Secure by Design

Lessons from the Nuclear Industry

Rob Barnes MEng AUS MIET MSyI GICSP

8/9th July 2024

ROLLS ROYCE SMR

Rolls-Royce SMR Ltd is a technology vendor offering a complete SMR power plant on a turnkey basis

Our development programme is fully funded with £495m through commercial equity and UK Government grant funding

Rolls-Royce SMR Ltd Shareholders

Rolls-Royce Group
60 years designing, manufacturing, supporting and operating nuclear technology

Constellation Energy (previously Exelon Generation Ltd)
Operates the largest U.S. fleet of zero-carbon nuclear plants with over 18.7GW from 21 reactors at 12 facilities

BNF Resources UK Ltd
Extensive investments in the energy space and represented and advised by BNF Capital Limited, an FCA regulated UK-based investment advisory

Qatar Investment Authority
Invests in the energy transition and funds technologies that enable low carbon electricity generation

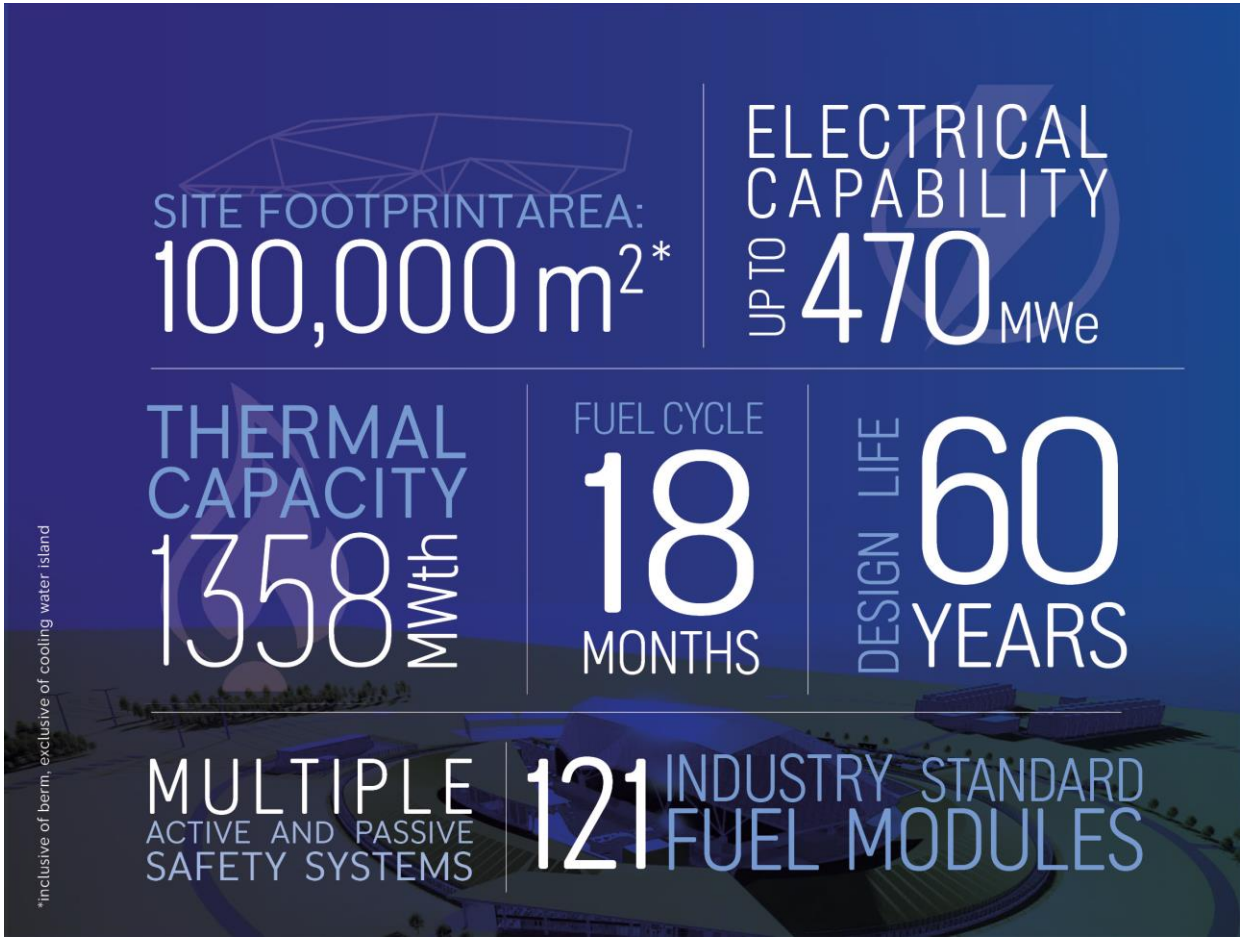
UK Government Grant Funding

UK Research and Innovation

