactor simulator to investigate human factors together] with a statistical testing facility incorporating a high performance workstation for software integrity testing

Explore

- Search existing facilities
- Seek user needs
- Identify options and constraints

Implement

- Develop seed capability ideas
- Equipment specifications
- Supporting development start

Establish

- Install and commission
- Quick wins
- Publicise and support

© Frazer-Nash Consultancy Ltd. All rights reserved.

Motivation and Challenges

- Growing use of SMART devices, which require qualification
- Ageing and obsolescence issues faced by active plant and new build
- The ability to test for functional performance prior to installation in plant is particularly useful.
- Capability currently held across manufacturers' own existing facilities and academic locations
- Leverage economy of scale and co-location

© Frazer-Nash Consultancy Ltd. All rights reserved.

Current UK capability

- Academic and commercial facilities distributed widely
- Excellent coverage for EMC and environmental
- Generally pay-by-hour for commercial testing
- In-house capability prevalent
- No central listing or organisation
- Specialist capability exists for radiation exposure
- Lack of test reactors is an issue

© Frazer-Nash Consultancy Ltd. All rights reserved.

Eliciting user needs

- Issued joint survey to seek user and provider inputs
  - Nuclear licensees, platform and equipment manufacturers
  - Note that roles can reverse depending on specific projects!
- Industry events and relevant experts

- Difficult to gain wide interest
- Testing for nuclear goes beyond most industrial applications
- Significant manufacturers are outside of the UK

© Frazer-Nash Consultancy Ltd. All rights reserved.

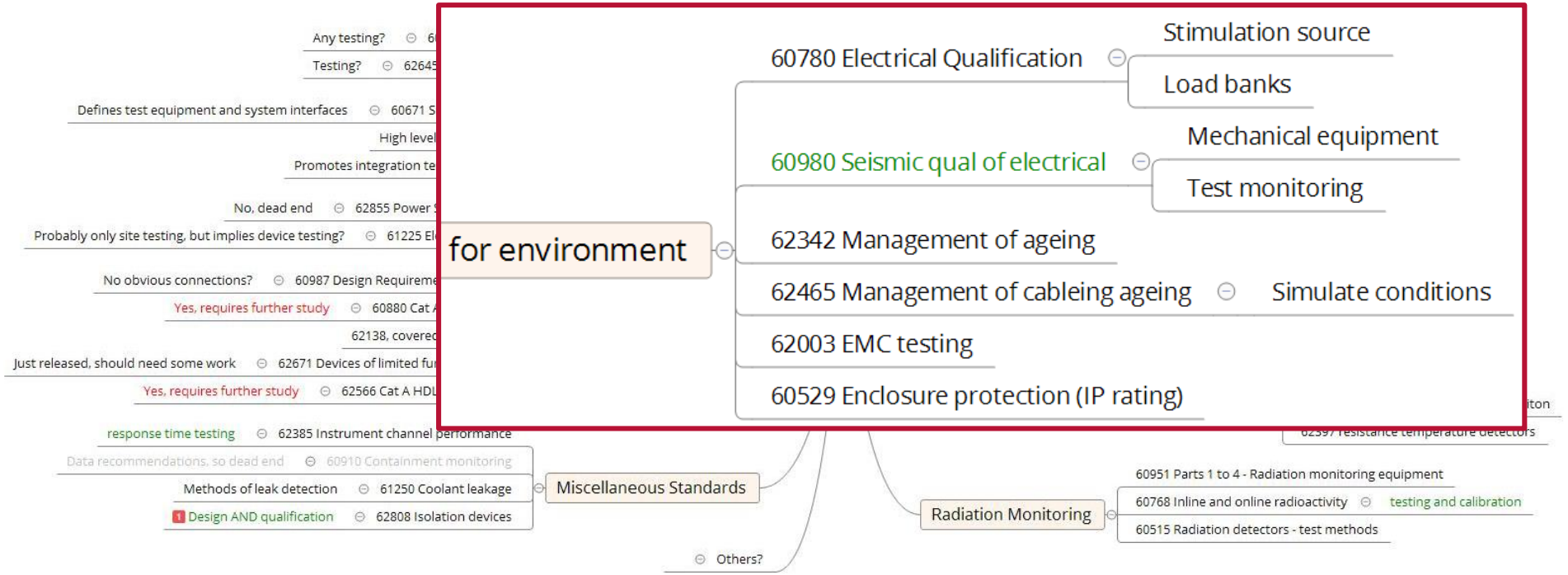
Response summary

- Mixed motivations for centralisation
- Need to respond to SMART device growth
- Broad and diverse requirements
- Generally small scale devices
- Seeking market capacity increase
- Co-location and knowledge transfer
- Time to market improvements
- Risk of common cause failure
- Query operating models
- Query intellectual properly and security

© Frazer-Nash Consultancy Ltd. All rights reserved.

SYSTEMS AND ENGINEERING TECHNOLOGY

Work backwords instead?



© Frazer-Nash Consultancy Ltd. All rights reserved.

Indicative capability

1. Testing of SMART electrical power equipment
   I. Statistical testing with a power interface
   II. Extension to ‘support’ functions such as HVAC
2. Seismic qualification
   I. Based on frequent demand from vendors*
   II. Requirements exceeding industrial or commercial equipment
3. Integration space for cross-vendor integration
   I. Neutral location for testing before site deployment
   II. Supported by appropriate stimulus and IT hardware

© Frazer-Nash Consultancy Ltd. All rights reserved.

Topics under investigation

- Distributed offer or single location
- Nature of capability to be delivered
- Equipment specification, purchasing and commissioning
- The ‘glue’ supporting development
- Leverage existing facilities and capability
- Exploring commercial models and locations

© Frazer-Nash Consultancy Ltd. All rights reserved.

Interested in how our we can help you integrate our research outputs into your organisation?

For operation and design

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

For regulatory acceptance

We recognise that regulatory acceptance is a key milestone in the adoption of new techniques. The project team welcomes your guidance and knowledge to steer our research to ensure it is aligned with the UK's regulatory regime. We seek to engage with the regulator to provide early insight into proposed methodologies that we hope will form part of future submissions.

For educators

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget. We're looking to engage with undergraduate and post-graduate students and provide material for your teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped for the UK's nuclear future.

Advanced safety cases

Allan Fairbairn, Topic Lead, Frazer-Nash Consultancy
Stephen Kidd, Topic Lead, Frazer-Nash Consultancy

1. Overview

R3.7.02 Research Aims

- Development of best practices and tools for the production of ‘optimal’ new safety cases. An optimised safety case is one which minimises the volume of documentation, delivers clarity and coherence (enhancing the understanding of safety), ease of use and ease of updating, promotes efficient regulation and reduces the time/cost from concept design to operation.
- This research is primarily focused on the operational safety case. What would a good safety case look like?
- Dissemination of research and development of outputs to relevant stakeholders.
- Engagement with relevant stakeholders to produce a viable plan for the introduction of outputs into the new build programme.

© Frazer-Nash Consultancy Ltd. All rights reserved.

R3.07.02 Staged Approach

- R3.7.02 will be undertaken in a logical sequence of project phases. These phases are:
  - Phase 1 – Review of Current Methodology
  - Phase 2 – Feasibility Study
  - Phase 3 – Guidance Development
  - Phase 4 – Deployment of Guidance

© Frazer-Nash Consultancy Ltd. All rights reserved.

Why do we need a Safety Case?

