CYBERSECURITY IN SPACE

HOW ELECTRONIC COMPONENTS CAN CONTRIBUTE TO SECURE SPACE SYSTEMS?

MICROCHIP®

Jeremy Plantier *– Principal Field Application Engineer*

Microchip At a Glance

Founded
February 14, 1989

Headquartered in
Chandler, AZ
‘The Silicon Desert’

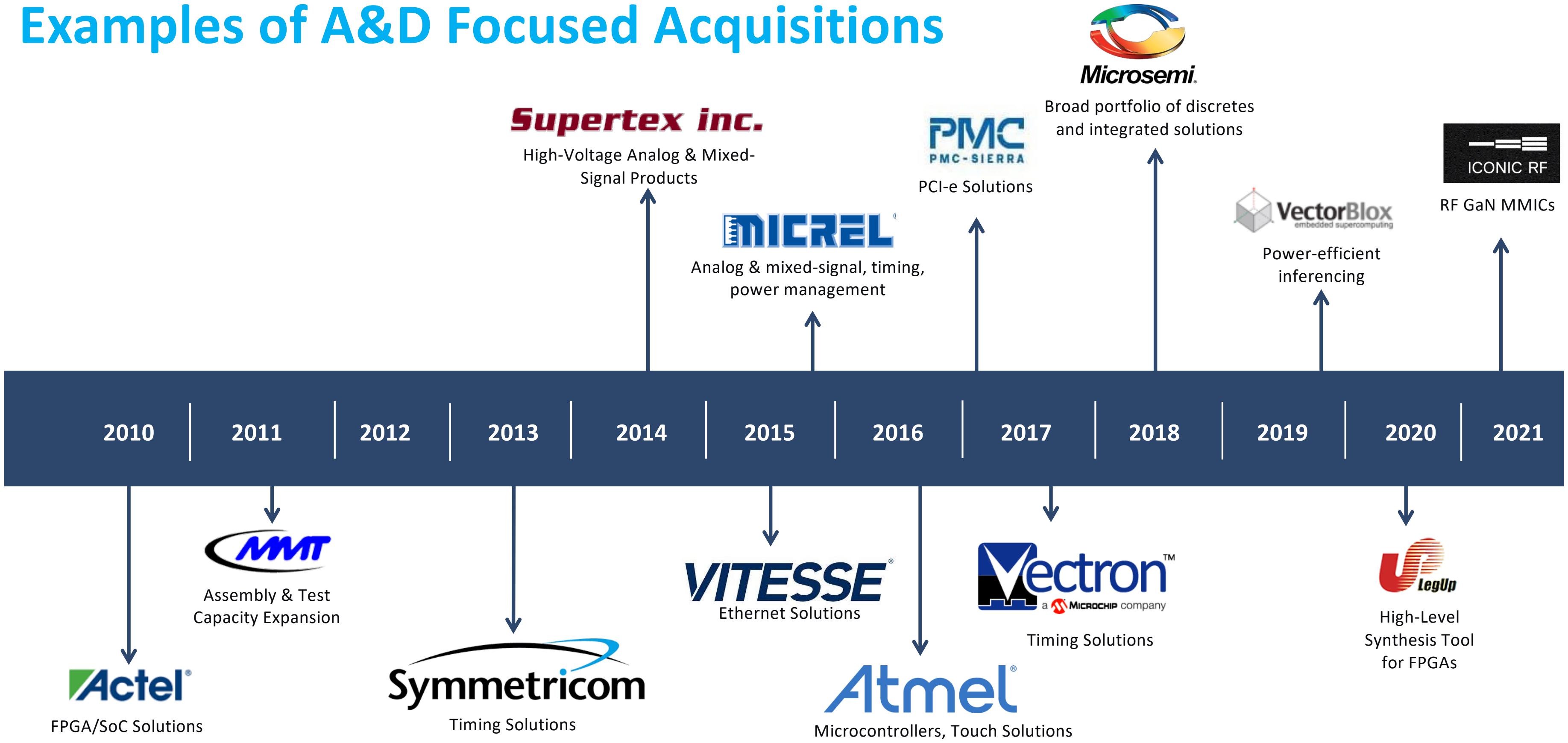
22,000+
Employees

100,000+
Product Offerings

$7.6B revenue
FY2024

Expanding Microchip Solutions Through Acquisitions

Examples of A&D Focused Acquisitions



2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021

Actel
FPGA/SoC Solutions

MMT
Assembly & Test Capacity Expansion

Symmetricom
Timing Solutions

Supertex inc.
High-Voltage Analog & Mixed-Signal Products

MICREL
Analog & mixed-signal, timing, power management

VITESSE
Ethernet Solutions

Atmel
Microcontrollers, Touch Solutions

PMC PMC-SIERRA
PCI-e Solutions

Vectron™ a MICROCHIP company
Timing Solutions

Microsemi.
Broad portfolio of discretes and integrated solutions

VectorBlox embedded supercomputing
Power-efficient inferencing

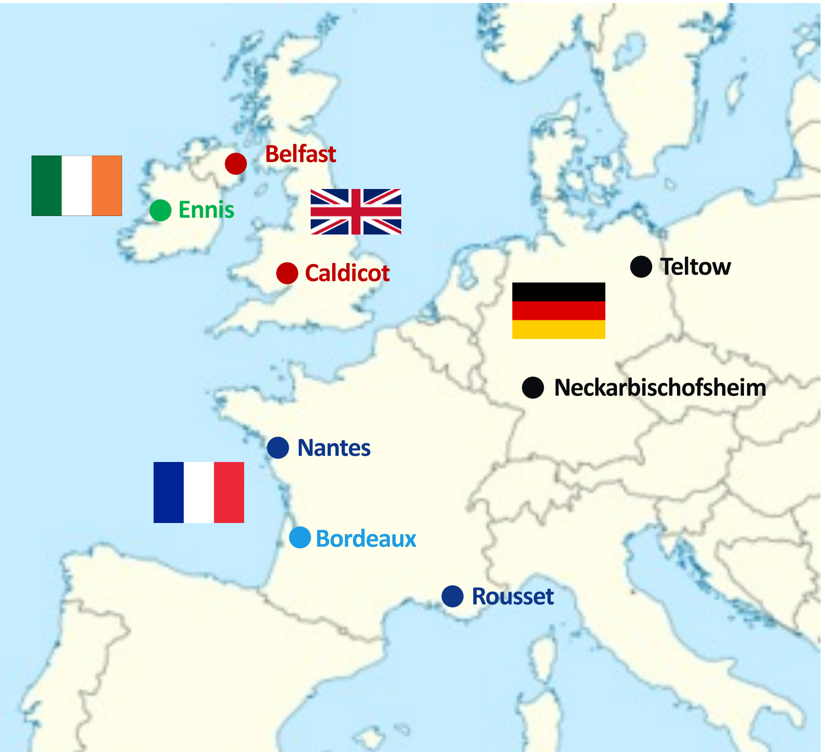
LegUp
High-Level Synthesis Tool for FPGAs

ICONIC RF
RF GaN MMICs

A&D Product Lines in Europe

Nantes, France

Rousset, France



- **Advanced Packaging UK**
  - ✓ Expertise in miniaturisation vs. size, power and reliability

- **ADG France**
  - ✓ Mixed Signal ASIC
  - ✓ Processors and Microcontrollers
  - ✓ Com interfaces and Memories
- **DPM France**
  - ✓ Power Modules
- **DPM Ireland**
  - ✓ Hi-Reliability Discrete
  - ✓ Power Modules
- **Vectron Germany**
  - ✓ Oscillators
  - ✓ RF SAW Filters
- **RF Microwave UK**
  - ✓ Amplifiers

Vectron™ a Microchip company

ICONIC RF a Microchip company

Bordeaux, France

Ennis, Ireland

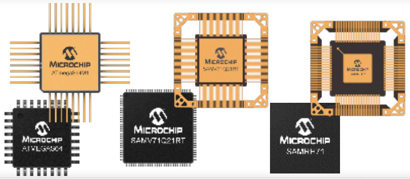
Belfast, UK

Teltow & Neckarbischofsheim, Germany

Largest Space Semiconductors Portfolio