Rolls-Royce SMR has received UK Government funding of £210m as part of Phase 2 of the Low-Cost Nuclear Challenge Project, administered by UKRI,

SMR

The Rolls-Royce SMR in numbers



Content

This presentation provides a brief insight into Secure by Design.

A more complete introduction is available from the Nuclear Innovation Programme, task R3.6.07.

01 **Nuclear control and instrumentation**
The technology and its role in safety

02 **Concept of Secure by Design**
What it is and why it is different

03 **Application**
How the concept is being applied to the SMR

04 **Lessons learned**
Parallels and insights for network engineering

Commercial reactors of the UK

Technological context of nuclear OT

1950s: Analogue electronics, gauges, chart recorders, switches and relays.

1960s: Lights, push buttons, and gauges. Electronics still predominately analogue.

1970s: There were no 1970s.

1980s: Software and programmable electronics. Computer terminals and screens appear in the control room.

1953

Magnox

(UK Design)

1965

Advanced Gas-cooled Reactor (AGR)

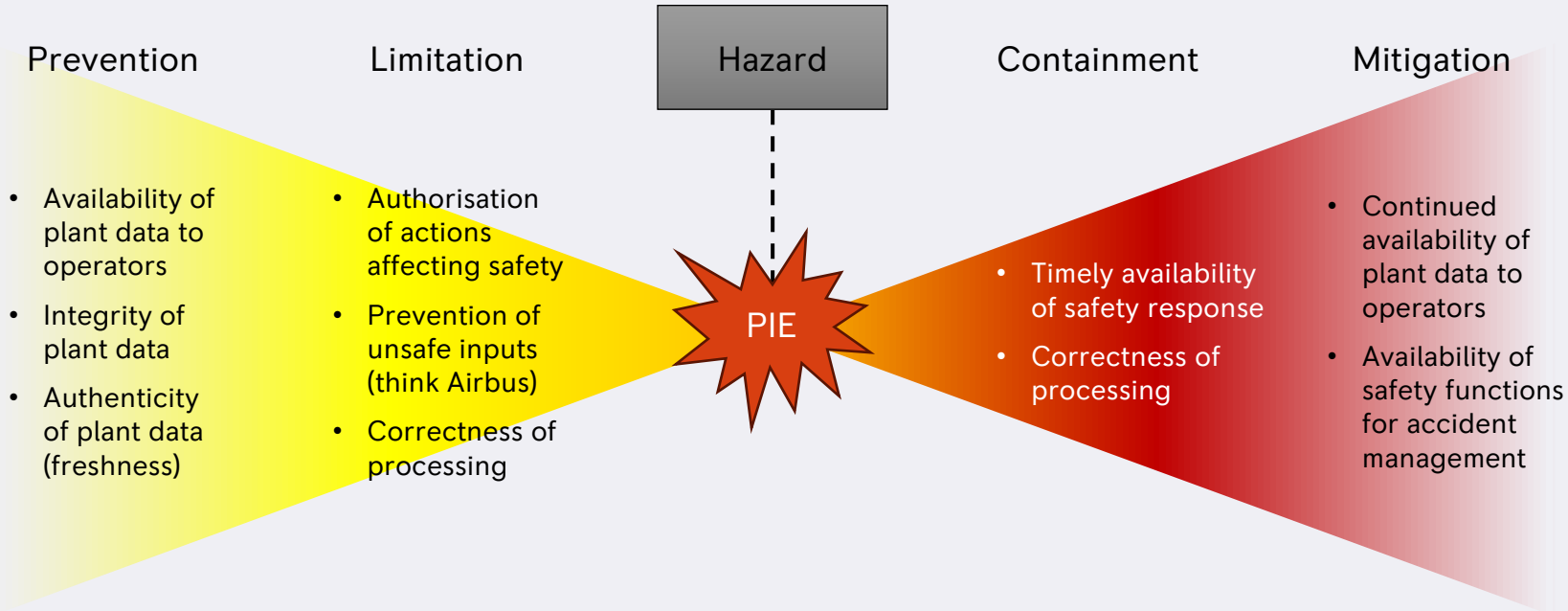
(UK Design)

