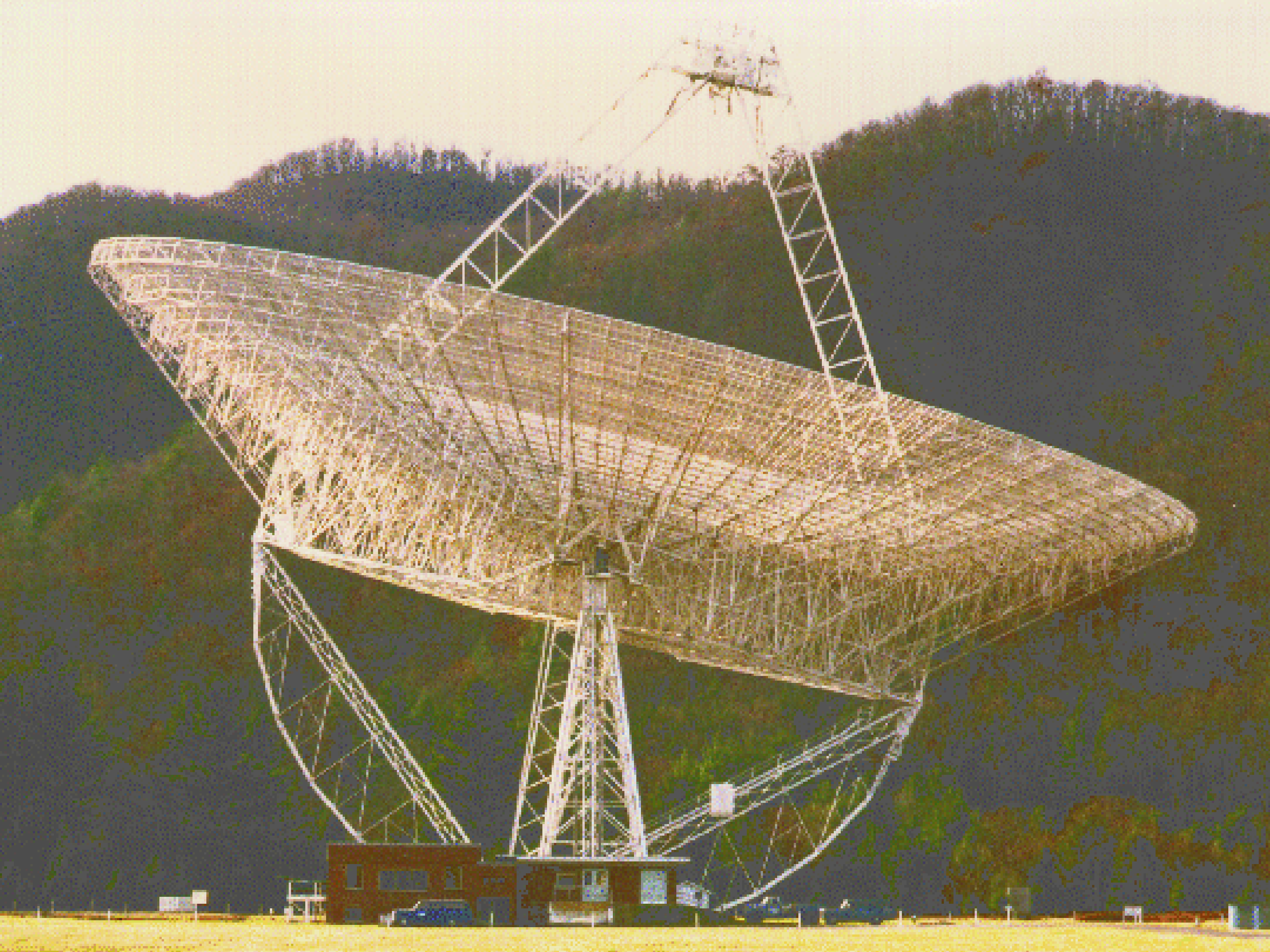
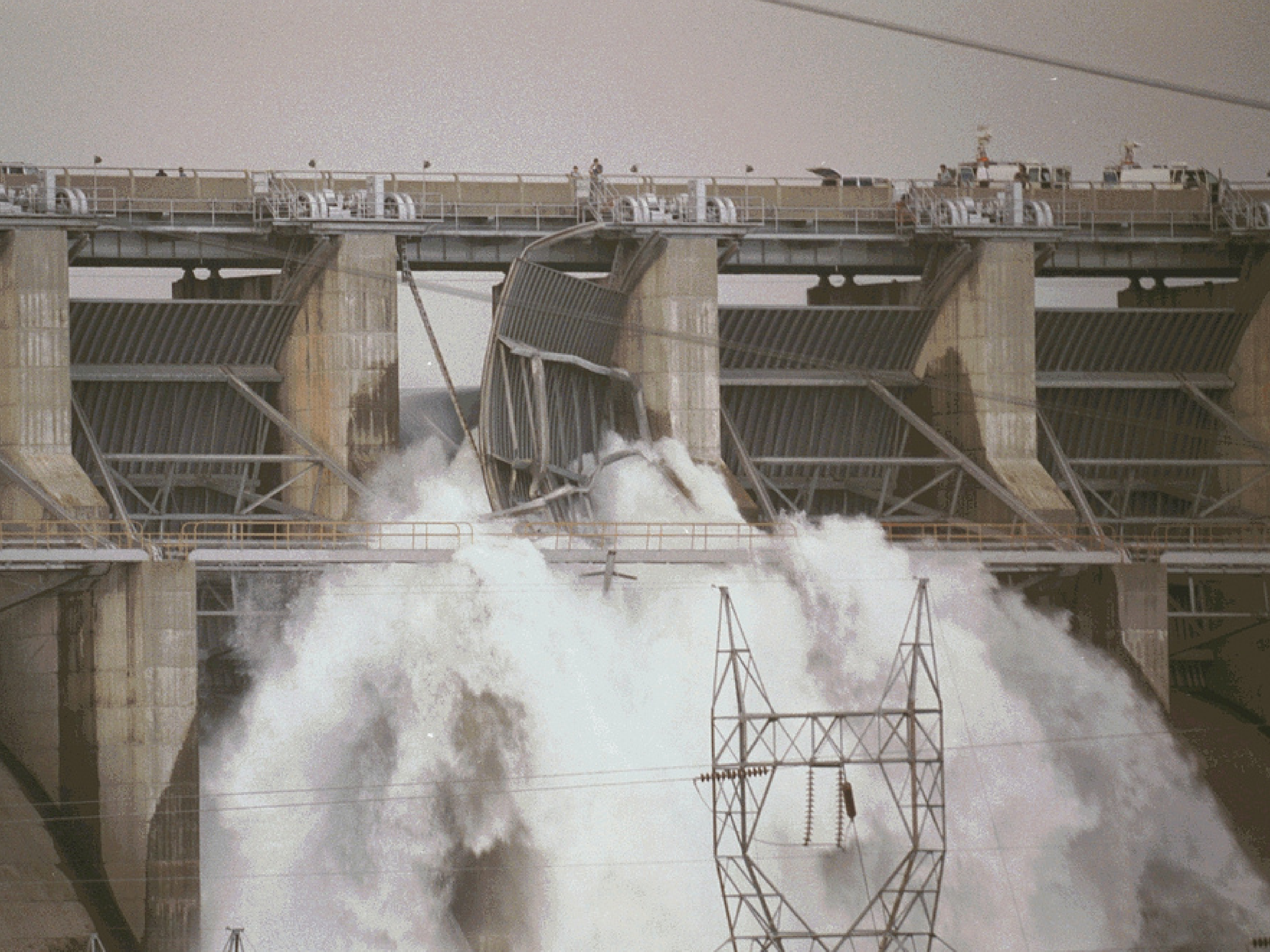
Space-Borne

Dependable Computing & High-Availability






HCG
和成
汽車
宏

Image Source: NASA

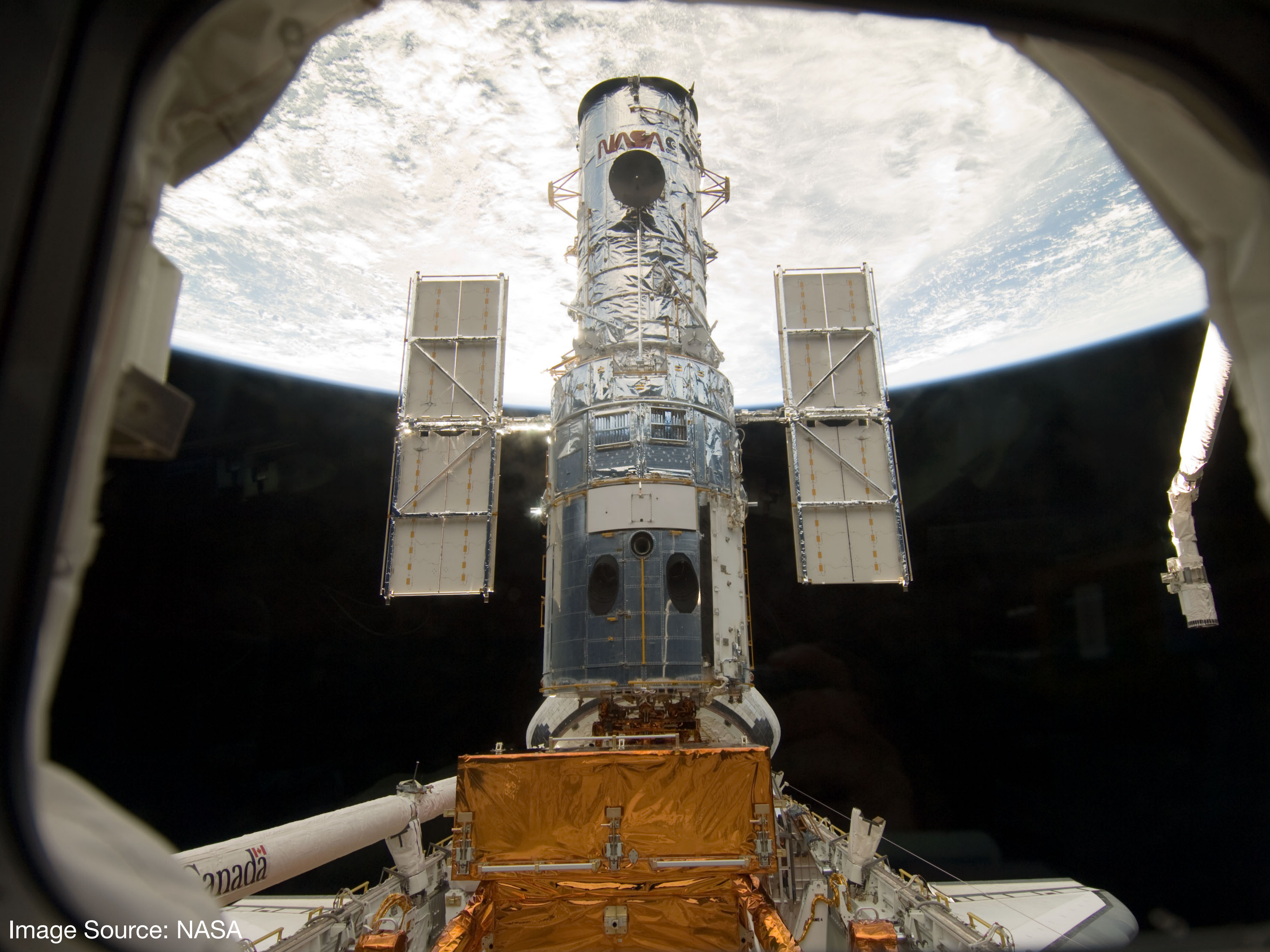


Image Source: NASA

TRL 9
- Actual system “flight proven” through successful mission operations

TRL 8
- Actual system completed and “flight qualified” through test and demonstration (ground or space)

TRL 7
- System prototype demonstration in a space environment

TRL 6
- System/subsystem model or prototype demonstration in a relevant environment (ground or space)

TRL 5
- Component and/or breadboard validation in relevant environment

TRL 4
- Component and/or breadboard validation in laboratory environment

TRL 3
- Analytical and experimental critical function and/or characteristic proof-of-concept

TRL 2
- Technology concept and/or application formulated

TRL 1
- Basic principles observed and reported

Design Restrictions for Electronics in Space

- Constrained power budget
- Form factor limitations
- Stress during launch
- Slim up- and downlink
- Operation in orbit

Image Source: ISC Kosmotras

Environmental Effects on Electronics in Space

- Extreme temperature shifts
- No heat dissipation through convection
- Radiation & Event Effects
  - Ionizing Dose, Displacement Damage, Latch Up
  - **Single- & Multi-Event Upsets**

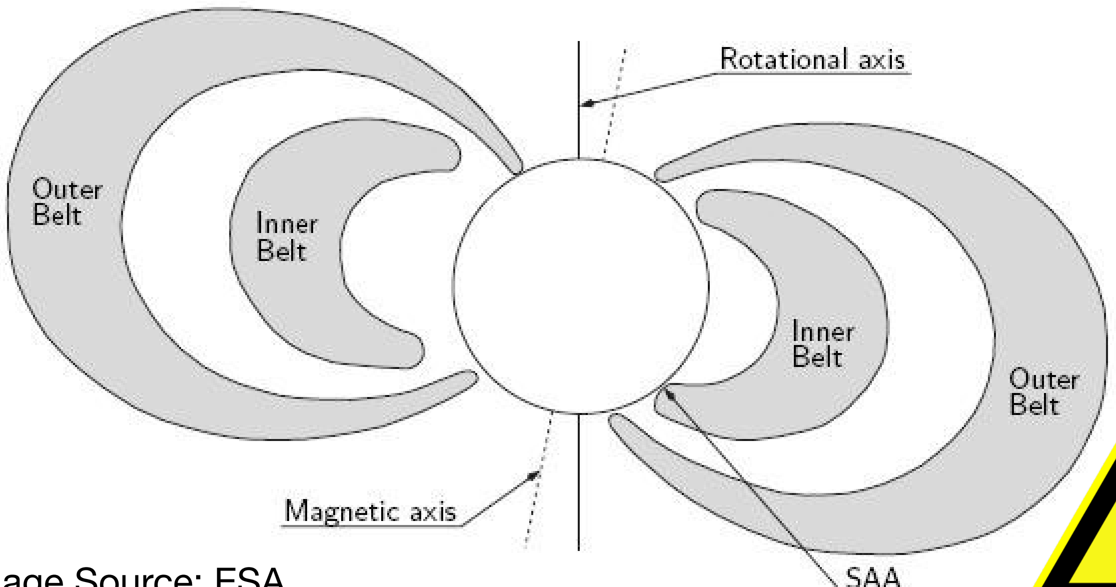
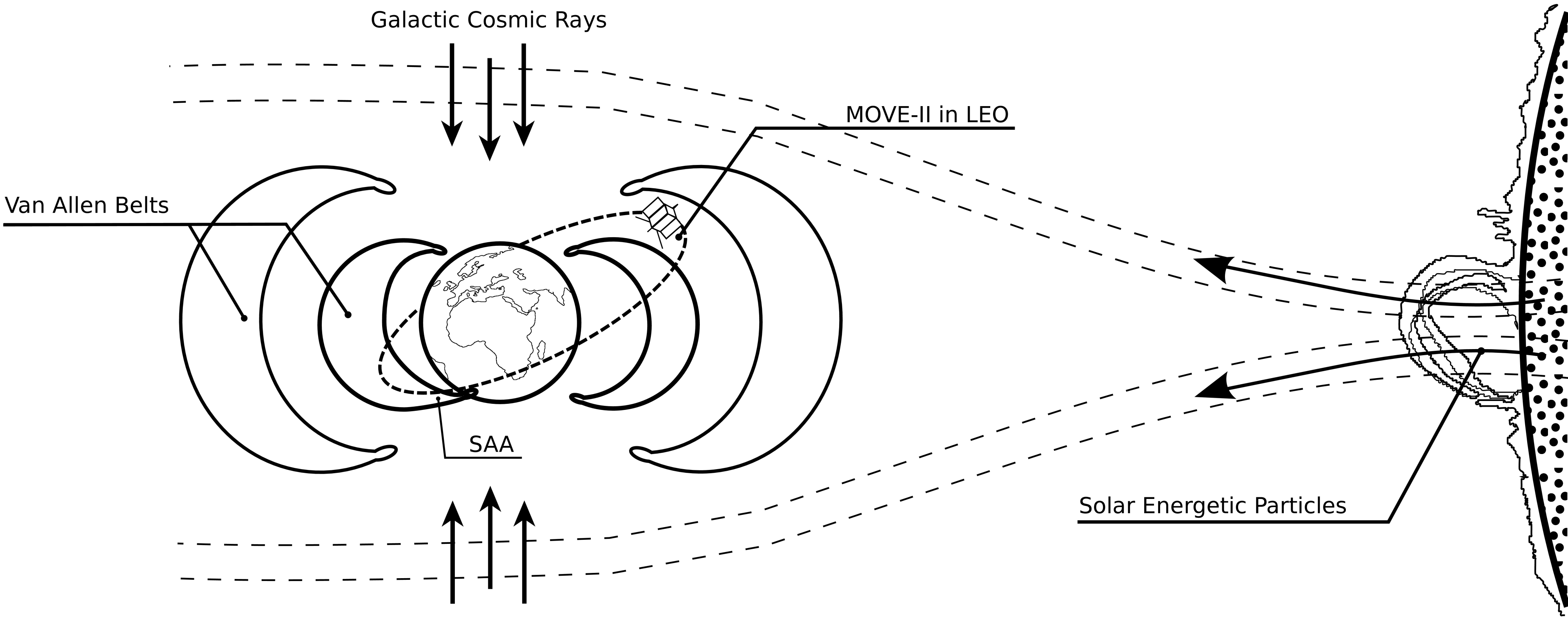
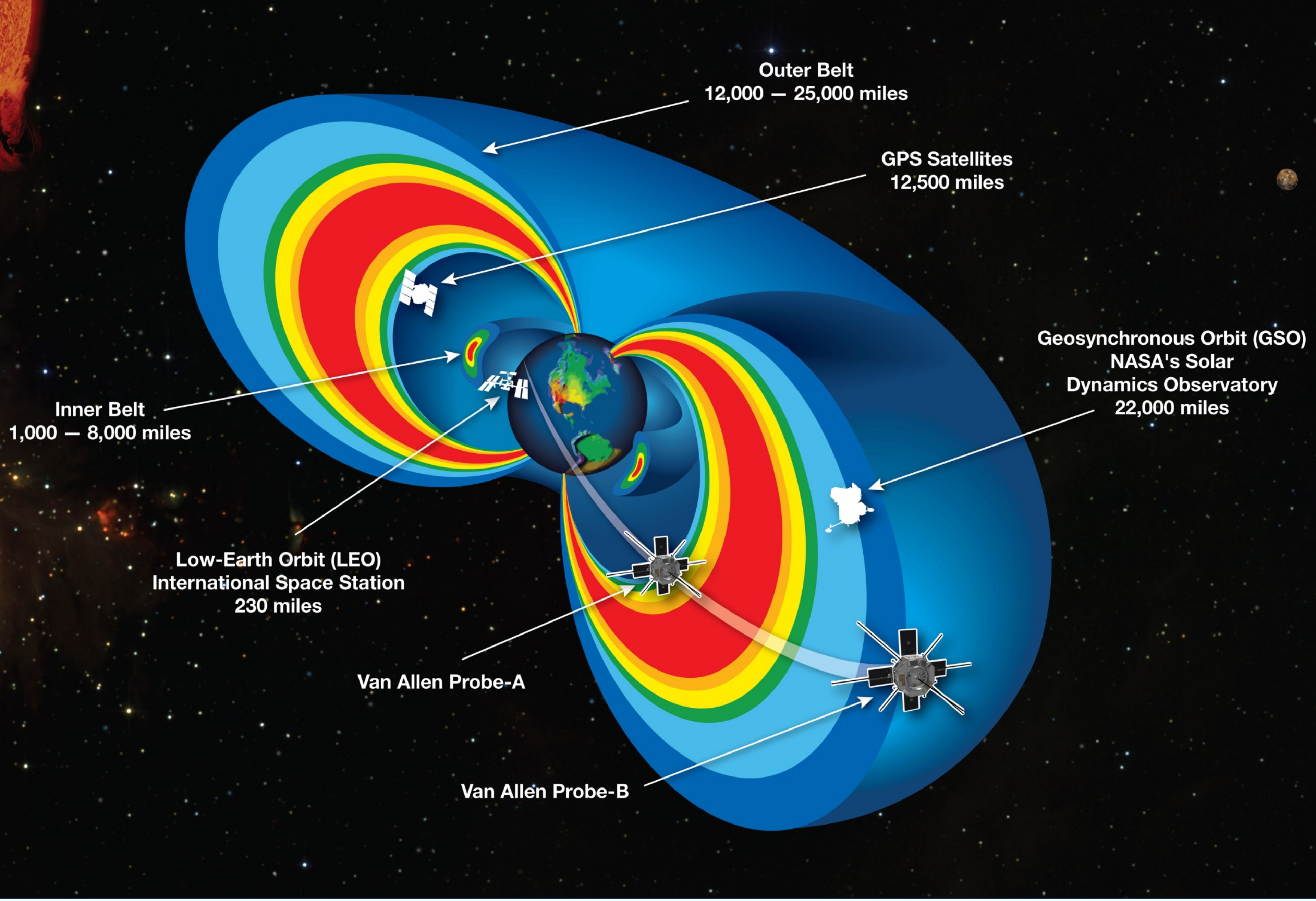
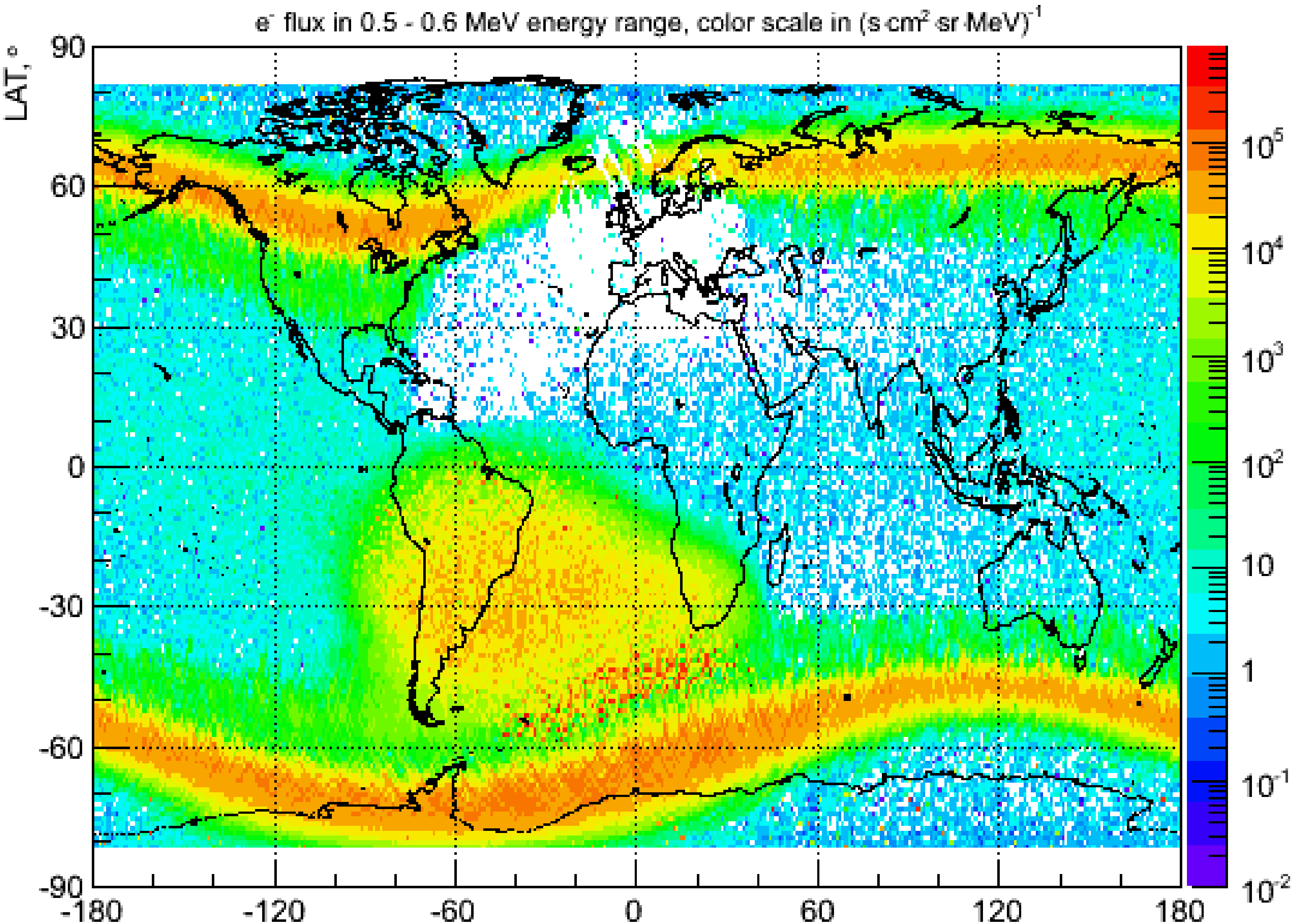