- In order to build and operate a NPP in the UK, the operator is required to obtain licenses and permissions from a number of different bodies and importantly in the context of a nuclear safety case, the Office for Nuclear Regulation (ONR) who will grant a nuclear site licence.
- The nuclear site licence is a legal document, issued for the full life cycle of the facility. A set of 36 licence conditions is attached to each nuclear site licence. These conditions require licensees to implement adequate arrangements to ensure compliance.
- The safety case is an operational document and is the tool for communicating to operators and other stakeholders how safety of the plant is maintained during normal operations and foreseeable fault conditions.
- A safety case is rarely a single document, it consists of the entirety of the body of evidence that demonstrates that the hazard presented by a plant or process is adequately controlled and mitigated such that the risk to workers and the public is ALARP.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Safety Case Lifecycle

Major Stages of Facility Lifecycle

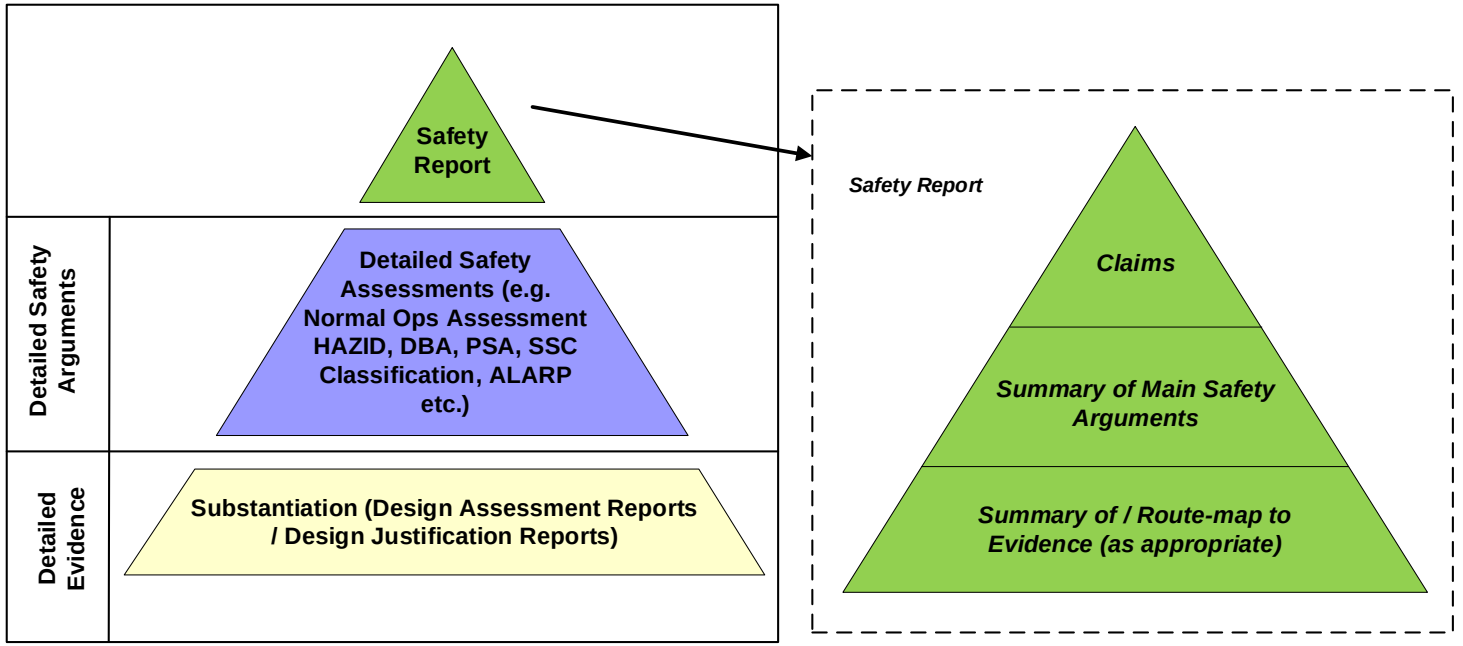
Early Design	Pre-Construction and Installation	Pre-Operation	Operation	Post Operation	Decommissioning
Preliminary Safety Report (PSR)	Pre-Construction Safety Report (PCSR)	Pre-Commissioning Safety Report (PCmSR)	Station Safety Report (SSR) / Operational Safety Case	Post-Operational Safety Case	Decommissioning Strategy
		Pre-Operational Safety Report (POSR)	Modifications		
			Periodic Review		

© Frazer-Nash Consultancy Ltd. All rights reserved.

Safety Case Structure

- Modern safety cases are generally based on a pyramidal structure such as that shown opposite.
- The top level safety report(s) presents the high level arguments, with the appropriate signposts to the detailed arguments and evidence.
- The level of detail increases down the pyramid from the top level safety report down to the low level technical calculations and analysis reports.

Typical Pyramid Safety Case Structure



© Frazer-Nash Consultancy Ltd. All rights reserved.

2. Review of Current Methodology (Phase 1)

So what is the problem?

- Current safety cases can often be perceived as:
  - Cumbersome and complex
  - Expensive to produce and maintain
  - Resource intensive
  - ‘like painting the Forth Bridge’
- High profile inquiries into safety failures such as the Nimrod report have identified issues and failings associated with the safety case processes, content and approvals.
- The output of existing processes is generally adequate, however, there is room for improvement.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Scope of Phase 1 - Review of Current Methodology

Existing Generation

New Build

Other High Hazard Industries

© Frazer-Nash Consultancy Ltd. All rights reserved.

… but also considered.

© Frazer-Nash Consultancy Ltd. All rights reserved.

What does good look like?

- No definitive source of recognised good practice and guidance.
  - IAEA, ONR TAGs and SAPs, OPEX (WNA, WANO, INPO etc.), Safety Directors Forum……
- The review of available guidance & experience derived the following attributes of a good safety case.
  - Accessible – information can be easily accessed by all stakeholders.
  - Auditable – the basis and origin of information can be traced.
  - Clear, Coherent & Intelligible – simple unambiguous language that can be easily understood.
  - Concise, Succinct, Proportionate – appropriate level of detail.
  - Demonstrably Complete – scope clearly defined and fully addressed.
  - Living – kept current.
  - Maintainable – can be easily modified and updated.
  - Representative – reflects the reality of the plant configuration and condition.
  - Valid – any durations or conditions on the validity are specified.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Identified areas of good practice

- A number of areas of existing good practice were identified during the review including:
  - Nuclear
    - Nuclear Safety Principles
    - Living Safety Cases
    - Safety Case Manual
    - Claims, Arguments and Evidence
  - Aviation
    - Standardisation across suppliers, operators and regulators
  - Oil and Gas
    - Industry wide forum to drive improvements in safety

© Frazer-Nash Consultancy Ltd. All rights reserved.

High-level findings

- Existing safety case practices have evolved over several decades
- Generally produce good quality output……..eventually
- No ‘one size fits all’

- Difficulties include:
  - Inconsistencies in approach
    - Different interpretations of guidance
    - No common language
    - No common training or accreditation
  - Methodologies / techniques
    - Similar but different
    - Comparison of output difficult
  - Configuration management
    - Establishing original design intent
    - Accessing supporting information
    - Maintaining living safety case
    - Traceability of ‘golden thread’

- Three themes identified for further consideration in Phase 2

© Frazer-Nash Consultancy Ltd. All rights reserved.

Theme 1: Standardisation

- Everyone does the same things differently, often for good reasons, but sometimes not.
- Opportunity to standardise some aspects of safety case production including:
  - Terminology / glossary – no common language across the industry.
  - High level principles – development of nuclear safety principles is identified as good practice. Some consistency in approach between different organisations would be beneficial.
  - Structure and content – develop guidance on high-level structure and content of safety case documentation, including:
    - High-level structure
    - Level of detail
    - Standard set of document types with purpose and content
  - Tools and methodologies – application of CAE, use of fault and engineering schedules, Safety Case Manual etc.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Benefits and Challenges

- **Potential benefits**
  - Avoid error traps caused by subtle differences in approach and interpretation
  - Increase efficiency and reduce costs by industry having one way of doing things
  - Similar structure and presentation would make production, review and approval more efficient
  - Bigger pool of SQEP resource available
- **Challenges**
  - Standardisation could be detrimental in some areas
  - Would require industry wide buy in and investment
  - Who would be responsible for the development and maintenance of standardised guidance and tools?