1988

Standardized Nuclear Unit Power Plant System (SNUPPS)

(US Design)

Nuclear OT (and IA) in the context of safety

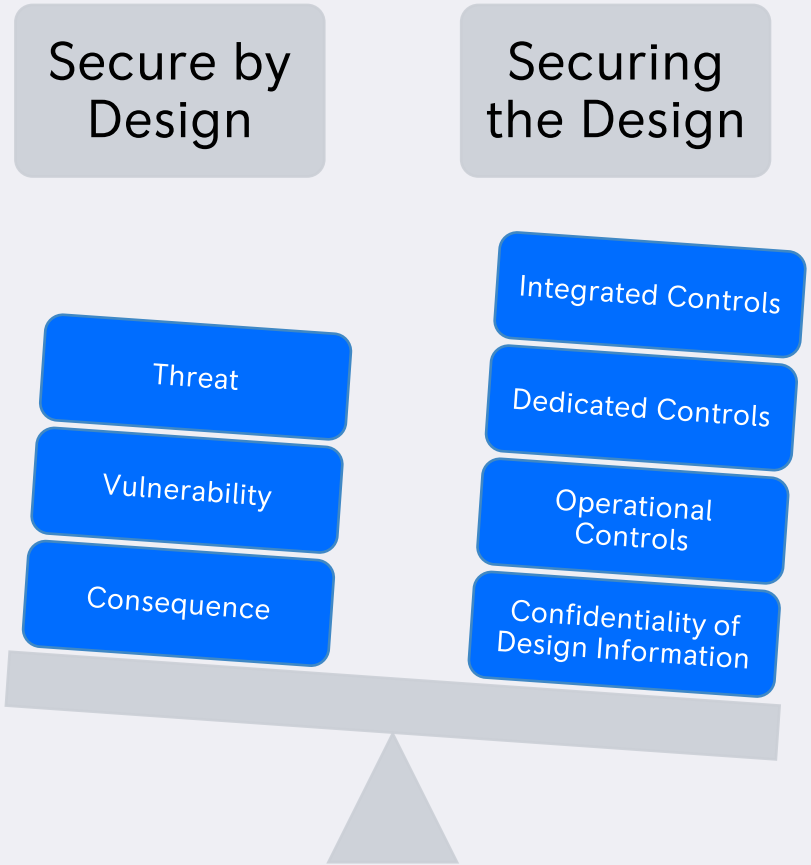


The goal of Secure by Design

The effectiveness of the security solution (i.e. risk reduction) must outweigh the inherent risk of the power station.

We can: reduce inherent risk, or increase effectiveness of security controls, or both.

Secure by Design is how we do the former, and Security Design is how we do the latter.