Image Source: ESA

Relevant Sources of High-Energy Particles

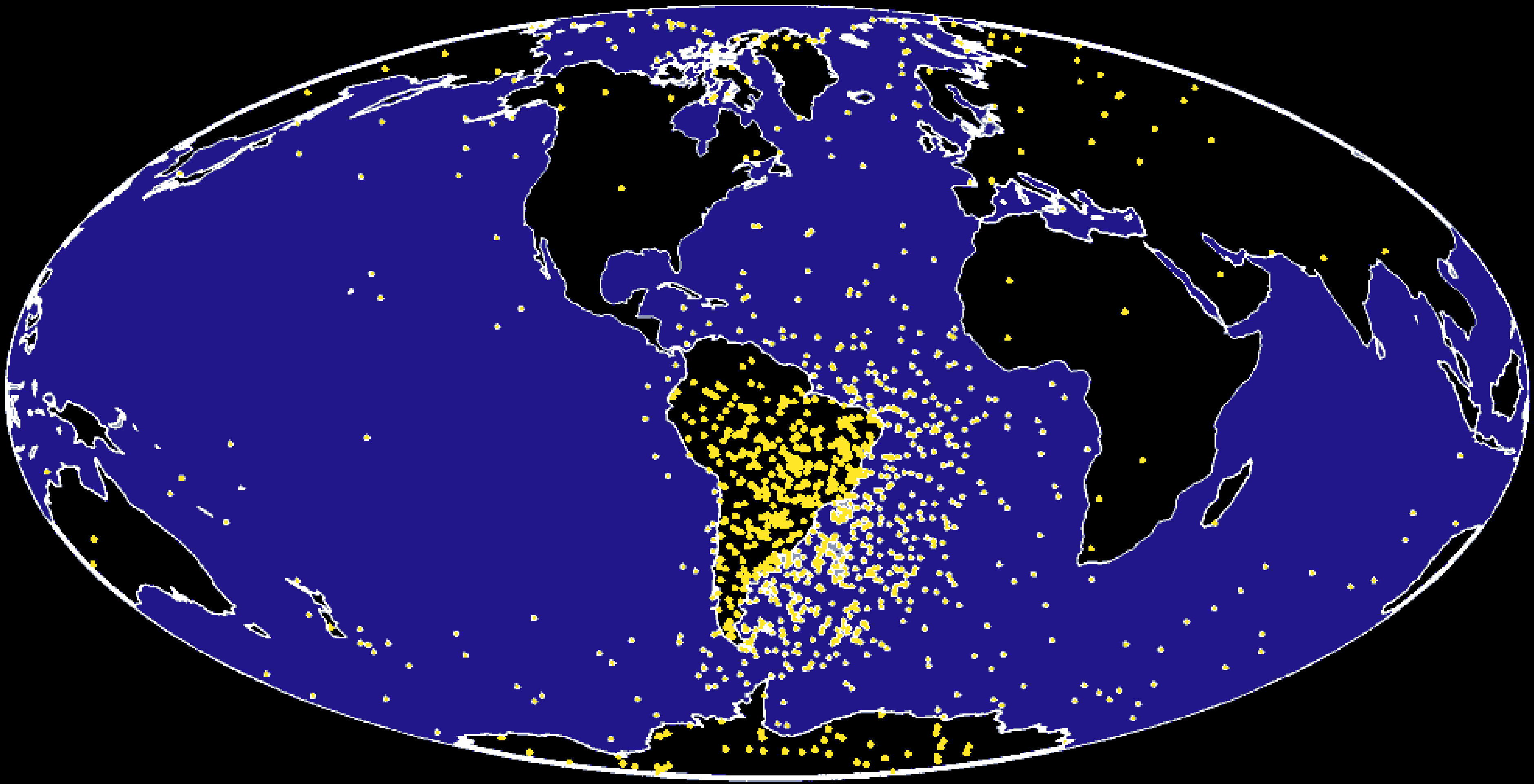



Outer Belt
12,000 — 25,000 miles
GPS Satellites
12,500 miles
Geosynchronous Orbit (GSO)
NASA's Solar
Dynamics Observatory
22,000 miles
Inner Belt
1,000 — 8,000 miles
Low-Earth Orbit (LEO)
International Space Station
230 miles
Van Allen Probe-A
Van Allen Probe-B



Source: Energetic Particle Telescope, ESA

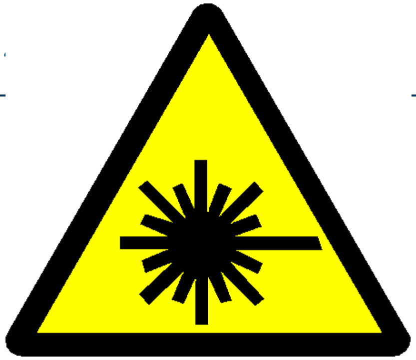
UOSAT-2 Memory Upsets



ESA/ESTEC The Netherlands

NOAA/NGDC Boulder

Rad-Hard Hardware



Components designed or tested to withstand radiation dosages up to a certain given threshold.

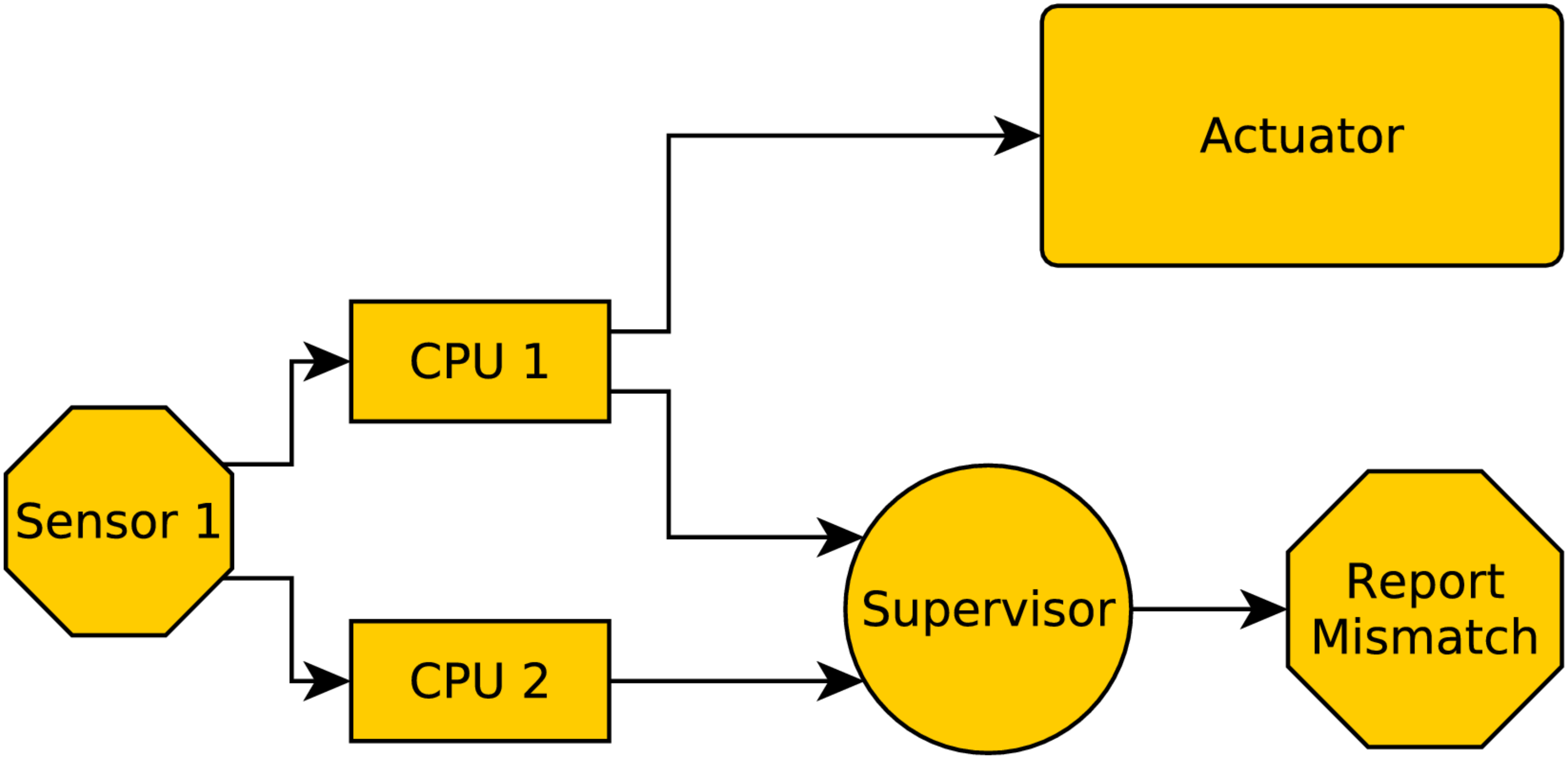
- Specialized manufacturing Techniques (SoI, ...)
- Shielding using aluminium, steel, lead, water, depleted boron, etc.
- Fail-Safe Logic & Architectures
- Software:
  - Error Detection And Correction (EDAC)
  - Fault detection, isolation & recovery (FDIR)
- → Extreme prices (> x1000)

Compute Consistency: The State of Affairs

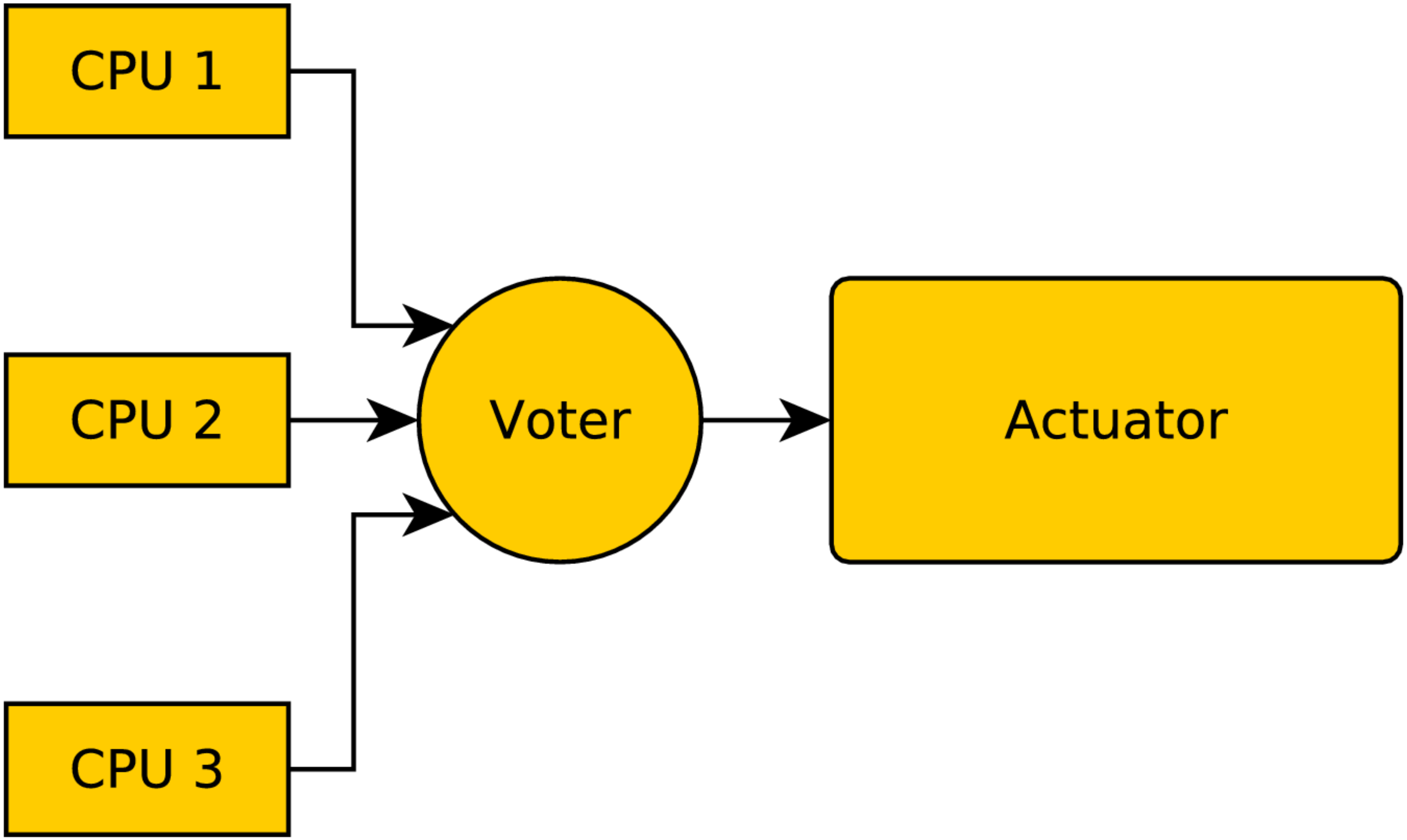
- Legacy Technology & Coarse Structures
- DMR/Supervised Processors
- TMR Approaches with COTS Processors
- TMR-ed Processor Designs (LEONx-FT)

- Ongoing Research:
  - NoCs, ManyCores & Grid Approaches

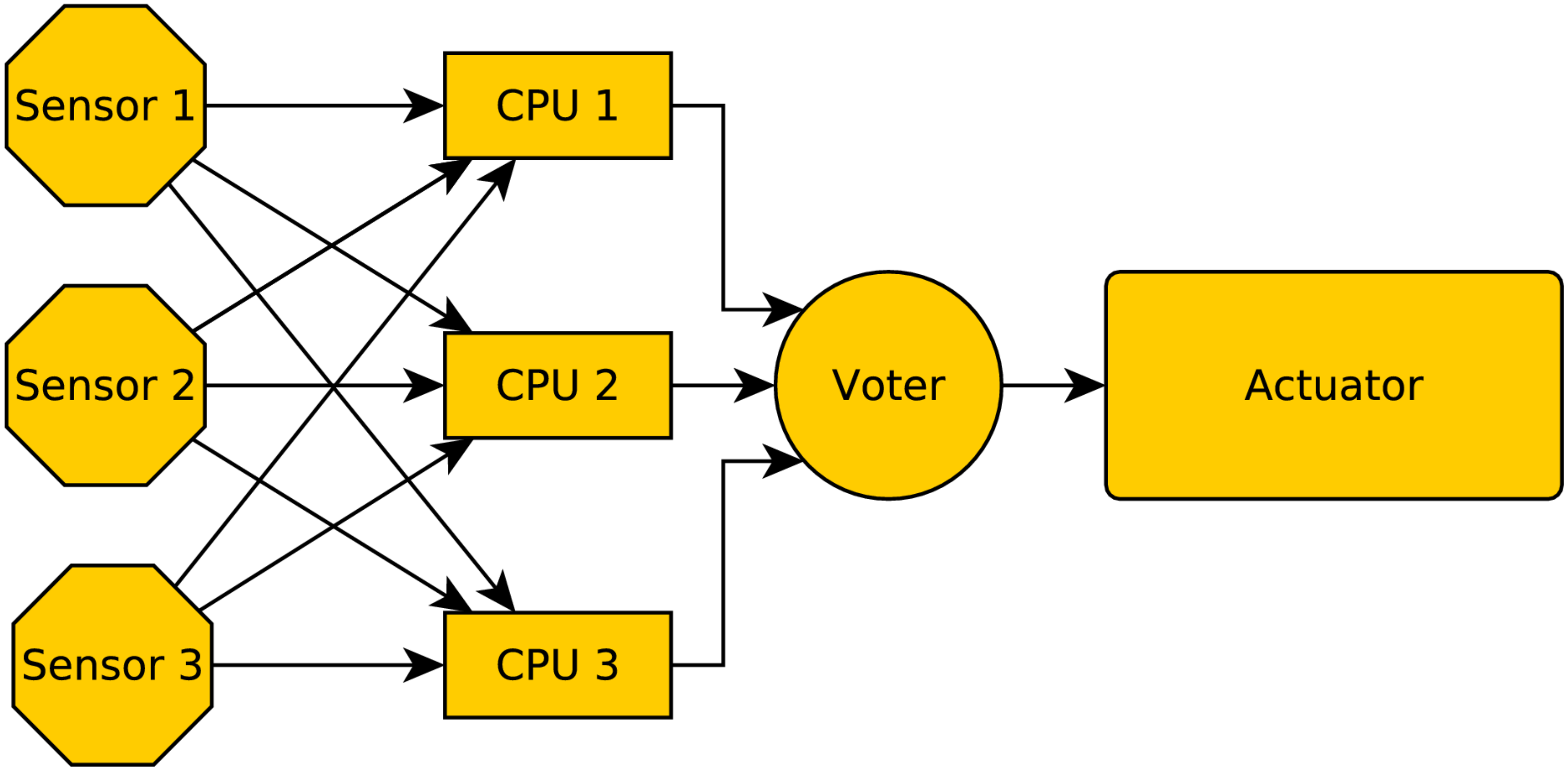
Dual Modular (Supervised) Redundancy



Majority Voting



Triple Modular Redundancy (TMR)



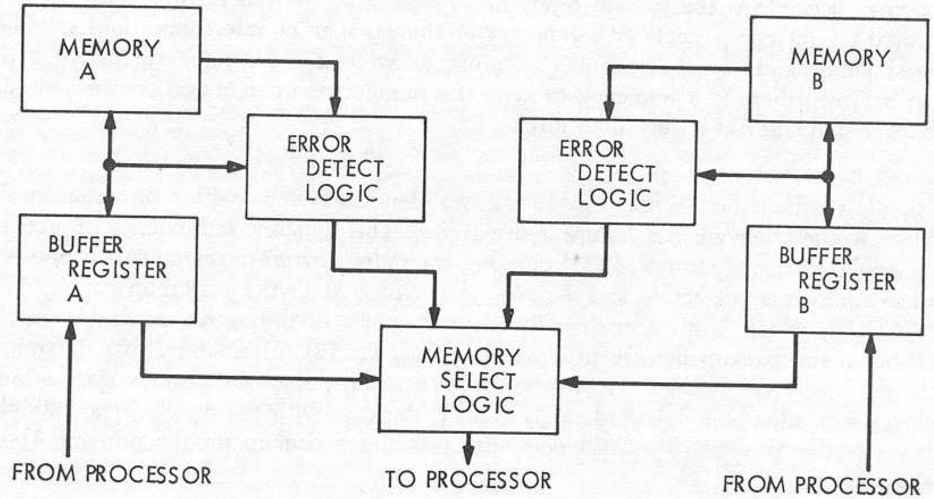


Figure 6.–Saturn 5–LVDC duplex memory diagram.

