
CIPHERA
PEACE OF MIND IN A DANGEROUS WORLD
Digital Resilience:
Protecting Spacecraft
Computing Platforms

Transformed Space Domain

- Satellite Services are essential part of modern society. ESA Cybersecurity :
  "Space is a fundamental pillar of any State in the world in terms of Economy, Security, Sustainability, Energy, Civil Protection and in the daily life of citizens"
- Larger LEO and MEO constellations and ecosystems offer multitenant services
- Satellite Systems (including ground stations) should be considered equally reachable by Cyber criminals and Rogue State actors
- Digital Resilience will be required property of future satellite constellations, services and ecosystems – but what is the metric/quality criteria?

Threats to Space Ecosystem

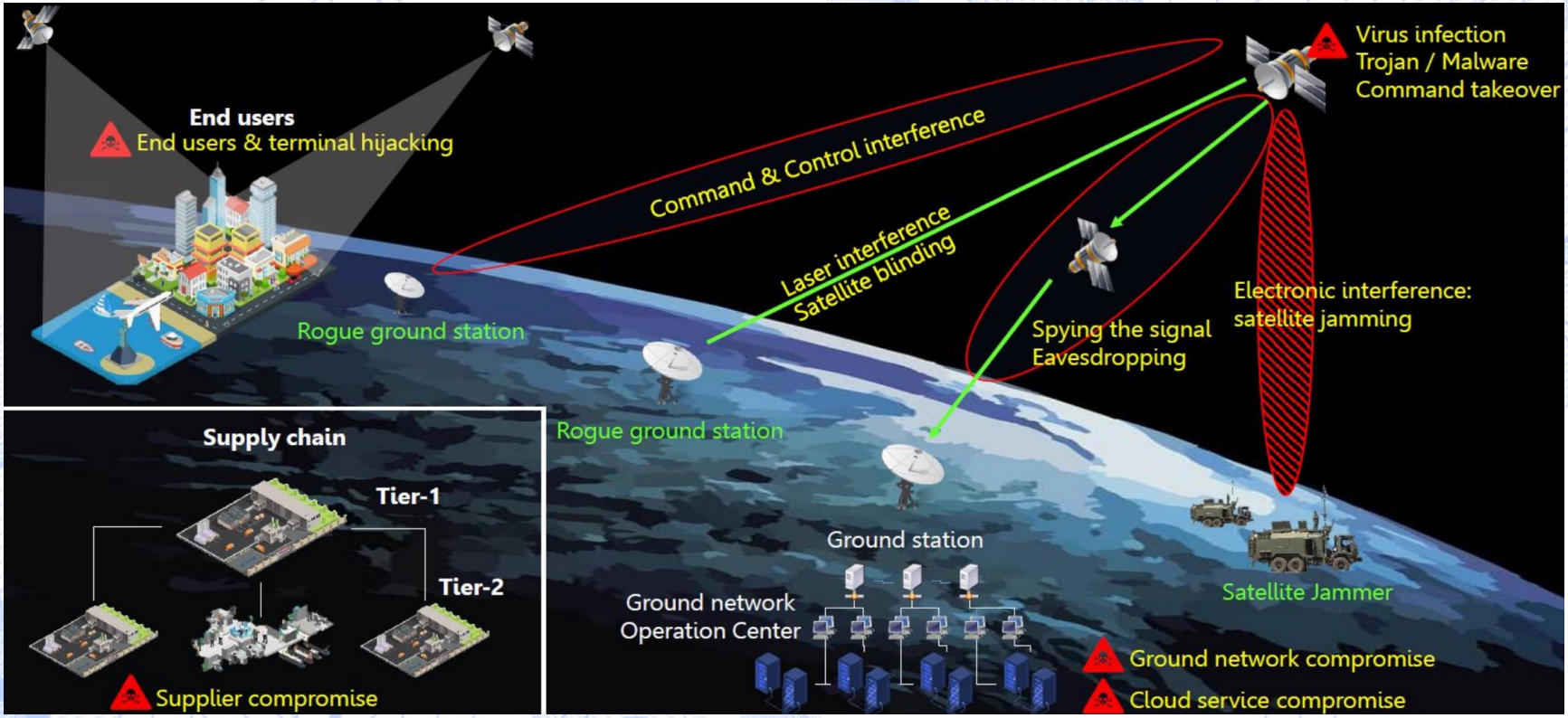


Image-source: ESA GSTP Cybersecurity Compendium Presentation 031122.pdf

Security to Space

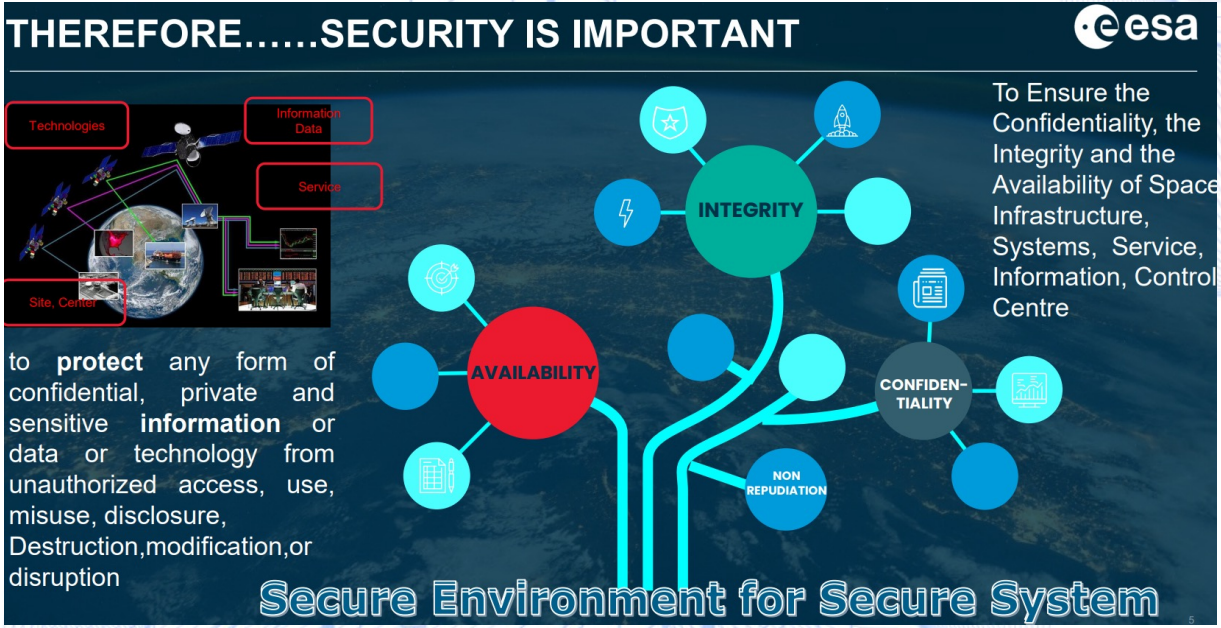
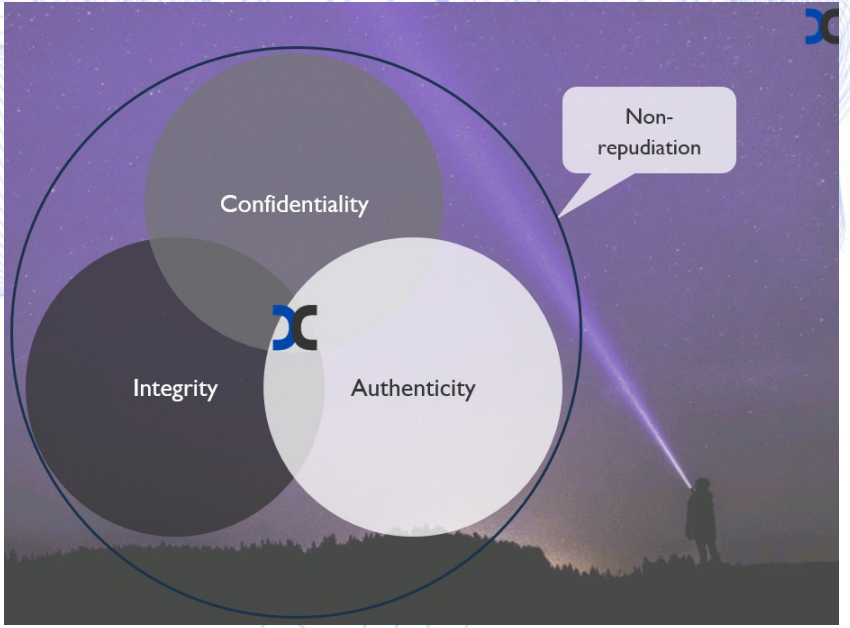