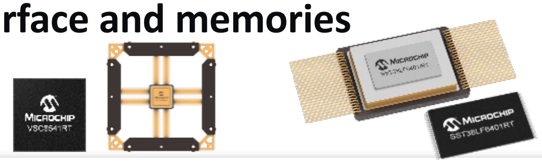
MPUs and MCUs

8-bit AVR®
32-bit SPARC V8 and arm M3 & M7
GNSS SoC



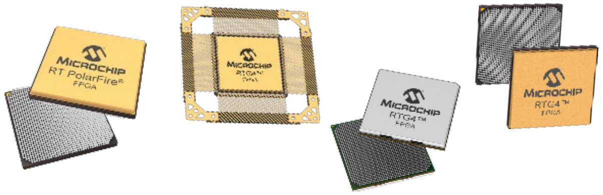
Communication Interface and memories

SpaceWire, Ethernet, CAN
SRAM
NVM memories



FPGAs

RT PolarFire®
RTG4™
RT ProASIC3®
RTAX™, RTSX-SU

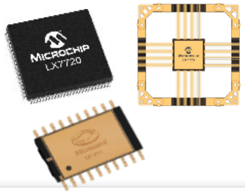


Power Solutions

Rad-hard JANS Diodes, Bi-Polar Small Signal Transistors
Rad-hard Isolated DC-DC Converter Modules
Custom Power Supplies 2 W to > 5 KW
Point of Load Hybrid Solutions
Electromechanical Relays

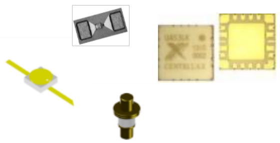
Mixed Signal Integrated Circuits

Telemetry and Motor Control Space System Managers
Power Supply protection



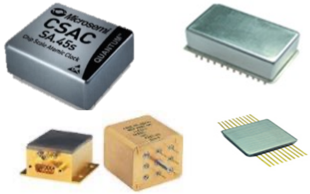
RF Products

Packaged and Chip Si and GaAs RF Diodes,
SAW filters,
Packaged and bare die GaN and GaAs MMICs
GaN on SiC HEMT transistors



Timing solutions and Oscillators

Ovenized Quartz Oscillators
Hybrid Voltage Controlled and
Temperature Compensated Crystal Oscillators
Cesium Clocks
Chip Scale Atomic Clock (CSAC)



MICROCHIP
Aerospace & Defense

Why do we need to worry about Cybersecurity?

Economic and National Security Crisis

- **2023 - Cybercrime cost > $1T/yr in total economic impact**
  - 2,200 Cyberattacks occur daily (generating $265B in revenue)
  - 80% of attacks were against end users in 2023 (primarily phishing)

- **Cybercrimes against infrastructure are a "National Security Threat"**
  - Energy, communications, hospitals, manufacturing, and transport are being shut down by ransomware
  - 2,000% increase in ransomware attacks from 2019 to 2023
  - 70% of ransomware attacks in 2023 were directed at manufacturing
  - Federal, State, International, and Insurance providers are enacting requirements and large penalties for "negligent" companies to force "good cyber hygiene"