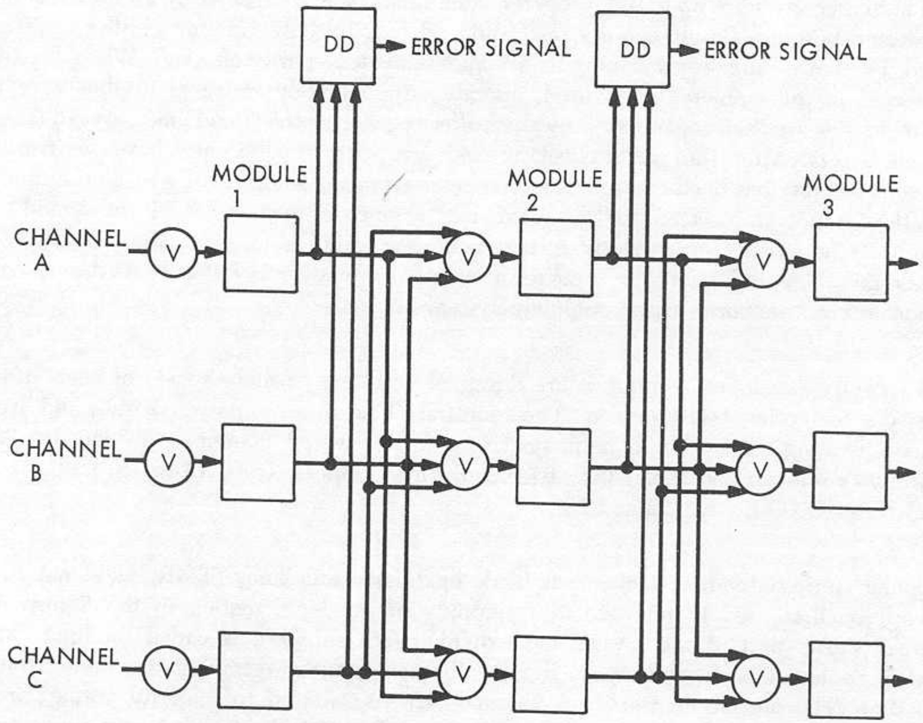
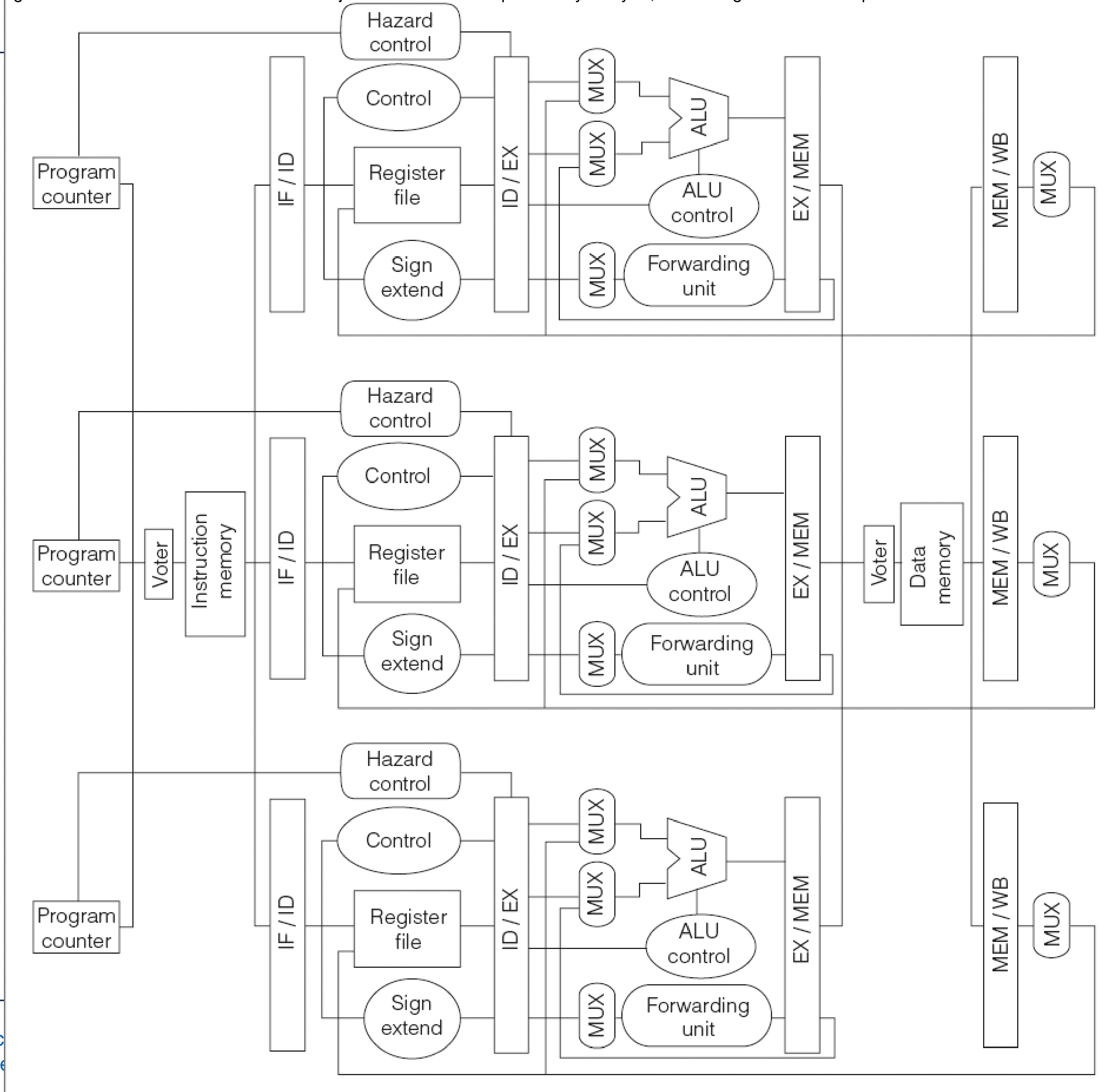


Figure 7.–Triple modular redundancy in Saturn 5–LVDC logic section.

Source: NASA, Office
of Logic Design

Source: Dongwoo Lee et. al.:A Novel Simulation Fault Injection Method for Dependability Analysis, IEEE Design & Test of Computers 2009 vol.26 Issue No.06 - November/December



Processors Commonly used in Spaceflight

- LEON Family
  - SPARCv8-like design, limited open source
  - -FT: fault-tolerance rad-hard version

- RAD6000: IBM RISC Single Chip

- RAD750, RADe5500
  - PowerPC derivates
  - Usually used for “number crunching”

- Custom Instruction Set Architectures (MIL-STD-1750A)
- Many small microcontrollers and custom ASICs

Compute Consistency Challenges

- Multithreading, Branch Prediction & Multi-level Caching
  - Add non-determinism
  - Make voting difficult, but not impossible
  - No way around that...
- Virtualization & Multicore CPUs
  - Make hardware voting impossible
  - Error detection through checksumming is still possible
  - But no recovery, thus external monitoring necessary
- Solutions for virtualized OBCs
  - Hypervisor-based voting
  - VM lockstepping
  - VM cross-validation

Image Source: NASA

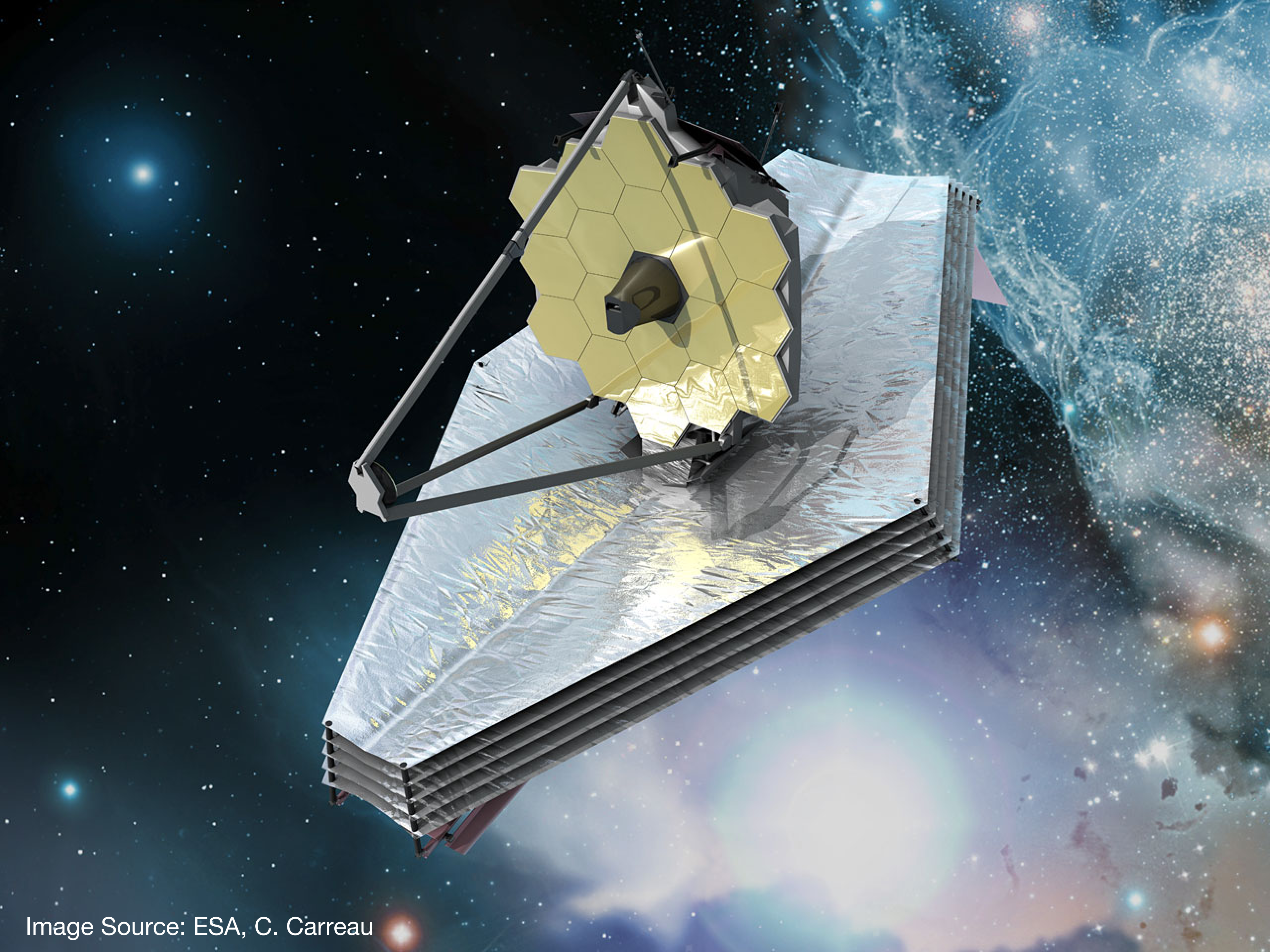
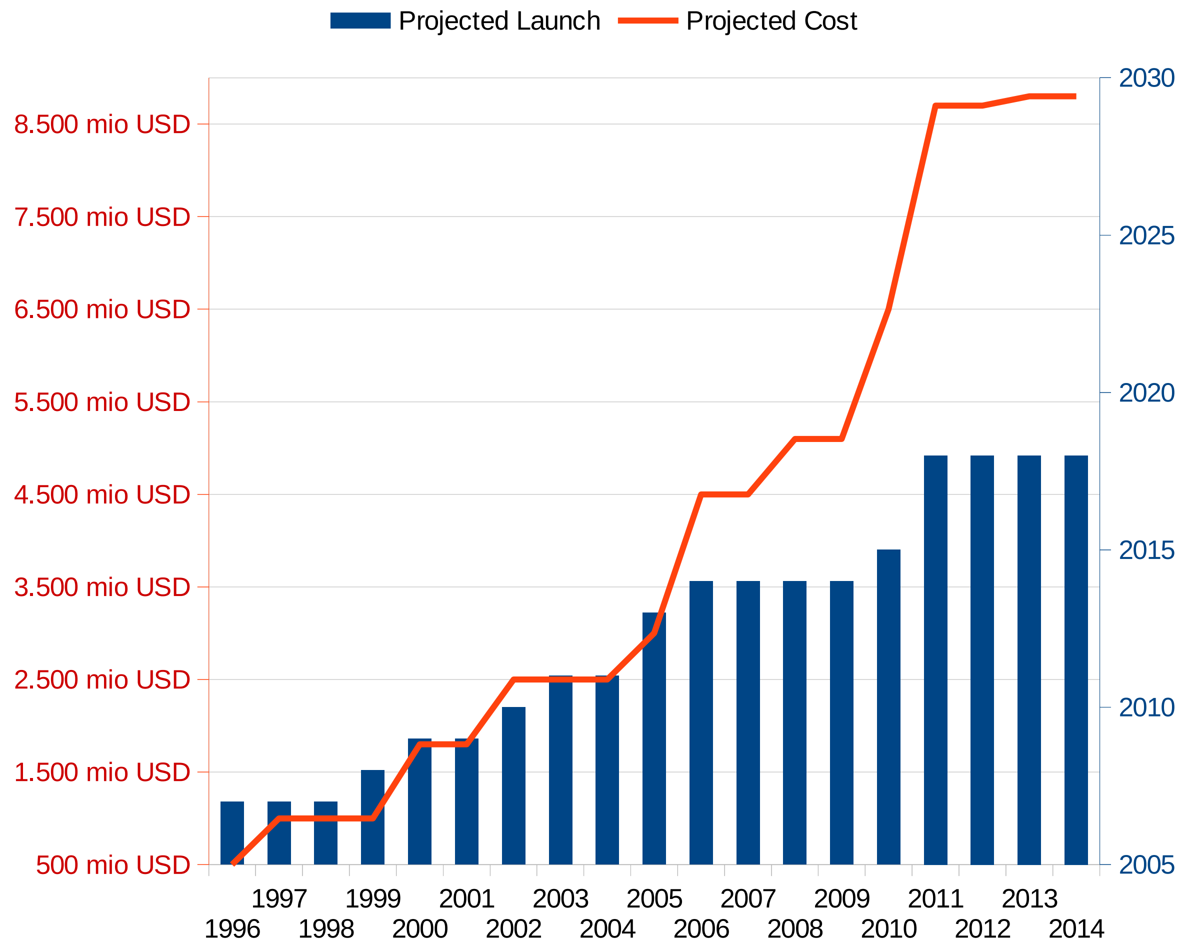


Image Source: ESA, C. Carreau

Spaceflight Progresses Slowly

- Why?
  - Space hazards
  - Technological readiness
  - Legal restrictions
  - Political issues

- Examples:
  - XMM/Newton 14y
  - Herschel 16y
  - Hubble 20y
  - Spitzer 20y
  - JWST 24y



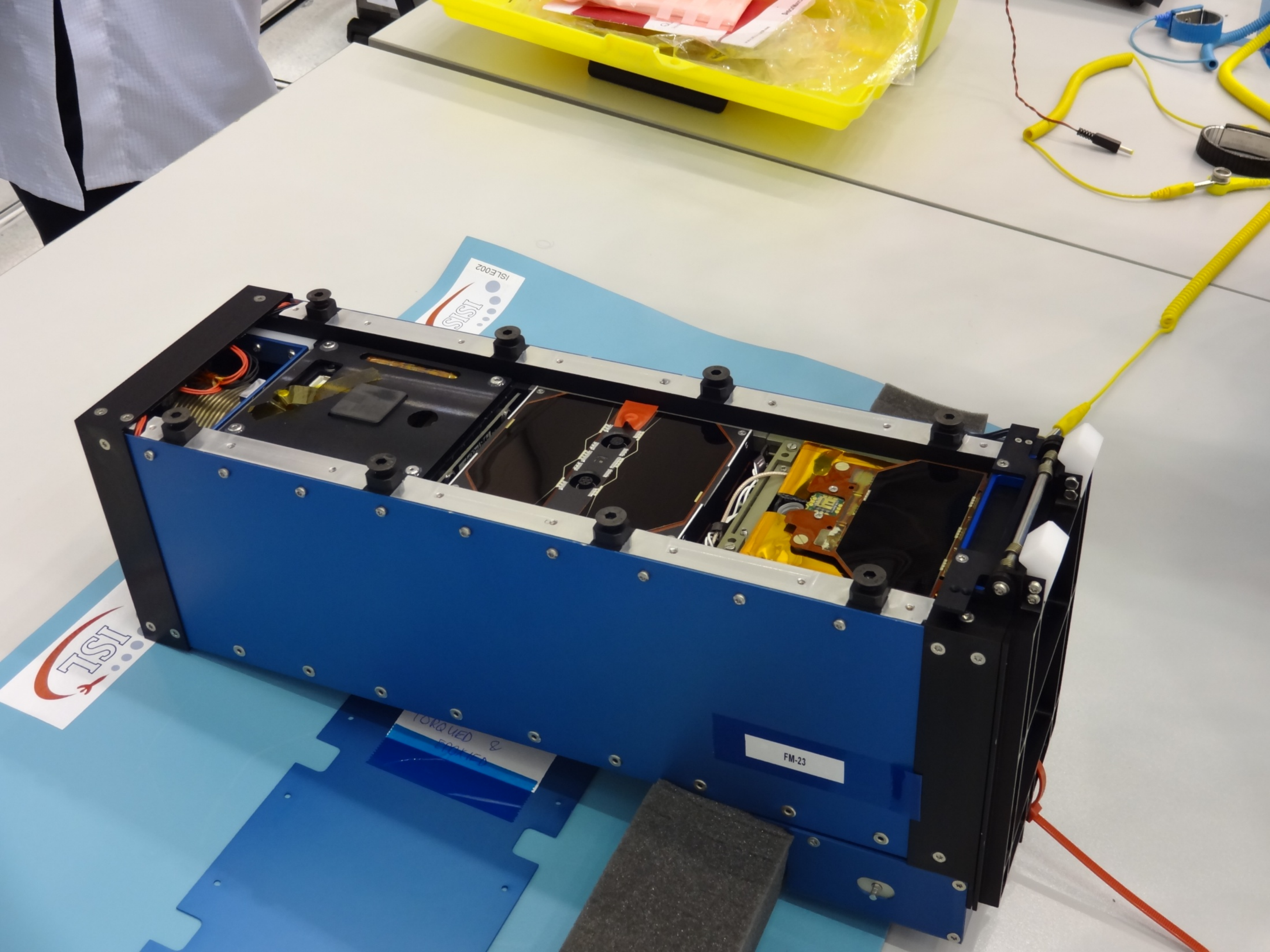
Source: jwst.nasa.gov

Satellite Miniaturization

- Microsatellites
  - 10 - 100 kg
  - MUCH easier to develop
  - Have become very popular for commercial spaceflight
  - Still somewhat expensive :-(

- Pico & Nanosatellites
  - 0.1 - 10kg
  - Fast & easy to develop
  - Minimal launch costs
  - Many university projects
  - SCIENCE!