© Frazer-Nash Consultancy Ltd. All rights reserved.

Theme 2: Information Management

- Many of the challenges in the production and maintenance of safety cases for current sites are associated with the accessibility and auditability of data
- Challenge for New Build as well as existing generation
- Opportunity to improve
  - Configuration control – how safety cases are modified and maintained.
  - Traceability / auditability – better linking of information.
  - Accessibility / visibility – faster and easier access to information.
  - Consistency – avoid unnecessary duplication, one version of the truth.

© Frazer-Nash Consultancy Ltd. All rights reserved.

Benefits and Challenges

- **Potential benefits**
  - Structured approach to development of the safety case
  - Single data entry ensures consistency
  - User rights allow improved configuration control
  - Provides complete ‘Golden Thread’
  - Data can be searched and manipulated in a variety of ways e.g.
    - Instant Fault Schedule Generation
    - Instant Engineering Schedule Generation
    - Interrogation of claims on individual Structures, Systems or Components
- **Challenges**
  - Could be overly restrictive and make the maintaining the safety case more onerous
  - Would require initial investment to establish useable framework
  - Would require investment in training of safety case team and all other stakeholders
  - Does not improve the quality of a poor safety case

© Frazer-Nash Consultancy Ltd. All rights reserved.

Theme 3: Training and Accreditation

- Following on from theme 1 (standardisation), there are a number of different licensees in the UK nuclear industry, all of whom have their own arrangements for the production and management of safety cases
- There is currently no accepted industry wide training or accreditation of nuclear safety practitioners
- Opportunities to improve the following areas
  - Standardised industry wide training on safety case development and hazard and fault assessment to provide common understanding of the basic safety case building blocks
  - Industry wide accreditation for nuclear safety case practitioners

© Frazer-Nash Consultancy Ltd. All rights reserved.

Benefits and Challenges

- **Potential benefits**
  - Establish a common set of competencies for safety case practitioners.
  - Provide confidence that individuals have a minimum level of training in safety case production tools and techniques.
  - Make it easier for authors, reviewers and regulators to move effectively between projects for different sites/licensees.
  - Reduce costs – individual licensees can focus time, effort and funding on training staff and contractors in the detail of their safety management systems.
- **Challenges**
  - Who would own and fund the training?
  - Who would be the accreditation body? An existing organisation or would a new entity be required?
  - Success would be dependent on industry wide adoption.

© Frazer-Nash Consultancy Ltd. All rights reserved.

3. Next Steps (Phase 2 Scoping)

What next?

- Phase 1 report currently in internal verification – opportunity to capture workshop feedback
- Phase 2 will further investigate a sub-set of the Phase 1 findings prioritised based on Phase 1 output and feedback from key stakeholders
- This is where you come in! We need your feedback on:
  - The topics we have identified in Phase 1 – are they appropriate? Are they of benefit?
  - The proposed way forward – will the output be useful to you?
  - Is there anything missing? – are there any areas or topics you would have expected to see that have not been identified?

© Frazer-Nash Consultancy Ltd. All rights reserved.

Interested in how we can help you integrate our research outputs into your organisation?

For design and operation

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

For regulatory acceptance

We recognise that regulatory acceptance is a key milestone in the adoption of new technologies. The design of this project and how it is delivered capitalises on the delivery partners' decades of experience in supporting regulatory activities. This experience is embedded in the project's outputs that are available to you.

For educators

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget. The project team seek to engage with undergraduate and post-graduate students and provide material for teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped with for the UK's nuclear future.

State-of-the-art review of CCF analysis in UK nuclear PSA

David Watson, Topic Lead, Jacobsen Analytics Ltd

Nuclear Innovation Programme – Safety & Security

Common cause failure (CCF) methodologies

State-of-the-art review and potential next steps

Dissemination Workshop, 27 March 2019

David Watson & Bert Commandeur
(Jacobsen Analytics)

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Overview of the project

Task 1 (Oct18-Apr19)

- **State-of-the-art (SOTA) review** of approaches to assessing CCF
  - How is CCF assessed in UK PSA? What are existing good practices?
  - Comparative review of CCF models

Task 2 (May19-Jun19):

- Send out **survey to participants –** designers, operators, regulators
- **Stakeholder workshop** (early June)
- Identify common problem areas in CCF analysis
- Focus on where **uncertainty in state-of-knowledge** has impacts on design process (cost, time, complexity)

Task 3 (Jun19-Nov19):

- Produce a **"roadmap" identifying relevant guidance** on addressing CCF
- Include existing UK 'best practices'
- Seek to address areas **where current approaches are inadequate**

Please talk to us in the break if you are interested in attending the workshop or would like to receive a copy of guidance reports as they become available.

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Task 1: State-of-the-art Review (1)

What is dependency?

$$\boldsymbol{P(AB) \neq P(A).P(B)}$$

Types of dependency

- **Functional dependency:**
  - E.g. system B will not operate if system A fails.
  - Usually arises because of the way systems depend on each other.

- **Physical dependency:**
  - E.g. high humidity causes redundant equipment to fail.
  - Dependencies not inherent to functioning of the design.

Task 1: State-of-the-art Review (2)

Which dependencies can we explicitly model?

- Shared equipment dependencies
- Functional dependencies
- Some human interactions
- Phenomenological dependencies (e.g. pressure too high for system B injection if system A failed to depressurise reactor)
- Well-characterised hazards (fire, flood, seismic)

Common Cause Failures – accounting for unknown dependencies

There always remains a residual risk from dependencies that are not well-characterised or modelled explicitly.

- Captured as **common cause failures.**

Dependency	Definition	Known dependencies	Unknown dependencies
Functional	Dependency **inherent to design,** operation & maintenance	Cooling, ventilation, signals, common parts, procedures, tools, operators, etc	Causes and failure coupling mechanisms not known – **common cause failure**.
Physical	Common **environmental condition** causes multiple failures	Area events (fire, flood), external events (air plane crash, earthquake), dynamic effects after LOCA, etc	

Task 1: State-of-the-art Review (3)

Key terminology in CCF analysis

Root cause

The root cause is the most basic reason or reasons for the component failure, which if corrected, would prevent recurrence