Selected Consumer Cyber Legislation

Legislation	Region	Date Approved	Date Effective	Overview
Product Security and Telecommunications Infrastructure Act - *Penalties > £10M or 4% of revenue*	UK	2022	April 2024	- Must inform buyers on how long they will receive SW updates before purchase - No universal passwords - Process for buyers to report issues
Radio Equipment Directive Article 3.3 Cybersecurity - Penalties *TBA before August 2024*	EU	2022	August 2025	- Safeguards to protect PII - Safeguards to protect against fraud - Safeguards to ensure updates are authenticated (secure boot & updates) - Harmonizing with **ETSI EN 303-654**
Cyber Resilience Act to improve security *- Penalties > €10M or 2% of revenue*	EU	April 2024	April 2027	- Voluntary until 2027 - 24 hours to report active incidents - Disclose and provide updates for the expected life of the product
Cyber Trust Mark Consumer Labelling - *Voluntary program for 12 months*	US	March 2024	Oct 2024	- Logo and QR code - Simple disclosure of update period
Security and Exchange Commission Cybersecurity risk report	US	2022	Dec 2023	- Public companies must disclose cybersecurity risk management policy - Attacks and vulnerabilities reporting

Cyber Security 2024: Key Takeaways

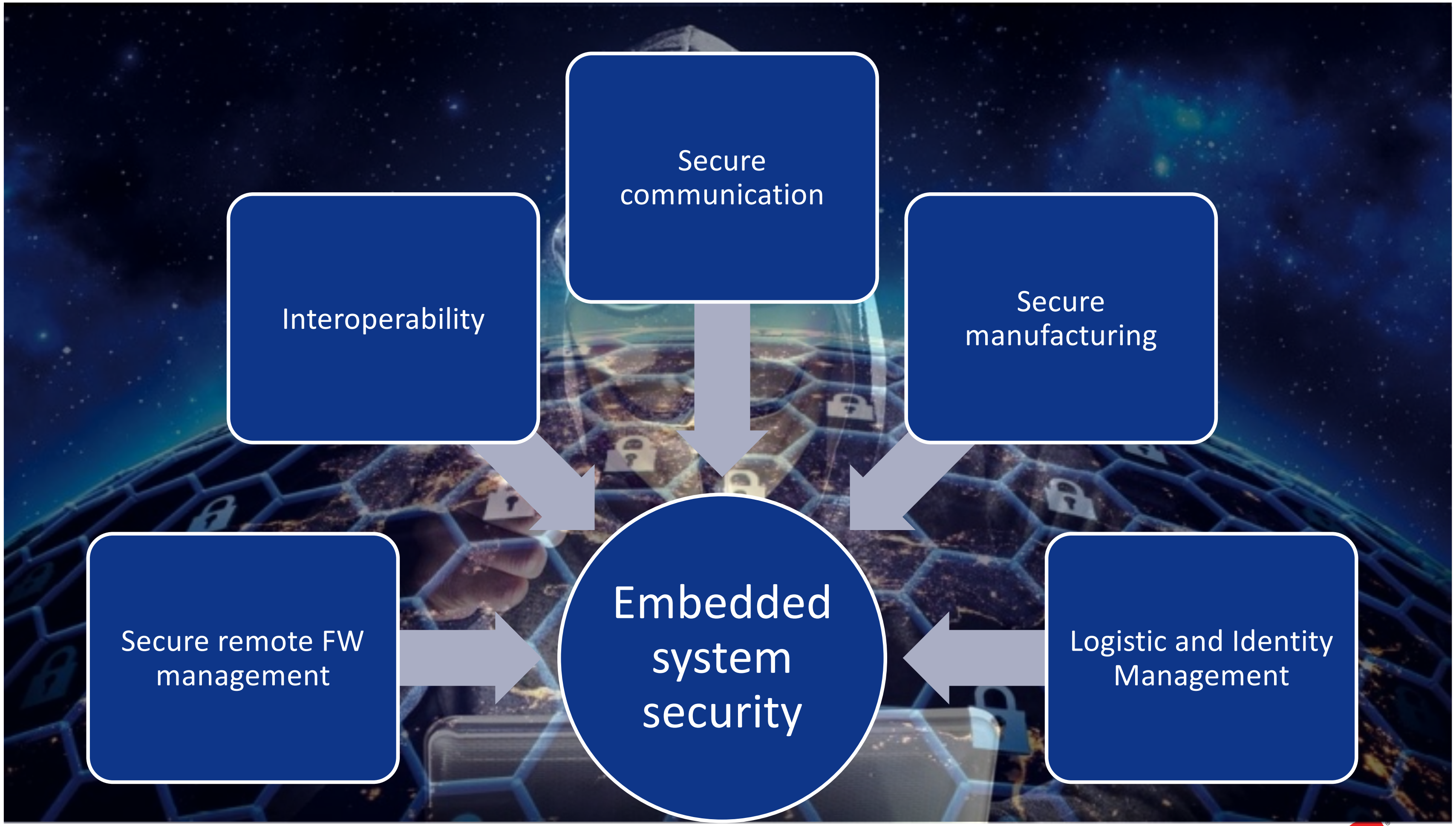
- **Security is no longer optional**
  - Requirements from Federal, Local, and Insurance Underwriters
- **Liability moving to software OEMs for damages**
  - Secure Software Development Frameworks - Required
  - Supply chain management - Required
  - Software Bill of Materials (SBOMs) – Required

- **Vulnerabilities need to be reported in days**
- **Patches need to be available in 30-90 days**

