SERESSA 2022

5th to 9th of December at CERN, Geneva

Radiation Hardening by Software – Part II

Advanced FDIR and Redundancy Concepts with COTS in Space

Stephan Busch, Fraunhofer EMI and Klaus Schilling, ZfT

Preface

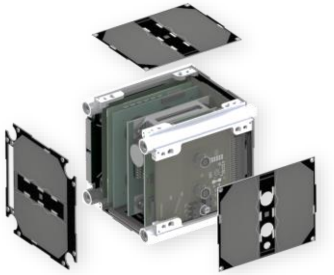
About Me

research and development in the context of **robust**, **flexible**, and **efficient** designs for innovative **small satellite** systems

- University of Würzburg, JMUW
- Center for Telematics, ZfT
- Fraunhofer Ernst-Mach-Institute, EMI

UNI WÜ

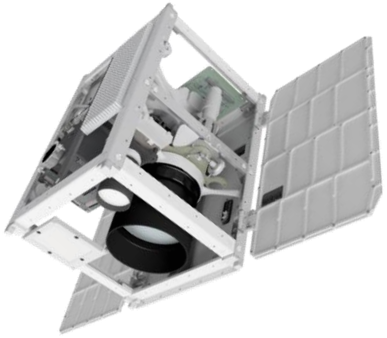
2007



ZENTRUM FÜR TELEMATIK

2015

Fraunhofer EMI



2018

Fraunhofer Ernst-Mach-Institute

Fraunhofer
EMI

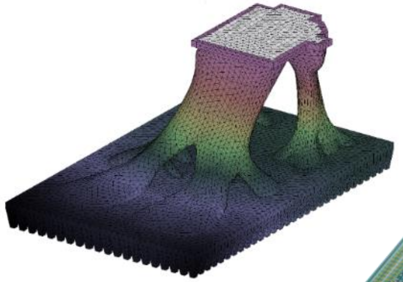
28 000 Staff

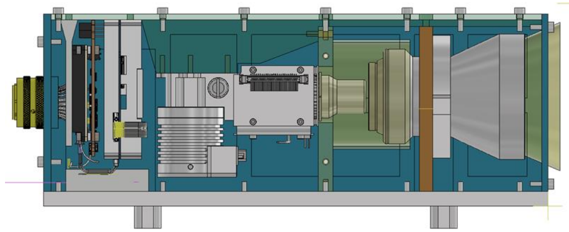
74 Institutes

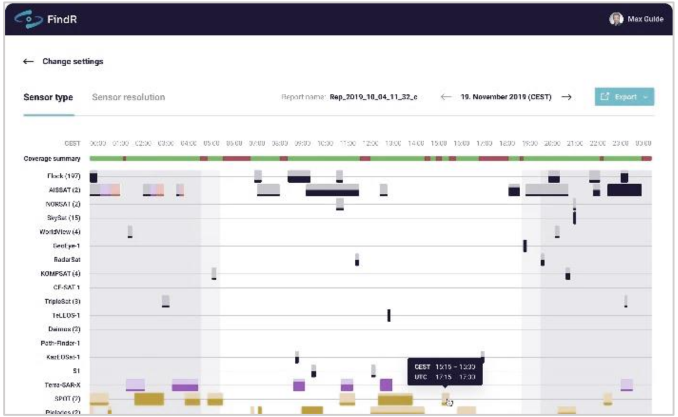
Hauptstandorte ●
Nebenstandorte ○
Itzehoe
Lübeck
Rostock
Stade
Bremerhaven
Hamburg
Oldenburg
Bremen
Berlin
Wolfsburg
Hannover
Potsdam
Teltow
Wildau
Braunschweig
Lemgo
Goslar
Magdeburg
Münster
Paderborn
Gelsenkirchen
Hamm
Soest
Cottbus
Oberhausen
Dortmund
Göttingen
Halle
Schwarzheide
Schkopau
Duisburg
Schmallenberg
Leuna
Leipzig
Kassel
Willich
Dresden
Zittau
Sankt Augustin
Aachen
Freiberg
Erfurt
Jena
Euskirchen
Gießen
Hermsdorf
Chemnitz
Wachtberg
Ilmenau
Remagen
Frankfurt
Hanau
Alzenau
Coburg
Mainz
Aschaffenburg
Bamberg
Bayreuth
Darmstadt
Würzburg
Erlangen
Kaiserslautern
Wertheim
Fürth
St. Ingbert
Mannheim
Nürnberg
Saarbrücken
Karlsruhe
Pfinztal
Regensburg
Straubing
Ettlingen
Esslingen
Stuttgart
Deggendorf
Augsburg
Freising
Garching
Freiburg
München
Weßling
Rosenheim
Kandern
Efringen Kirchen
Holzkirchen
Prien