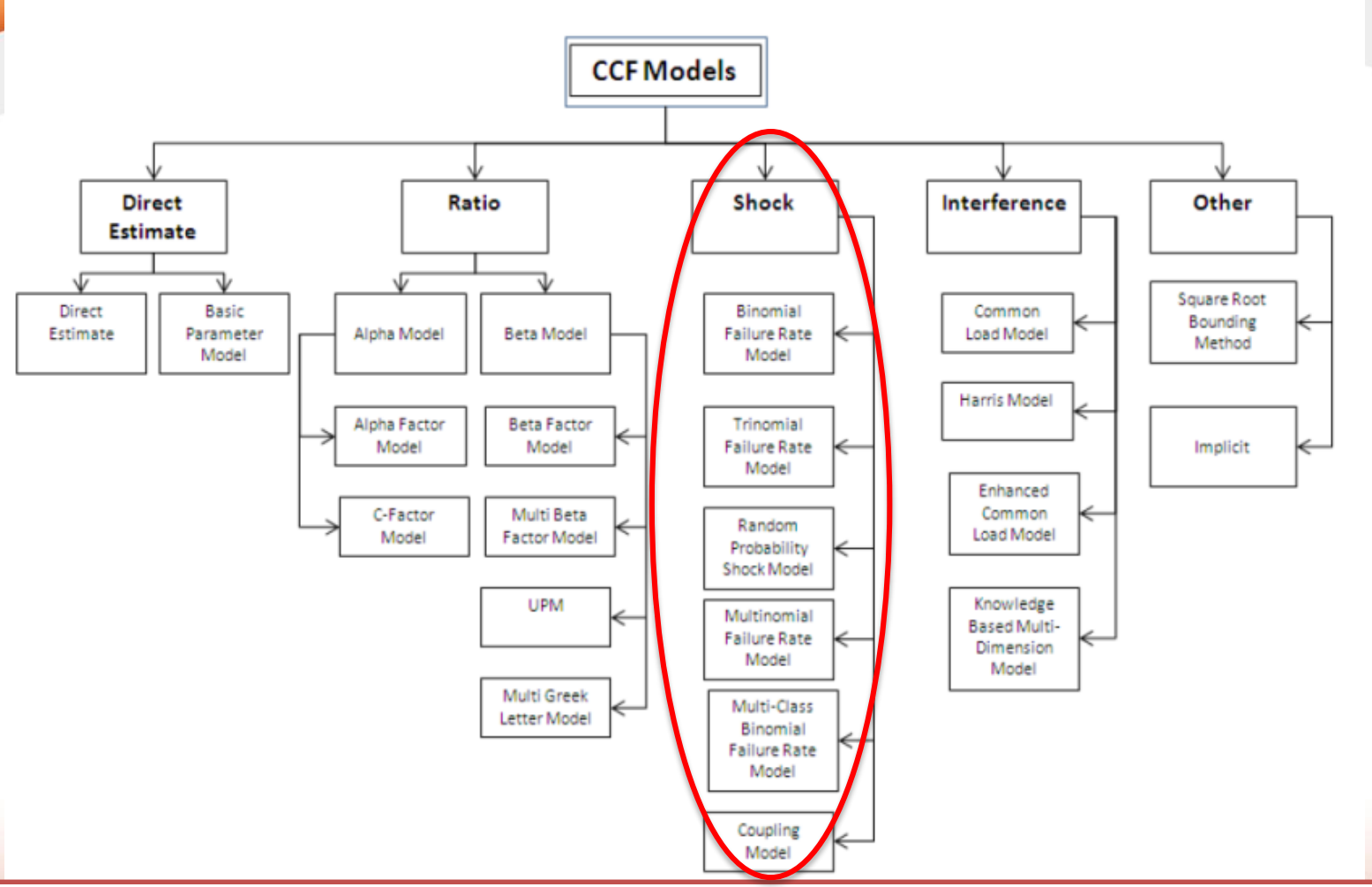
Coupling factor

A coupling factor (or coupling mechanism) creates the condition for multiple components to be affected by the same cause, e.g. sharing the same installation procedure or external environment.

Defences against dependent failures

Properties of a system or components that defend against CCF. This could be strategies that prevent the root causes of failure or strategies that break coupling mechanisms by decreasing the similarity of components and their environment.

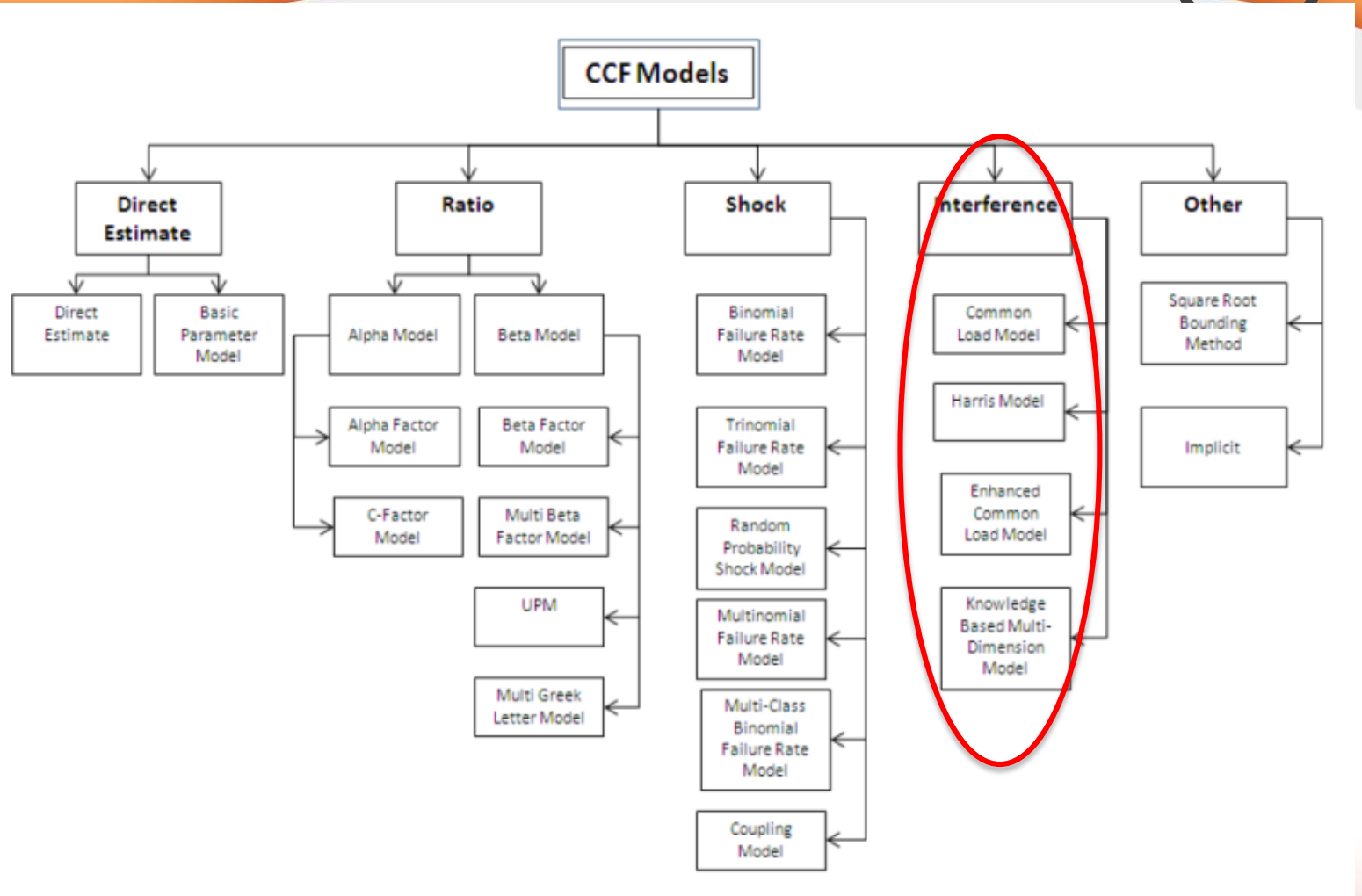
Task 1: State-of-the-art Review (4.1)



Shock Model : model frequency of "shocks" to components, and the probability those shocks cause damage

➢parameters (e.g. shock rate) cannot be estimated directly from data.