Image-source: ESA GSTP Cybersecurity Compendium Presentation 031122.pdf



Achievable Security with Cryptography

Cyber Resilience to Space

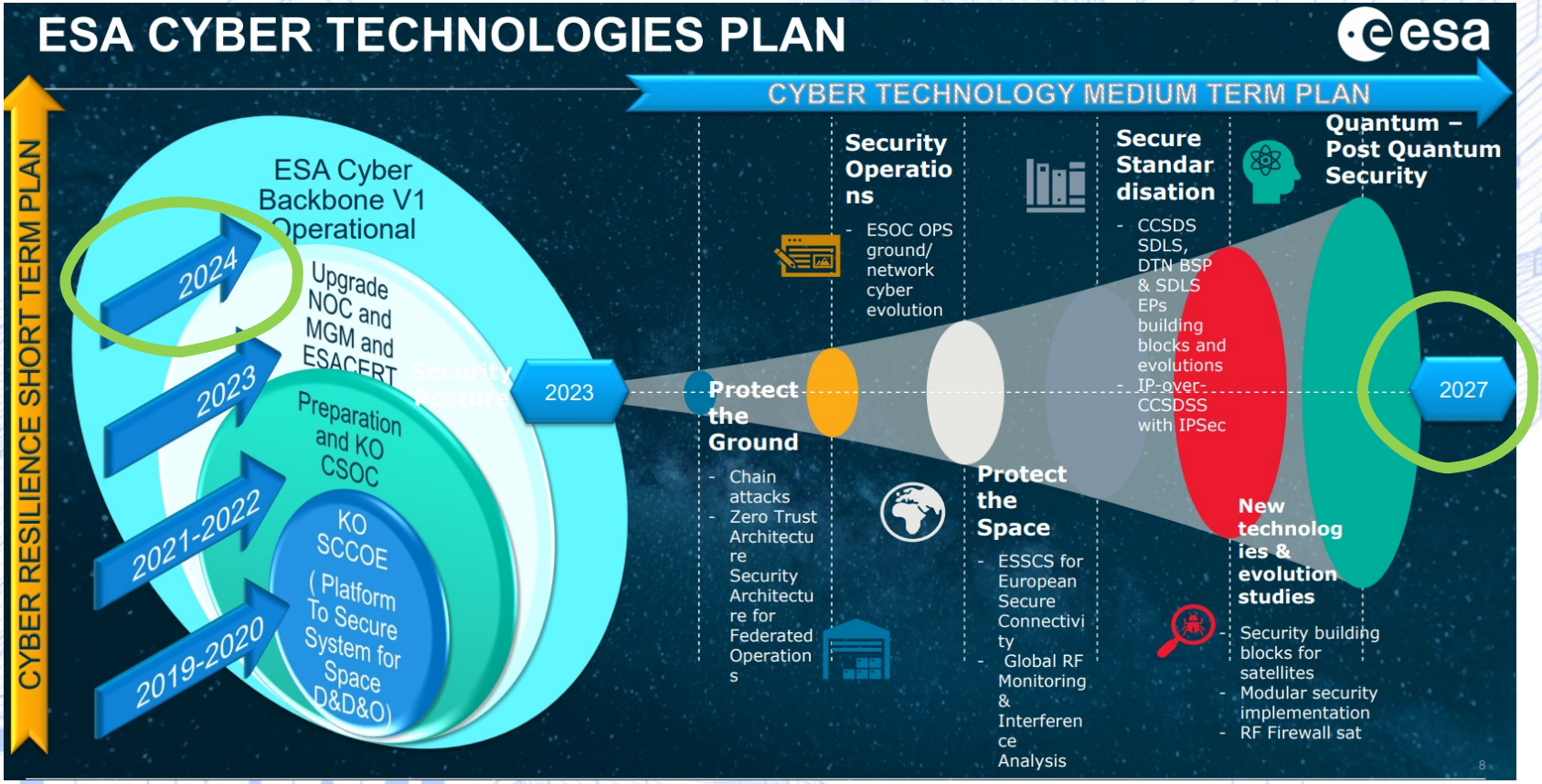


Image-source: ESA GSTP Cybersecurity Compendium Presentation 031122.pdf

What is needed I

