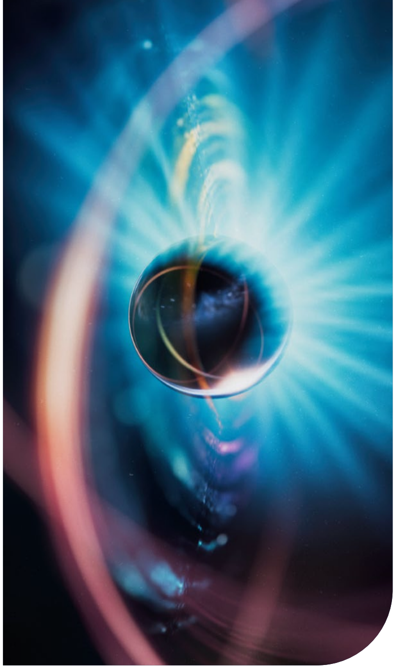
Nuclear renaissance and cyber security

By Sergej Gurenko, Cloud Security Architect, Reliance Cyber

RelianceCyber

THOUGHT LEADERSHIP E-BOOK SERIES



Nuclear renaissance and cyber security

INTRODUCTION

We are living in the era of nuclear renaissance. This article explores the cybersecurity challenges associated with Small Modular Reactors (SMRs). There are over 80 SMR designs in development across 18 countries, with about ten designs approaching real-life deployments.

The promise of SMRs is to miniaturise and industrialise the deployment of the mini-nuclear reactors with minimal service requirements and a lifespan of 60-80 years. SMRs are promised to be inherently safer than traditional reactors. This article explores the role of cybersecurity in modernised nuclear and SMRs.

RECENT PRO-NUCLEAR COMMITMENTS

In recent years, opposition to nuclear energy has waned due to technical advancements, climate change, and energy security concerns. Politicians, technocrats, and green energy enthusiasts are gathering more data and concluding that nuclear is mandatory to achieve significant progress with Europe's and U.S. green commitments and sustain the remaining heavy industry. Below is a brief list of recent pro-nuclear commitments:

- The UK government has committed to building eight new nuclear reactors by 2030 as part of the Energy Security Strategy.
- France has announced plans for new reactor construction to maintain energy independence and meet climate targets.
- Germany decided to extend the operational life of its remaining nuclear plants beyond the previously planned phase-out.
- The U.S. Inflation Reduction Act introduced tax credits for existing nuclear plants and support for advanced reactor technologies.
- Amazon, Google, and Microsoft have announced significant investments in nuclear energy to meet the growing energy demands of their A.I. operations.

Written by:
Sergej Gurenko, Cloud Security Architect, Reliance Cyber

What is a Small Modular Reactor?

SMRs are significantly smaller, typically generating less than 300 megawatts (MWe), compared to traditional reactors that often exceed 1,000 MWe. SMRs utilise modular technology, enabling factory fabrication of components that can be shipped and assembled on-site, reducing construction time and costs. They incorporate advanced safety systems designed to function passively without external power or human intervention, making them inherently safer than traditional reactors. Due to their smaller footprint, SMRs can be installed in various locations, including remote areas and sites with limited infrastructure. The lower initial capital investment and reduced financial risk associated with SMRs make them more attractive to investors.