Number of patches and time to fix is a major new support cost for OEMs

- Awareness growing that “weak” security can be very expensive

Embedded Security for Space Application



Secure communication

Interoperability

Secure manufacturing

Secure remote FW management

Embedded system security

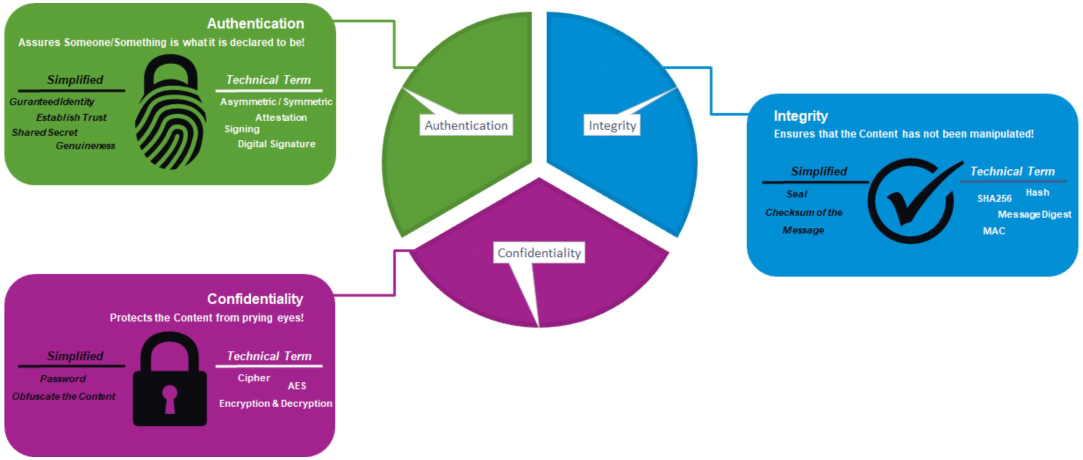
Logistic and Identity Management

Today’s weaknesses

- Security by design : embedded security is now being **considered but hard to implement**
- Lack of education : The **chain of trust** principle is not well understood, complex, hard to implement and consequently **incorrectly implemented**
- Keys/Certificates mishandling**: Private keys** are being handled by software at best and **left accessible in the clear** of the system memory
- **Backdoors** are consequently left open to hackers – they attack the weakest point, in IoT, the **unsecure software** and exploit the **user habits**
- **Manufacturing is not trustable nor scalable,** not secure and create scalability issues

Secure Systems for Space ?

- **Secure systems deployed in other industry based on 3 fundamentals**



Authentication

Assures Someone/Something is what it is declared to be!

Simplified

GuranteedIdentity

Establish Trust

Shared Secret

Genuineness

Technical Term

Asymmetric / Symmetric

Attestation

Signing

Digital Signature

Authentication

Integrity

Confidentiality

Integrity

Ensures that the Content has not been manipulated!

Simplified

Seal

Checksum of the Message

Technical Term

SHA256

Hash

Message Digest

MAC

Confidentiality

Protects the Content from prying eyes!

Simplified

Password

Obfuscate the Content

Technical Term

Cipher

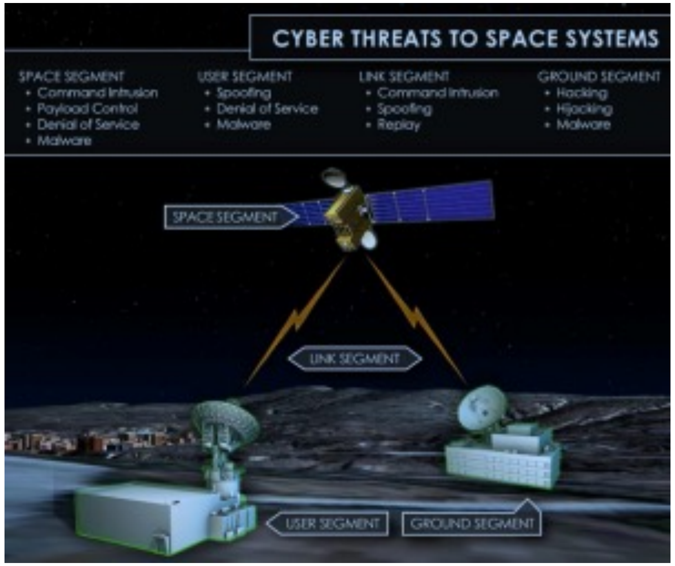
AES

Encryption & Decryption

- **Requires public algorithmes for more interoperability & robustness.**

- **Secure key management becomes the main challenge.**

- **Targeted use cases for space**
  - Secure Telemetry / Telecommand connectivity (Earth <-> Space) – Ongoing CNES activity
  - Secure inter satellites communication
  - Secure space stations, robotics & rover interaction
  - Reconfigurable Platform & Feature integration