Image Source: NASA (t), Planet Labs (b)


FM-23
ISLE002

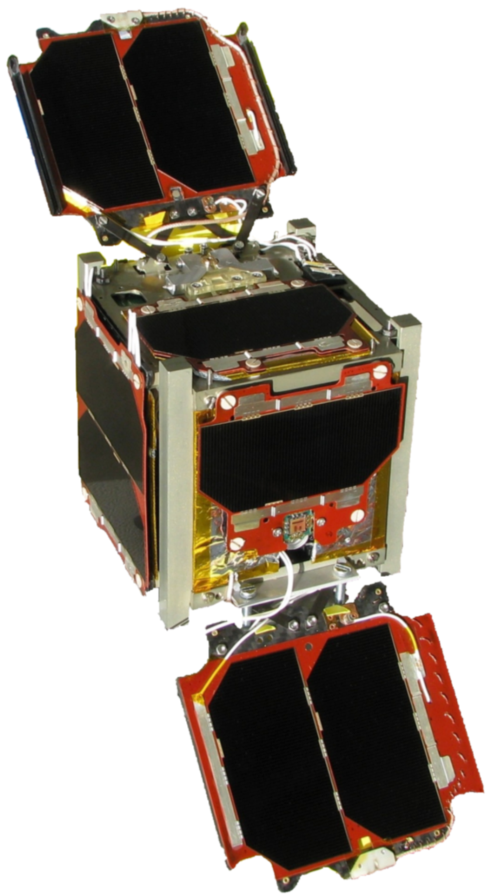
Nanosatellites - First-MOVE

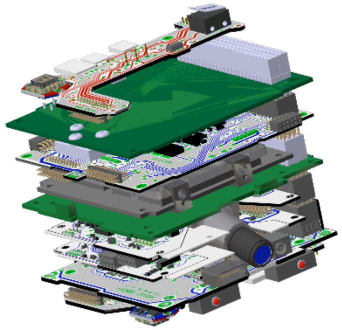
- “Completed” in 2011
- Launched in 2013
- 1 Unit CubeSat, 912g, $10cm^3$

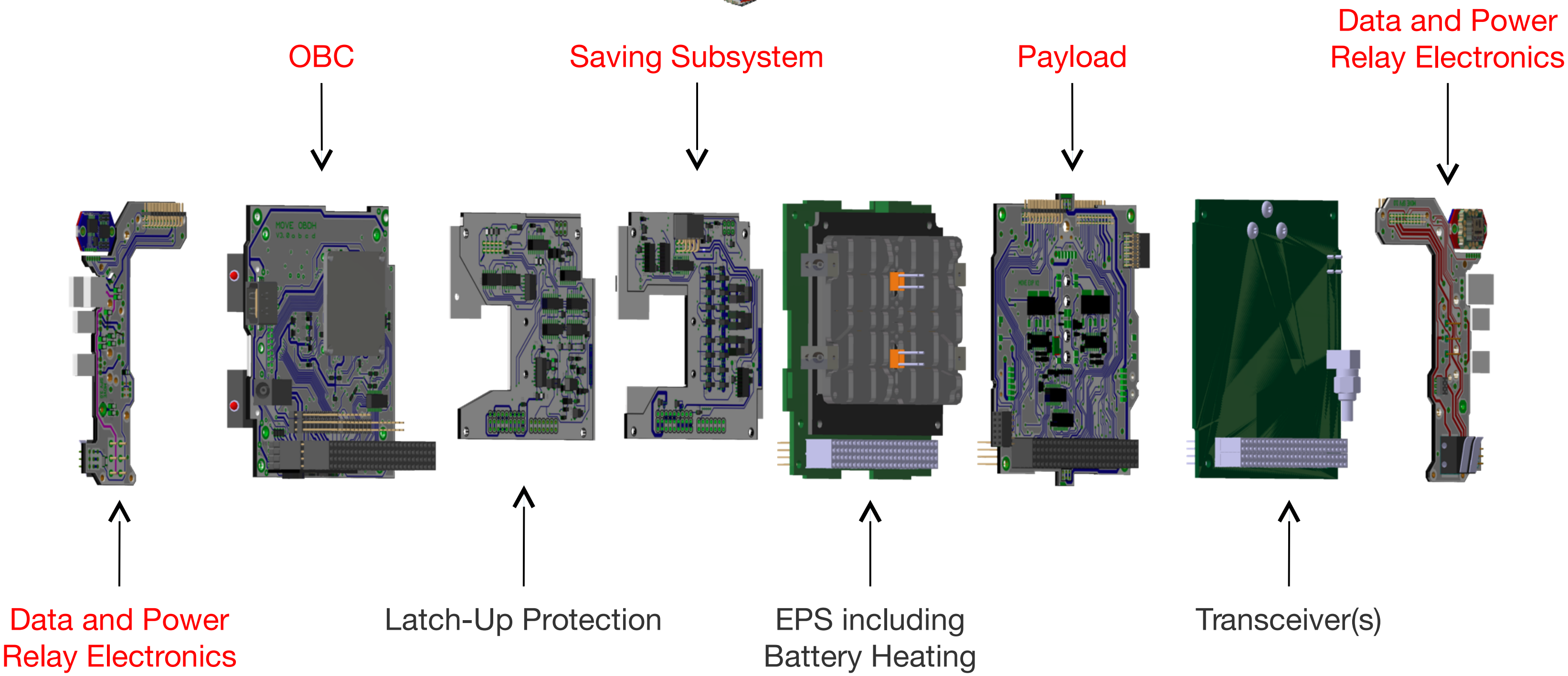
- Technology demonstration
- UHF up- VHF downlink

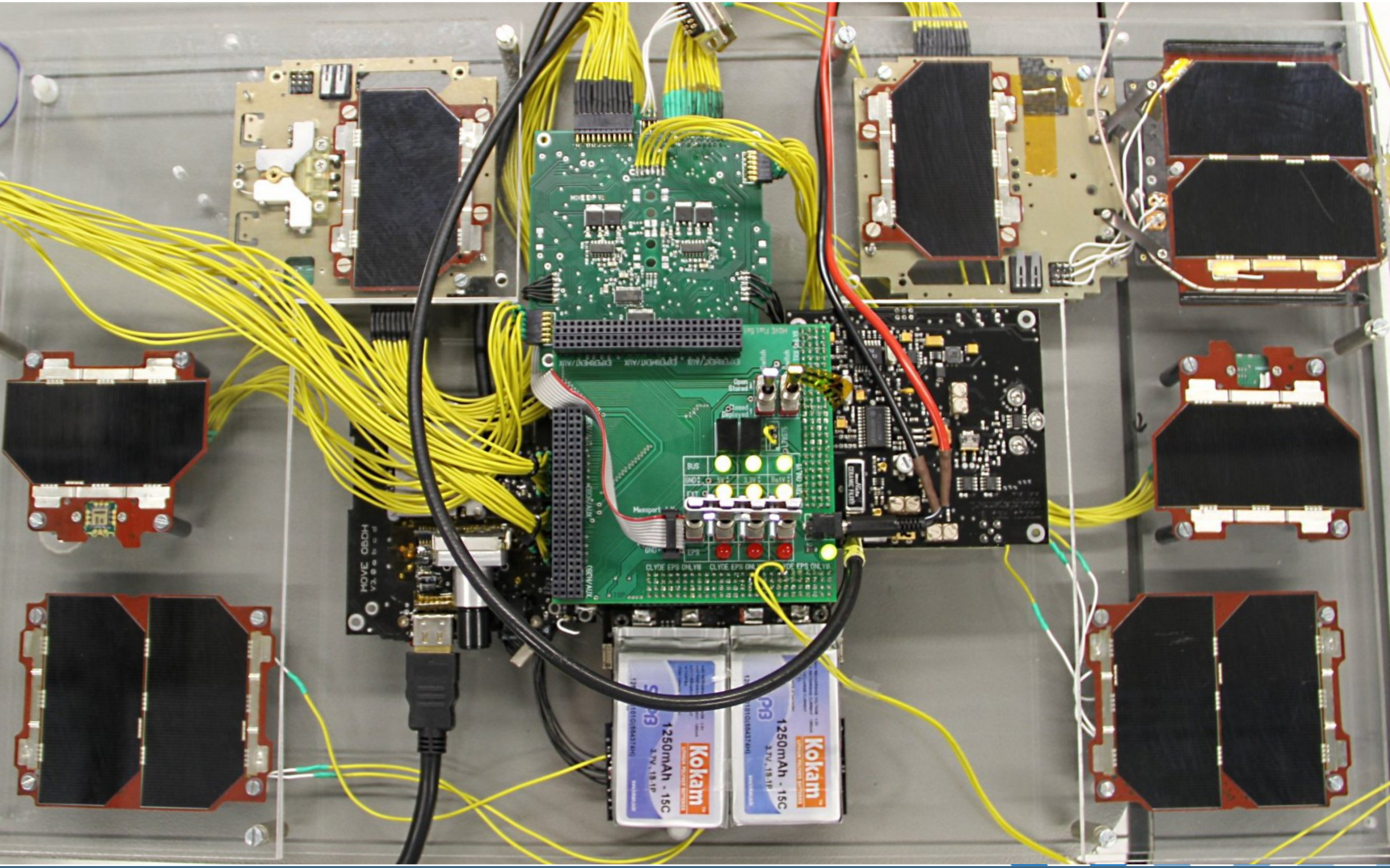
- ARM926 (ARMv5TEJ ISA)
- 512KB MRAM
- 256MB Flash
- 200mW - 1.4W power consumption
- Custom OS

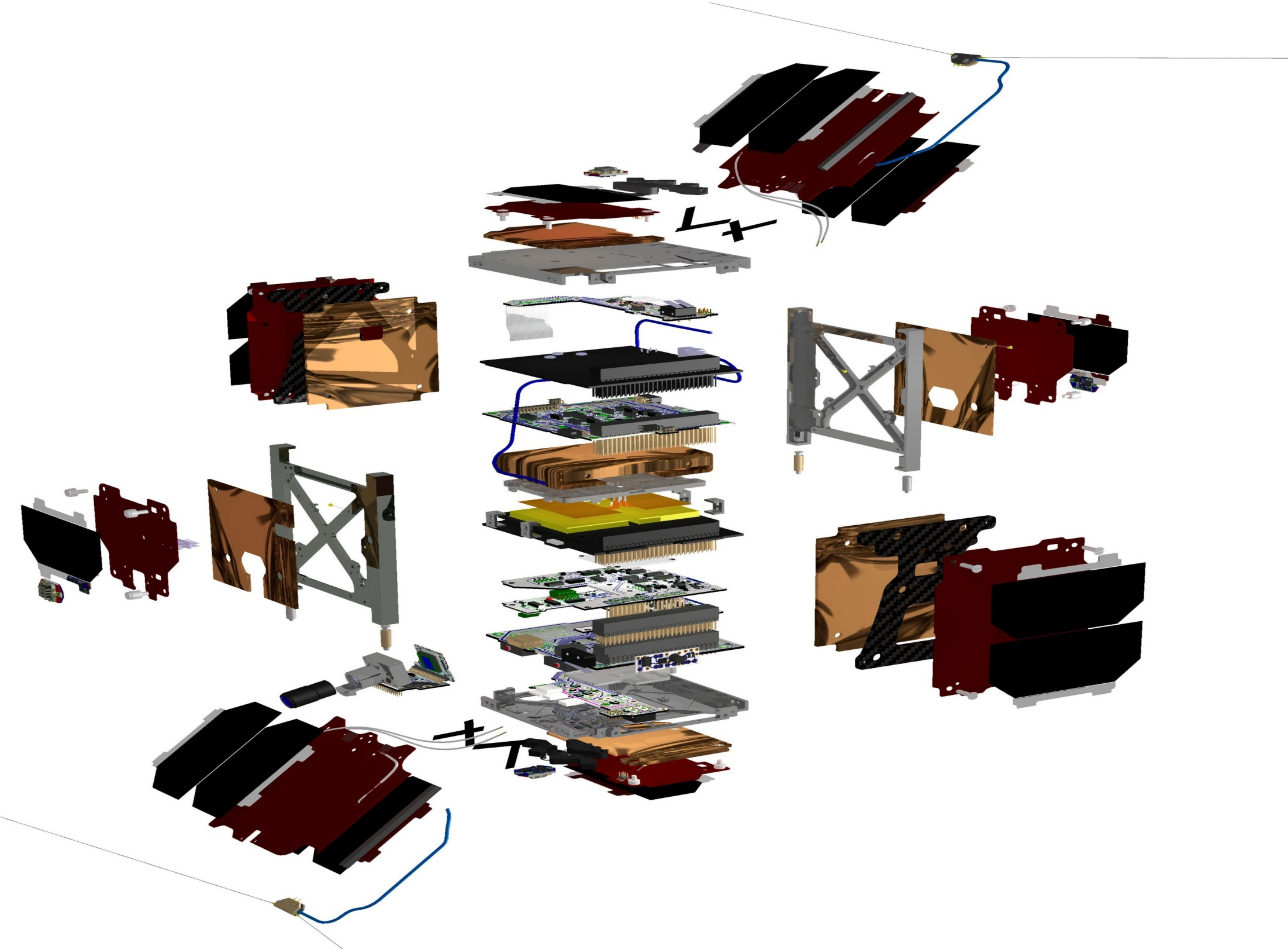
- Cost: ~200k USD/EUR incl. launch



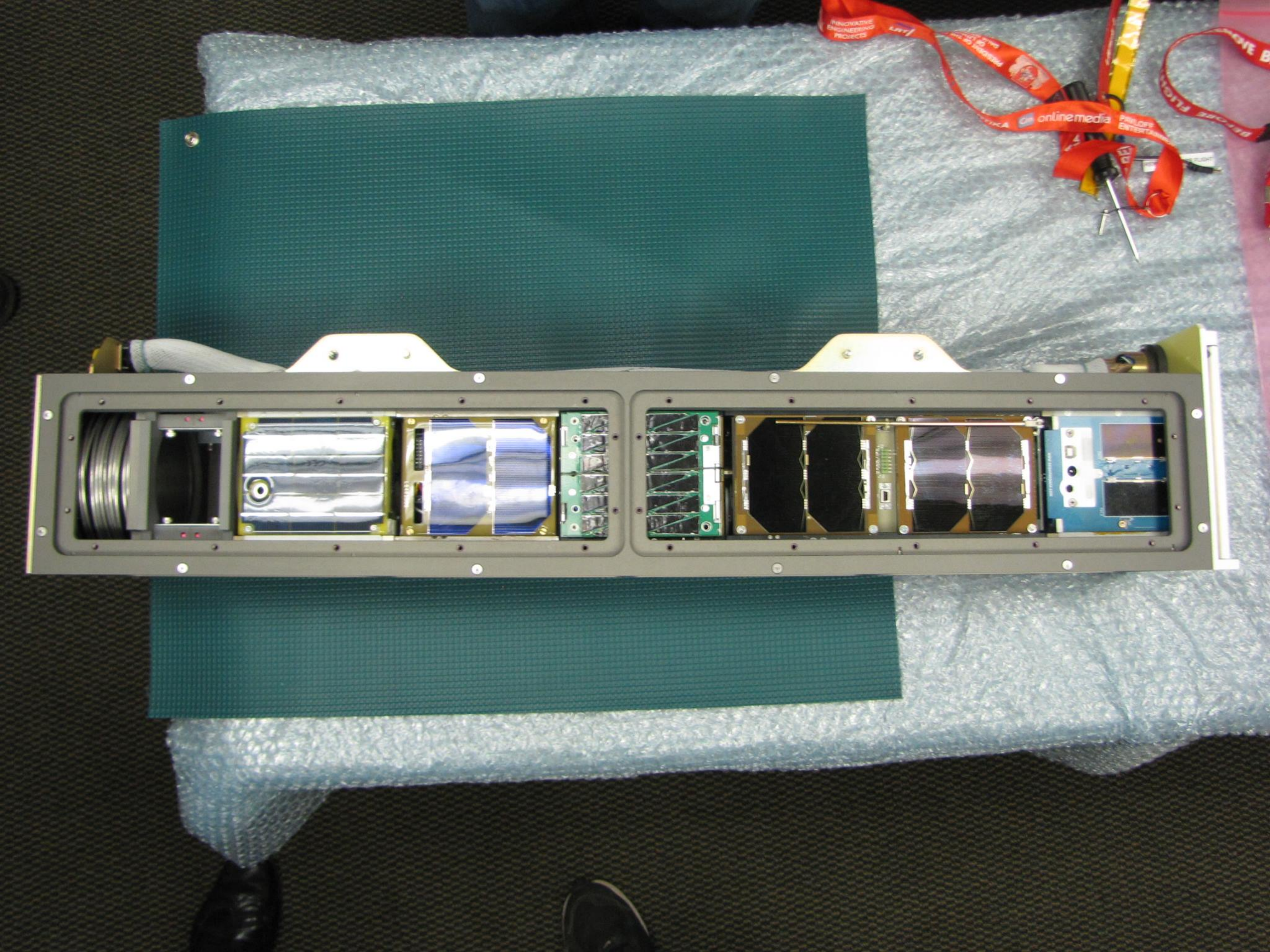


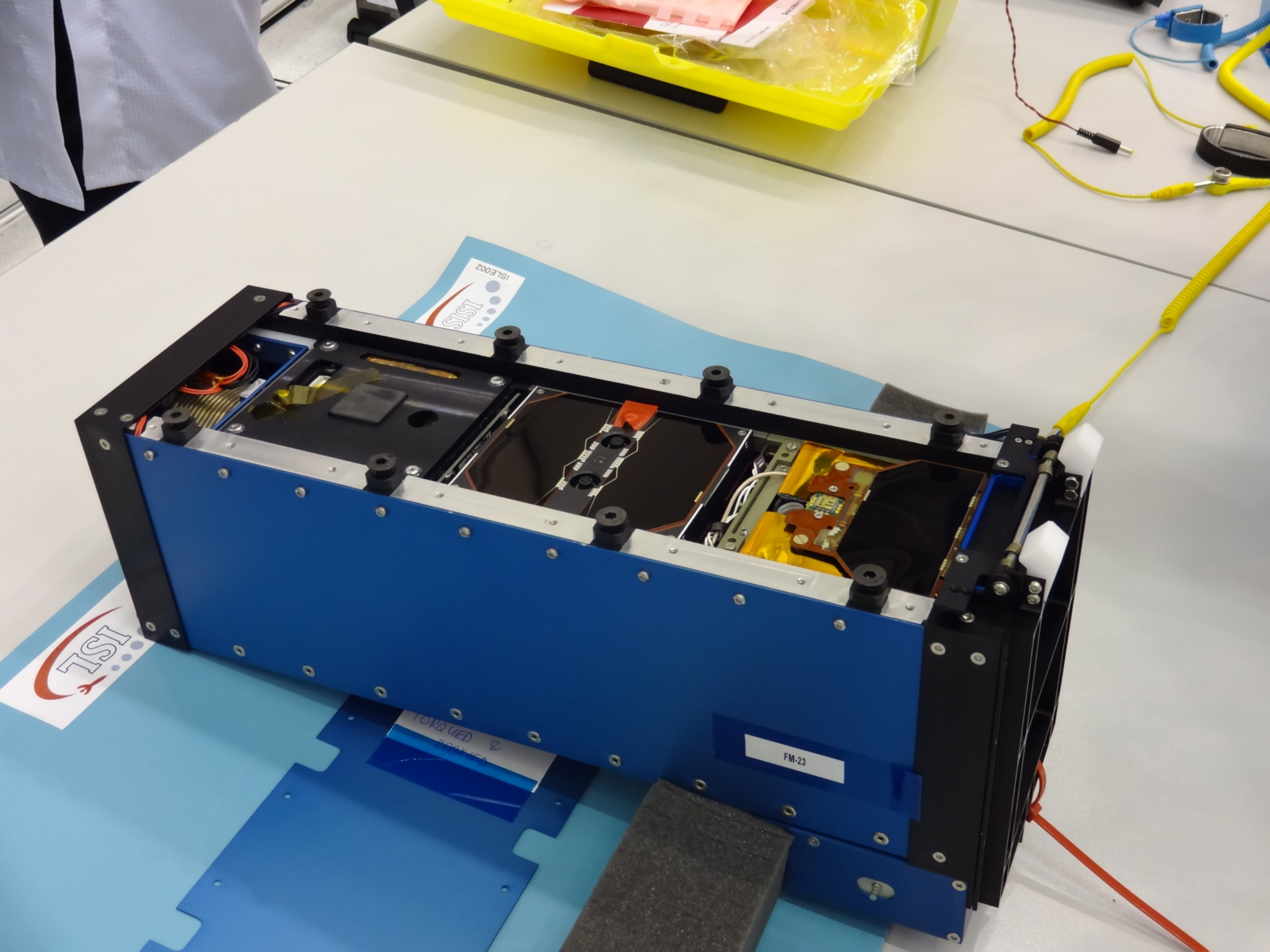

OBC
Saving Subsystem
Payload
Data and Power
Relay Electronics
Data and Power
Relay Electronics
Latch-Up Protection
EPS including
Battery Heating
Transceiver(s)