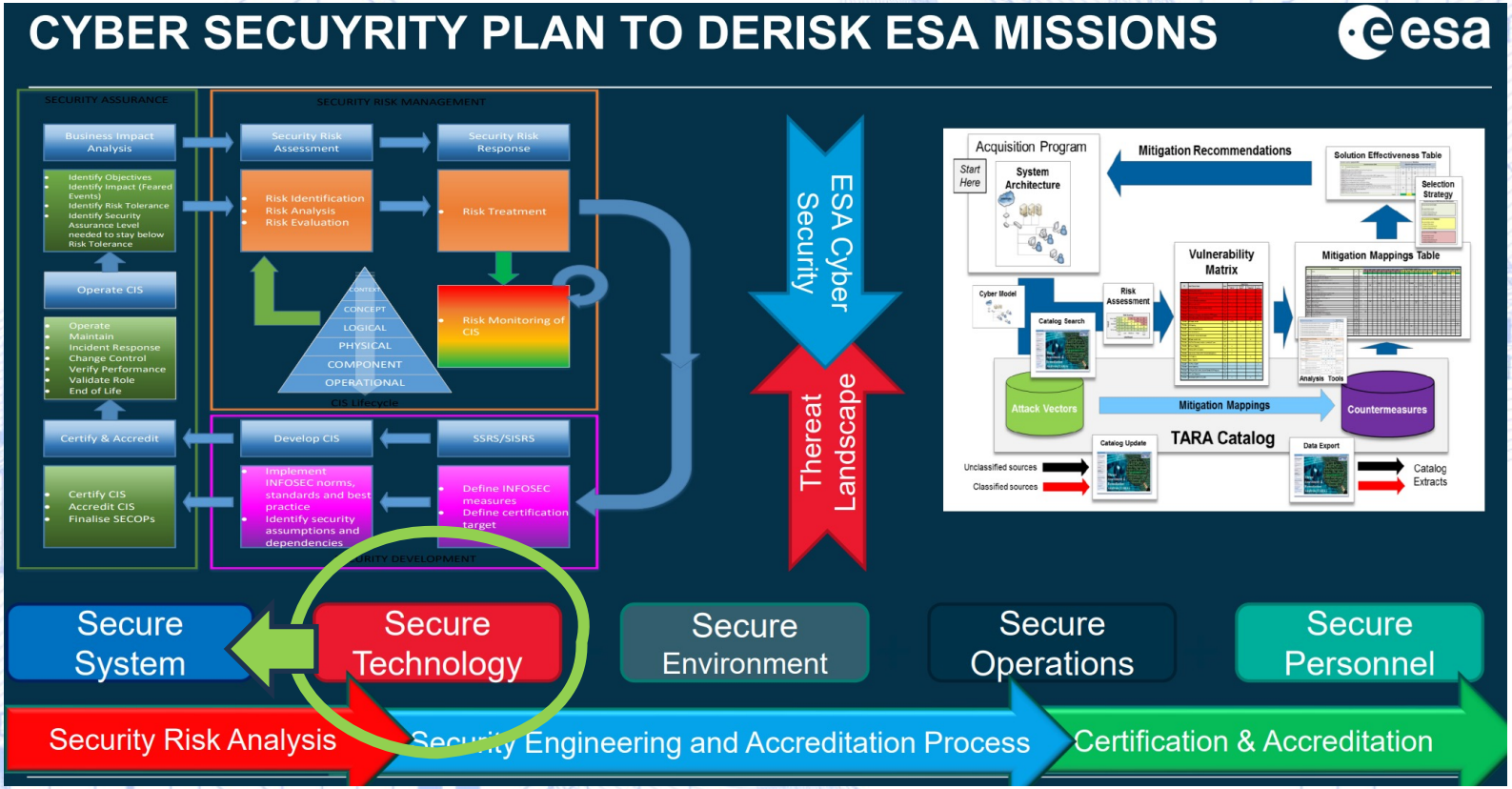


Image-source: ESA GSTP Cybersecurity Compendium Presentation 031122.pdf

What is needed 2

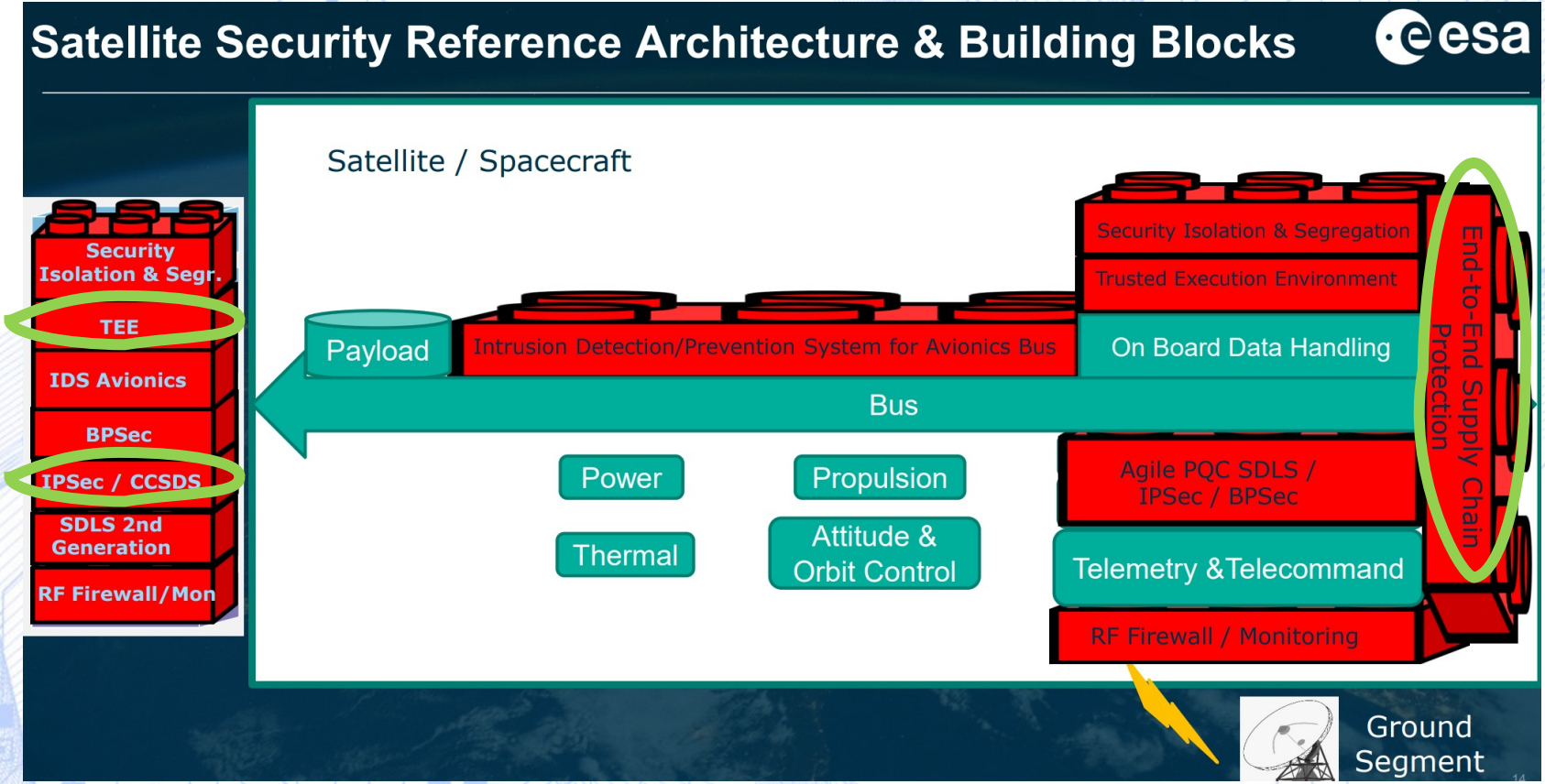


Image-source: ESA GSTP Cybersecurity Compendium Presentation 03122.pdf

How about Platform and Payload?