Building security into engineering

Secure by Design is more than a set of principles, requirements or verification tests - it is an overall approach to engineering security into products; therefore, it must be integrated fully into engineering, and be part of “business as usual”.

Design principles

- Eliminate or reduce hazards at source
- Avoid software or programmable electronics for most-critical safety functions
- Require security controls on actions affecting safety*

Engineering governance

- Security is a stakeholder by default – opt-out, not opt-in
- Security built into engineering processes
- Require formal sign-off from security at review gates

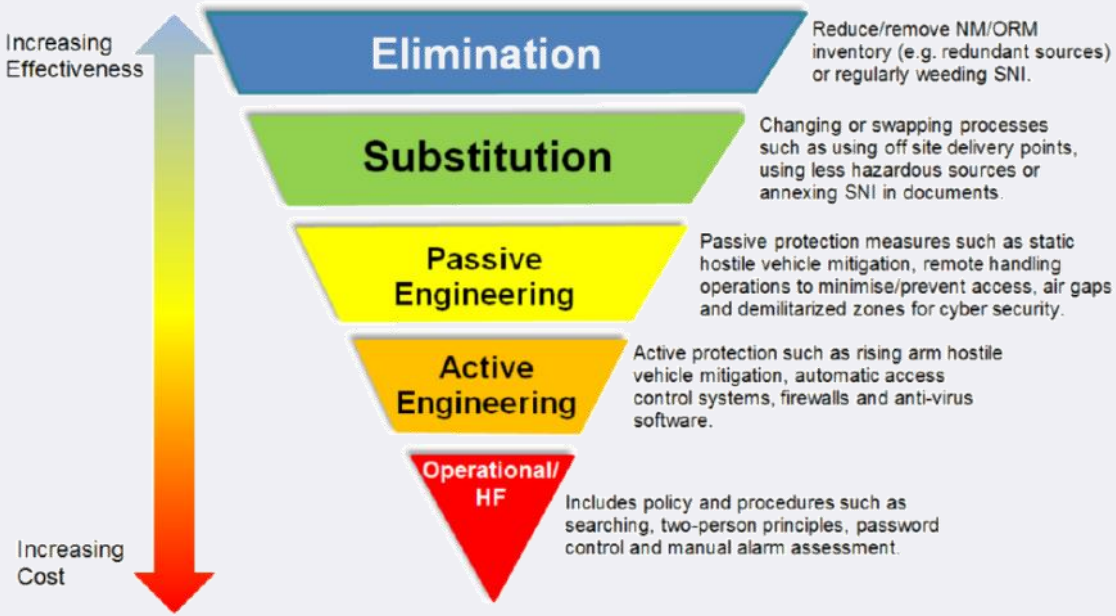
Cross-domain risk management

- Security controls can increase the difficulty for adversaries
- Quality controls can reduce vulnerabilities
- Safety controls can prevent or mitigate the impacts from successful attacks