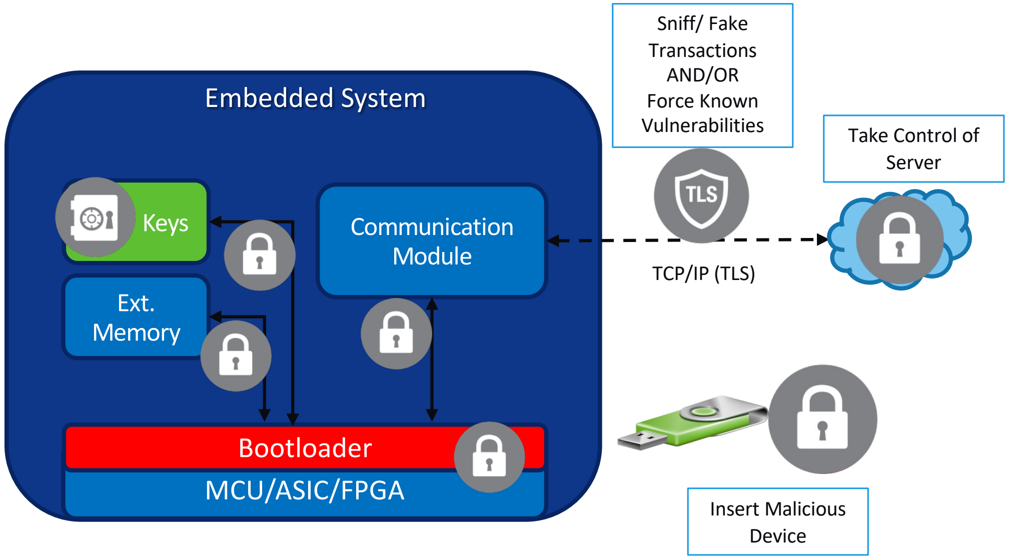


Everything starts with : Threat Modelling

Defining Hack-resilient systems

- **Define system requirements**
- **Risk Analysis**

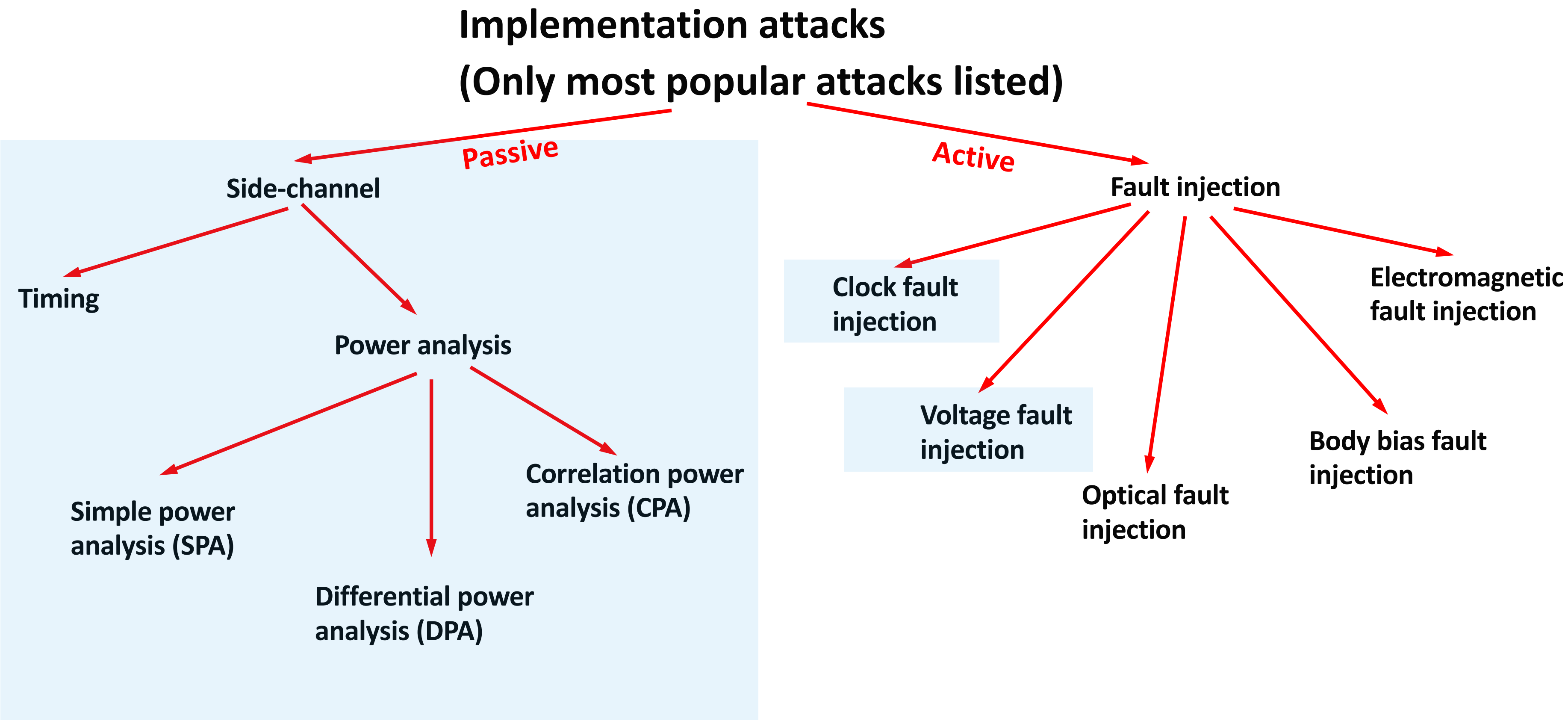
→ Security Implementation



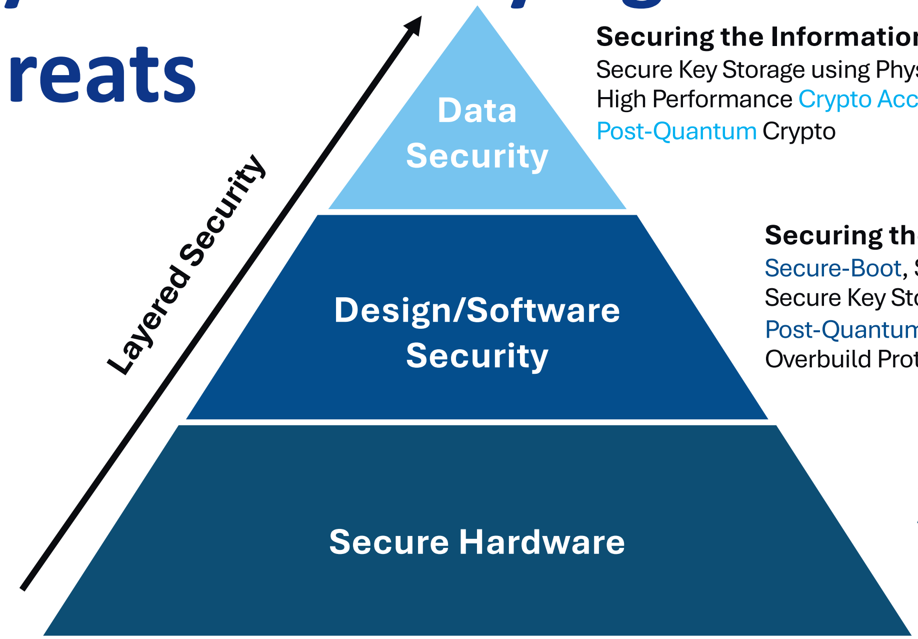
Output of the Threat Model = USE CASES

Consider Microchip security partners

Hardware Attacks Clarification


Implementation attacks
(Only most popular attacks listed)
Passive
Active
Side-channel
Timing
Power analysis
Simple power analysis (SPA)
Differential power analysis (DPA)
Correlation power analysis (CPA)
Fault injection
Clock fault injection
Voltage fault injection
Optical fault injection
Body bias fault injection
Electromagnetic fault injection