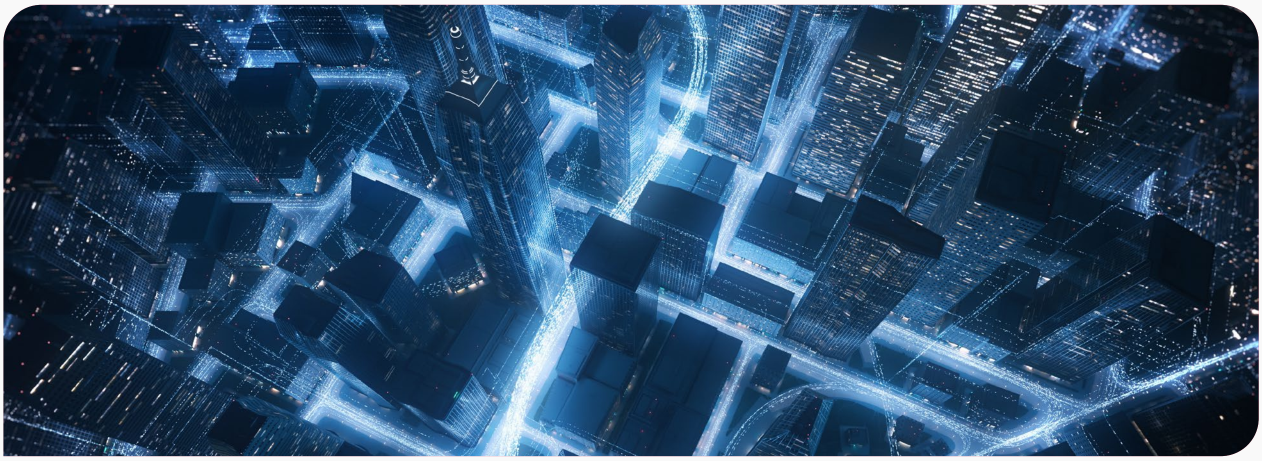
What is the role of the IT and Cyber in SMRs?

SMRs incorporate numerous IT elements and computerised sensors as part of their design and operational framework. They utilise sophisticated computerised control systems that monitor and manage reactor operations. The controls rely on a variety of sensors that provide real-time data on temperature, pressure, radiation levels, and coolant flow. Exposing SMR sensors to modern cloud-hosted advanced data analytics will enable predictive maintenance and operational efficiency. Many SMR designs support remote monitoring and control capabilities, allowing operators to manage the reactor from a distance. Given the reliance on digital technologies, SMRs should incorporate cybersecurity technologies to protect against potential cyber threats.

Can we just apply the same cybersecurity standards and solutions we used with traditional nuclear power plants?

SMRs present unique cybersecurity challenges compared to traditional nuclear power plants. Here are the key challenges associated explicitly with SMRs:

- **Increased Attack Surface:** SMRs can be deployed in greater numbers and in more varied locations than traditional reactors, increasing the potential points of attack. This decentralised deployment means that securing multiple sites becomes more complex and resource intensive.
- **Supply Chain Vulnerabilities:** The construction of SMRs involves multiple suppliers and prefabricated components, increasing the risk of supply chain attacks. Cyber adversaries may target the various suppliers involved in the production of SMR components, potentially compromising the integrity of critical systems.
- **Compact Design, Reduced on-site personnel, and Less Physical Protection:** The compact design of SMRs means they may have smaller physical perimeters and less on-site security compared to larger traditional reactors. SMRs typically require fewer on-site personnel for day-to-day operations, making it more difficult to physically secure the infrastructure.
- **Combination of Cyber and Physical Risks:** The integration of cyber systems with physical operations means that a successful cyber-attack could lead to physical consequences, such as unauthorised access to nuclear materials or disruption of safety systems.
- **Challenges due to Evolving Regulatory Frameworks:** As SMR technology is new, existing regulatory frameworks may not adequately address the unique cybersecurity risks associated with these reactors.
- **Dependence on new and emerging A.I. and ML technologies:** The use of advanced digital technologies like artificial intelligence (AI) and machine learning (ML) for operations can enhance efficiency but also introduce new cybersecurity vulnerabilities if these systems are not properly secured.



How much ongoing support is required to ensure SMR is secure throughout the entire 60-80-year lifespan?

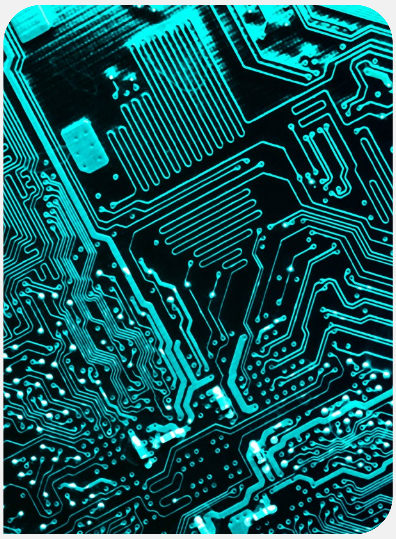
Increased attack surfaces, supply chain vulnerabilities, the combination of cyber-physical threats, regulatory hurdles, and reliance on advanced technologies all contribute to a complex cybersecurity landscape that must be carefully managed to ensure the safe operation of these innovative reactors. Addressing these challenges will require ongoing collaboration between industry stakeholders, regulators, and cybersecurity experts. Regular upgrades are essential for addressing security vulnerabilities and protecting sensitive data against emerging cyber threats. Because of the rapid progress in electrical and computer technologies, it makes sense to modernise and perform mid-life cycle upgrades for SMRs.

