



# How do you secure a jet engine? (And what do FPGAs have to do with that?)

FPGA Frontrunner | Thales, Reading | 23/11/23

Simon Bowles

Product Cyber Security Specialist

Rolls-Royce Defence



The information in this document is proprietary and confidential to Rolls-Royce and is available to authorised recipients only - copying and onward distribution is prohibited other than for the purpose for which it was made available.

Rolls-Royce content only

1 ©2023 Rolls-Royce  
Not Subject to Export Control

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







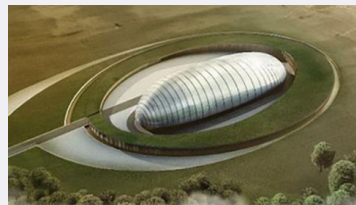
Civil



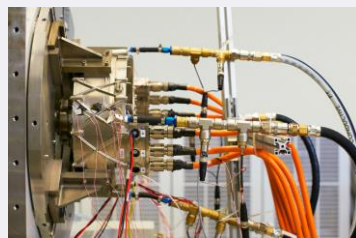
Defence



Power Systems



Electrical







PIONEERING THE POWER TO PROTECT

### Space Operations

Space Exploration



Satellites - Power & Control



Micro Reactor For Space Exploration & Propulsion



Micro Reactor For Base Power



Lunar Base Space Station

### Aerospace Operations

Hypersonic Missiles



Hypersonic



Wingman



Effectors



Surveillance



Sustainable Fuel Powered Air Forces



Tempest



Future Vertical Lift



Electric Trainer



### Base Operations

Ground Source Heat Pump

Small Modular Reactor (SMR)

Synthetic Fuel Plant

Synthetic Fuel

Smart Microgrid

Synthetic Fuel Powered Ships



Hybrid Electric Ships



Integrated Full Electric Propulsion



### Naval Operations

Unmanned Surface Vessel (USV)



Dreadnought Submarine



Micro Deployable Reactor



Unmanned Underwater Vessel (UUV)



Directed Energy Weapons



Deployable Hybrid Microgrid



### Land Operations

Hybrid Electric Vehicles







*Solar winds*



*Viasat / log4j*



*Stuxnet*



*Triton*

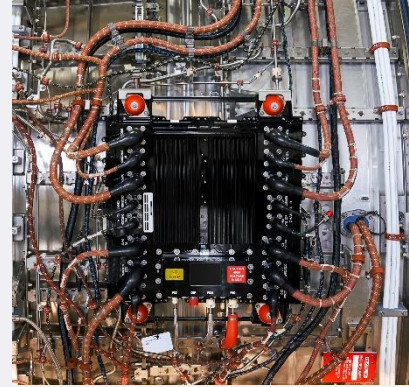
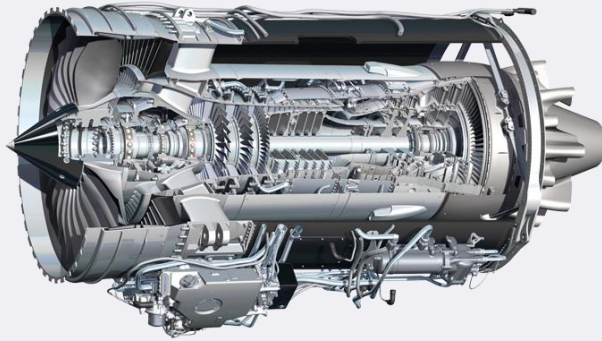