Layered Security Against Physical and Cyber Threats

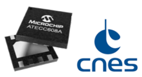


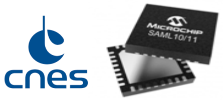
Securing the Information
Secure Key Storage using Physically Unclonable Function (PUF)
High Performance Crypto Accelerators
Post-Quantum Crypto

Securing the Application and Infrastructure
Secure-Boot, Secure Provisioning
Secure Key Storage using Physically Unclonable Function (PUF)
Post-Quantum Crypto
Overbuild Protection

Securing the Hardware
Secure Manufacturing
Anti-Tamper (Detection and Response)
Side Channel Countermeasures
NIST-certified Accelerators

Delivers Unparalleled Security for Critical Space Infrastructure


Secure Elements
TA101RT


32-bit Microcontrollers
SAMV71
SIP RT (SAME54RT + TA101RT)
SAMRHM7+
- Rad Hard SoC
- MCU + Secure Element (HSM)

FPGA

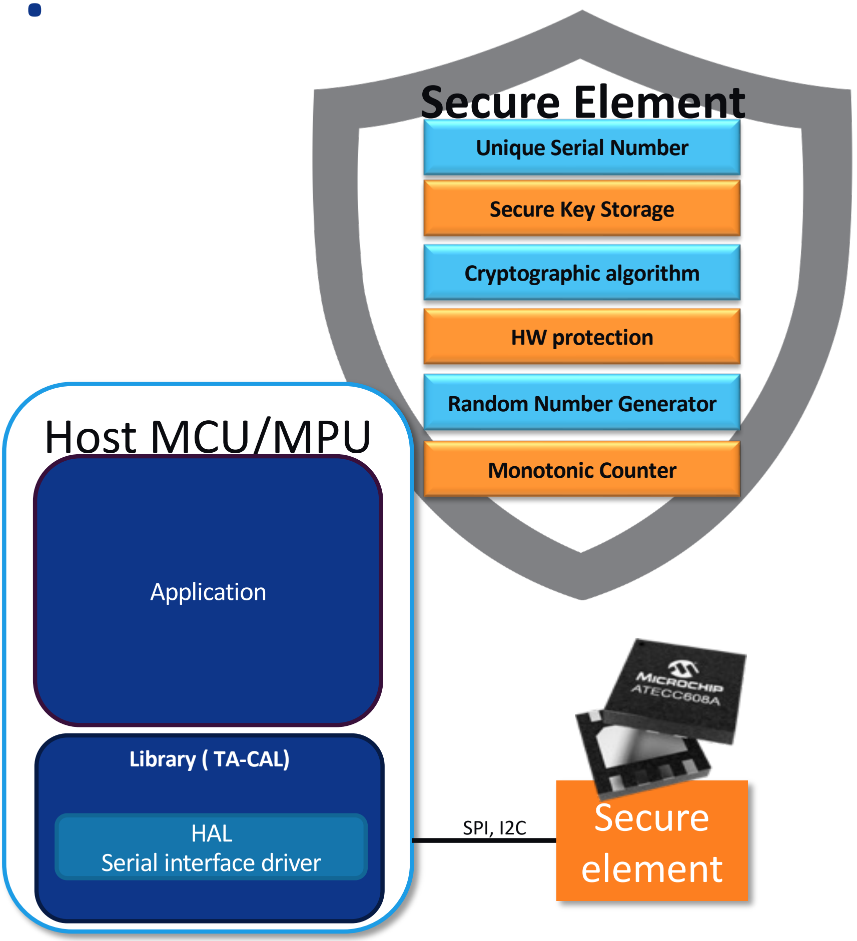
PolarFire &
PolarFire SoC

64-Bit RISC-V
Microprocessors

MICROCHIP Aerospace & Defense

What is a Secure Element ?

- Unique identity
- Protected KEYs for a *lifetime*
- Cryptographic acceleration
- Scrambled and encrypted memory
- Random Number Generator
- Monotonic counters



Secure Element

Unique Serial Number

Secure Key Storage

Cryptographic algorithm

HW protection

Random Number Generator

Monotonic Counter

Host MCU/MPU

Application

Library (TA-CAL)