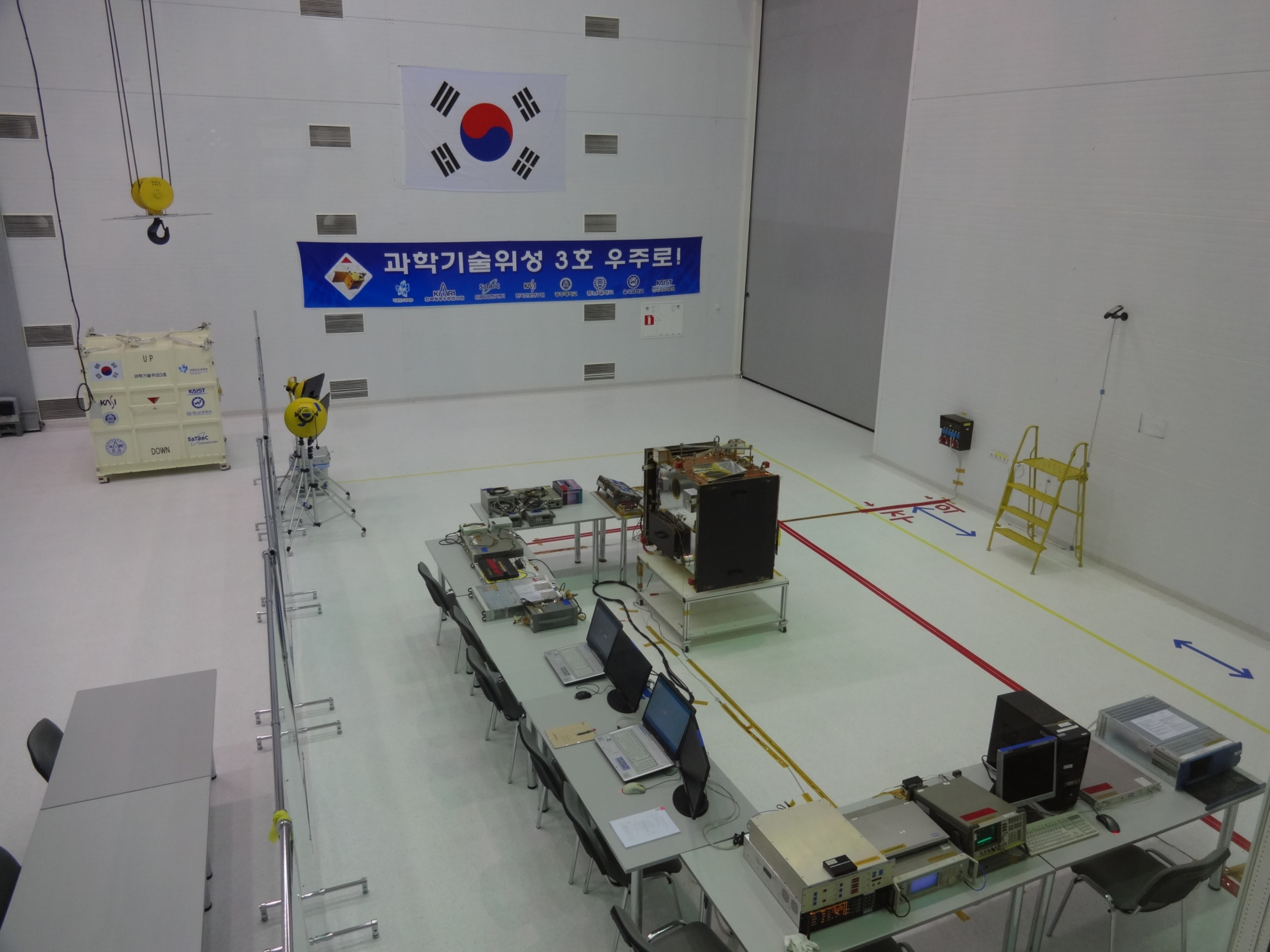

Kokam
1250mAh · 15C

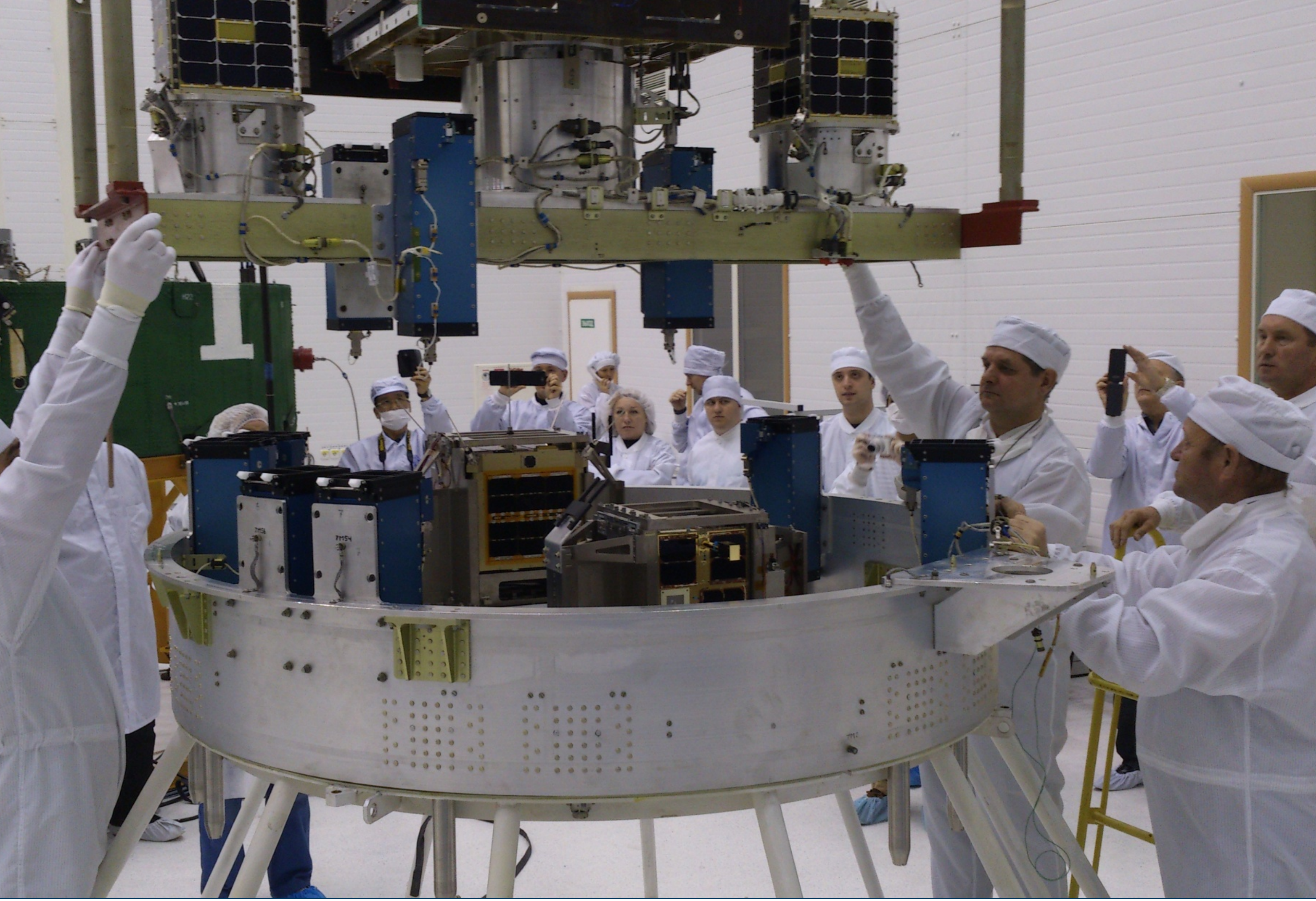



ISL
ISL
ISL03-13
ISL03-11
ISL03-09


onlinemedia


ISLE002
ISIS
ISL
TORQUED &
FM-23

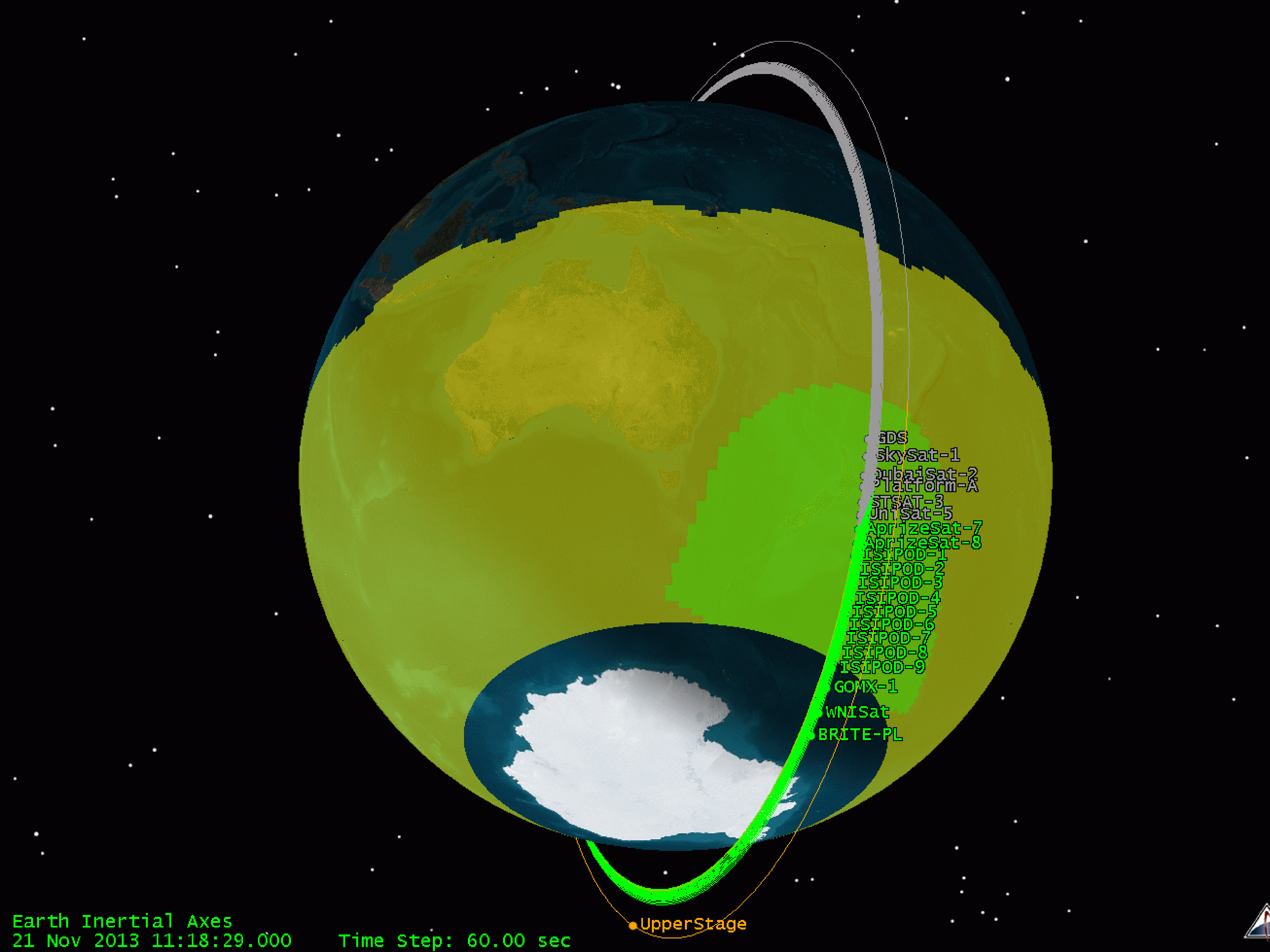

과학기술위성 3호 우주로!
UP
DOWN
KAIST



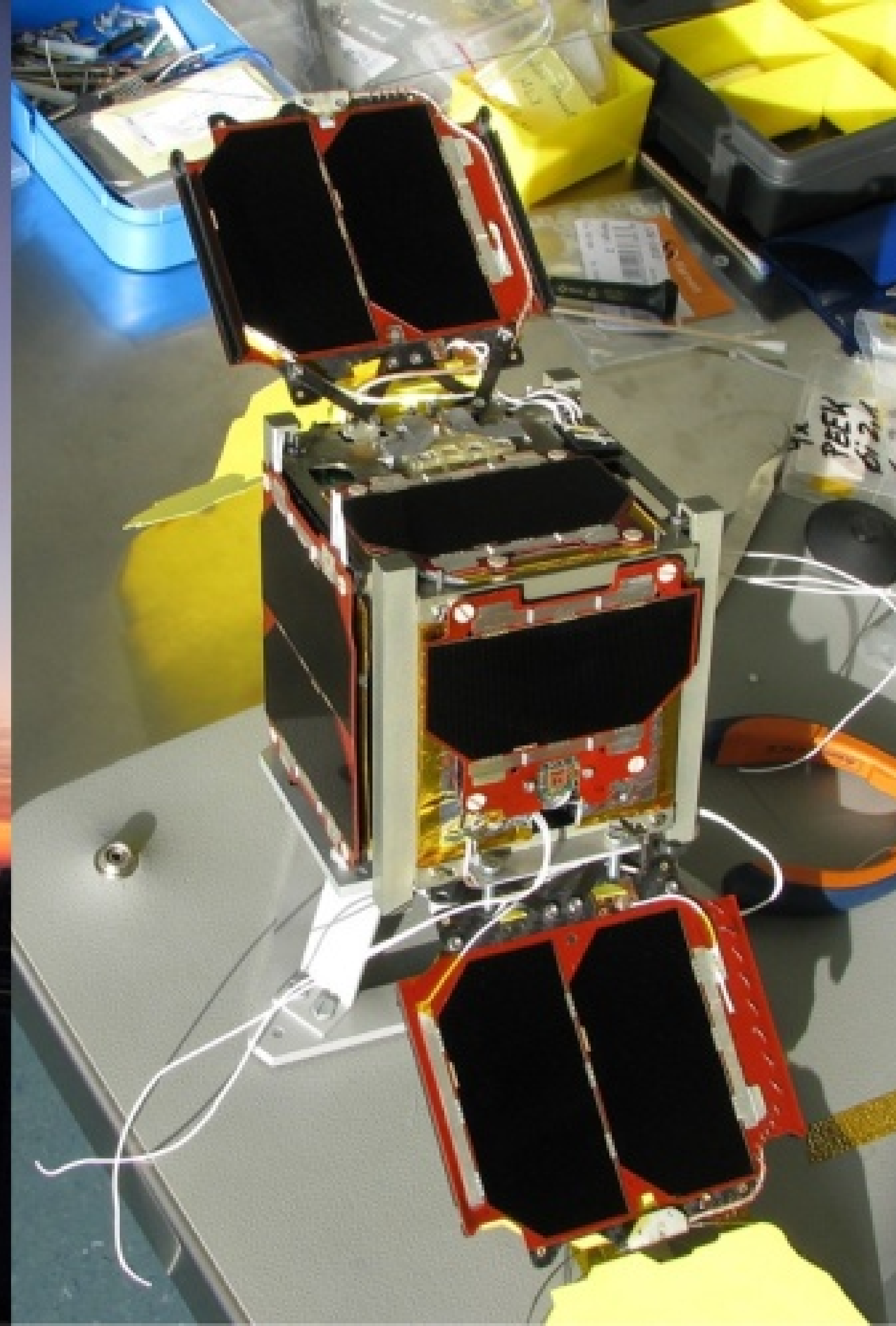

КОСМОТРАС
ROSCOSMOS
YUZHNOYE
YUZHMASH
KazEOSat
SURREY
Deimos-2
elecnor
UniSat 6
SaudiSat-4
Hodoyoshi-3,4
ほどよし
3,4
東京大学
AprizeSat
9 & 10
SpaceQuest
TabletSat-Aurora
Sputnix
BRITE-Toronto
BRITE-Montreal
XPOD Systems
SFL
BugSat-1
21 CubeSats
ISIS
ISL
QuadPack Systems

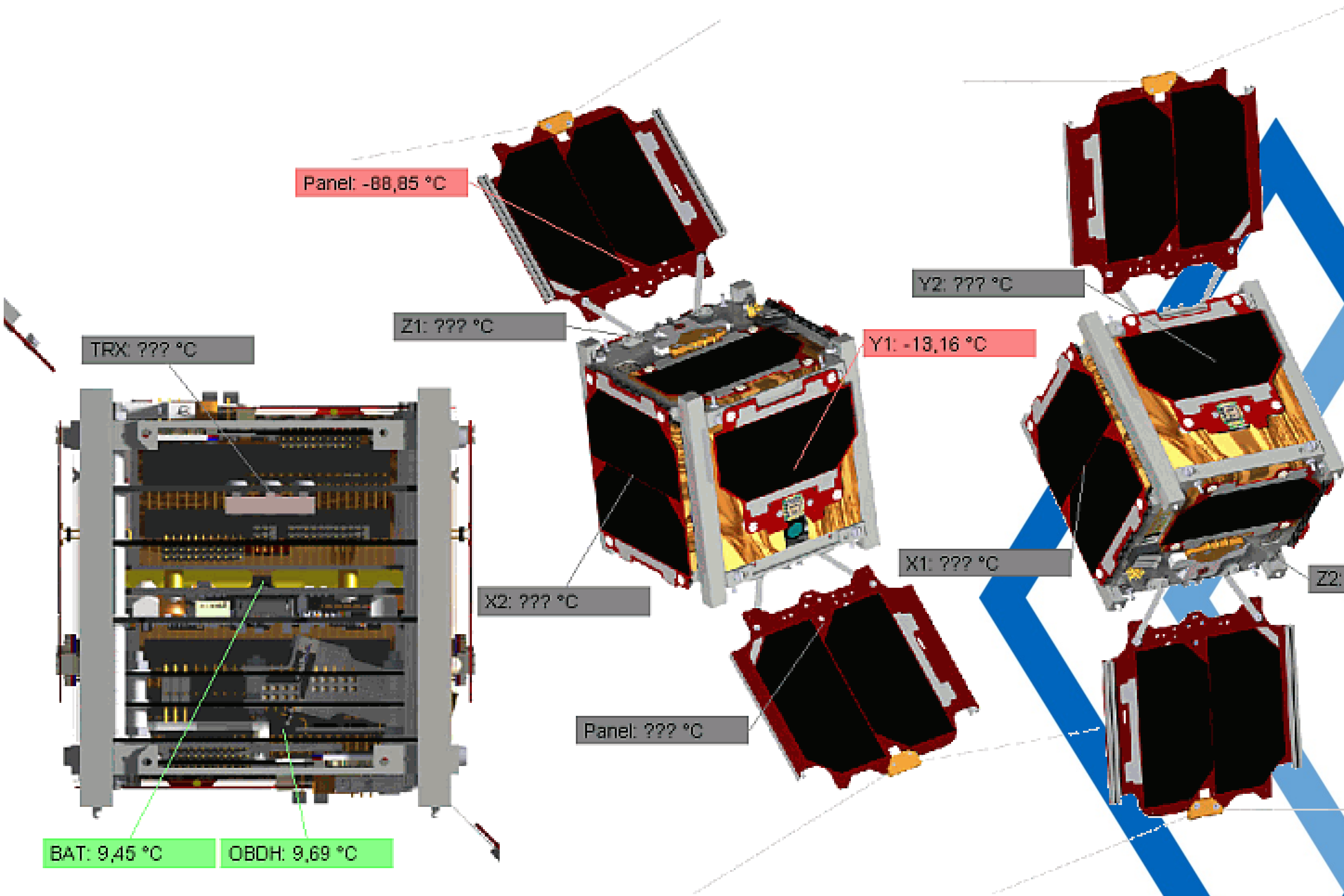

КОСМОТРАС


YUZHMASH
YUZHNOE
esa


GDS
SkySat-1
DubaiSat-2
Platform-A
STSAT-3
UniSat-5
AprizeSat-7
AprizeSat-8
ISIPOD-1
ISIPOD-2
ISIPOD-3
ISIPOD-4
ISIPOD-5
ISIPOD-6
ISIPOD-7
ISIPOD-8
ISIPOD-9
GOMX-1
WNISat
BRITE-PL
UpperStage
Earth Inertial Axes
21 Nov 2013 11:18:29.000
Time Step: 60.00 sec


XMM

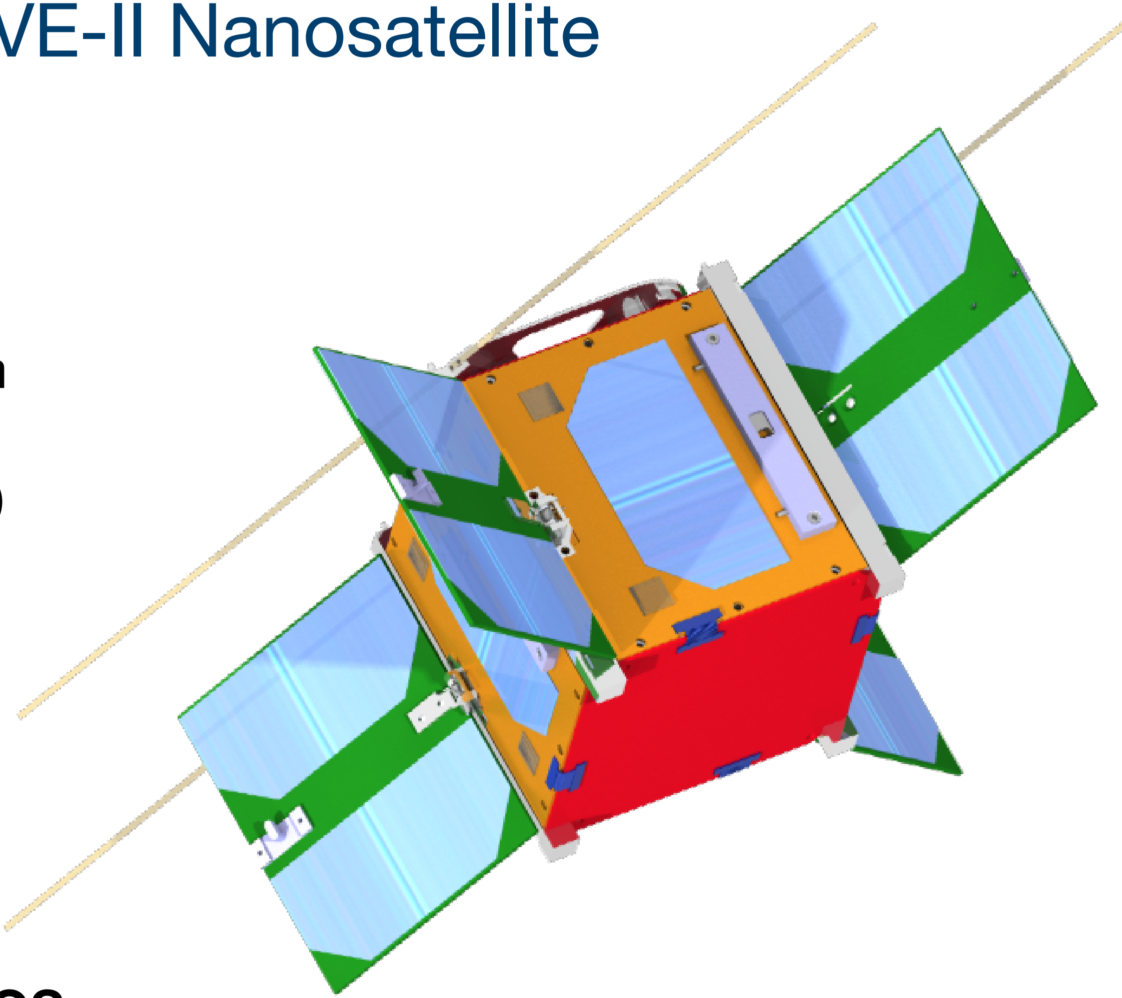

Panel: -88,85 °C
Z1: ??? °C
TRX: ??? °C
Y1: -13,16 °C
Y2: ??? °C
X1: ??? °C
Z2: ??? °C
X2: ??? °C
Panel: ??? °C
BAT: 9,45 °C
OBDH: 9,69 °C