Fraunhofer Ernst-Mach-Institute

Compact Camera Payloads → Small Satellite Demonstrators → Geoanalytics







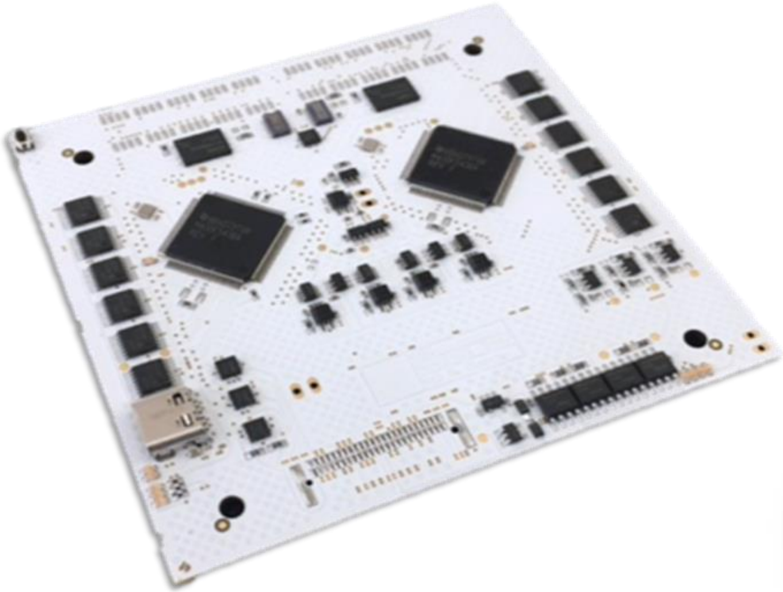
← Change settings

Sensor type Sensor resolution

Report name: Rep_2019_10_04_11_32_c ← 19. November 2019 (CEST) → Export

Agenda

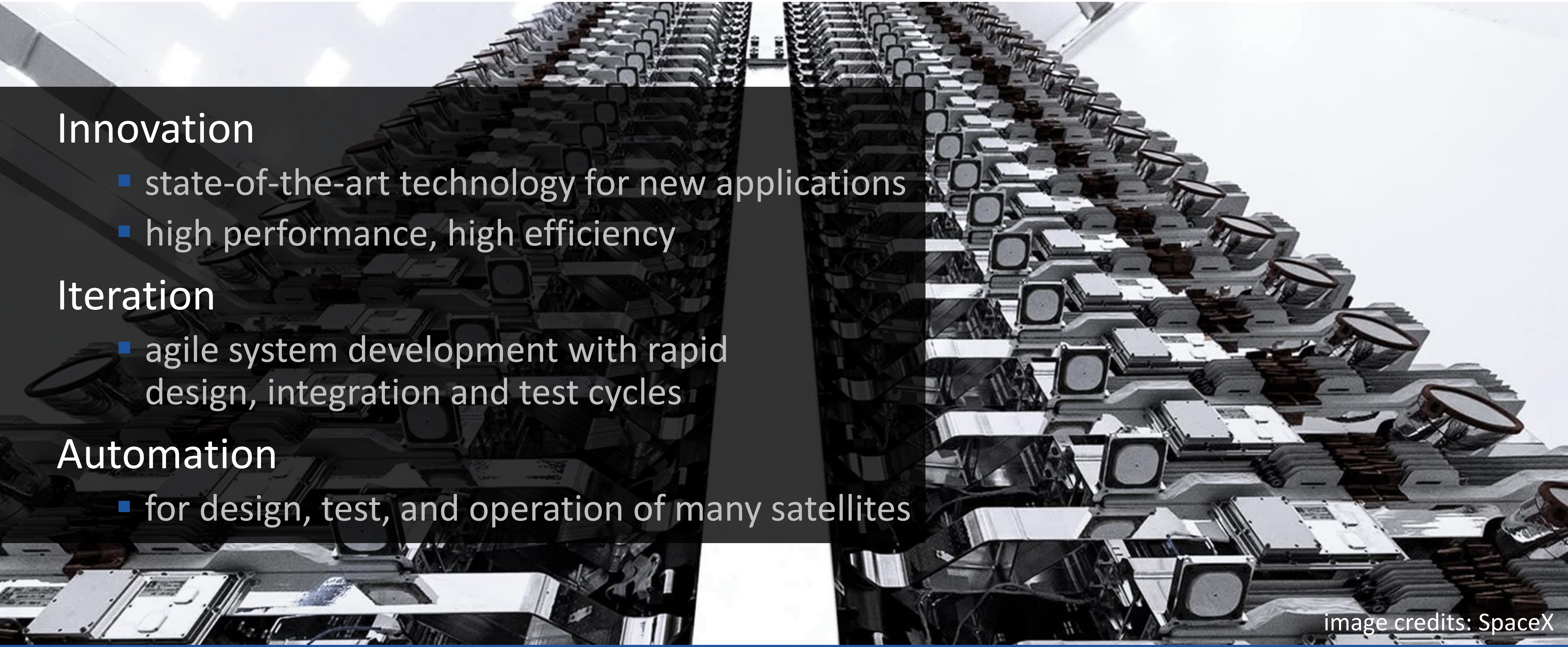
- ❑ Preface
- ❑ Introduction
- ❑ Mitigation Concepts
- ❑ Example System Design
- ❑ On the Horizon
- ❑ References



Julius-Maximilians-UNIVERSITÄT WÜRZBURG Pico-Satellite Bus *UWE*

Introduction

New Approaches for NewSpace



Innovation

- state-of-the-art technology for new applications
- high performance, high efficiency

Iteration

- agile system development with rapid design, integration and test cycles

Automation

- for design, test, and operation of many satellites

image credits: SpaceX

The chance of COTS in NewSpace

Onboard Autonomy

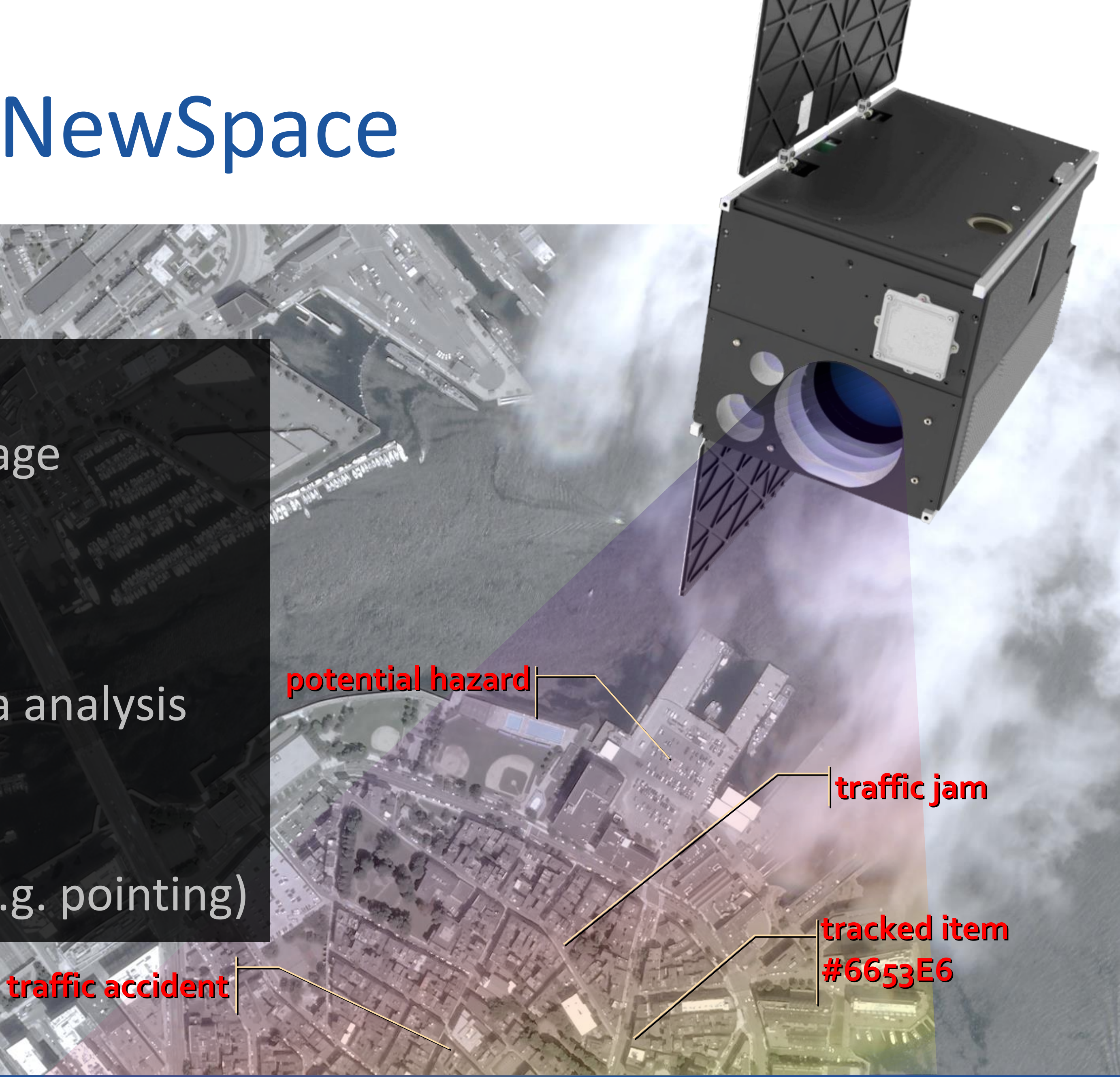
- onboard AI, deep learning based image classification and segmentation
- real-time information extraction