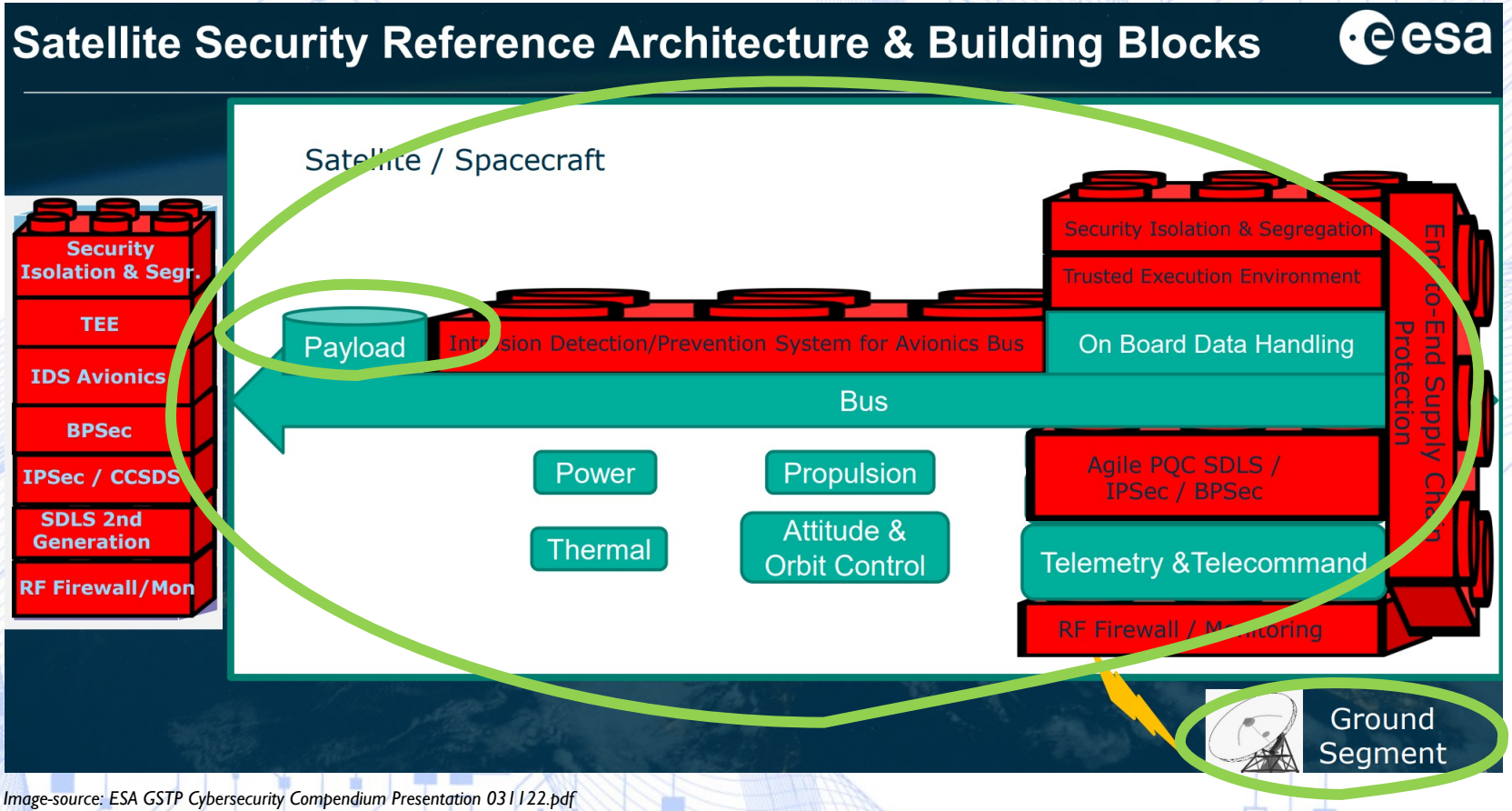
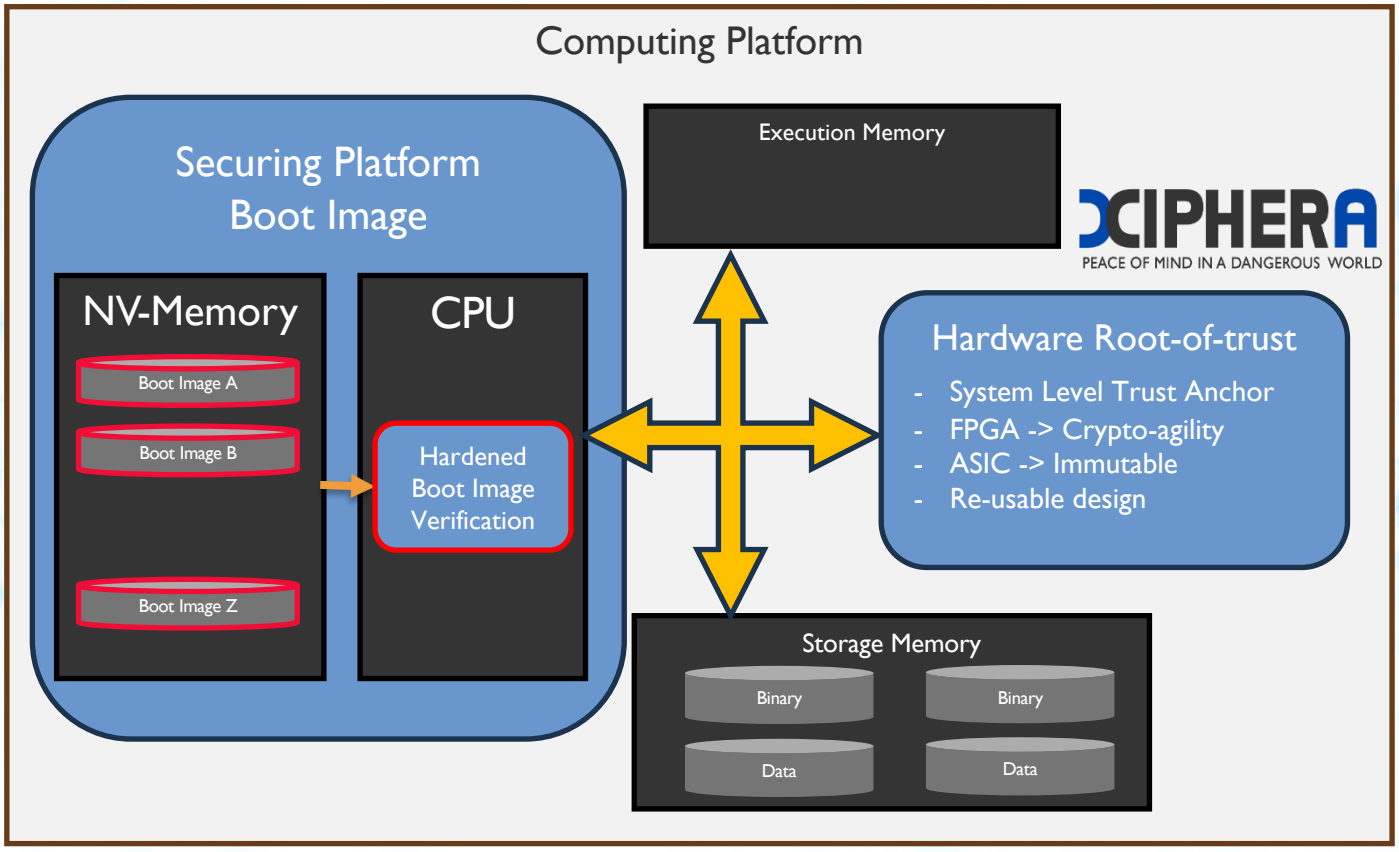