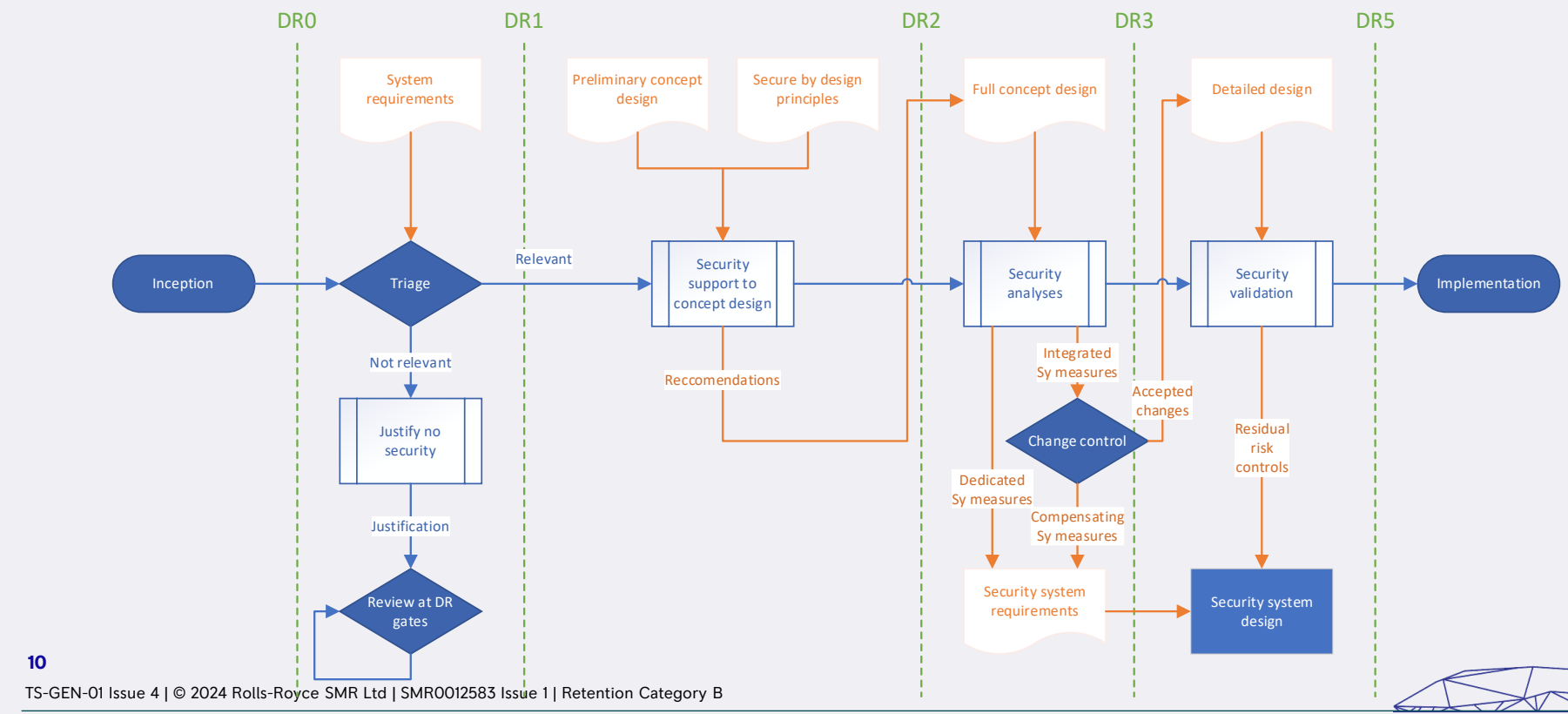
Nuclear industry approach to Secure by Design