Advanced FDIR

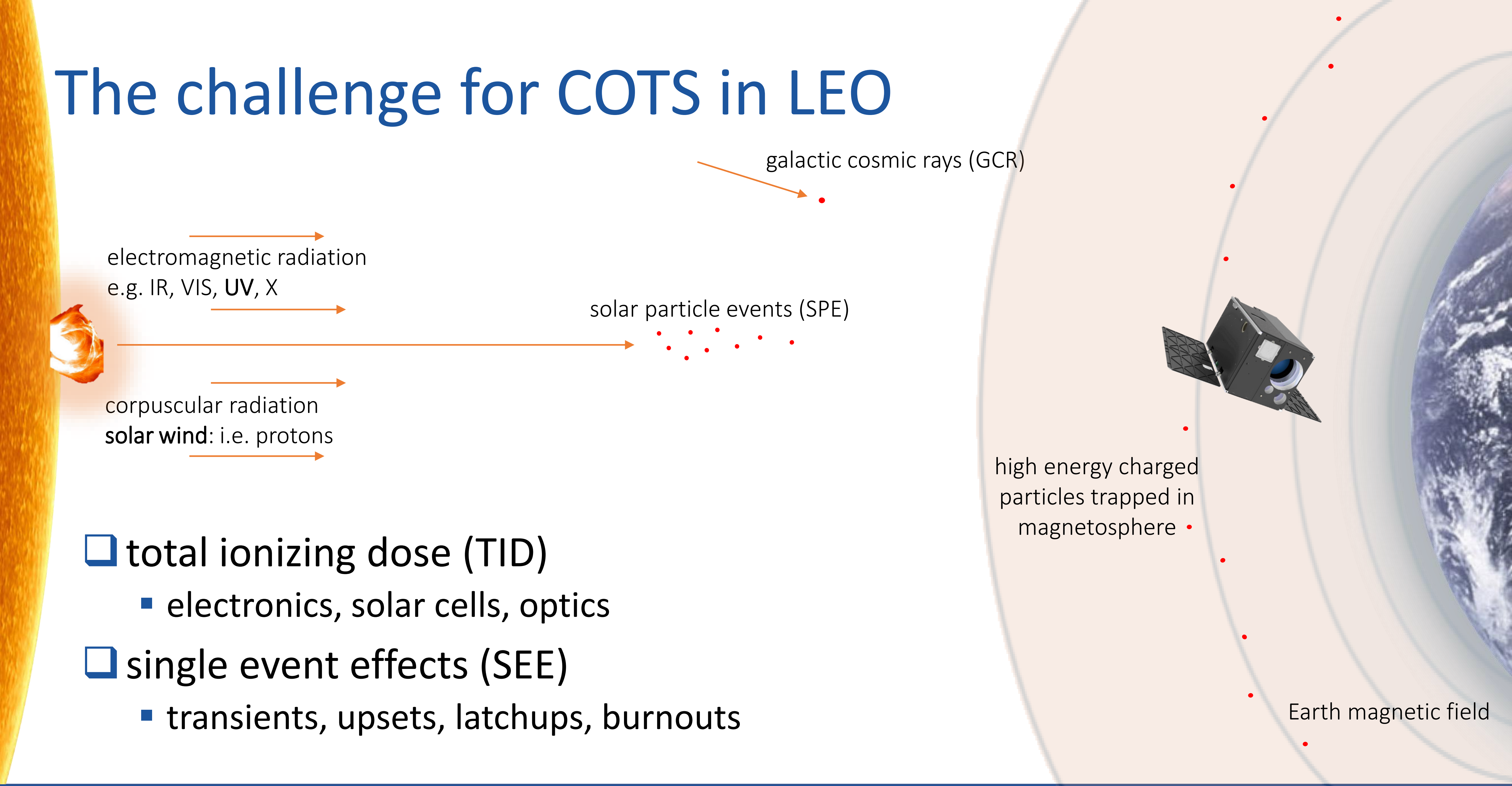
- onboard AI for advanced sensor data analysis and anomaly detection

Payload-in-the-loop

- Optimization of image acquisition (e.g. pointing)