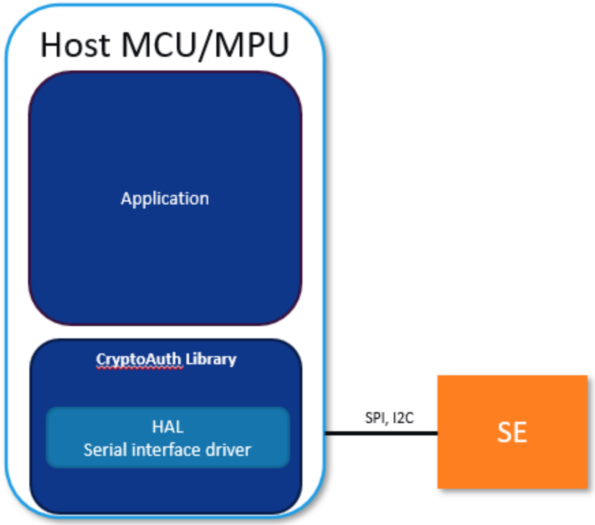
HAL
Serial interface driver

SPI, I2C

Secure element

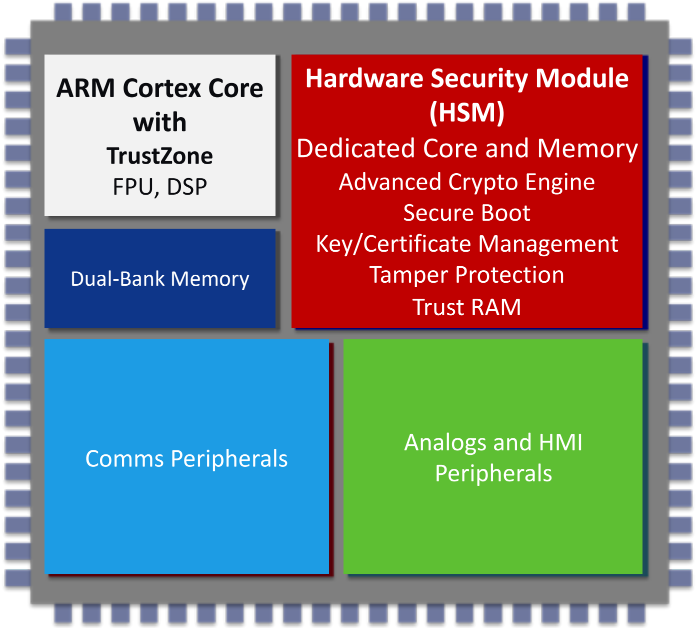
Increase Security by Hardware Isolation

Secure Elements SE



- Physical protection of keys
- HW accelleration of secure function
- True random number generation

Trusted Execution Enviroment TEE + embedded Hardware Secure Module (HSM)



- TEE handles all security related tasks
- Trusted OS or bare metal

Hardware Security Module

Establishing a Root of Trust

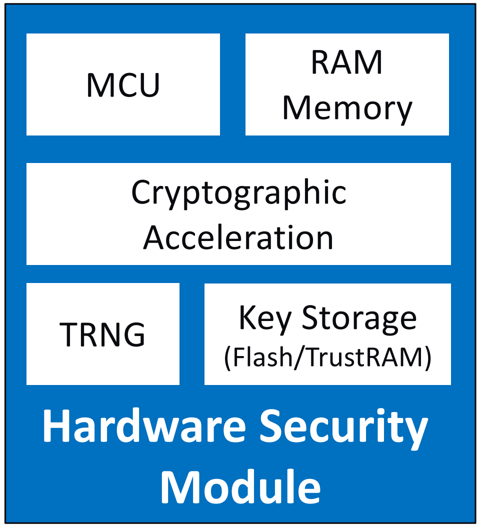
- **Separate CPU/SRAM/HSM:**
  - Creates a hardware protected isolated security subsystem
  - Can work with TrustZone® to extend Secure Enclave to Memory and Peripherals
  - Dedicated secure RAM for key management and storage (TrustRAM)
  - Key Storage with optional encryption

- **Hardware Cryptography:**
  - True Random Number Generator (TRNG): NIST 800-90B
  - The hardware Cryptographic accelerators include AES, TDES, Chacha20, SHA, RSA, ECC, DH, Poly1305, etc.

- **HSM architecture is flexible allowing Microchip to easily implement new algorithms and additional requirements such as DICE**
  - Secure OTA HSM FW Updates and Secure Boot

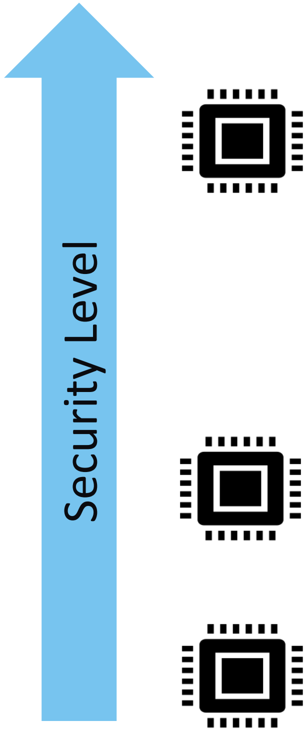
- **Automotive HSM Support (SHE, Evita Full, Bosch)**
- **HSM provisioning options: TrustFlex, TrustCustom**

- **Available on PIC32CK (Cortex® M33) and PIC32CZ (Cortex® M7)**



Microchip Cybersecurity Architectures

Not a one size fits all approach



Security Level

- **Secure Element (SE)**
  - Shares no resources with the host, electrically isolated
  - Tamper-proof
- **Hardware Security Module (HSM)**
  - Isolated secure enclave with dedicated MCU and secure RAM
  - Fastest cryptographic engines with the widest range of operations
  - Provides most secure MCU-based solution for key management and secure storage
- **Hardware Security Module – Lite (HSM-Lite)**
  - Shares host CPU for management operation; does not expose keys/secrets to host
  - Fast cryptographic engine with wide range of operations
  - Dedicated secure RAM for key management and storage
- **Crypto Accelerators**
  - Off-loads cryptographic operations from the host CPU
  - Most recent Microchip 32-bit products include crypto accelerators

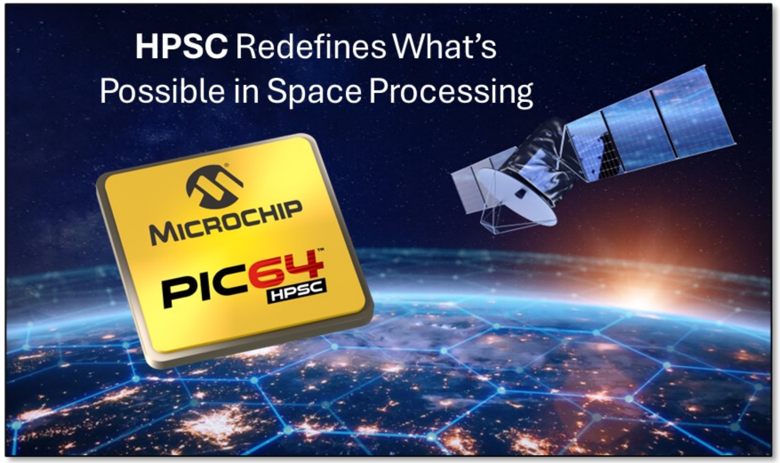
Summary

- **Space applications show the same vulnerabilities than any others field…**
  - But the criticity is highly different.
  - Many stages of the application process deployment must be considered.
  - Both sides (Earth base stations and remote space application) are impacted.
  - A mixed HW/SW solution must be considered, that involves electronic components designed to tackle this challenge.
  - High integrated security comes with expertise.

