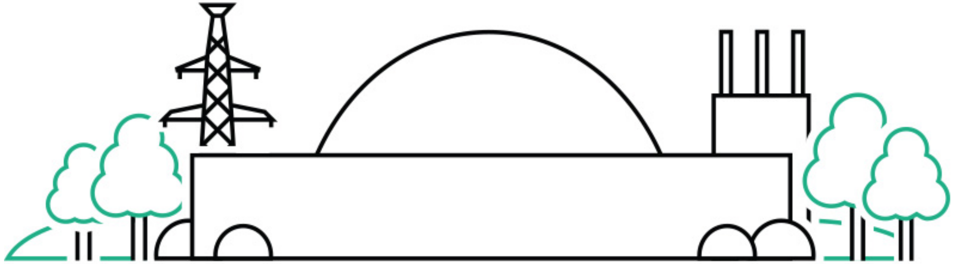
Office for
Nuclear Regulation

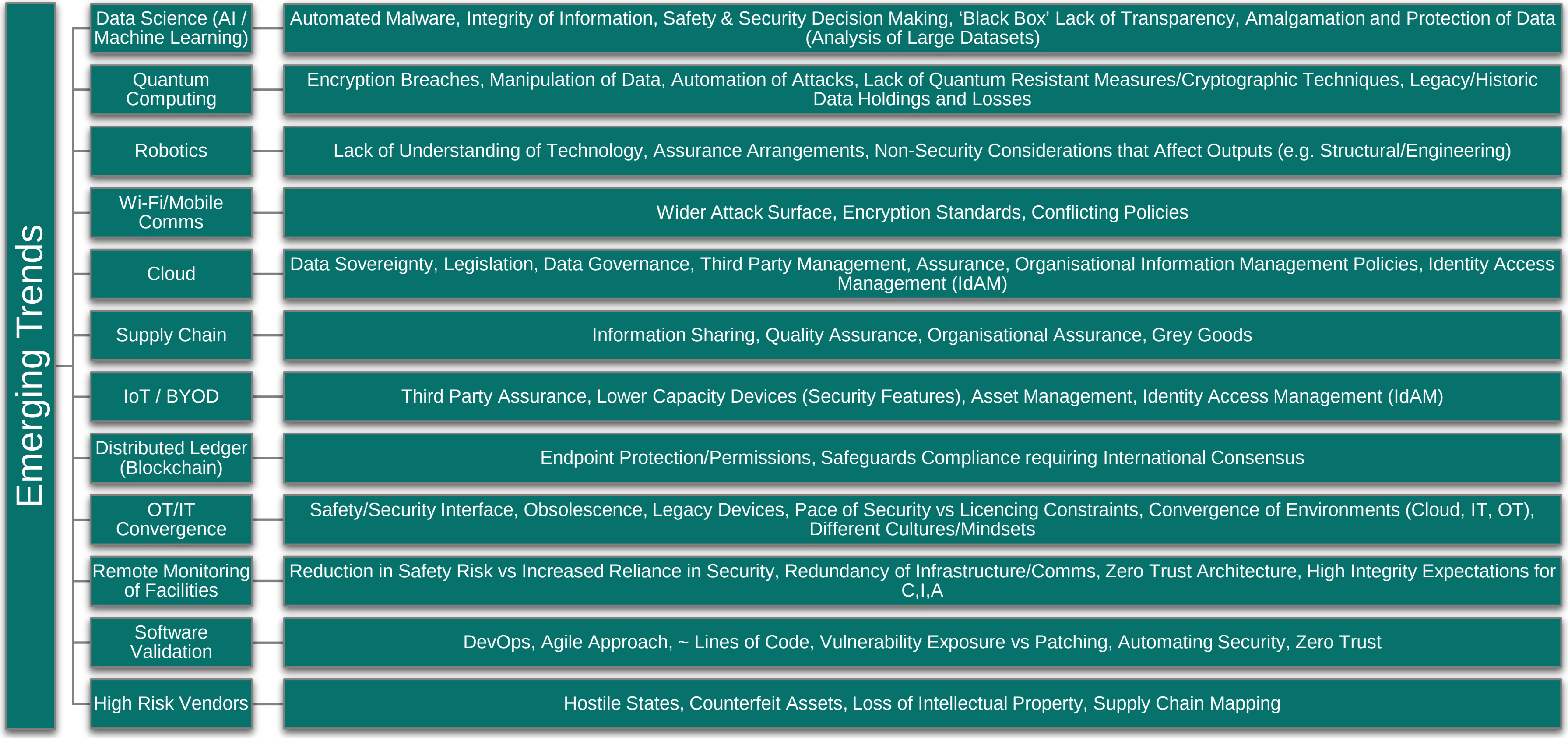
Regulating AI for Nuclear Security

Warren Cain
Superintending Inspector
Nuclear Transport & Storage

8th February 2024



What Emerging Trends Will Require Changes to Regulations?