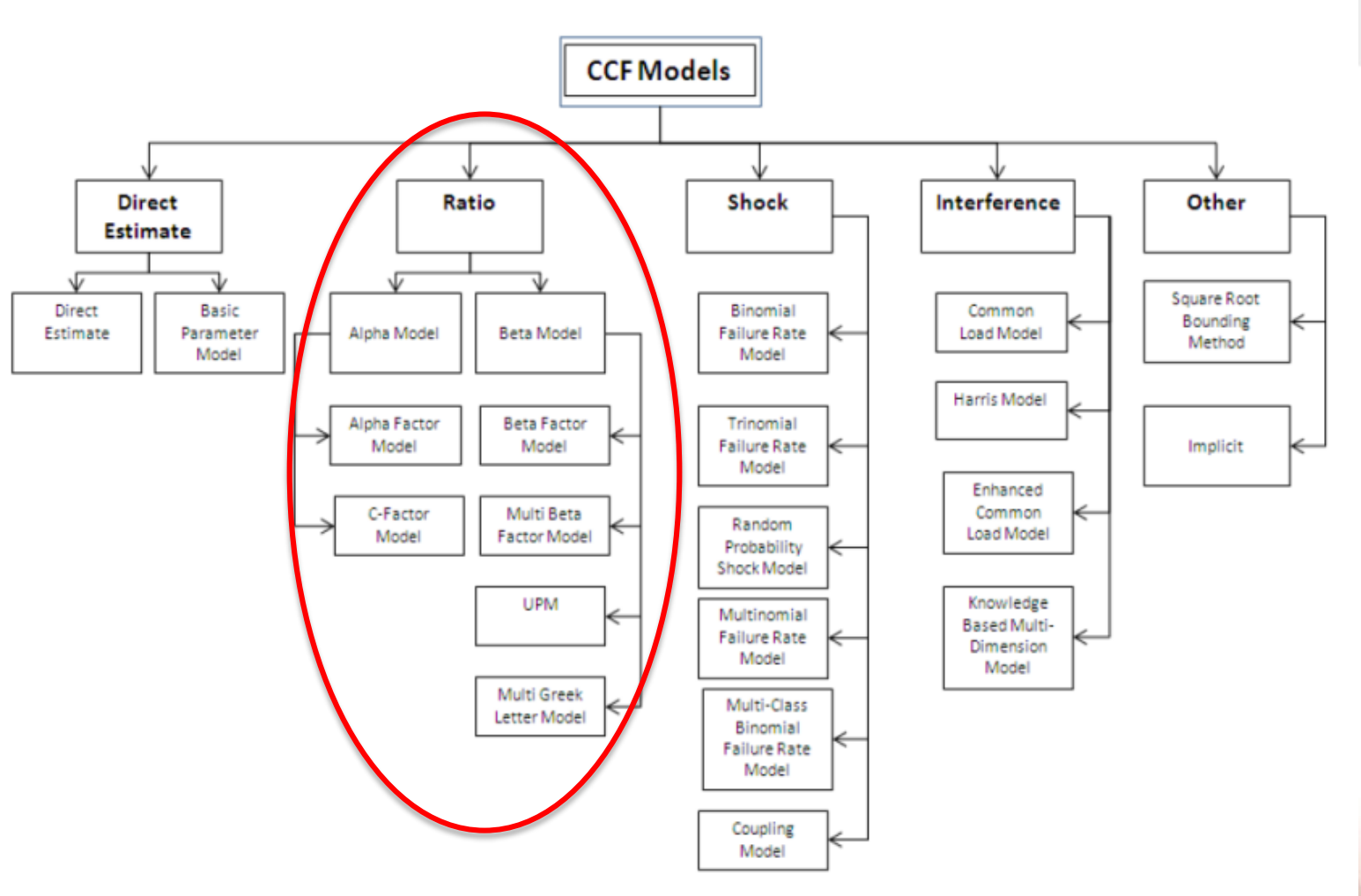
Task 1: State-of-the-art Review (4.2)



Interference Models (Common Load Model): model rate of stresses and component resistances. Useful for modelling highly-redundant systems.

➢not widely used in UK (but is in Nordics & Germany).

Task 1: State-of-the-art Review (4.3)



Ratio Models use simple relationships and historic failure data.

- Ratio models have been widely used in UK PSA.

Task 1: State-of-the-art Review (5)

Ratio models

Beta Factor

- Simplest quantitative ratio model.
- Assumes a constant fraction of total failures can be attributed to CCF.
- Assumes all components in group fail (conservative in larger groups).
- Was widely-used in early years of PSA in US.

Alpha Factor

- More powerful—and closer to best-estimate—than Beta Factor.
- Failure probabilities for *k* out of *n* components in group.
- Much of CCF data collection done with this model in mind.
- Amenable to uncertainty analysis.

Unified Partial Method (UPM)

- Qualitative method relying on judgement.
- Like quant. Beta Factor, assumes simple relationship between independent and dependent failures.
- Unlike Alpha and Beta, allows credit to be taken for known defences against CCF.

Task 1: State-of-the-art Review (6)

Comparative review of currently-used models

- UPM, Coupling Model, Extended Common Load Model, Beta Factor, Multiple Greek Letter (MGL) and Alpha Factor
- Criteria included: ease of use, realism, mathematical basis, reliance on expert judgement, availability of suitable data and handling of uncertainty
- No one model best in all scenarios

Initial review of good practice

- Highlighted existing UK good practice
- Alpha Factor considered good practice when suitable data available
  - Best-estimate measure of risk, real-world data.
  - Allows for uncertainty analysis.
- However, UPM good practice when suitable data **not** available.
  - Relative measurement of risk.
  - Systems most vulnerable to CCF identified, allowing designer/operator to eliminate CCF root causes and/or break coupling factors.

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Initial feedback from participant surveys (1)

Stakeholders who've agreed to participate in project:

Project participants asked to take part in a survey to be used to inform the discussions at the workshop.

Amongst other things, survey asks:

- How CCF is currently assessed in each organization, including which data are used.
- To describe any areas where they believe currently-available methods are not sufficient to quantify best-estimate CCF parameters.
- To outline where such uncertainty impacts on the design processes for safety-significant equipment, including on capital and operational costs.
- To explain where limitations of currently available assessment methodologies are having a significant impact on risk insights

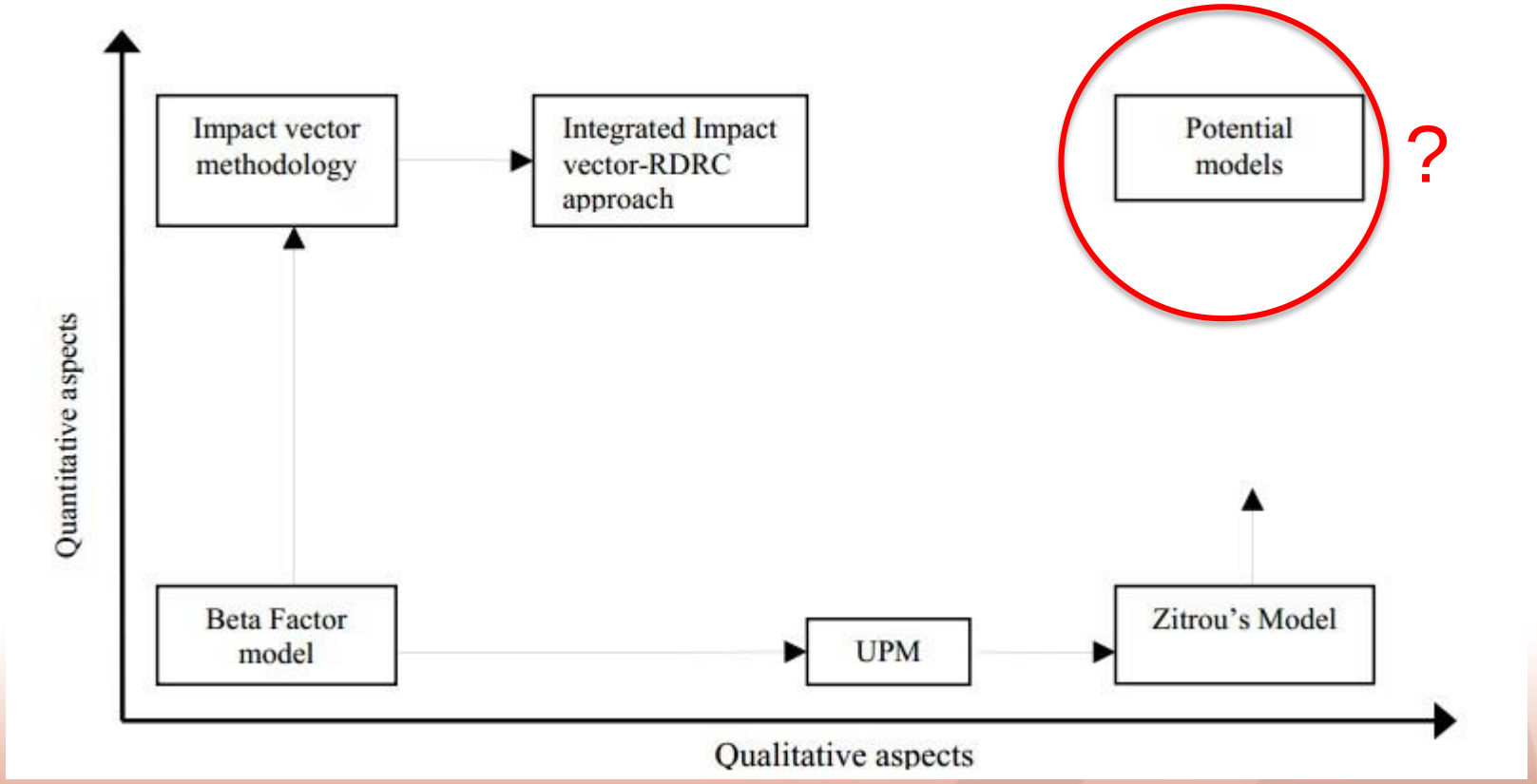
Initial feedback from participant surveys (2)