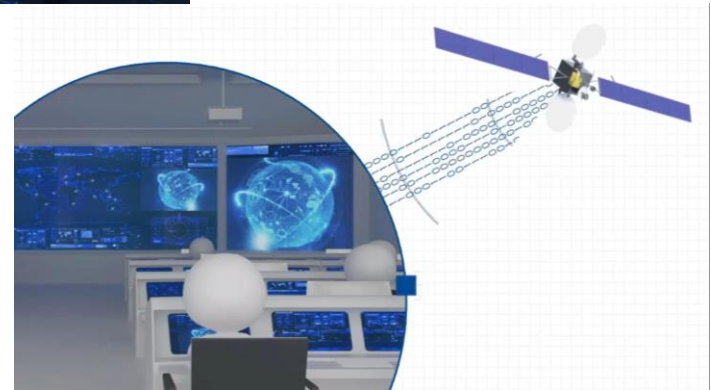
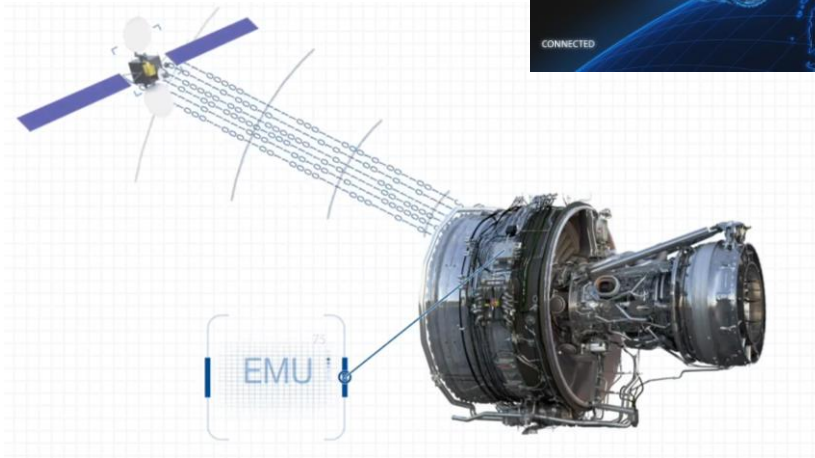
*Pipedream*

*.....What's next?*



# Securing Cyber - Physical Systems





## Pearl 16 - The “Intelligent Engine”

Connected, Comprehending, Contextually aware



---

**“If it’s not secure, you can’t be confident it’s safe”**

**If safety-related operational technology is not secure, you can’t be confident it’s safe:** absolute safety and security cannot be achieved; the assurance of safety-related systems involving digital technology relies on effective cyber security to reduce the risk of harm to an acceptable level.

<https://electrical.theiet.org/guidance-and-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/>



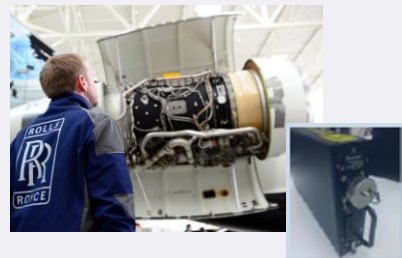


## FPGAs

Current uses in Rolls-Royce

### Health Monitoring

Analogue data acquisition, format conversion, ARINC429 interface and signal validation



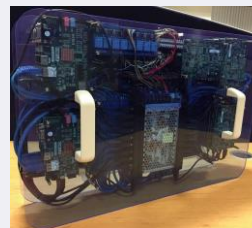
### Power Converters & motor drives

High speed signal processing and control, e.g. current and voltage measurements, field oriented control algorithms, safety time-critical electrical protection



### Processor technology development

Implementing solutions rapidly on FPGA e.g. PQC and PUF







### Austere Environments

- -55° C to 125° C
- Single Event Effects
- Sand, water, moisture, lightning, EMC, vibration...

### Certification and Compliance

- FAA / EASA Safety and Cybersecurity Certifications
- US DoD / UK MOD cybersecurity compliance
- DO356 / DO178 up to **DAL A**
- Platform/customer-specific requirements

### Safety Critical

- Must be secure while also failing safe.
  - **Fail secure – but not safe – is not an option.**
- Extremely fast power-up and boot times: ~100-200ms.

### Long Development and Support Lifecycles

- Years-long development lifecycles
- 20-50 yr operational lives
- Infrequent updates







## Areas of interest

Can you think of other hard problems we should be investigating?

System monitoring

Root-of-Trust implementation (e.g. Subset of TPM functionality)

Ensuring the supply chain of the FPGA components.

Encryption features built in to support AES encryption / decryption, authentication, and secure boot

How can we use an FPGA's extra processing power to enhance the product security?

Update & support over product lifecycle – *Decades!*

How can we maintain the security of a compromised system?







**Safety is our top priority**

**To be safe, we need to be resilient**

**To be resilient, we need to be system thinkers**