- **Microchip holds a major position in the cybersecurity for space by…**
  - Offering a leading & sophisticated portfolio of hardware and software solutions dedicated to the space industry.
  - Offering cybersecurity expertise within the different market addressed.
  - Being a long-time leader in providing solutions for aerospace actors.

HPSC – Redefining What’s Possible For Space

- **NASA JPL awarded contract to Microchip to develop the next-generation High-Performance Spaceflight Computing (HPSC) processor**
- **Provides >100X compute over current solutions**
  - **26K DMIPs** from multi-core, fault tolerant **RISC-V CPUs**
  - Optimized for **spatial and temporal partitioning**
  - **Vector engine** to accelerate AI / ML
- **Integrated TSN Ethernet in alignment with 802.1DP for Aerospace**
- **Defense – Grade Security including hardware accelerated post-quantum (ML-KEM, ML-DSA)**
- **Scalable Radiation Performance to enable any mission profile with a single H/W and S/W solution**
- **Target initial availability: Q1’2025**



Canada
Architecture, Design, Test
Management

France
Radiation, Qual, Manufacturing

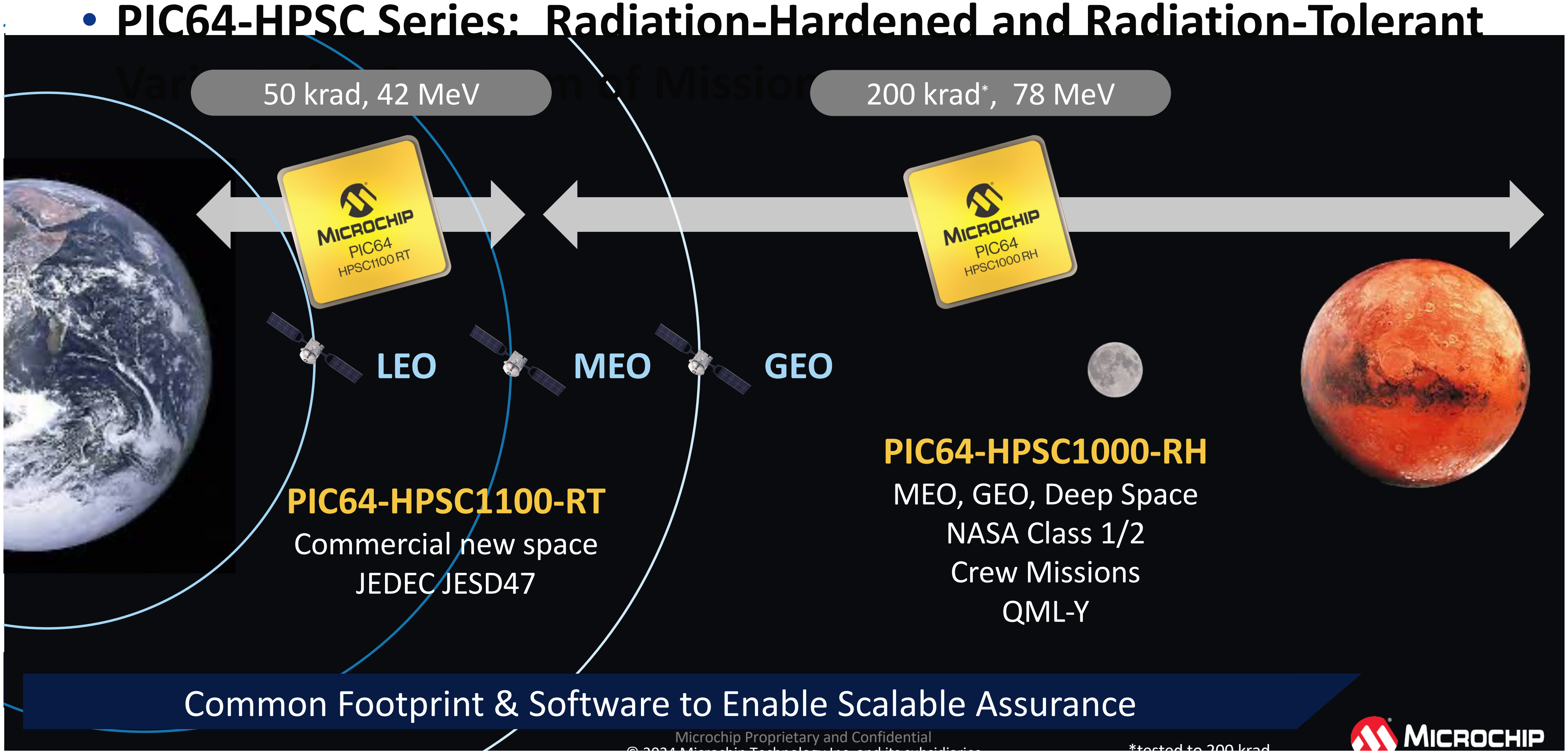
USA
Foundry, IP, NASA/JPL Sponsorship

EU
IP

Reference Single Board Computer design initiative w ESA

HPSC – From Low-Earth Orbiting to Deep Space

- **PIC64-HPSC Series: Radiation-Hardened and Radiation-Tolerant Vari [illegible] m of Missio**



PIC64-HPSC1100-RT
Commercial new space
JEDEC JESD47

PIC64-HPSC1000-RH
MEO, GEO, Deep Space
NASA Class 1/2
Crew Missions
QML-Y

Common Footprint & Software to Enable Scalable Assurance

Microchip Proprietary and Confidential

*tested to 200 krad

Thank You!

MICROCHIP
Aerospace & Defense