Initial survey responses from highlight areas to explore at workshop:

- Digital I&C systems CCF
- CCF large groups of components
- Modelling inter-system CCF using Risk Spectrum and CAFTA
- Validation of UPM using real-world data
- Good practice guidance on e.g. sensitivity analysis
- Accounting for new manufacturing processes or vulnerabilities (e.g. cyber) when assessing CCF.
- Managing PSA/CCF when safety systems are passive/inherent.
- Simultaneity of CCF events (crediting recovery actions)

Possible next steps (1)
Quantitative vs qualitative?

Are there ways to combine the strength of these two model types?



Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Possible next steps (2)
Could UK industry make use of the OECD ICDE project?

- The OECD runs multinational collaboration project on CCF, known as ICDE.
- US, France, Canada, Japan, Finland, Germany, Sweden, Spain and S Korea are members. UK currently not participating.
- Member countries have access to:
  - the best available CCF data, including info on root causes and coupling factors.
  - Development of defences against root causes such as indicators for risk-based inspections.
- Some qualitative reports are publicly available – Tasks 2 and 3 will explore how UK industry can best make use of these.

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

What are some of the wider benefits of this project?

- As the project progresses, PSA analysts from the participating organisations will have the opportunity to meet and learn from each other.
- This will hopefully lead to further industry collaboration in future.
- The project authors have made new connections with nuclear safety teams in upcoming UK ANR and SMR designers.

Thank you for listening!

Question & Answer Session

Interested in how our we can help you integrate our research outputs into your organisation?

For licences and reactor developers

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

For regulators

We recognise that regulatory acceptance is a key milestone in the adoption of new techniques. The project team welcomes your guidance and knowledge to steer our research to ensure it is aligned with the UK's regulatory regime. We seek to engage with the regulator to provide early insight into proposed methodologies that we hope will form part of future submissions.

For educators

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget.
We're looking to engage with undergraduate and post-graduate students and provide material for your teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped for the UK's nuclear future.

Jacobsen analytics
ENGINEERING RISK SOLUTIONS

Common categorisation and system classification methodologies and tools

Mandy Roberts, Topic Lead, Rolls Royce

Common Methodology for Security Categorisation and Classification

Reactor Design: Safety & Security Research & Development Dissemination Workshop

Mandy Roberts, Safety and Licensing Team Leader, Rolls Royce (Civil Nuclear UK)

27 March 2019

This information is provided by Rolls-Royce in good faith based upon the latest information available to it; no warranty or representation is given; no contractual or other binding commitment is implied.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Common Methodology for Security Categorisation and Classification

Contents

1. Introduction
2. Background
3. Programme
4. Results so far
5. Outlook

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Objectives and Benefits

- Safety function categorisation and classification of structures, systems and components (SSCs) is a **UK regulatory expectation**
  - It can enable a proportionate approach to facility design and operation with respect to safety.
- This project aims to develop **complementary common methodologies and tools** for functional categorisation and SSC classification which may be applied to security (including sabotage).
- May inform the **Graded Approach** required by ONR's Security Assessment Principles (SyAPs)

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Background – Safety Cat & Class

- 3 Steps:

1. Categorise functions (A, B, C)
Category depends on consequence and likelihood

2. Classify equipment (1, 2, 3)
Class depends on contribution to safety function
(principal, significant, other)

3. Assign **architecture requirements, codes and standards**, and assign **hazard-withstand requirements**

- **Hope to do something simplistic for security**

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Programme

Project Phase	Task Description	Status
Phase 1	International Literature Search report	Complete (Jan 2019)
	1.2A Forum Engagement Plan technical note &	Complete (Jan 2019)
	1.2B Review of current UK Practices report	Complete (Jan 2019)
	High level requirements capture and report	Complete (Feb 2019)
	Rationalised, lower-level requirements (from stakeholders) and summary report	In progress (29 March 2019)
	Plan to develop the methodology and tools, and how to compare it to the requirements technical note.	In progress (5 April 2019)
Formal hold point		
Phase 2	Methodology for function categorisation, equipment classification, through-life implications (e.g. codes and standards) and comparison with requirements report.	18 September 2019
	Plan for the dissemination of material technical note	18 September 2019
	Present at formal dissemination event	30 April 2020

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Stakeholder Engagement Forum

- Set up a stakeholder group with security representatives from the following organisations:
  - Context
  - EDF Energy
  - Frazer Nash Consultancy
  - GNS
  - Magnox
  - Moltex Energy
  - NNL
  - ONR
  - Sellafield
  - Springfields / Westinghouse
  - VAI forum, which in itself is a group of various organisations – currently communicating via their chair
- Engagement is entirely voluntary
- Benefit for the forum is to engage is to shape the outcome, which they might end up using

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

International Literature Search

Summary of findings:

- Some parallels were found between safety and security
- Safety categorisation relatively straightforward – easy to identify significance of SSC contribution to safety
- Less obvious in security
- New methodologies related to security may link existing security jargon, but may be more **evolutionary** rather than revolutionary

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Current UK Methodologies

Summary of findings:

- Security classification of programmable I&C systems (Operational Technology, OT) is well established through IEC 62645