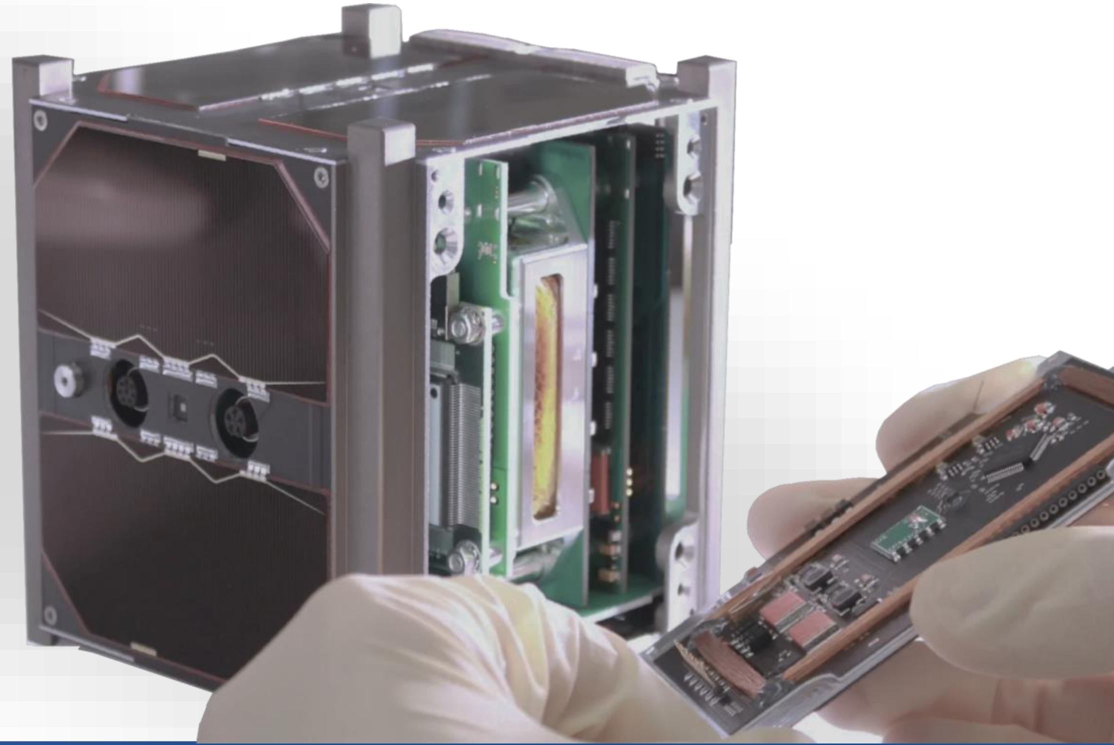
The challenge for COTS in LEO


galactic cosmic rays (GCR)
electromagnetic radiation
e.g. IR, VIS, **UV**, X
solar particle events (SPE)
corpuscular radiation
solar wind: i.e. protons
high energy charged particles trapped in magnetosphere
Earth magnetic field

- ❑ total ionizing dose (TID)
  - electronics, solar cells, optics
- ❑ single event effects (SEE)
  - transients, upsets, latchups, burnouts

Advanced FDIR and Redundancy Concepts with COTS

» How to provide a
reasonable level of robustness
for modern system architectures based on
commercial-of-the-shelf hardware
to allow dependable operation in the
hazardous space environment «



Mitigation Concepts

Robustness

robustness = reliability + fault-tolerance

the ability of a system to…

1. accomplish its designated operations during intended lifetime under normal conditions (reliable)
2. continue at least reduced operations in the event of the failure of some of its components (fault-tolerant)

Reasonable level of robustness for a small satellite

- most failures are not inherently destructive and can be recovered
  e.g. by power cycles, complex recovery procedures by ground control
- at least the key components have to be implemented robustly to enable recovery
  i.e. OBC + EPS + COM

General Concepts of Radiation Effects Mitigation

radiation effects mitigation for COTS based designs

robustness of COTS based systems by design hard- and software design can be achieved by avoidance, conservative design, or redundancy and recovery

Hardware

- shielding
- non-sensitive operation modes
- component selection
- device redundancy
- protection circuits

Software

- information-redundancy
- time-redundancy
- code-redundancy
- reduced operation duty cycle
- fault detection, isolation, and recovery mechanisms (FDIR)

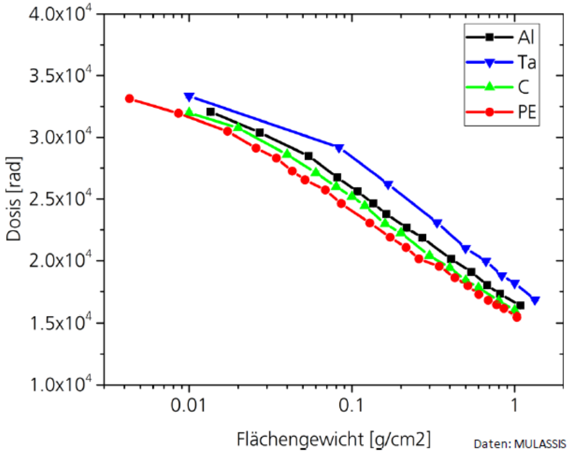
[Maurer et. al., 2008]

Hardware: Effect Reduction

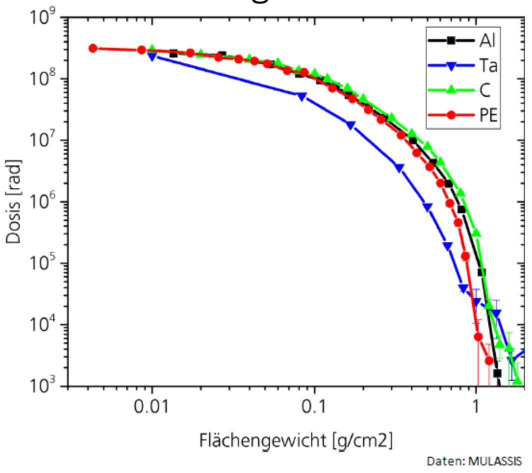
- ❑ Shielding of critical components
  - protons: light materials, e.g. PE (Polyethylene)
  - electrons: high-Z materials, e.g. Ta (Tantal)

- ❑ Non-sensitive operation modes
  - partial power down of unused hardware exploiting reduced duty cycle
  - low clock frequency reduces probability for SET

Shielding of Protons



Shielding of Electrons



[Höffgen, 2021]

Hardware: Component Selection

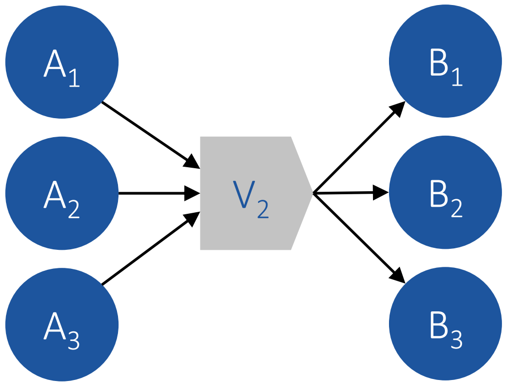
- ❑ Radiation tolerant COTS
  - bipolar integrated circuits
  - MRAM (Magnetoresistive RAM), FRAM (Ferroelectric RAM), Flash
- ❑ De-Rating
  - conservative component selection, large margin for relevant specification parameters
- ❑ Target minimization: reduced surface of vulnerability
  - prefer reduced complexity (i.e. sensitive nodes)

Hardware: Tolerant System Design

❑ Device redundancy

- parallel loosely coupled operation
  e.g. parallel switches, diodes, LDOs
- voting circuits
  e.g. TMR (triple modular redundancy)