Emerging Trends

Data Science (AI / Machine Learning)	Automated Malware, Integrity of Information, Safety & Security Decision Making, 'Black Box' Lack of Transparency, Amalgamation and Protection of Data (Analysis of Large Datasets)
Quantum Computing	Encryption Breaches, Manipulation of Data, Automation of Attacks, Lack of Quantum Resistant Measures/Cryptographic Techniques, Legacy/Historic Data Holdings and Losses
Robotics	Lack of Understanding of Technology, Assurance Arrangements, Non-Security Considerations that Affect Outputs (e.g. Structural/Engineering)
Wi-Fi/Mobile Comms	Wider Attack Surface, Encryption Standards, Conflicting Policies
Cloud	Data Sovereignty, Legislation, Data Governance, Third Party Management, Assurance, Organisational Information Management Policies, Identity Access Management (IdAM)
Supply Chain	Information Sharing, Quality Assurance, Organisational Assurance, Grey Goods
IoT / BYOD	Third Party Assurance, Lower Capacity Devices (Security Features), Asset Management, Identity Access Management (IdAM)
Distributed Ledger (Blockchain)	Endpoint Protection/Permissions, Safeguards Compliance requiring International Consensus
OT/IT Convergence	Safety/Security Interface, Obsolescence, Legacy Devices, Pace of Security vs Licencing Constraints, Convergence of Environments (Cloud, IT, OT), Different Cultures/Mindsets
Remote Monitoring of Facilities	Reduction in Safety Risk vs Increased Reliance in Security, Redundancy of Infrastructure/Comms, Zero Trust Architecture, High Integrity Expectations for C,I,A
Software Validation	DevOps, Agile Approach, ~ Lines of Code, Vulnerability Exposure vs Patching, Automating Security, Zero Trust
High Risk Vendors	Hostile States, Counterfeit Assets, Loss of Intellectual Property, Supply Chain Mapping

ONR’s Approach to Regulating Innovation

- Our outcome focused regulatory regime is technology neutral and therefore does not seek to prescribe individual design solutions.
- This enabling approach provides a constructive, open and safe environment for innovative solutions to thrive.
- As a regulator we are expected to minimise regulatory burden and be open to innovation, however that openness cannot come at any cost. Ultimately, we are here to protect society.
- We support industry to realise the benefits of new technologies and novel approaches by providing a stable, yet progressive, regulatory regime that enables cost-effective safety and security.
- This approach aligns to UK Government expectations to deliver a proportionate regulatory approach that removes unnecessary burdens and provides confidence to those we regulate.