Image-source: ESA GSTP Cybersecurity Compendium Presentation 031122.pdf

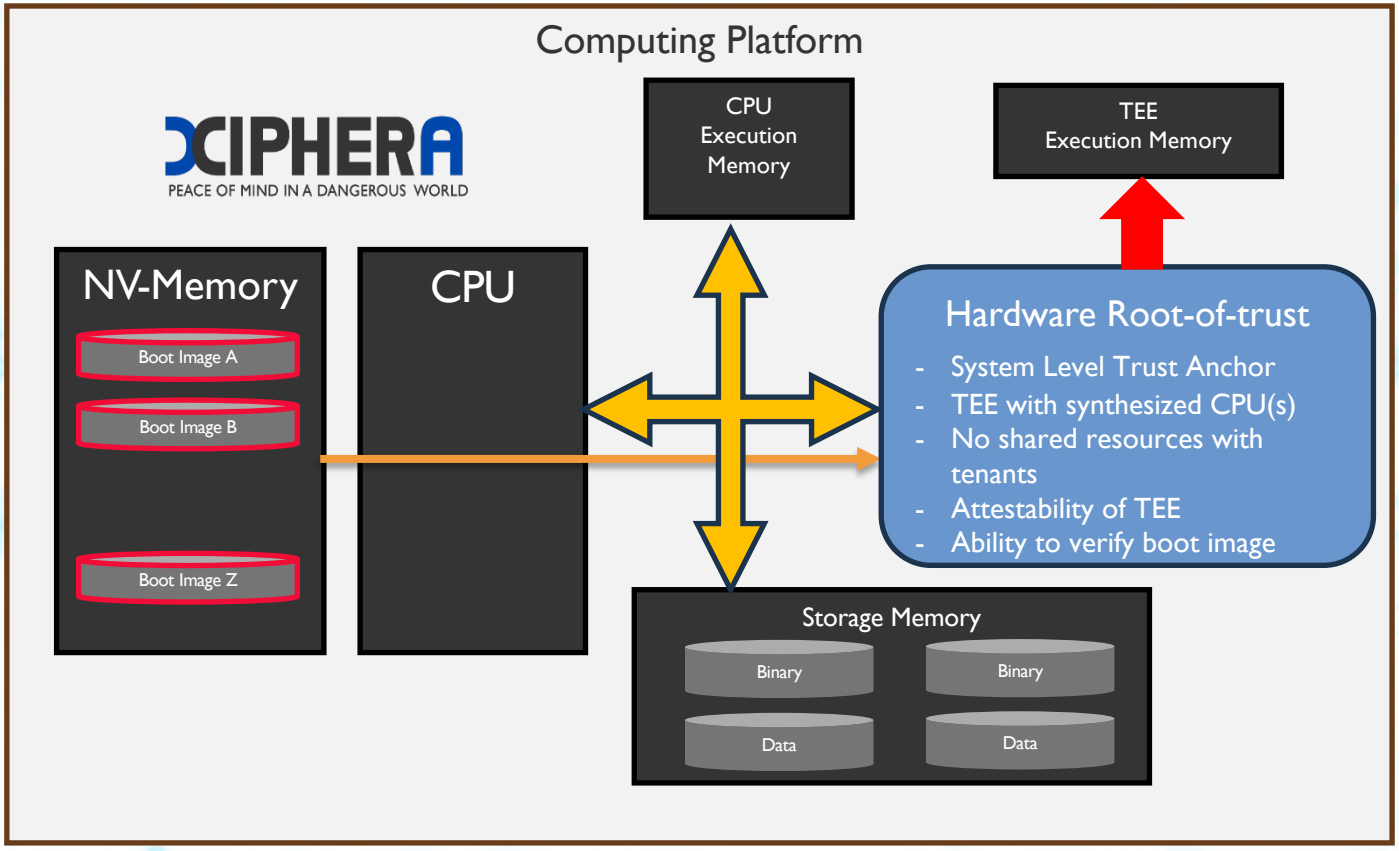
Protecting Spacecraft Computing Platform

Enables:
- Tamper free OS
- Cryptography (PQC)



Enables:
- Payload verification
- Cryptographic Services
- Zero Trust Platform

Even More Protection



HW-ROT with TEE enables:

- All HW-ROT functions
- Secure Multitenancy
- Physically isolated code execution
- CPU vulnerabilities can be eliminated
- Host system independent data protection