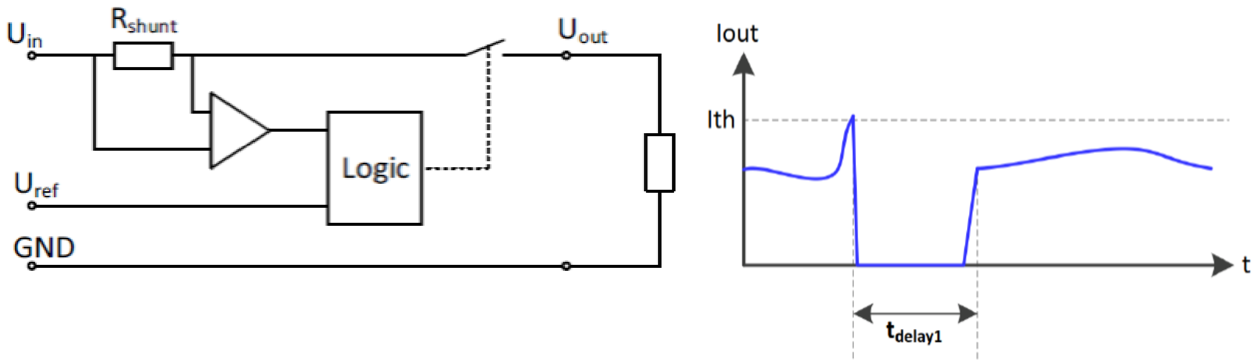
Triple redundancy with single voter



❑ Protection circuits

- damage protection,
  e.g. current limiter, latchup protection
- watchdog timer recovery

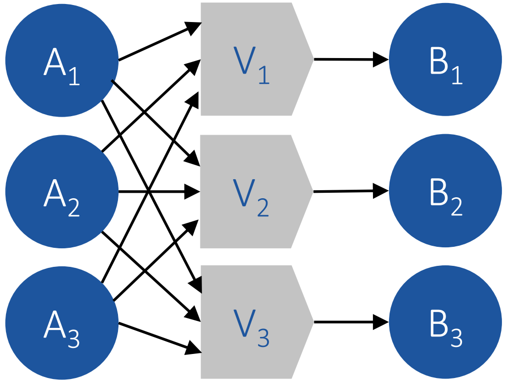
Latchup Protection



Hardware: Tolerant System Design

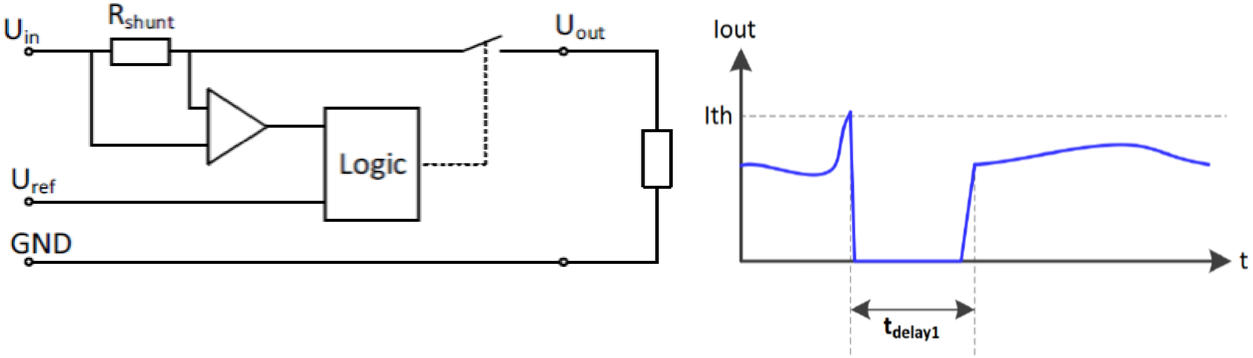
- ❑ Device redundancy
  - parallel loosely coupled operation
    e.g. parallel switches, diodes, LDOs
  - voting circuits
    e.g. TMR (triple modular redundancy)

Triple Modular Redundancy (TMR)



- ❑ Protection circuits
  - damage protection,
    e.g. current limiter, latchup protection
  - watchdog timer recovery

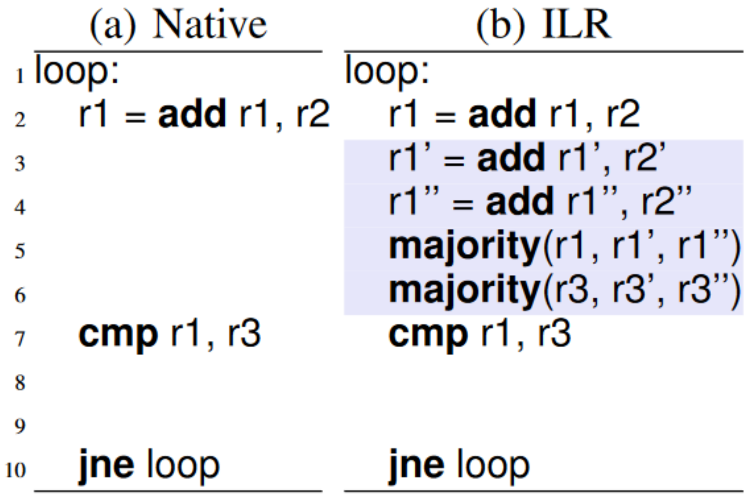
Latchup Protection



Software: Redundancy

- Information redundancy
  - state verification
    e.g. periodical check of register settings
  - error detection and correction (EDAC) codes and memory scrubbing
    e.g. parity, CRC, Hamming or Reed-Solomon codes
    periodic memory scan mitigates cumulative errors
- Code redundancy
  - redundant software images
  - redundant instructions for critical calculations (ILR)
    source-2-source compilers generate “hardened” code
- Time redundancy
  - execute redundant operations subsequently on the same hardware

Example: Instruction-Level Redundancy (ILR)



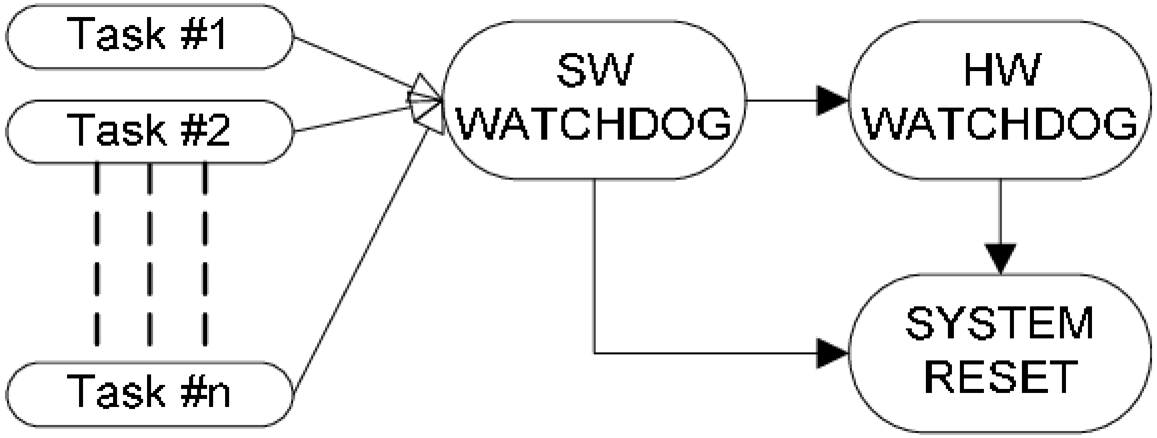
```
(a) Native               (b) ILR
loop:                    loop:
   r1 = add r1, r2          r1 = add r1, r2
                            r1’ = add r1’, r2’
                            r1” = add r1”, r2”
                            majority(r1, r1’, r1”)
                            majority(r3, r3’, r3”)
   cmp r1, r3               cmp r1, r3


   jne loop                 jne loop
```

[Kuvaiskii et.al, 2016]

Software: Monitor and Recover

- Software Watchdog
  - monitor task execution, communication link, or external device
  - execute recovery procedures
    e.g. checkpoint recovery, reset of a task or entire system,
    initiate power cycle of external hardware, etc.