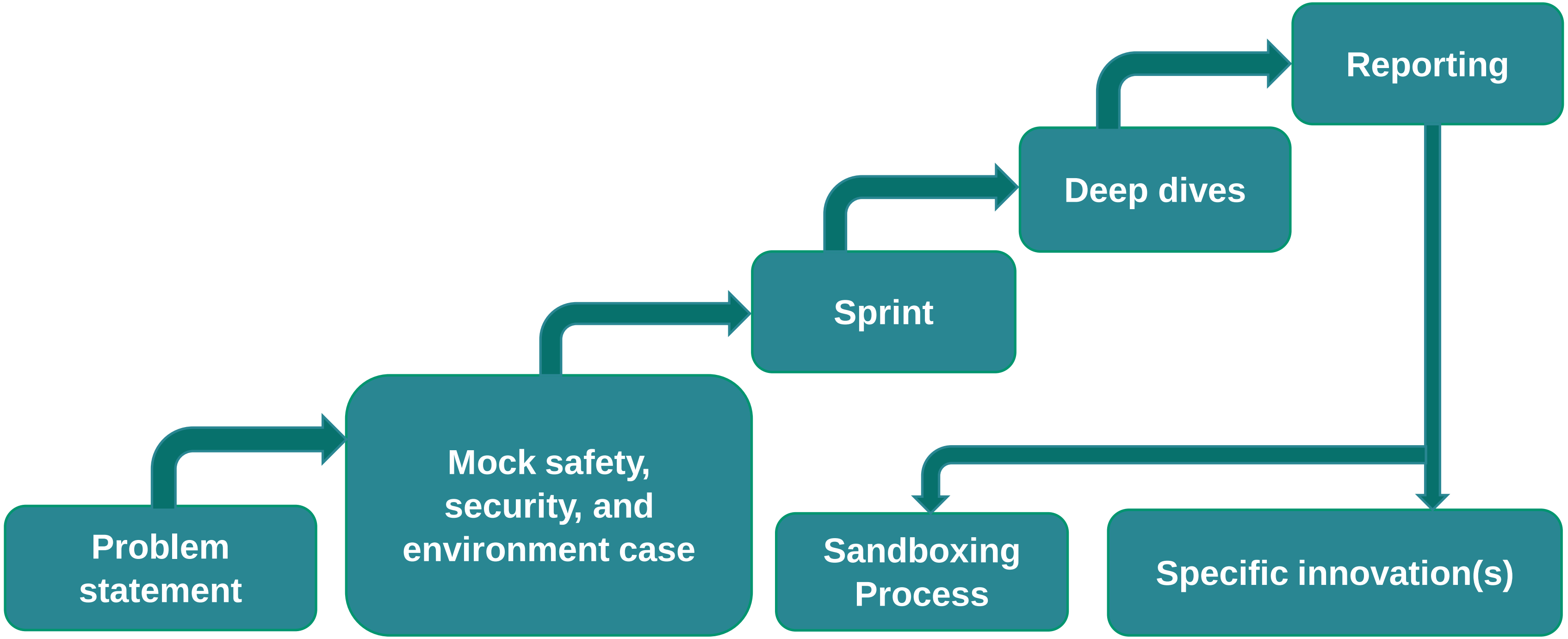
ONR Office for Nuclear Regulation

Approach to regulating innovation

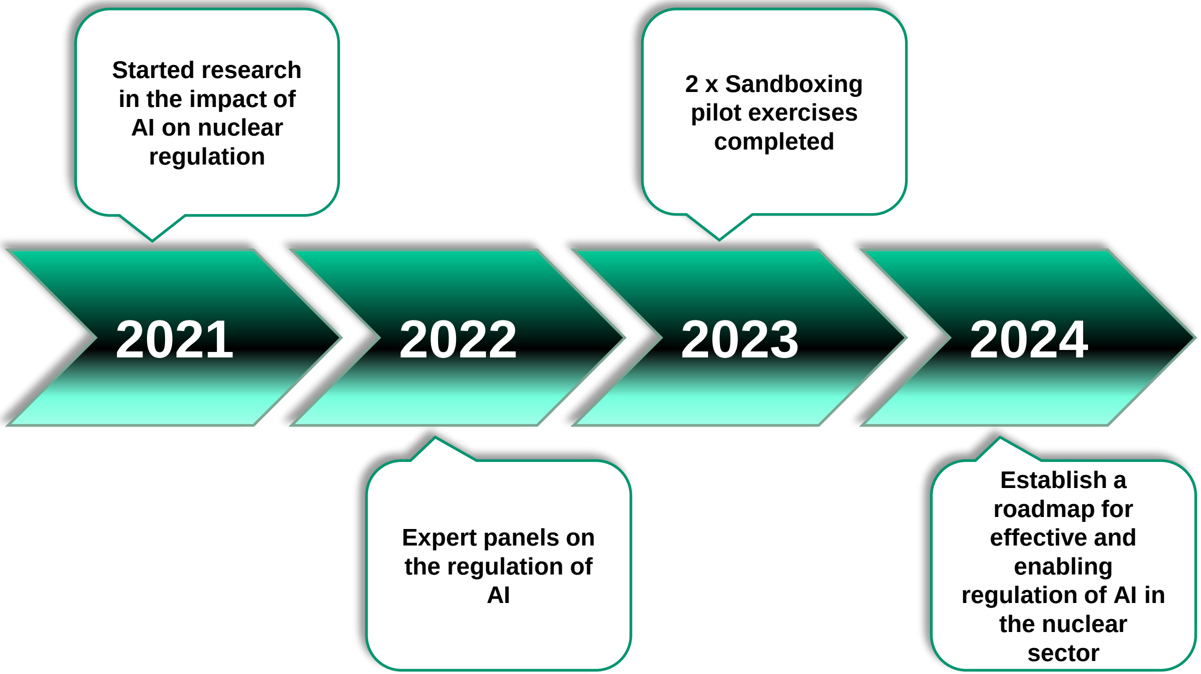
Regulatory Sandboxing

- Although our outcome focused approach is inherently flexible to accommodate innovation, dutyholders must adequately demonstrate that safety, security and environmental requirements have been met.
- This can be challenging for particularly novel innovations where there is little relevant good practice and experience of deployment to draw on.
- Sandboxing gives regulators, academia and industry the opportunity to work together to explore potential deployments and provides important input for the development of regulatory frameworks.
- It is now a key element in ONR’s approach to enabling innovation where it is in the interest of society and consistent with regulatory expectations.