Securing HW and SW components

Zero trust

Absolute isolation

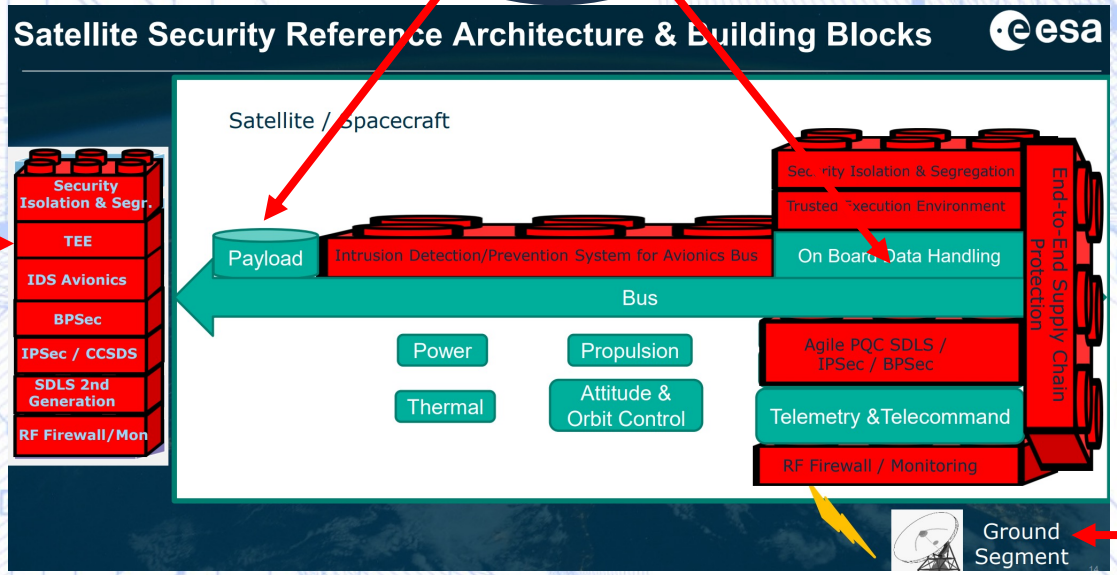


Image-source: ESA GSTP Cybersecurity Compendium Presentation 031122.pdf

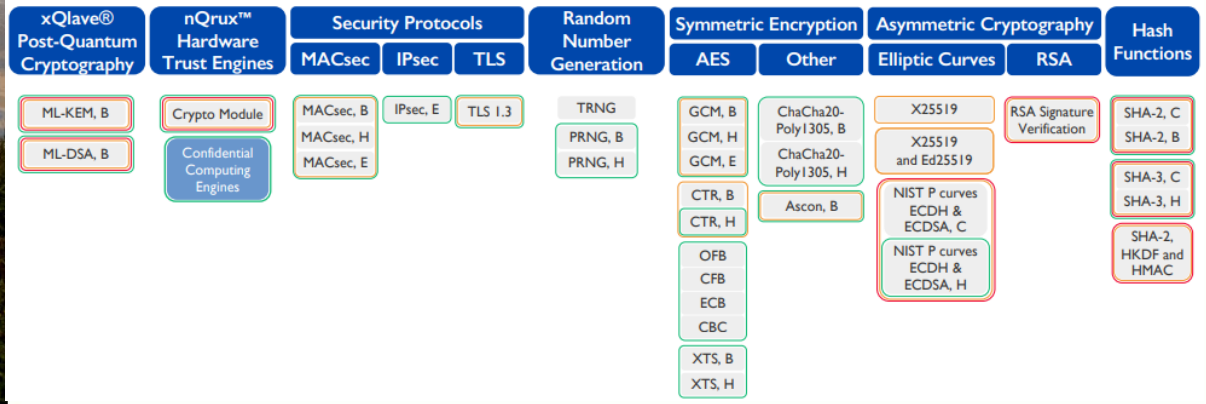
Ground Stations Protectable

Enable Digital Resilience today

- Threat analysis and risk assessment needed
- Design security to solution from the day one
- Quantum Computing Threat requires actions
- Supply Chain Threats are real
- No more easygoing Security in Space Domain

Technology is available today

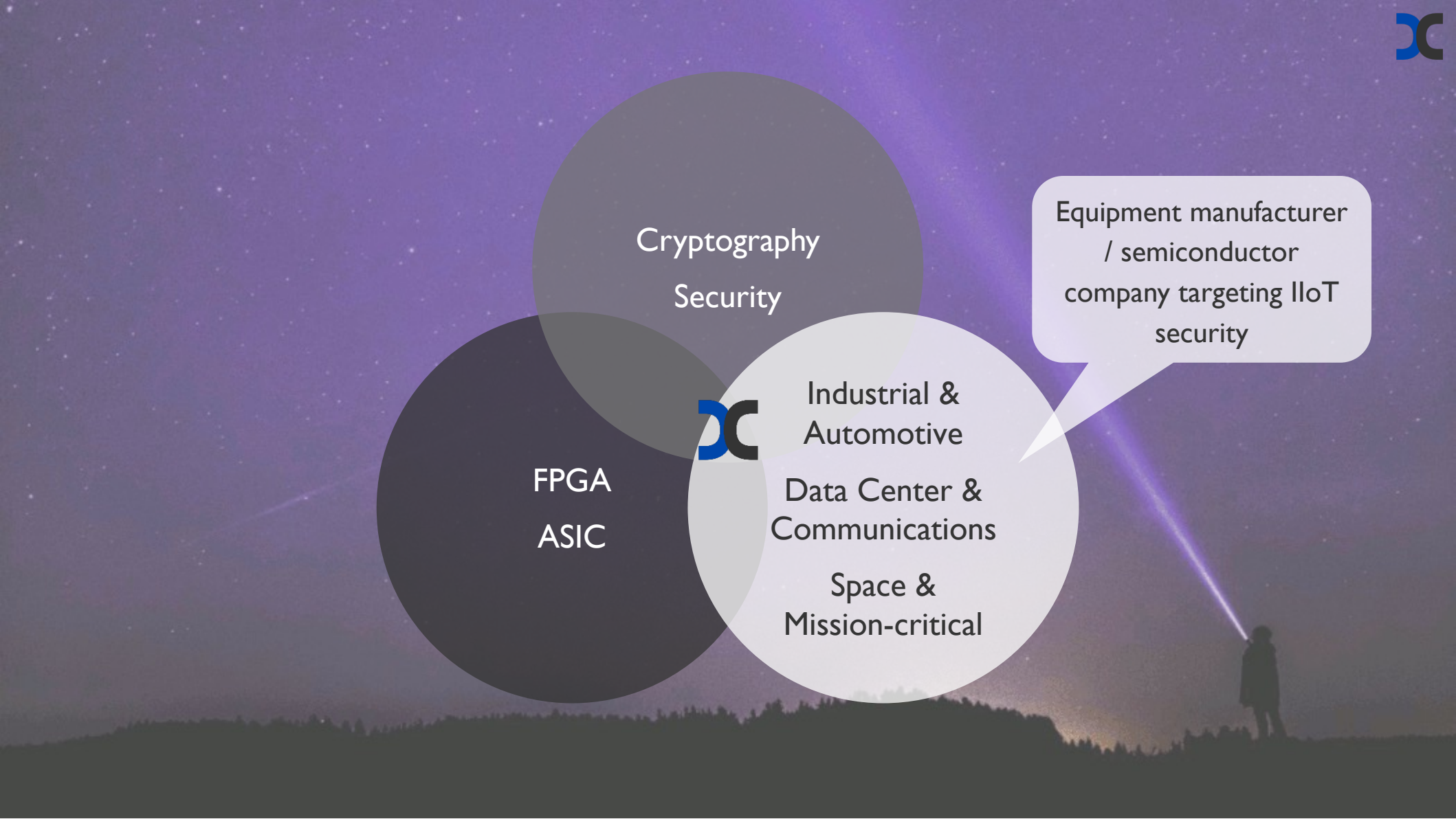
Xiphera Portfolio




XIPHERA
Let's secure your business together.
Xiphera Ltd.
www.xiphera.com
sales@xiphera.com

Xiphera Ltd.