[Abaffy et.al. 2010]

Example System Design

The UWE Satellite Bus

A **robust**, flexible, and efficient satellite bus

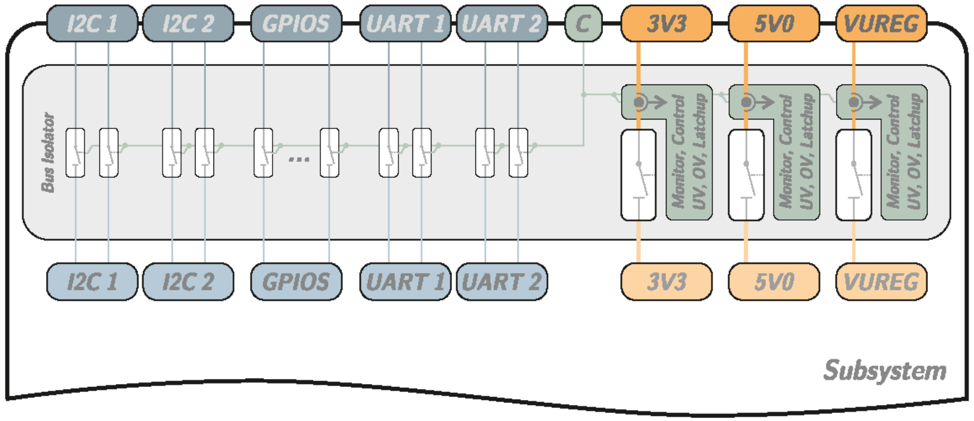
- UWE-3: Attitude Control (launch 2013)
- UWE-4: Electrical Propulsion (launch 2018)

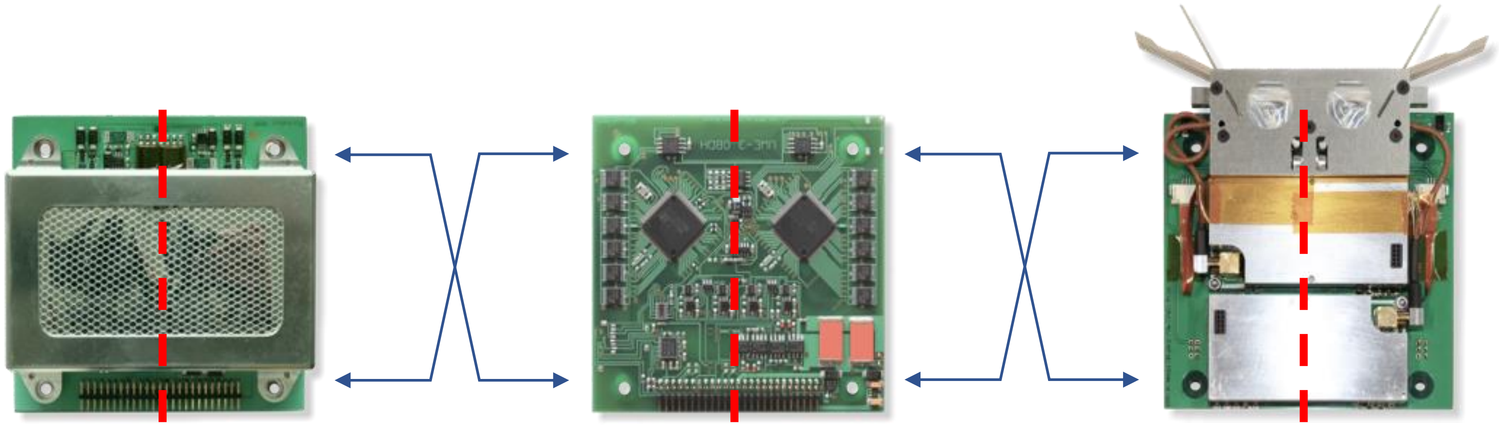
Julius-Maximilians-UNIVERSITÄT WÜRZBURG

The UWE Satellite Bus

- ❑ Modular architecture
- ❑ Standardized subsystem interface
- ❑ Redundancy of core components