Regulatory Sandboxing Process



Timeline of AI Regulatory Innovation at ONR



2021

Started research in the impact of AI on nuclear regulation

2022

Expert panels on the regulation of AI

2023

2 x Sandboxing pilot exercises completed

2024

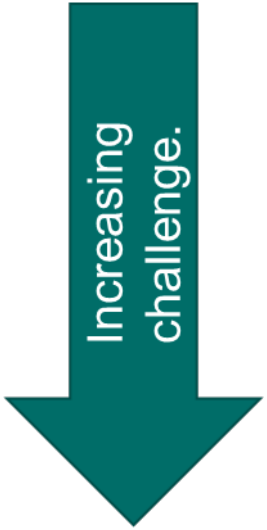
Establish a roadmap for effective and enabling regulation of AI in the nuclear sector

www.onr.org.uk/documents/2021/onr-rrr-121.pdf

Developing an Approach to the Regulation of AI

Three broad opportunities for the deployment of AI:

- **Advisory**
- **Supervisory**
- **Control**



Development of AI Systems

- Good systems for development, configuration control, training data, cyber security

Understand Performance Characteristics of the AI Systems

- How to understand performance and transfer info from other sectors

Confidence in Performance of AI Systems

- Challenges with testing
- Phased to build confidence / experience

Dealing with Failure

- Define / recognise failure. Use existing models (e.g. defence in depth)

Develop Skills and Experience Including Understanding the complexities of behaviours between humans and AI

ONR AI Regulatory Sandboxing Projects

Structural integrity:

Use AI to derive information from plant to inform structural integrity claims in a safety case to help demonstrate reliability. It is thought that this will assist in the development of digital twins and probabilistic assessment to demonstrate asset in-service operational life.

Robotic arm in a glovebox:

Use AI for real-time application to inform operations and understanding stresses and potential environmental constraints to, for example, optimise robotic movements.

Sandboxing Lesson Learnt

- Two AI sandboxing experiments conducted.
- The sandboxing open approach encouraged participants to undertake a genuine exploration of the issues and solutions in an **open-minded** and **inclusive** manner.
- The representation of **diverse views** from attendees with a range of backgrounds is vital to the success of sandboxing.
- The use of **problem/opportunity statements** provided a valuable focus to the sandboxing and generated a common understanding of the purpose.
- Sandboxing around **specific applications** of AI, rather than abstract consideration, allowed discussions to get to the crux of the issues surrounding AI deployment in nuclear.

Office for Nuclear Regulation

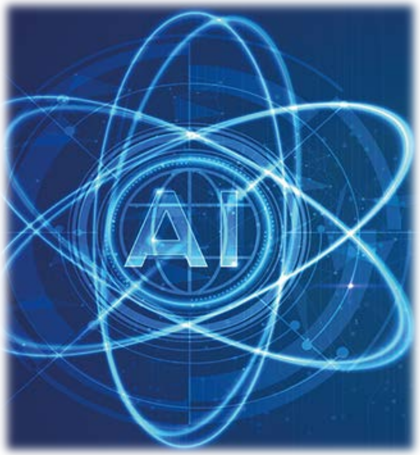
Environment Agency

ONR/Environment Agency Final Report

Regulators' Pioneer Fund (Department for Science, Innovation and Technology): Pilot of a regulatory sandbox on artificial intelligence in the nuclear sector

General Considerations for the Use of AI the Nuclear Sector

- Must demonstrate that AI represents the best available technique and that risks are reduced As Low As Reasonably Practicable (ALARP).
- The level of authority associated with the AI system.
- The safety, security and environmental significance of the application.
- The level of continuous learning – whether the AI is deployed as a static model or continuously learning.
- The complexity of the application.
- Given these uncertainties, deployments of AI systems with potential safety, security and environmental significance consequences should be undertaken in a phased manner to build up confidence and experience.



Regulatory AI Next Steps

- Regulatory sandboxing has become a key element in ONR’s approach to enabling innovation in the nuclear sector. In particular, it helps ONR demonstrate that it is open to innovation where it is in the interest of society and consistent with safety, security and safeguards expectations.
- ONR and the Environment Agency are keen for this project’s outcomes to be fed into existing work, for example, the work being undertaken through the Nuclear Institute’s AI4Nuclear initiative
- ONR and the Environment Agency will continue working to define a regulatory approach to the use of AI in the nuclear industry
- ONR, the US Nuclear Regulatory Commission and the Canadian Nuclear Safety Commission are developing a principles paper on the regulation of AI.

Office for
Nuclear Regulation

Any Questions?