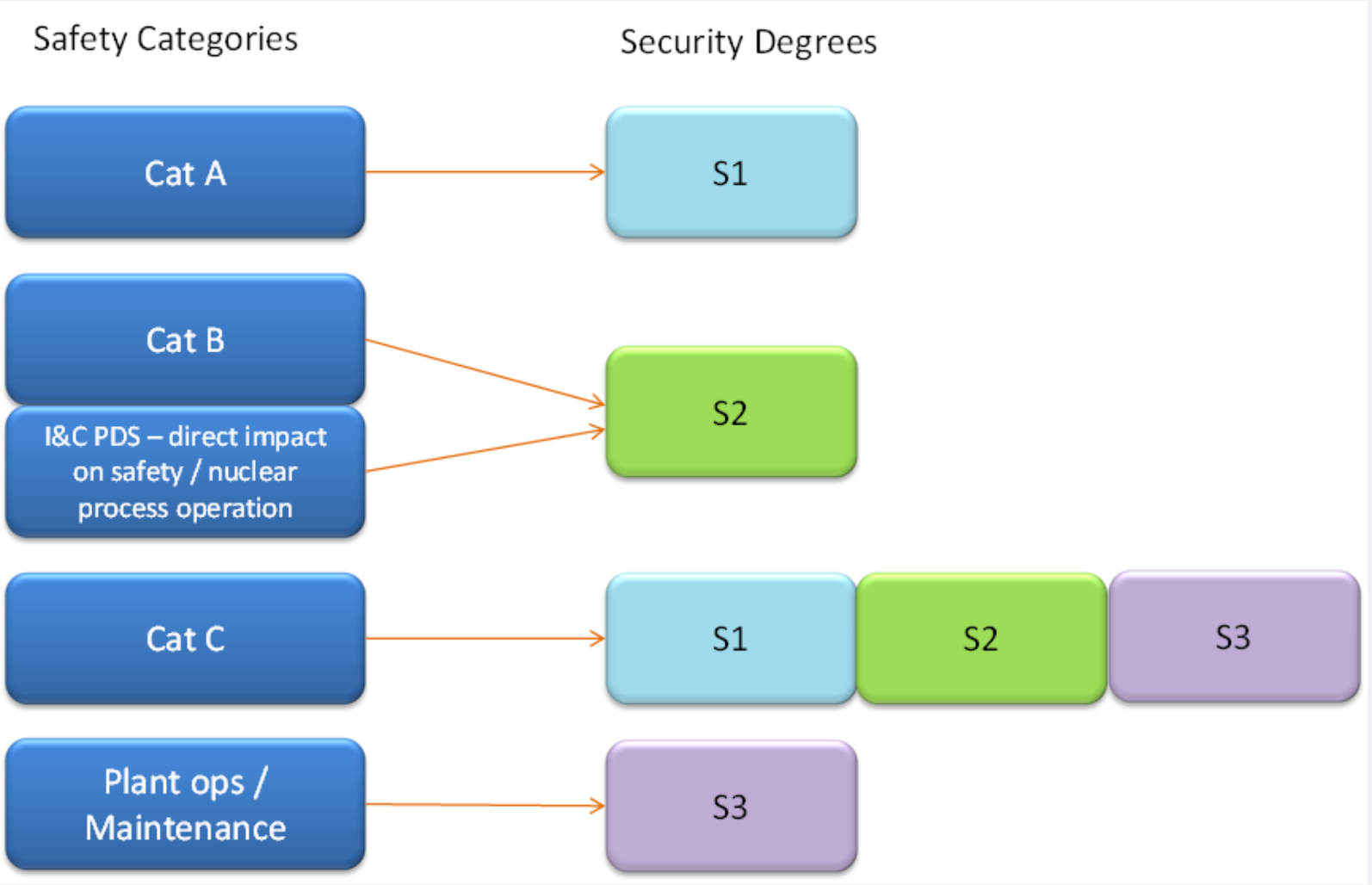
- IEC 62645 does not separate categorisation and classification steps, but combines them into a **single step**

- Graded approach reflected in other standards*, as well as a framework to help in the coordination between safety and cybersecurity requirements**.

* IEC 60880; 62138; 62566 **IEC 62859

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Current UK Methodologies (continued)



- IEC 62645: 3 security degrees S1, S2, S3 (not “classes”), with S1 being the highest

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

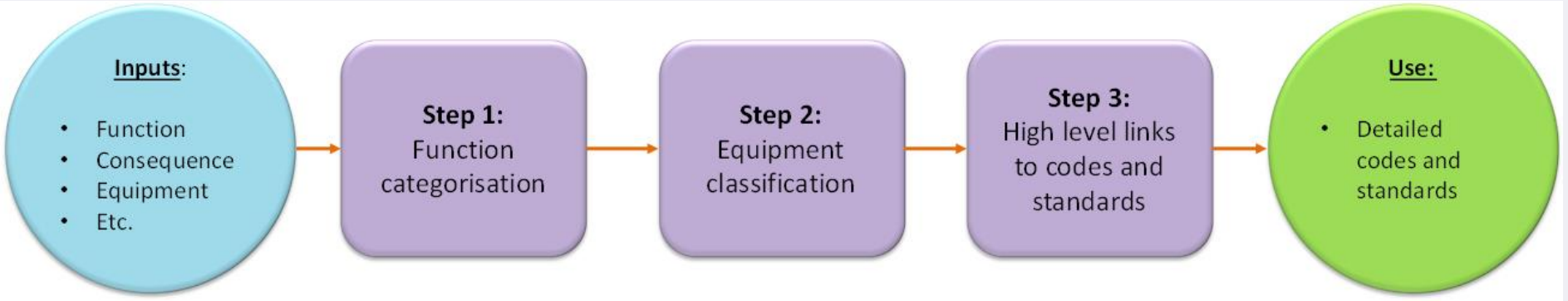
Overview

- Simple, easy to use
- Link to existing “security speak”
- May have slightly different schemes for:
  - Theft
  - Sabotage
- May suggest 2 or 3 methodologies (from very simple to more complex), where licensees can chose depending on their circumstances

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Requirements Capture Overview (continued)

- For a more complex methodology we envisage a 3-step process:



Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Step 1: Categorisation of Functions

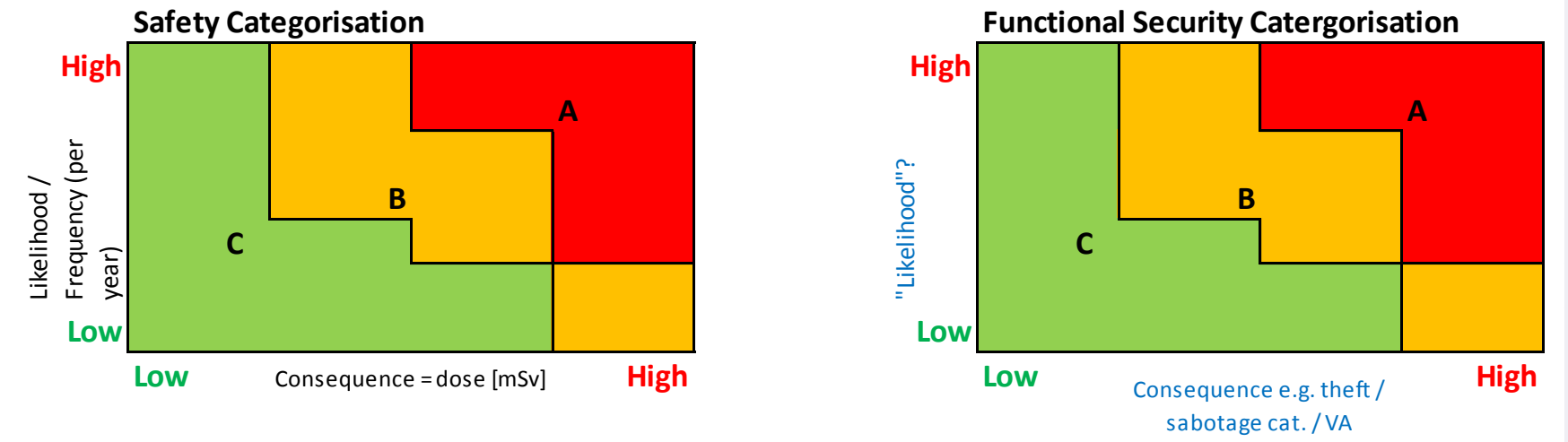
- Outputs: For more complex methodology expect to use A, B, C
- Categorisation (of function) depends on:
  - Consequences / outcomes
  - Categorisation for theft / security group
- Categorisation for sabotage (= VAI)
- Likelihood / potential extent of requiring the function

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Possible Methodologies

Step 1: Categorisation of Functions

- **Option 1** (complex) - draw parallels from safety cat & class approaches



- **Option 2** (medium complexity) - link directly to postures, e.g. Routine = C, Robust = B, Fortified = A

- **Option 3** (simplest) – may be a combination of Options 1 and 2

- Other options may appear as the project progresses

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Step 2: Classification

- For more complex methodologies, classification (of equipment) depends on:
  - Category of function (from previous step)
  - Contribution of equipment to that function
- For these methodologies, expect to use 1, 2, 3
- Challenges:
  - I&C already has an established process (IEC 62645)
  - Also need to classify operator actions (e.g. response force)

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Possible Methodologies

Step 2: Classification

- Option 1: draw parallels from safety methodology

Contribution	Function: **Cat A**	**Cat B**	Cat C
Principal	**Class 1**	**Class 2**	Class 3
Secondary	**Class 2**	Class 3	Class 3
Other	Class 3	Class 3	Class 3

- Option 2: somehow additive?