UNISEC Subsystem-Interface

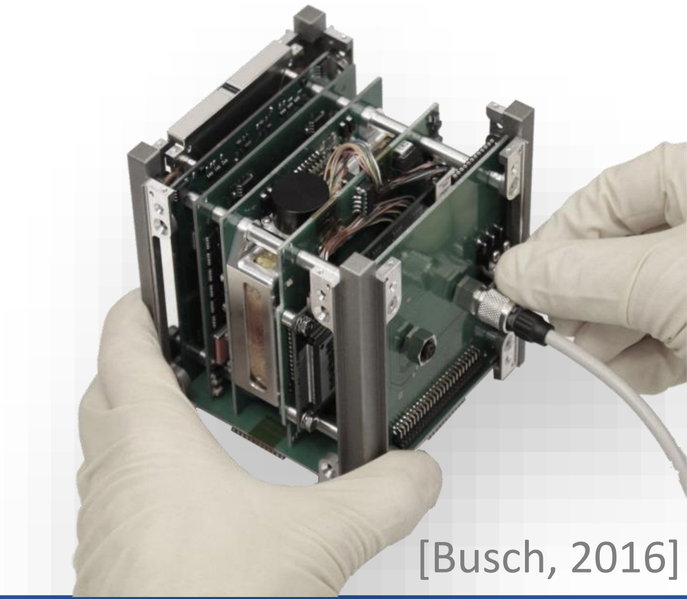




EPS

OBC
Core Module

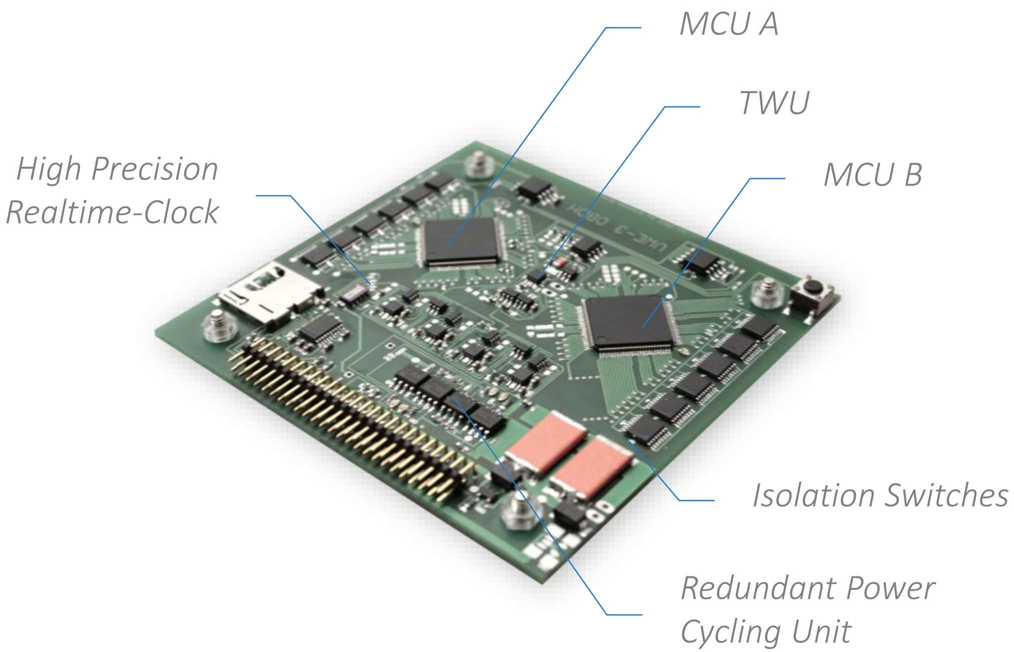
COM

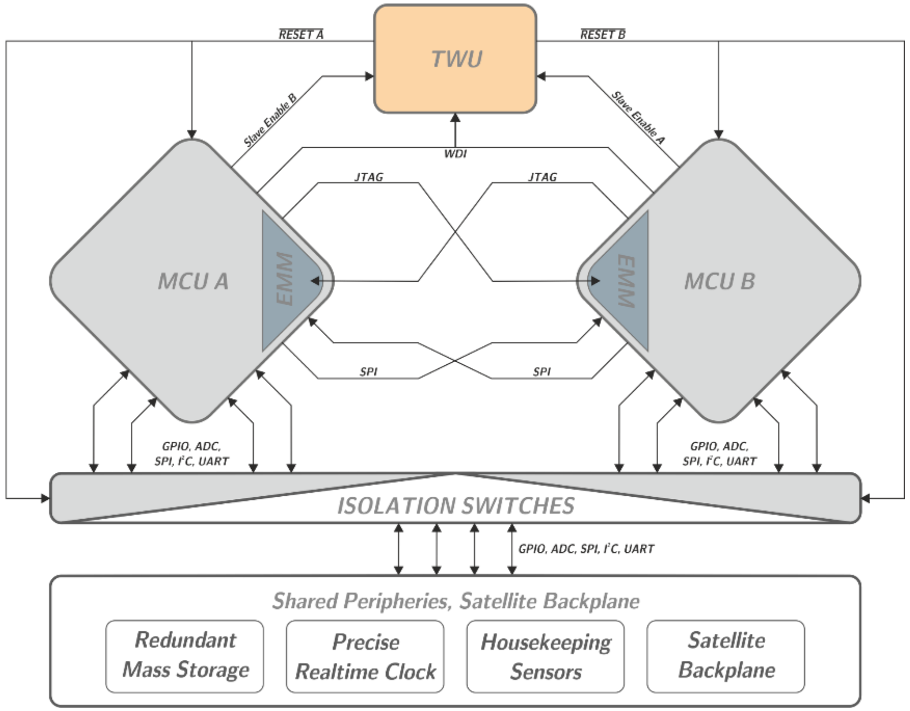


[Busch, 2016]

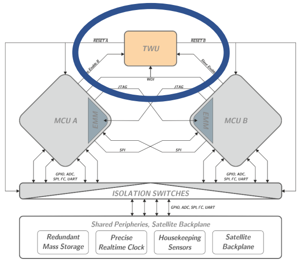
Robust and Efficient OBDH Core Module

- ❑ optimized as dedicated housekeeping und autonomous FDIR module
- ❑ two redundant microcontrollers units (MCU) in warm-backup
- ❑ less than 10mW total power consumption