Reproduced from Office for Nuclear Regulation (ONR) CNS-TAST-GD 11.4.1 Issue 1.1

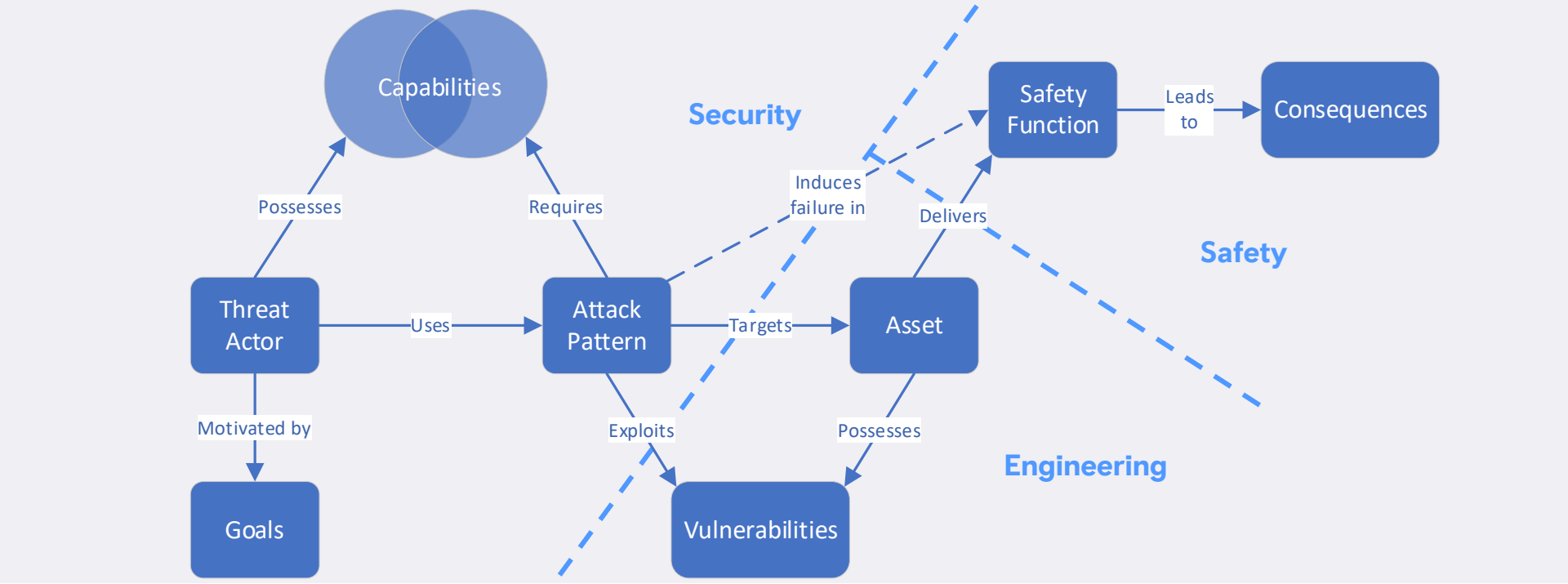
Hierarchy of controls



How we practice Secure by Design



The effect of secure by design



Parallels with information technology

There are some important differences: Not knowing the nature of the traffic and what functions it supports means that much of the risk is outside of scope, whereas nuclear site licensees are accountable for all their risks.

Examples in network security

- Secure by design
  - Out-of-band management of infrastructure and security devices
  - Tunnelled client traffic – all untrusted traffic is encapsulated
- Integrated security
  - Device hardening
  - Span ports to support NIDS

ROLLS ROYCE SMR

Experience from applying Secure by Design to the Rolls-Royce SMR

Security is a quality, just like safety or reliability and quality is a market differentiator.

A reputation for high-quality products will attract customers.

Lessons learned

- Security must be a default stakeholder in every system – opt out, not opt in
- Do security early and do it often
- Have a security team that is adequately resourced to support engineering activity
- Keep security involved in design decisions
- Challenge the underlying design

What's next for SMR security?

We have completed Generic Design Assessment Step 2, during which our secure by design methodology and supporting security analysis methodologies were assessed by our regulator to be adequate

Next steps

- GDA Step 3
  - Apply methodologies, generate evidence, learn
  - Earn our Design Acceptance Certificate (DAC)
- First order and site licensing
- Beyond - off-site connectivity for:
  - Telephony and Wide-Area Network (WAN)
  - Equipment health monitoring and remote support
  - Security Operations Centre (SOC)
  - Emergency preparedness and response

ROLLS ROYCE SMR

Secure by Design in the Rolls-Royce SMR

Learn more about nuclear Secure by Design from the Nuclear Innovation Programme.

Summary

- Establish secure design principles, and support their application
- Security is a stakeholder by default
- Reduce security risk at source
- Practice cross-domain risk management
- Integrate security into engineering governance
- Greater integration of security measures into existing stuff leads to less reliance on dedicated security measures

rob.barnes@rolls-royce-smr.com