The MOVE-II Nanosatellite

- 1U CubeSat
- 8W power budget
- UHF/VHF + S-Band Comm

- On-Board Computer (~2W)
  - Application Processor
  - 64 MB ECC-SDRAM
  - 8MB MRAM
  - I^2C + SPI + GPIO

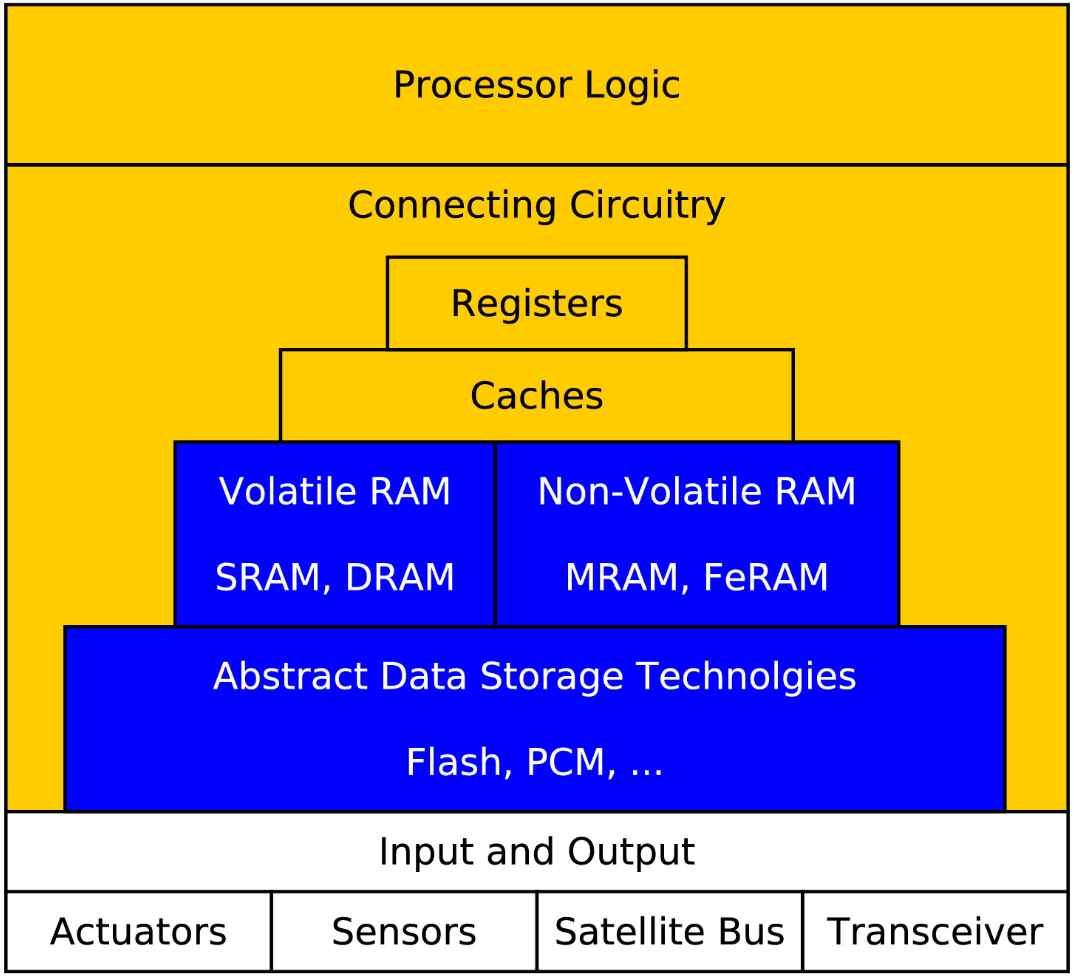
- Autonomous debugging
- Efficient protocol stack
- **Size optimized standard OS**



How to Achieve System Dependability

- Classics
  - Proven legacy technology
  - Specialized space-grade components
- Holy Grails
  - More robust manufacturing techniques
  - New Technologies
- Redundancy
  - Supervised fail-over (Dual Modular)
  - Voting (Triple Modular)
- Software Measures

Achieving System Dependability



Dependable Data Storage on Modern Memory

- Foundation for advanced consistency concepts

- System Storage
  - RTOS Firmware, Kernel + Userland, ApplicationCode
  - Small footprint but consistency critical

- Payload Data Storage
  - Data storage for scientific data
  - Only lossy technology available (MLC-flash)
  - Large & challenging throughput requirements

- Volatile Memory

Protecting Operating System Data, an Example

Application	logger
API	POSIX
Virtual File System	Virtual File System
File System	File System Infrastructure
Block Abstraction	blockdev
Device Abstraction	/dev/eeprom0
Device Driver	SPI driver
Memory Technology	EEPROM

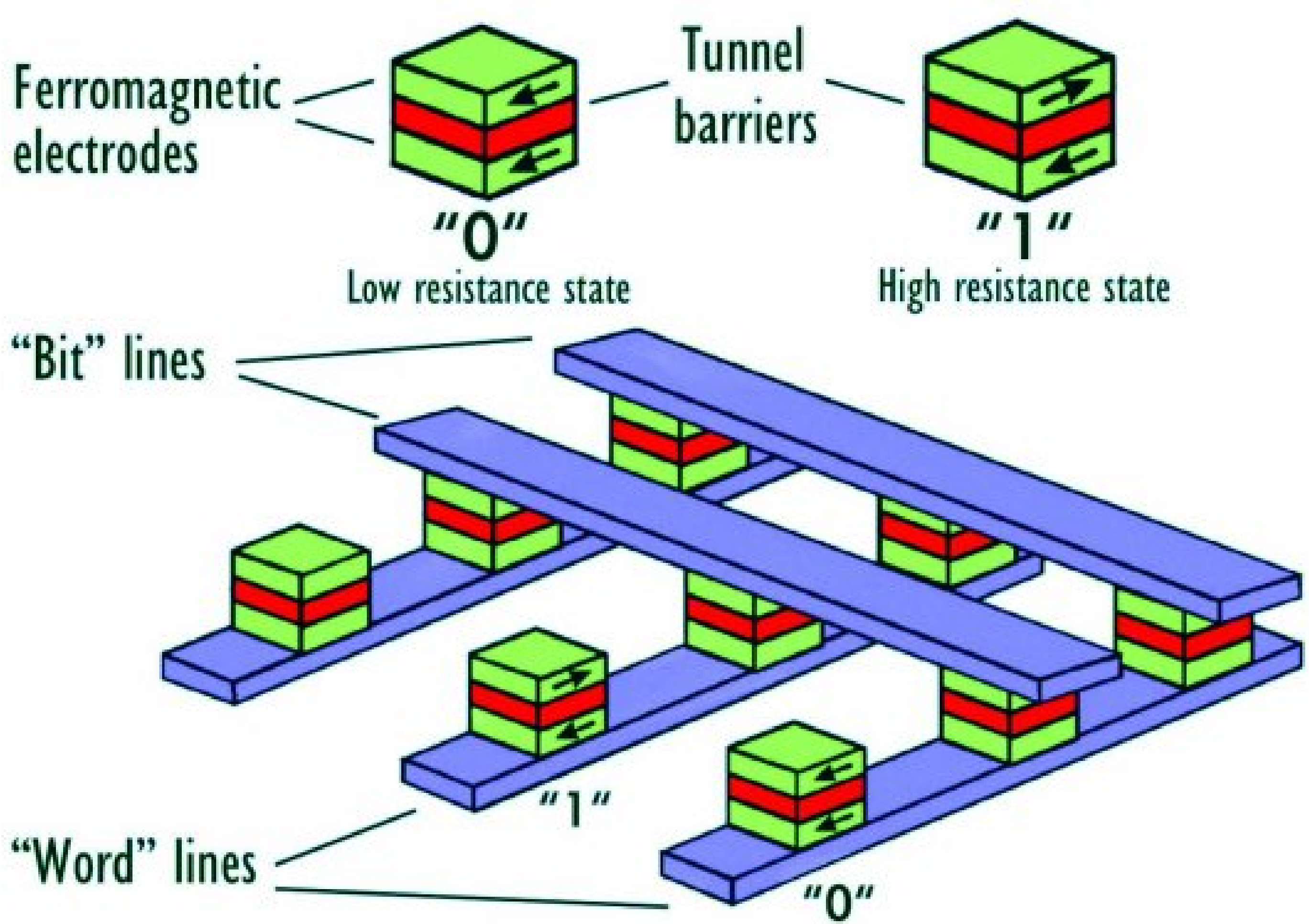
Protecting Operating System Data, an Example

Application	logger
API	POSIX
Virtual File System	Virtual File System
File System	File System Infrastructure
Block Abstraction	blockdev
Device Abstraction	/dev/eeprom0
Device Driver	SPI driver
Memory Technology	EEPROM

Protecting Operating System Data, an Example

Application	logger
API	POSIX
Virtual File System	Virtual File System
File System	File System Infrastructure
Block Abstraction	blockdev
Device Abstraction	/dev/eeprom0
Device Driver	SPI driver
Memory Technology	EEPROM

Magnetoresistive RAM

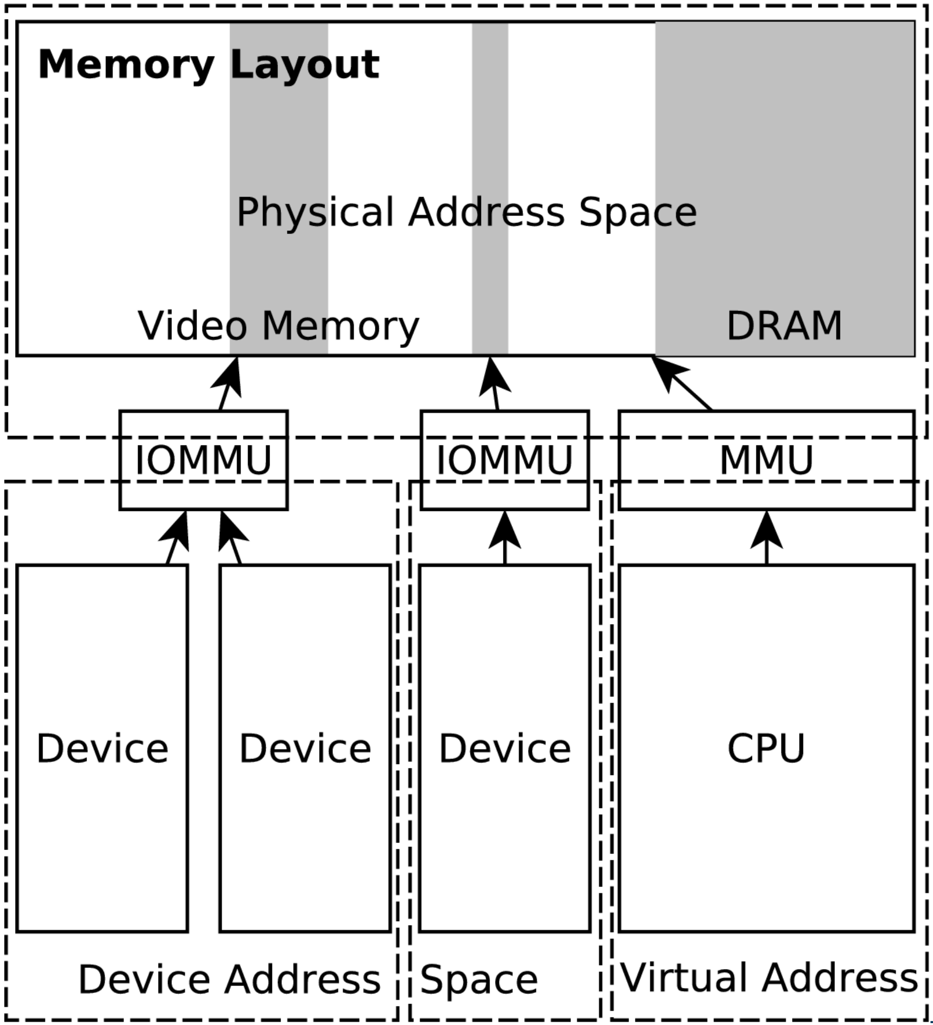


Source: Fert A, George J-M, Jaffres H, Mattana R and Seneor P, Europhysics News 34(6) 227, 2003

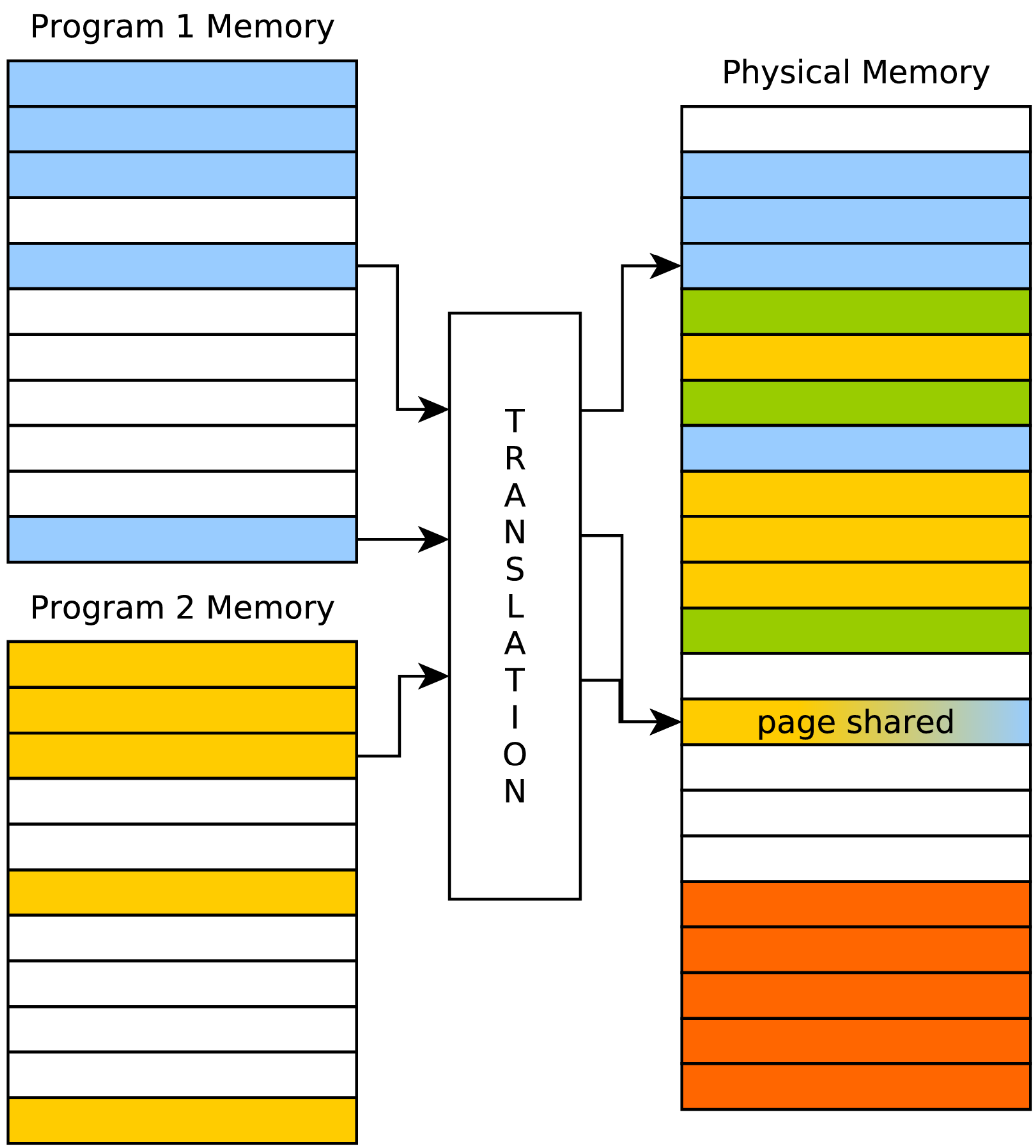
High-Rel Data Storage on MRAM

Application	Application
API	API
Virtual File System	Virtual File System
File System	File System Infrastructure
Block Abstraction	
Device Abstraction	
Device Driver	Memory Mapping
Memory Technology	MRAM