- Finnish company founded in 2017
- Hardware-based security solutions with standardised cryptographic algorithms
- Secure and efficient cryptographic IP cores for digital logic (FPGAs and ASICs)
- All products and solutions designed fully in-house
- Committed roadmap to future cryptographic standards


Cryptography
Security
FPGA
ASIC
Industrial &
Automotive
Data Center &
Communications
Space &
Mission-critical
Equipment manufacturer / semiconductor company targeting IIoT security

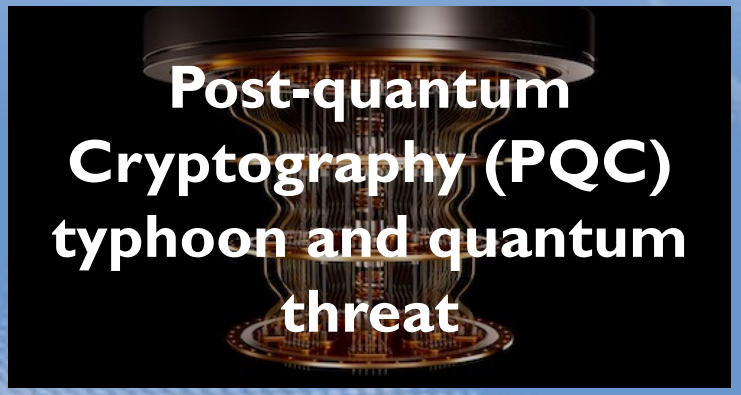
We protect critical systems by designing security directly into hardware.

Strong technical background in security

Broad and modern portfolio

Uncompromised confidentiality

The Time Is Now

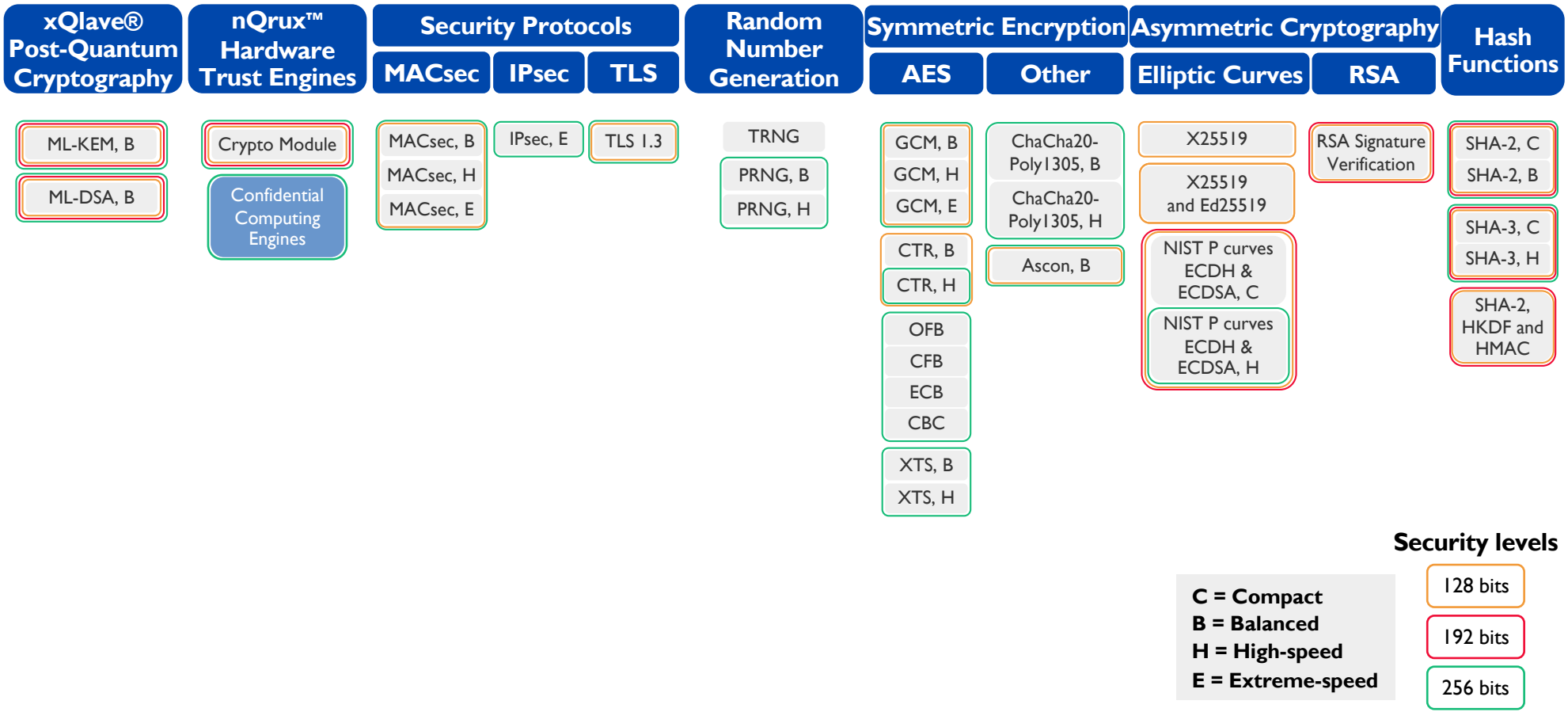


Software vs Hardware

Application

FPGA/ASIC
cryptography and keys

Xiphera Portfolio



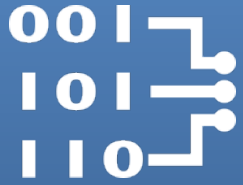
Why Xiphera?

Compact / high-performance solutions

Agile and nimble team

Fully hardware-based implementations

Roadmap to future cryptographic applications



In-house designed products & cryptographic expertise

Ability to support both VHDL and SystemVerilog design flows

To Summarise

Cryptography is the foundation for security.

Xiphera protects your critical systems by designing security directly into hardware.

We have a committed roadmap for future's cryptographic standards.


XIPHERA
Let's secure your business together.
Xiphera Ltd.
www.xiphera.com
sales@xiphera.com

Appendix

Example Customer Cases

EMEA Satellite Tech Company

- **Customer pain:** Securing the ground station ↔ satellite communication link
- **Solution:** Xiphera AES IP core securing both confidentiality and authenticity

Abstraction Levels