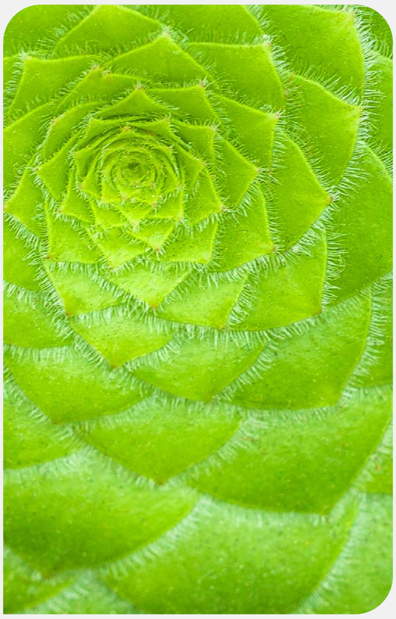
Conclusions

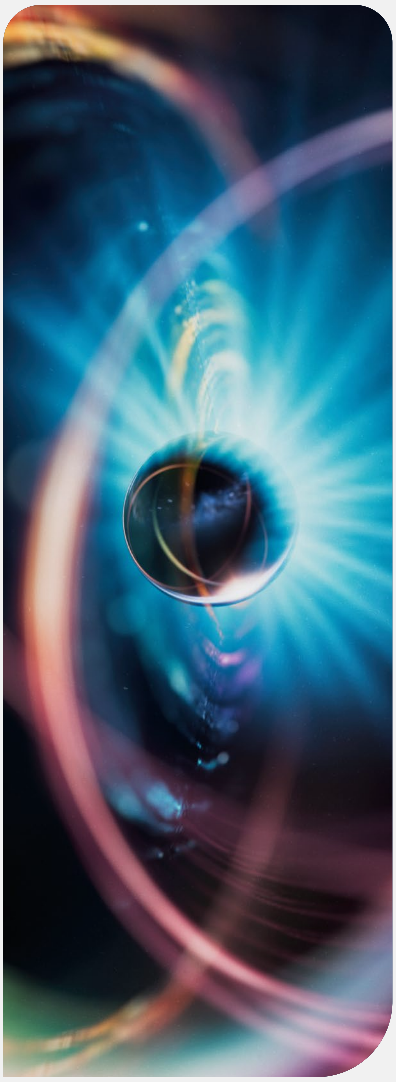
Power plants are considered Critical National Infrastructure (CNI) in the UK. In contrast to power distribution networks, power plants are more secure due to security measures, stringent regulatory oversight, and advanced safety protocols designed to protect against both physical and cyber threats. However, SMRs may blur the line between power plants and distribution networks due to their decentralised deployment and modular design. The nuclear industry has a good foundational set of cybersecurity standards; however, SMRs face unique cybersecurity challenges due to increased attack surfaces from decentralised deployments, supply chain vulnerabilities from complex supplier networks, and reliance on commercial technologies.

Many SMR designs support remote monitoring and control capabilities. Their compact design reduces physical security and on-site personnel, increasing dependence on digital defences. Additionally, evolving regulatory frameworks may not adequately address these risks, necessitating adaptive measures. Integrating advanced technologies like A.I. and machine learning enhances efficiency but can introduce new vulnerabilities that must be managed carefully.

Cybersecurity must be an integral part of SMR build and lifecycle. Because technology is developing rapidly, the SMR suppliers should be ready to deliver multiple mid-life upgrades. We can learn from the aviation industry's Mid-Life Upgrades (MLUs) packages strategy, where significant systems are updated or completely replaced to enhance performance, safety, and compliance with evolving regulations around the aeroplane 10–15-year mark.







Nuclear renaissance and cyber security

Explore the leadership series

RelianceCyber

reliancecyber.com