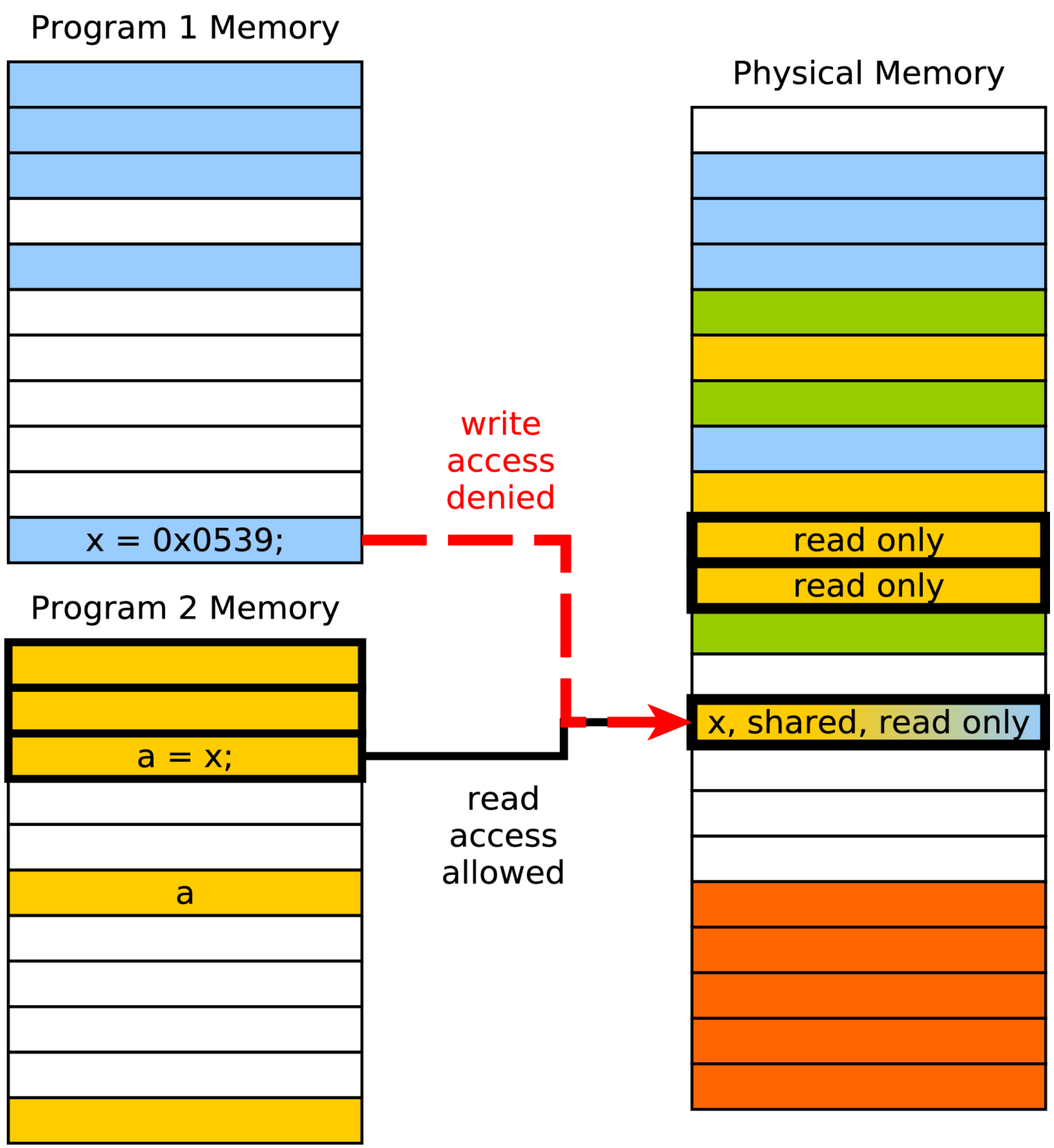
Virtual & Physical Memory



Virtual Memory Mappings

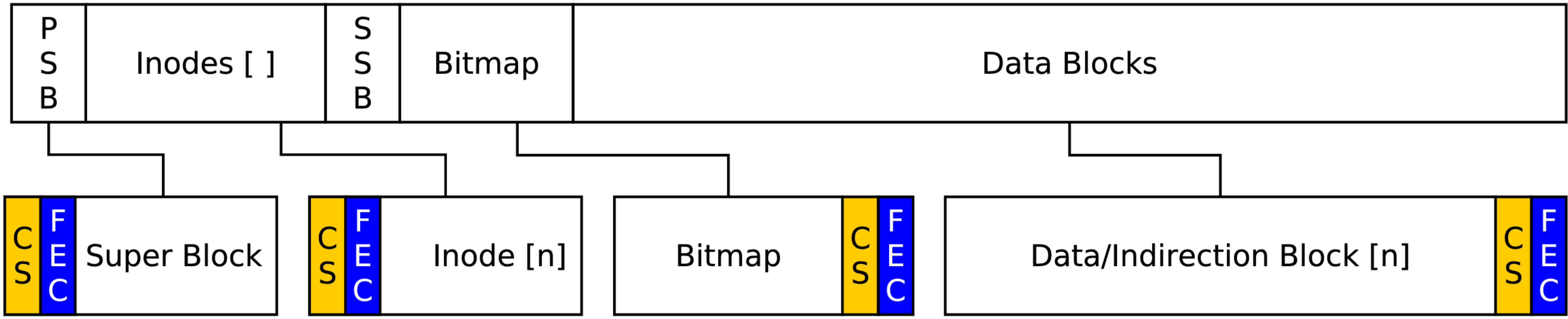


Memory Protection



FTRFS: A Fault-Tolerant Radiation-Robust File System for Space Use

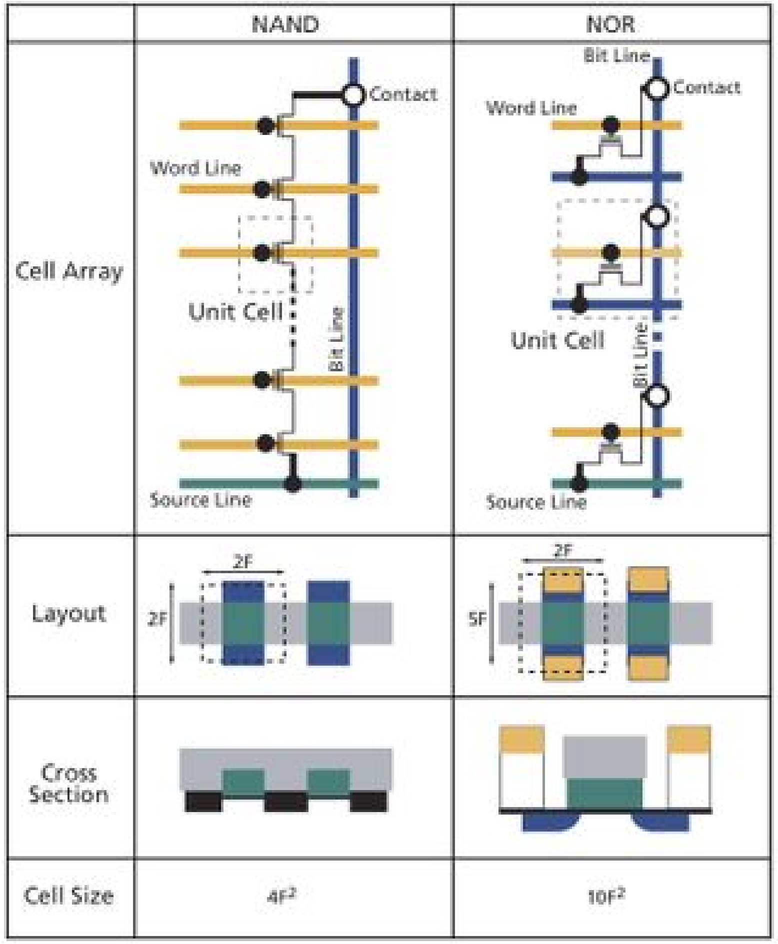
- **Dynamic, variable EDAC strength**
- Erasure coding using Reed Solomon
- CRC32 to enhance performance
- Memory protection

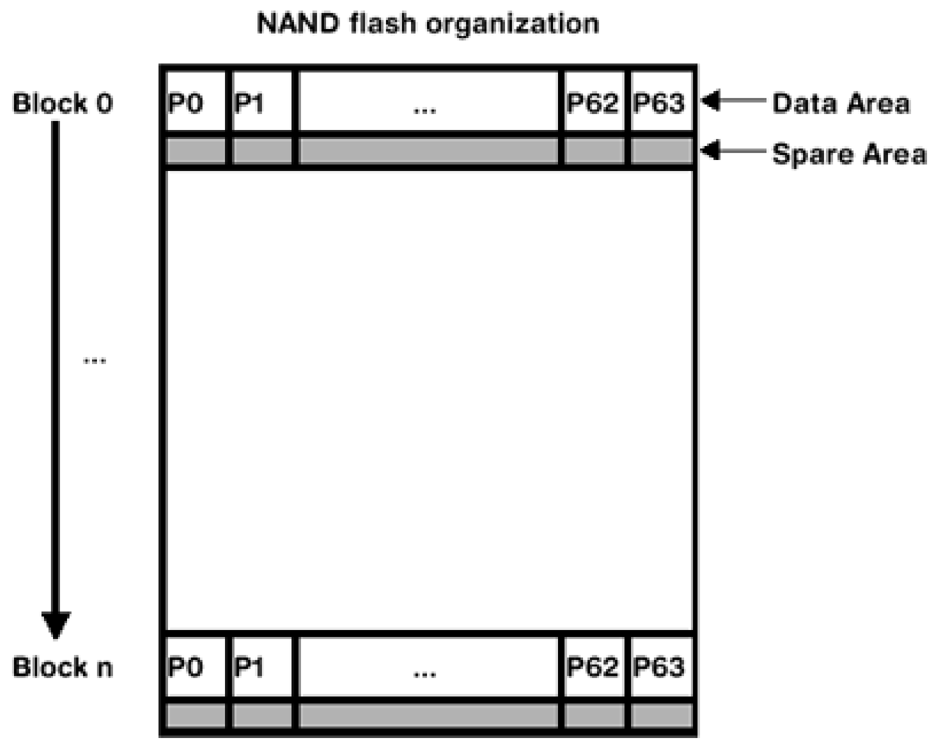


Dependable Data Storage on Modern Memory

- Foundation for advanced consistency concepts
- System Storage
  - RTOS Firmware, Kernel + Userland, ApplicationCode
  - Small footprint but consistency critical
- Payload Data Storage
  - Data storage for scientific data
  - Only lossy technology available (MLC-flash)
  - Large & challenging throughput requirements
- Volatile Memory

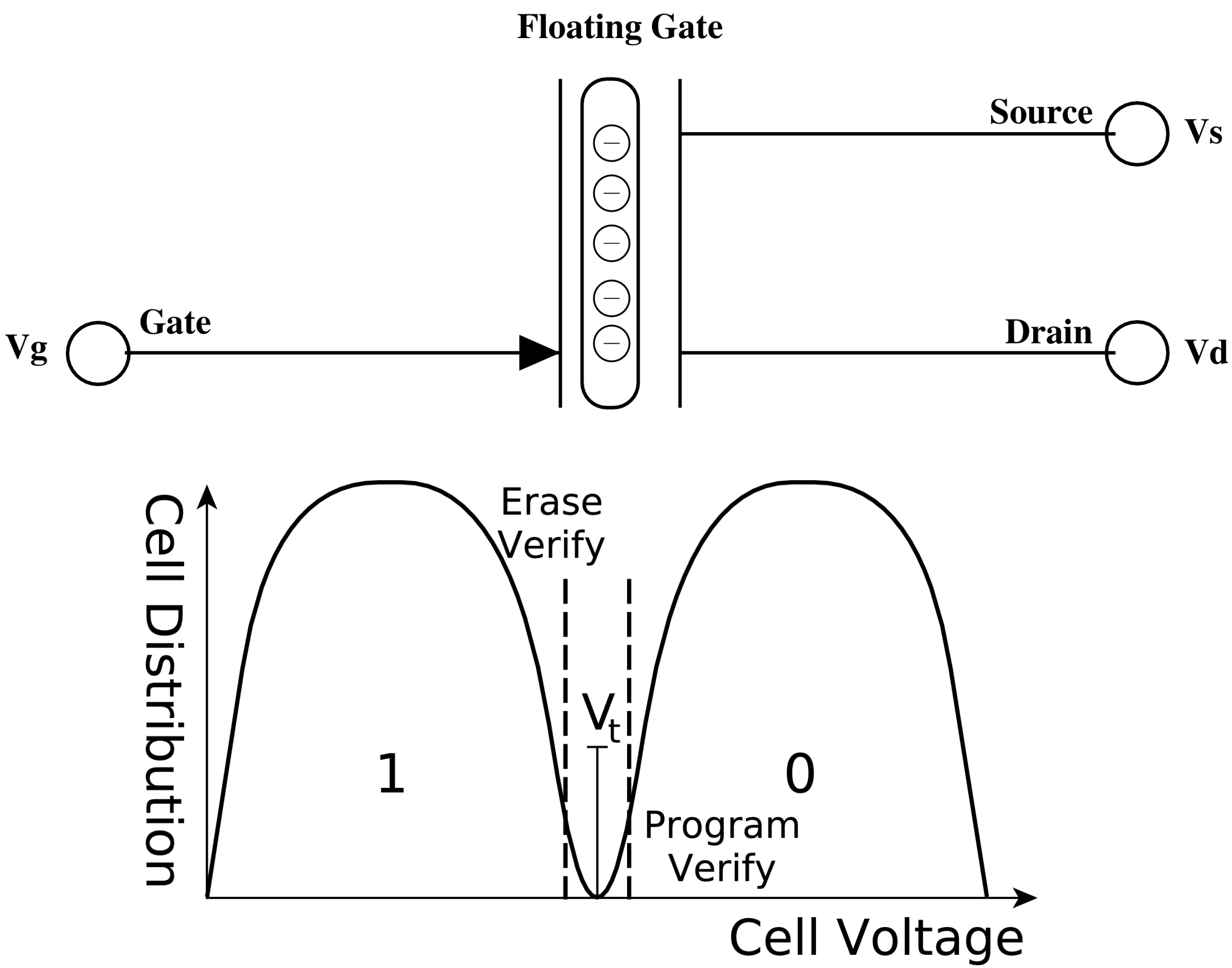
NAND & NOR Flash Memory



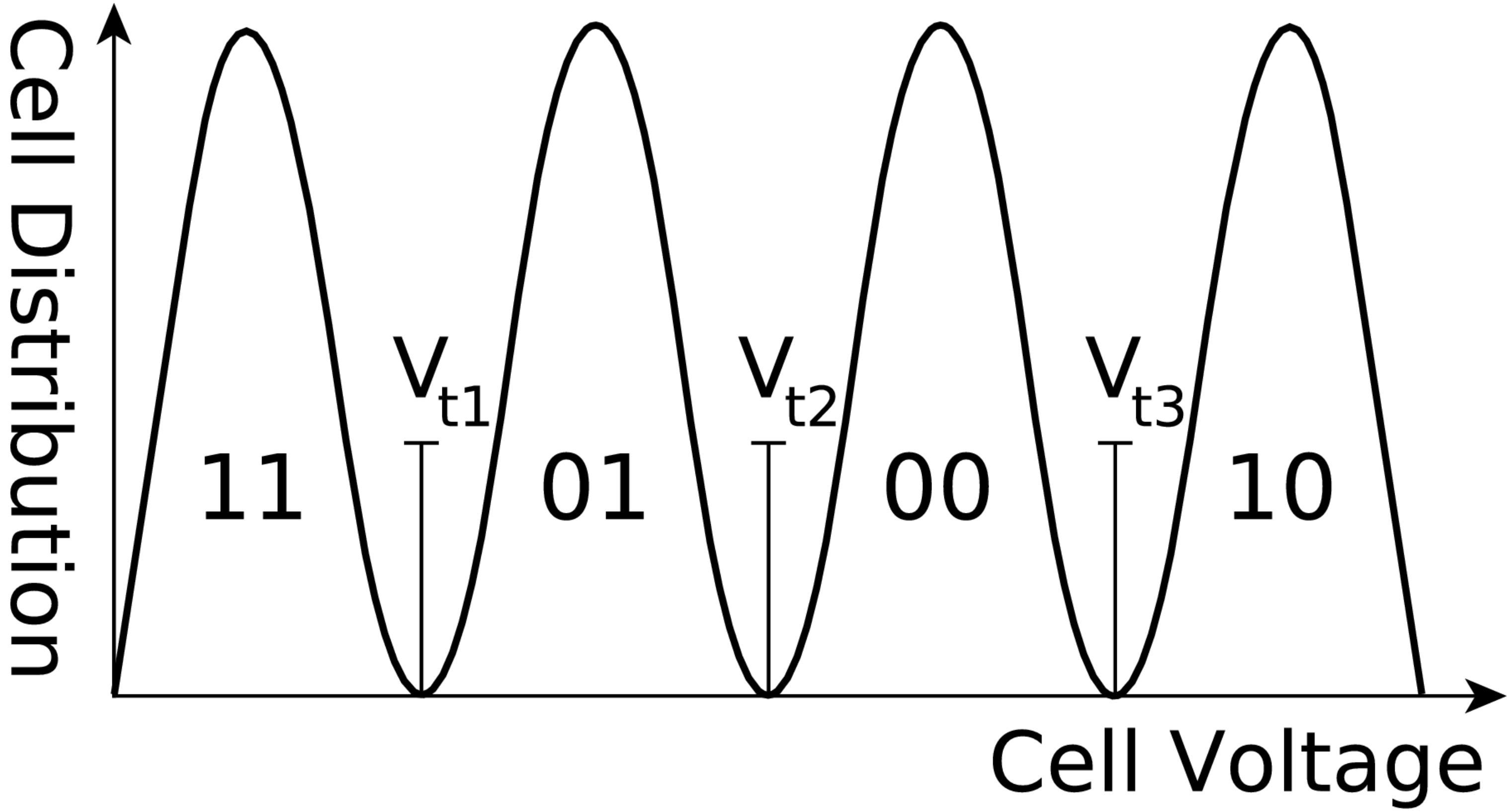


Source: Wind River Systems (L), SEGGER Microcontroller (R)