- Other options may appear as the project progresses

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Step 3: Link to Architecture, Codes and Standards etc.

- Link to existing classification schemes, e.g.
  - I&C has S1 to S3
- May need to consider:
  - Hazard withstand
  - Reliability

    Note: likely to be much less onerous targets than for safety, because of operator involvement in all functions
- “Architecture” requirements will make use of postures where possible
  - “multiple”, “rapid”, etc.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Summary of future activities

- Initially the idea was to see whether parallels could be drawn from safety cat & class
  - On the basis that the ONR's Security Assessment Principles (SyAPs) expectations are similar to Safety Assessment Principles (SAPs)
- However, some stakeholders gave very strong feedback, e.g.
  - They would not be able to implement any even vaguely complex methodology;
  - It is not clear that assigning more labels (categories, classes) in addition to already existing labels (theft cat, sabotage cat/ VAI, outcomes, postures) would aid their security cases
- Therefore, we may end up with 2 or 3 methodologies, ranging from something very simple to something more complex, from which licensees could select.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Nuclear Exploitation

Interested in how our we can help you integrate our research outputs into your organisation?

In design and operation

Our research can provide benefits at any stage of a reactor life-cycle. We are keen to share our engineering approaches to safety and security in reactor design and operation with both current licensees and future reactor developers. Our research is demonstrating the cost savings that can be achieved using new approaches to treating safety and security.

In regulatory acceptance

We recognise that regulatory acceptance is a key milestone in the adoption of new technologies. The design of this project and how it is delivered capitalises on the delivery partners' decades of experience in supporting regulatory activities. This experience is embedded in the project's outputs that are available to you.

In education

Advanced technologies are only one part of delivering a thriving future UK nuclear sector. Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget. The project team seek to engage with undergraduate and post-graduate students and provide material for teaching programmes. The project is scoped to provide students with the knowledge and insights they need to be equipped with for the UK's nuclear future.

Non-Confidential Information
© 2019 Rolls-Royce
Not Subject to Export Control

Exploitation: how can we help?

James Cornish, Exploitation Manager, Frazer-Nash Consultancy

Exploitation: How can we help?

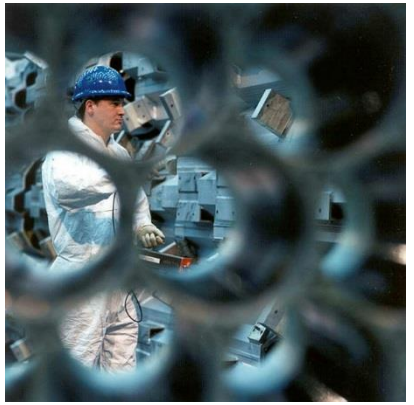
Aim

To answer the three key questions:

1. What is exploitation?
2. Why is it important?
3. How do we make it happen?

How

- Exploitation: what and why?
- For design and operation
- For policy makers
- For equipment manufactures
- For educators
- How you can get involved



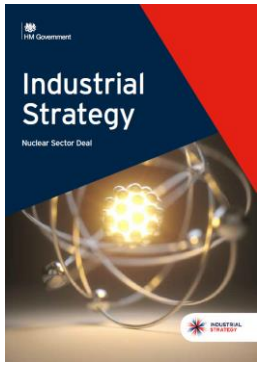
© Frazer-Nash Consultancy Ltd. All rights reserved.

Exploitation: What & Why

What

Collaborating with industry, academia and government to drive the adoption of our work to bring measureable benefits to UK PLC.

Why



- Investment is a once in a generation opportunity.
- Our sector needs to demonstrate the value of the investment, why is it worth investing?
- Why we need to engage with you; to ensure we are focused on delivering research outputs that bring benefit to your organisations.

© Frazer-Nash Consultancy Ltd. All rights reserved.

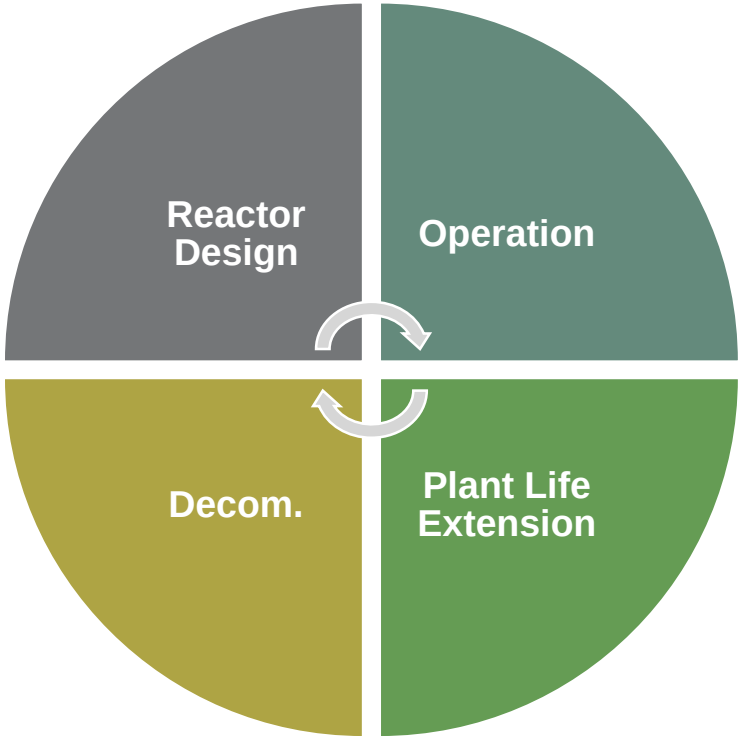
For Design & Operation

- Our research is applicable throughout the reactor lifecycle.

Gen IV	SMRs	AMRs
Gen III+	AGRs	PWRs

- As you have seen the research is aimed to:

↑ Security Performance	↓ Cost
↑ Safety Performance	↓ Time



© Frazer-Nash Consultancy Ltd. All rights reserved.

For Design & Operation

You need to justify any investment required to adopt a new approach.

We can help!

Understand → Explore → Investment Case

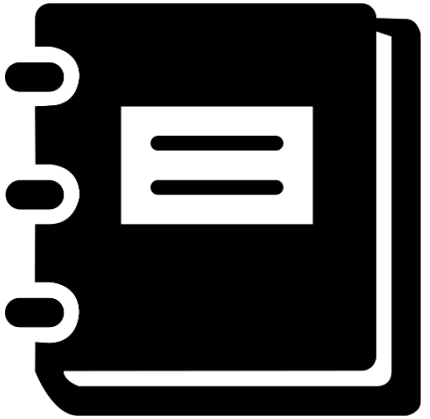
© Frazer-Nash Consultancy Ltd. All rights reserved.

For Policy Makers

- Some our research findings may impact existing policy.

Existing Policy	Areas for new policy	Evidence

- We can help you interpret the research finding to help you make decisions based on evidence.
- Two way engagement.
- Key to ensuring adoption by industry.



© Frazer-Nash Consultancy Ltd. All rights reserved.

For Educators

- Our future workforce needs to be equipped with the expertise to deliver future projects safely and on budget.

  - **Undergraduate study**
  - **Postgraduate study**
  - **Doctoral & Post-Doctoral Research**

© Frazer-Nash Consultancy Ltd. All rights reserved.

Feedback & Getting Involved

- We value your feedback today and on the overall project.
- Opportunity to feedback and indicate which projects you are interested.
- Specific topic leads will be in touch with you about what's going on.

www.innovationfornuclear.co.uk

www.innovationfornuclear@fnc.co.uk

© Frazer-Nash Consultancy Ltd. All rights reserved.

Thank you
Have a safe journey home

Nuclear Innovation Programme – safety and security

Innovationfornuclear@fnc.co.uk

www.innovationfornuclear.co.uk