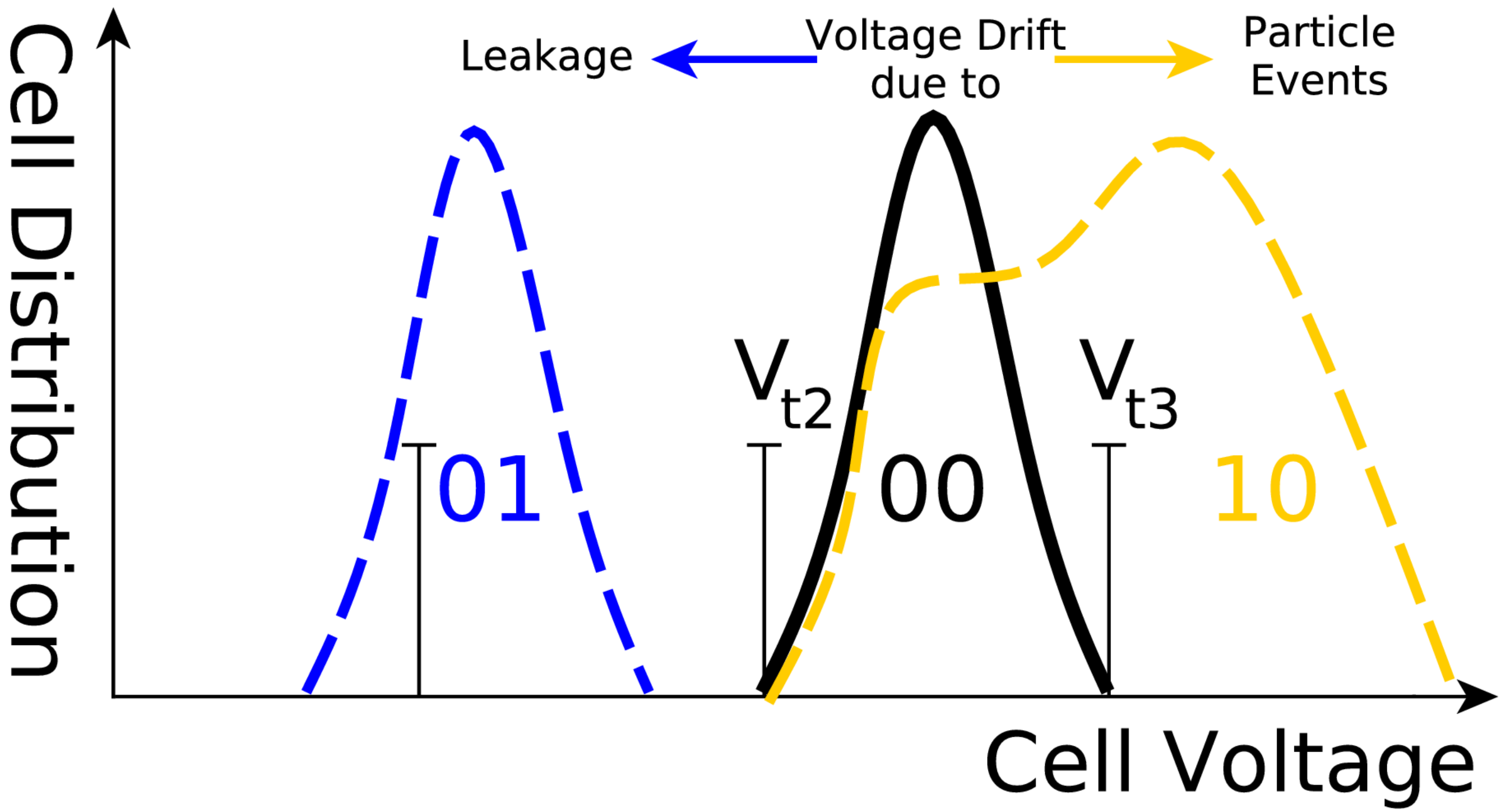
Single-Level Cell Flash



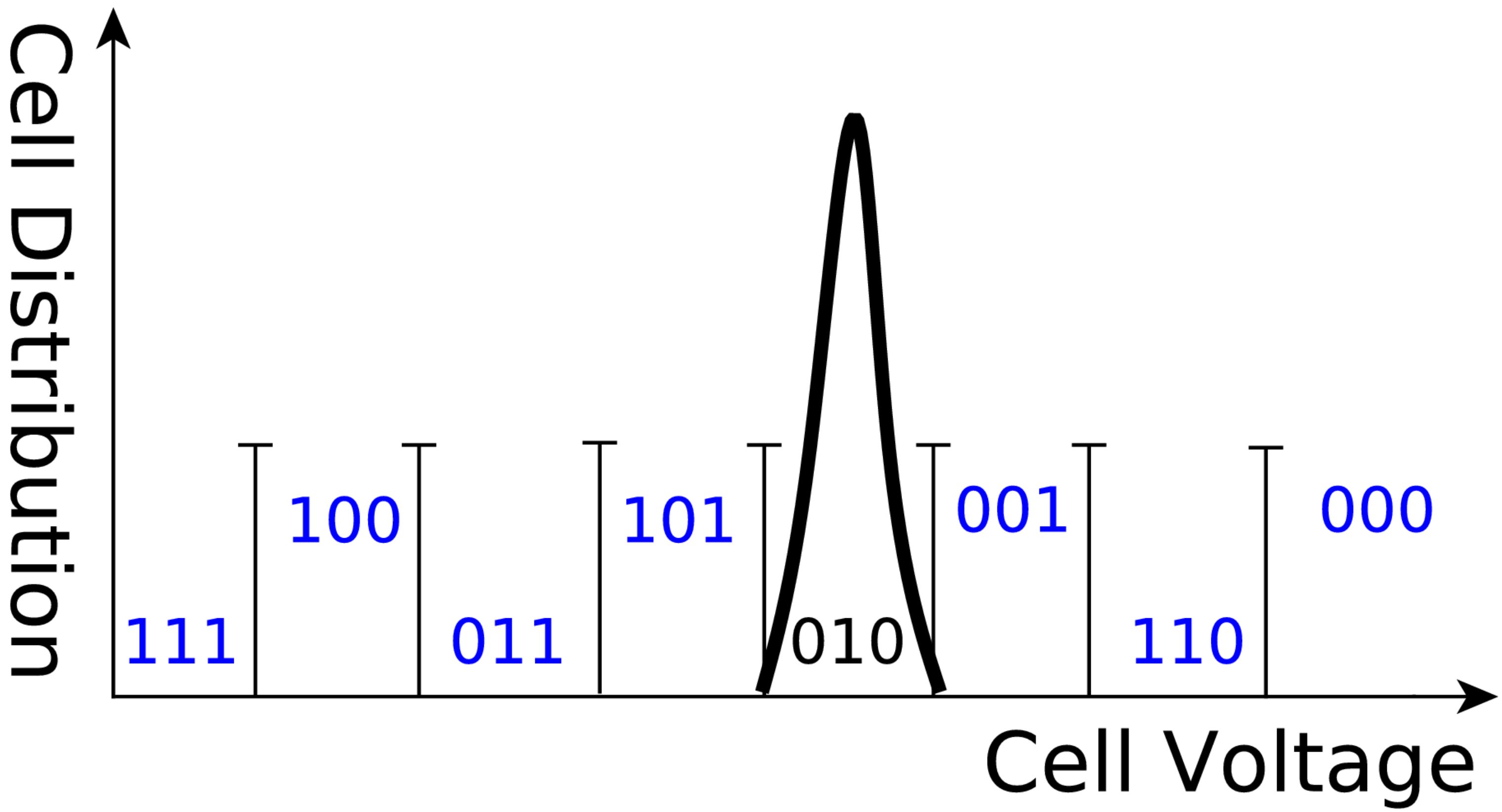
Multi-Level Cell Flash



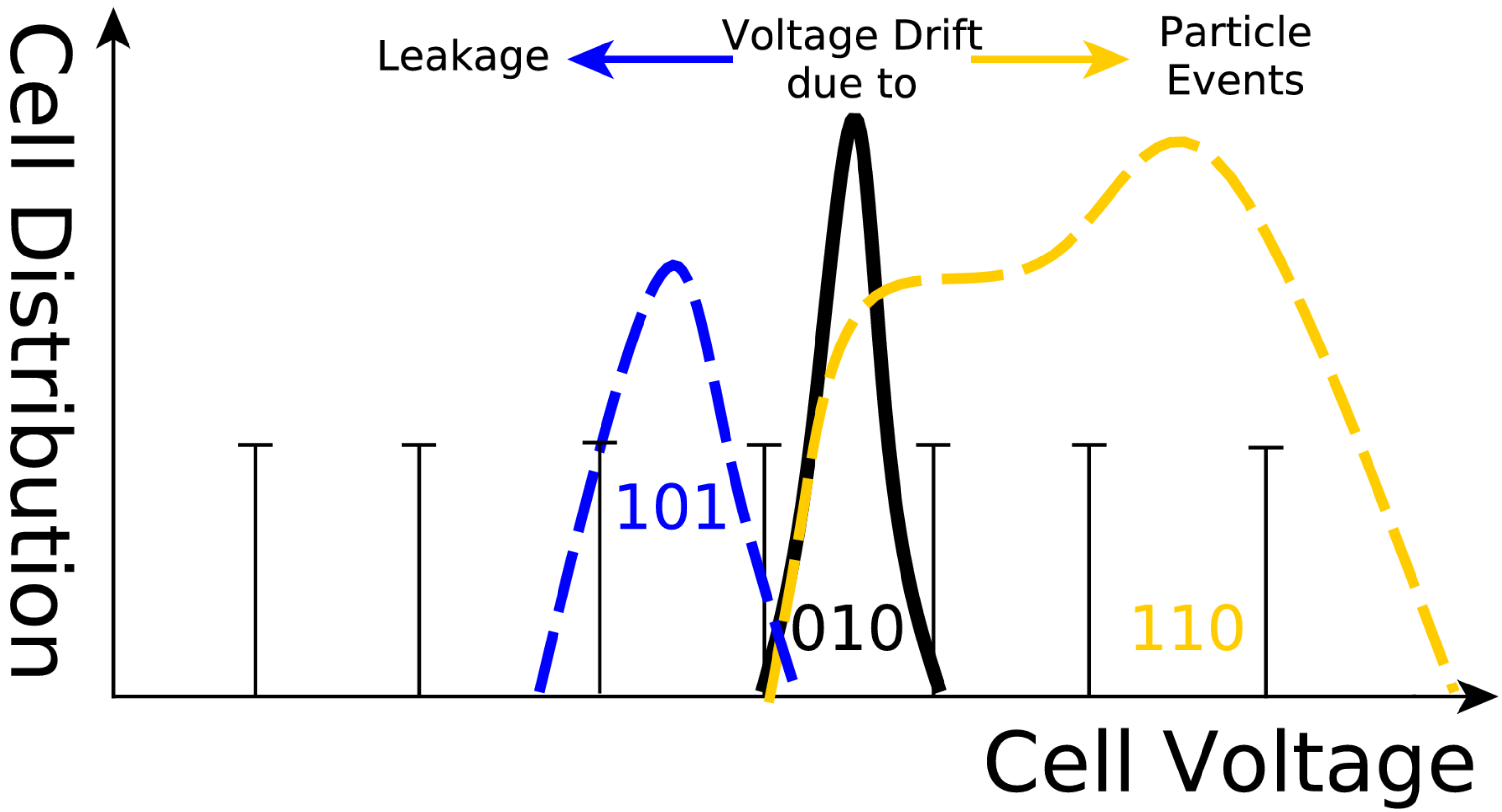
Data Corruption in Multi-Level Cell Flash



Higher Order Multi-Level Cell Flash

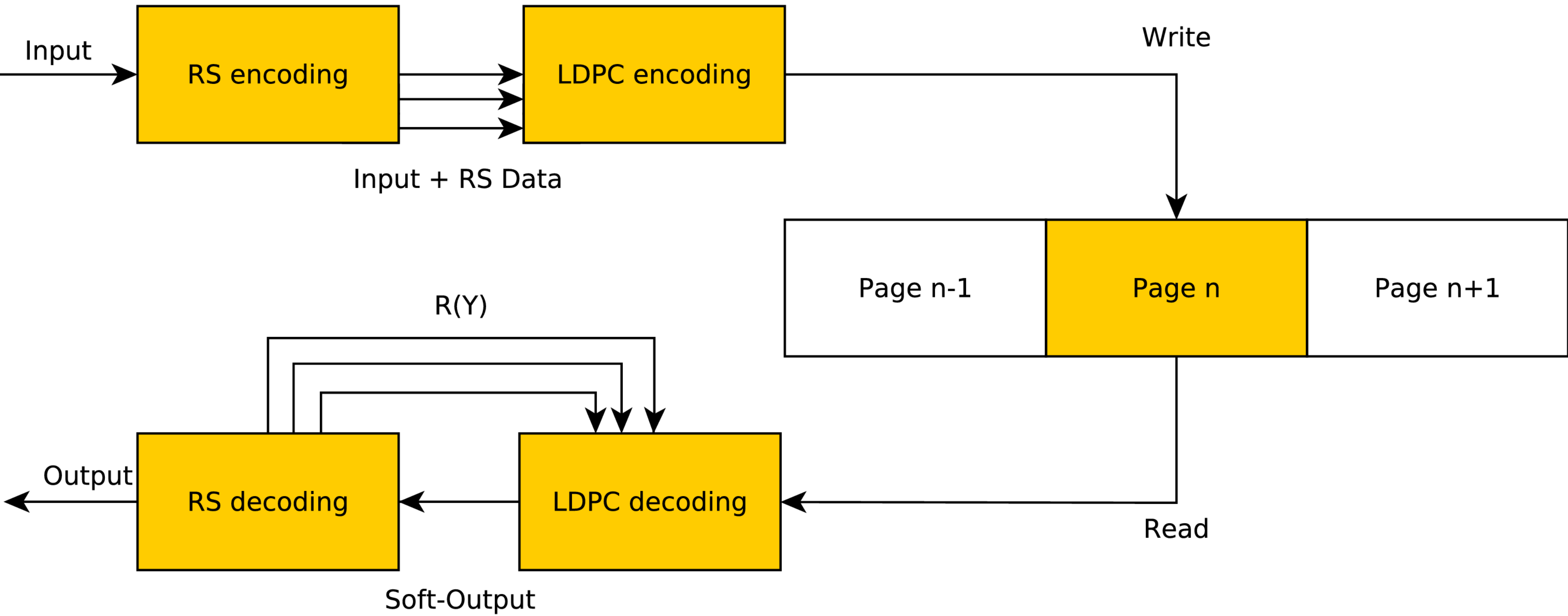


Data Corruption in Multi-Level Cell Flash

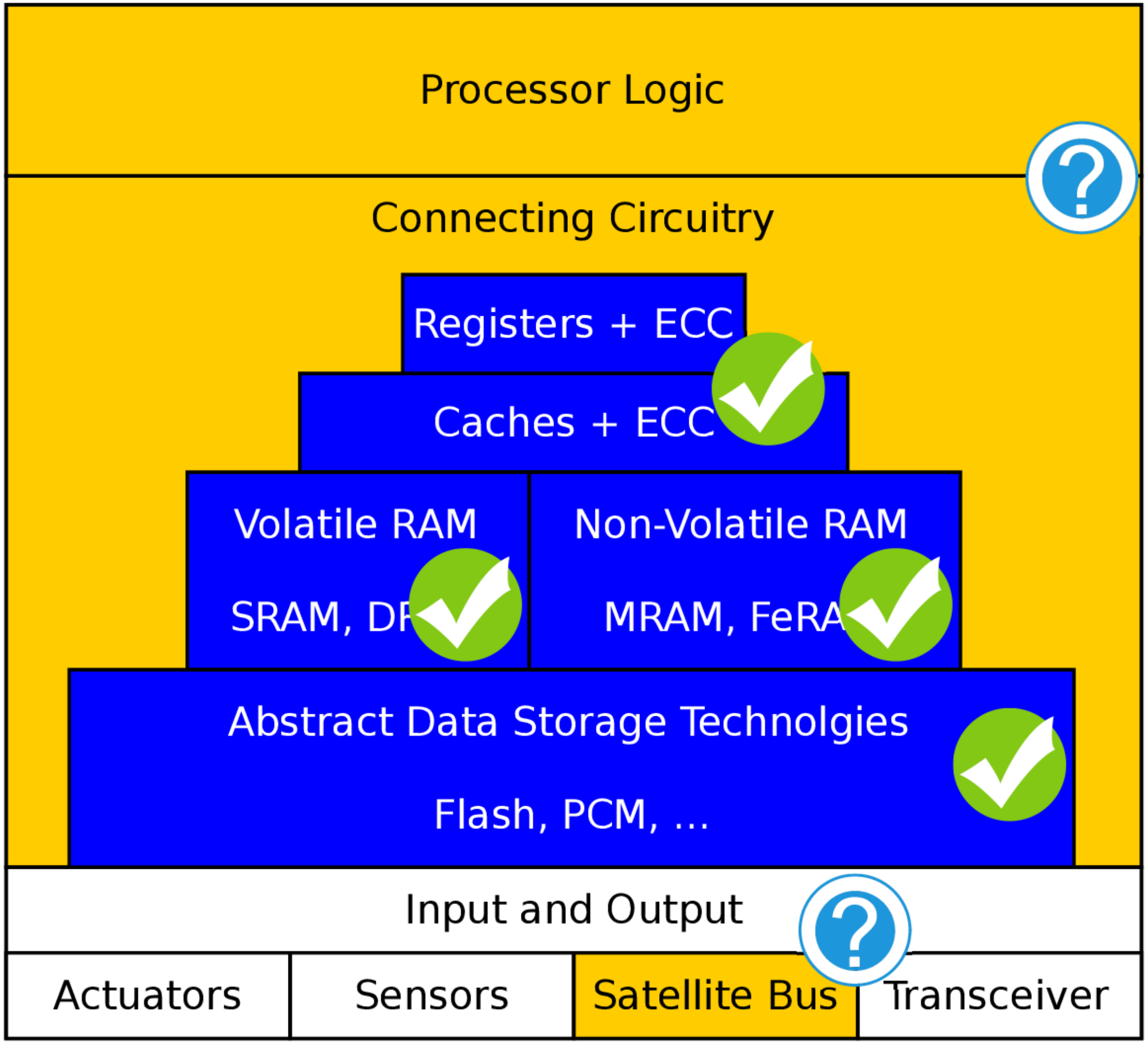


Adapting Erasure Coding for modern MLC-Flash

- MTD-Mirror: a dependable software layer for NAND-flash
- Two Erasure Coding Layers
  - Reed-Solomon to counter multi-bit errors and state-machine issues
  - LDPC to counter single-bit errors



What's Next?



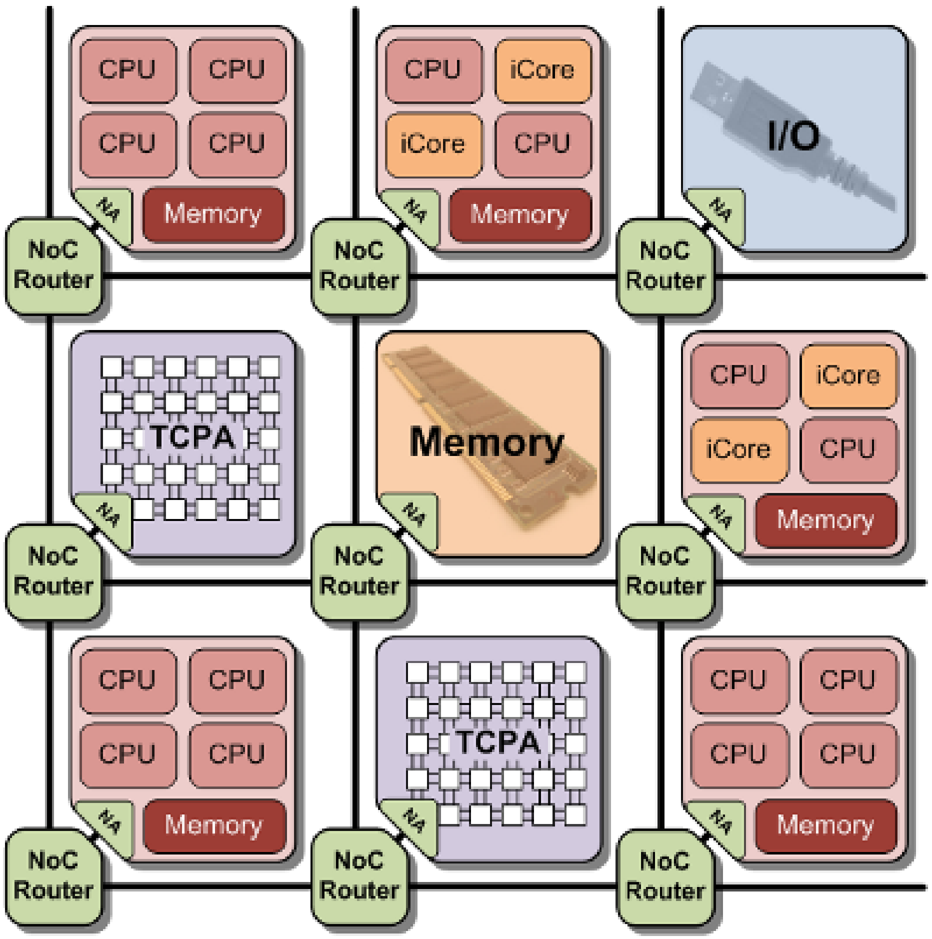
Processor Logic
Connecting Circuitry
Registers + ECC
Caches + ECC
Volatile RAM
SRAM, DR
Non-Volatile RAM
MRAM, FeRA
Abstract Data Storage Technolgies
Flash, PCM, ...
Input and Output
Actuators
Sensors
Satellite Bus
Transceiver

Compute Consistency: The State of Affairs

- Legacy Technology & Coarse Structures
- DMR/Supervised Processors
- TMR Approaches with COTS Processors
- TMR-ed Processor Designs (LEONx-FT)

- Ongoing Research:
  - NoCs, ManyCores & Grid Approaches

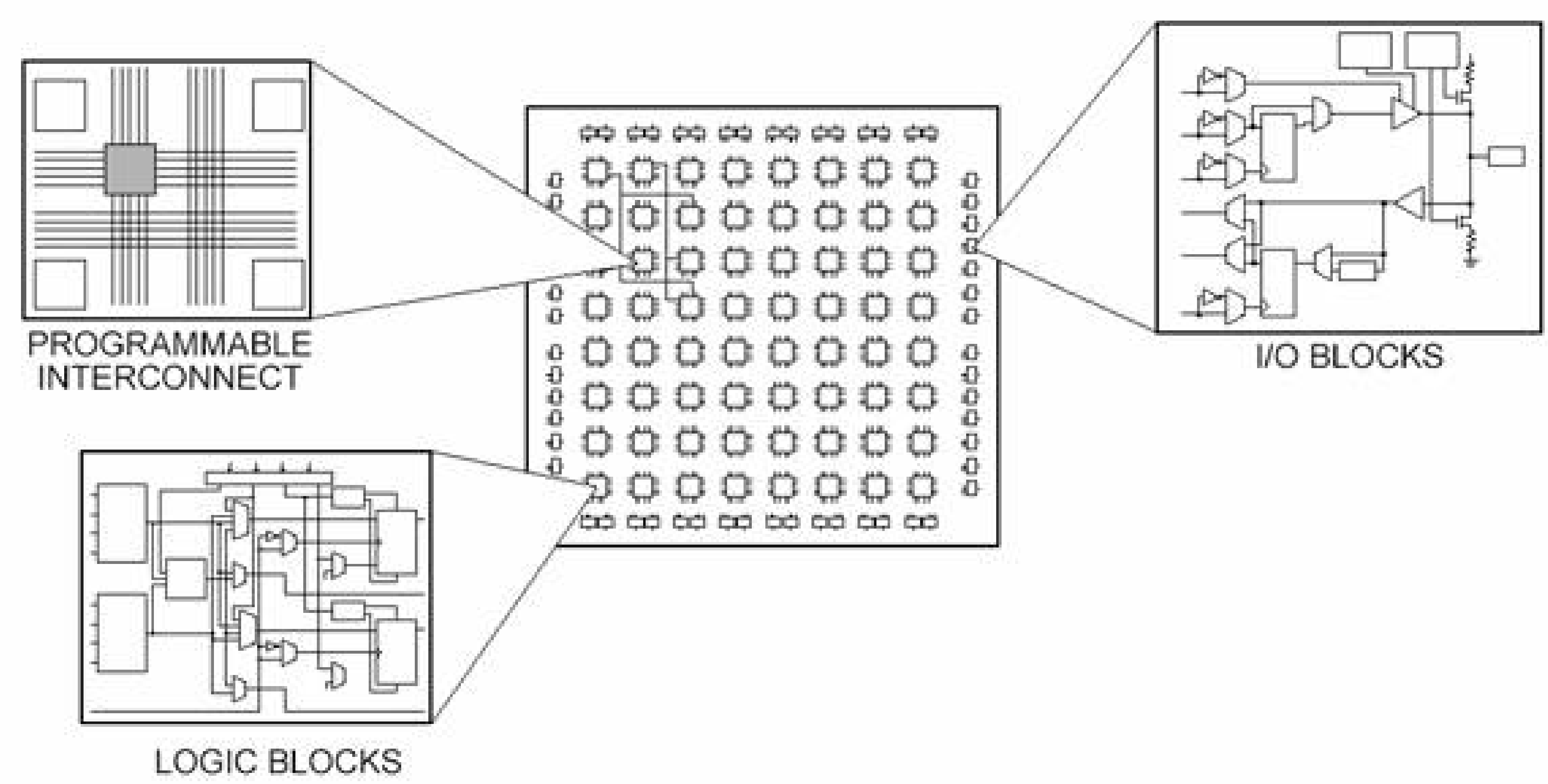
NoCs & Many Cores



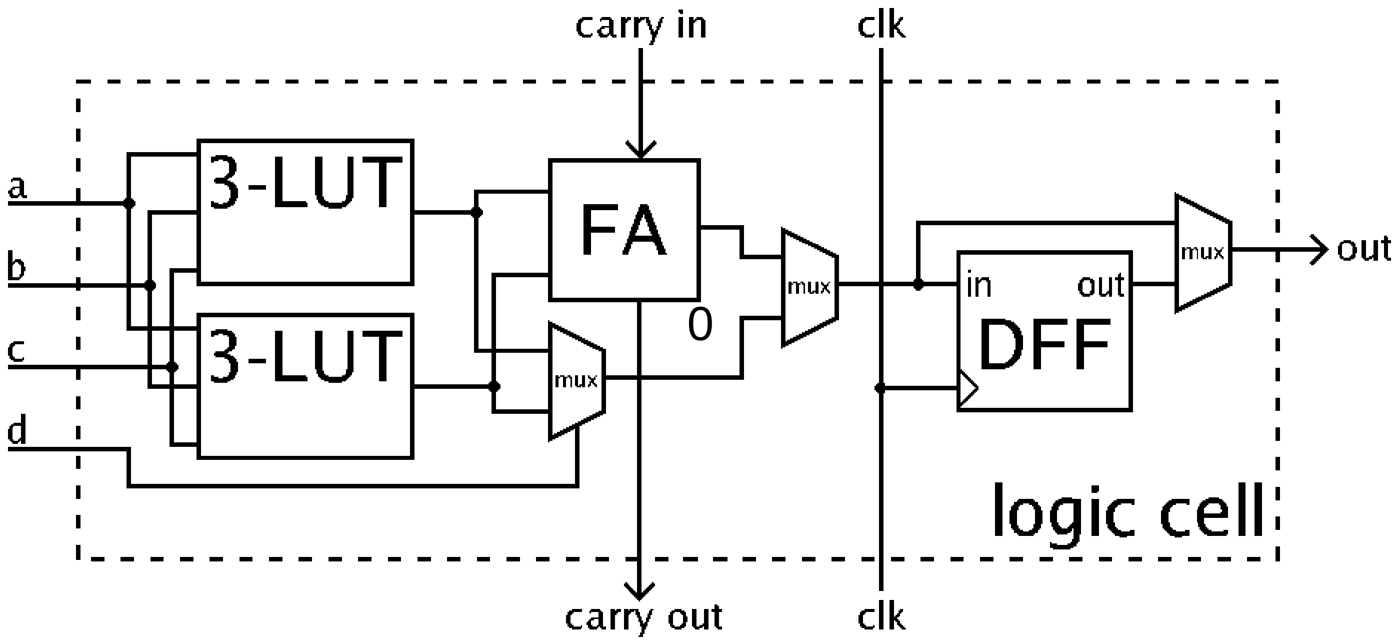
Source: Teich J. et al: “Invasive NoCs – Autonomous, Self-Optimising Communication Infrastructures for MPSoCs,”, University of Erlangen, 2012

FPGAs and Dependability

- Excellent fault-recovery protential



- Excellent fault-recovery protential:
  - Partial reconfiguration
  - Reconfiguration using different routing



FPGAs and Dependability: Core Issues

- Reliable Storage of Designs (“solved”)
- Compute Performance
- **Fault Detection**

Thanks for Listening!

Questions?

Mail to:
christian.fuchs@tum.de
or
Talk to me later :)