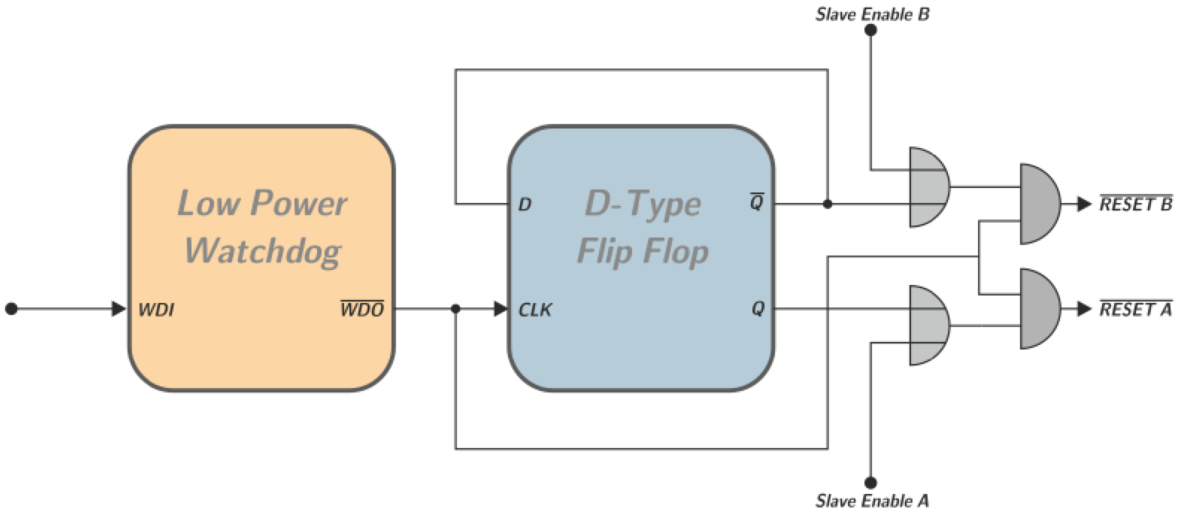


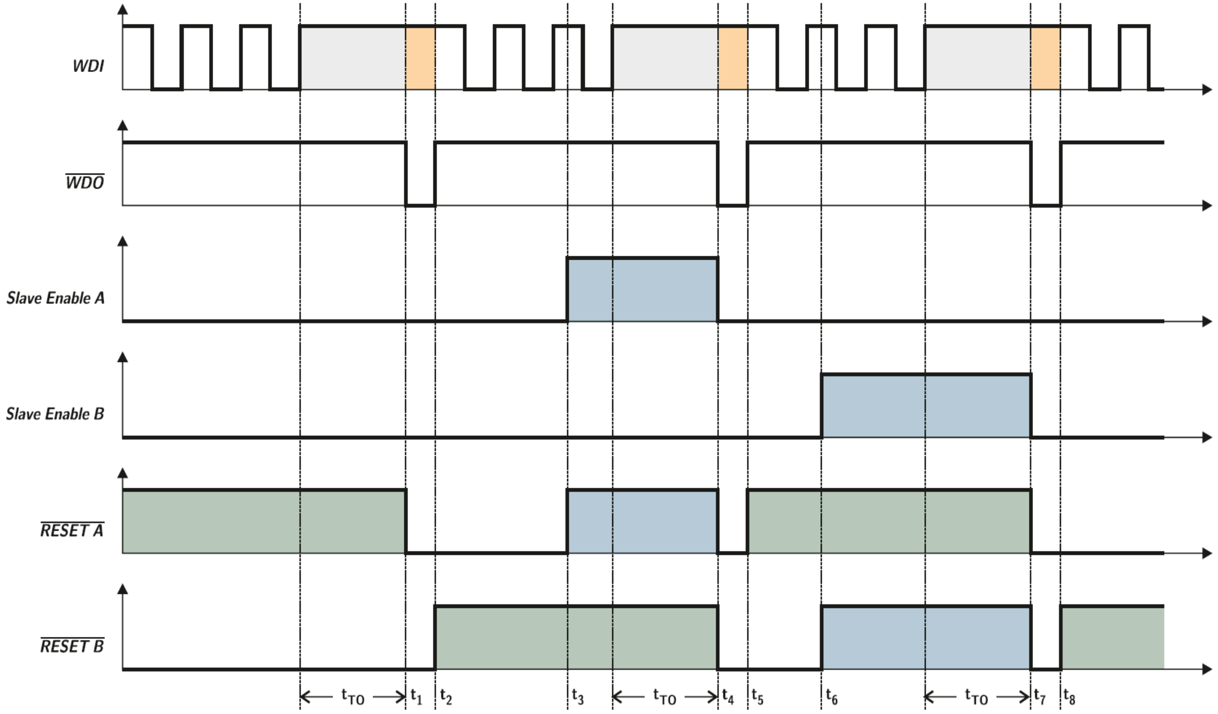


Robust and Efficient OBDH Core Module

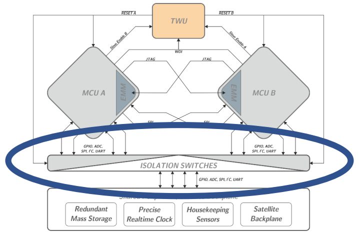


- ❑ Toggle Watchdog Unit (TWU)
  - autonomous reconfiguration
  - reset and switch-over
  - allow slave enable

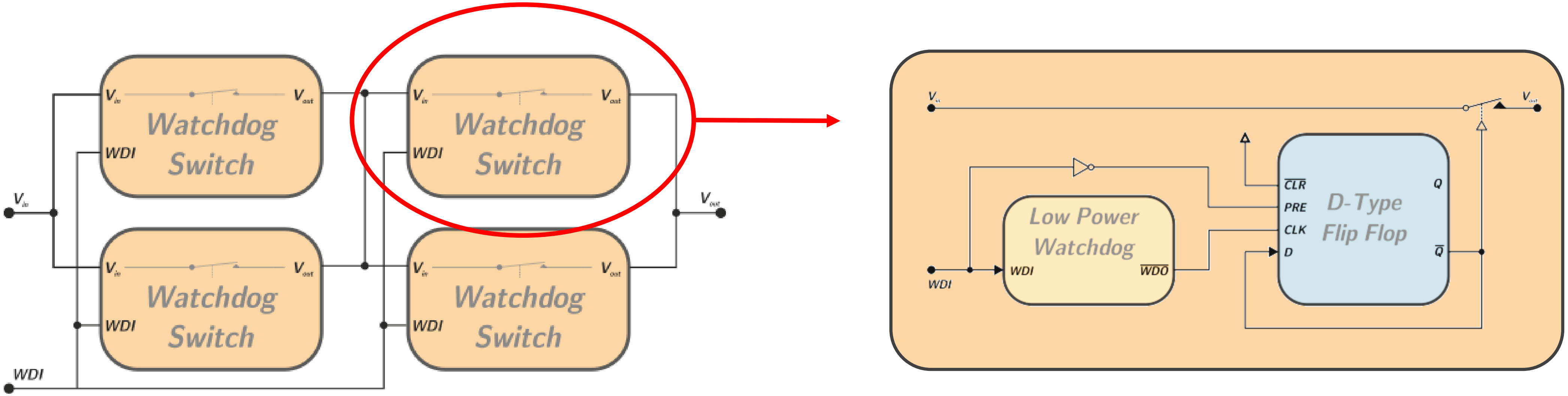




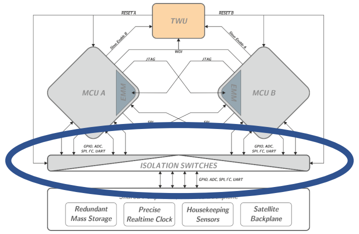
Robust and Efficient OBDH Core Module



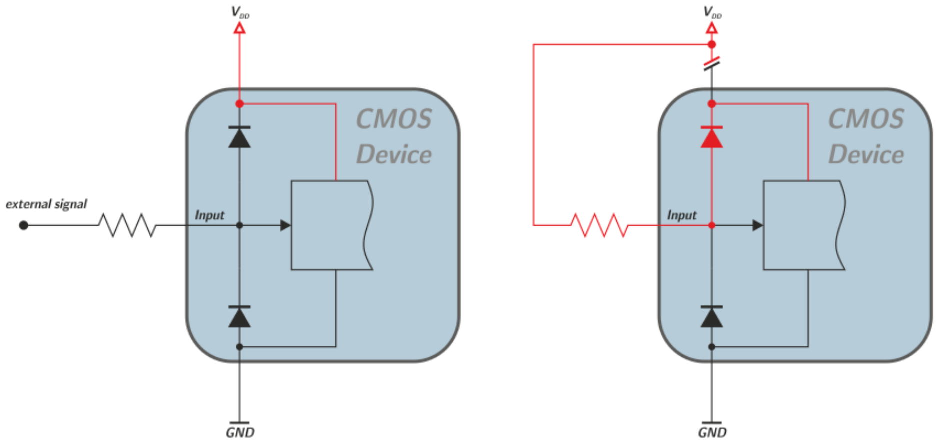
- ❑ Power Cycling Unit (PCU)
  - loosely coupled redundancy
  - intrinsic majority voting

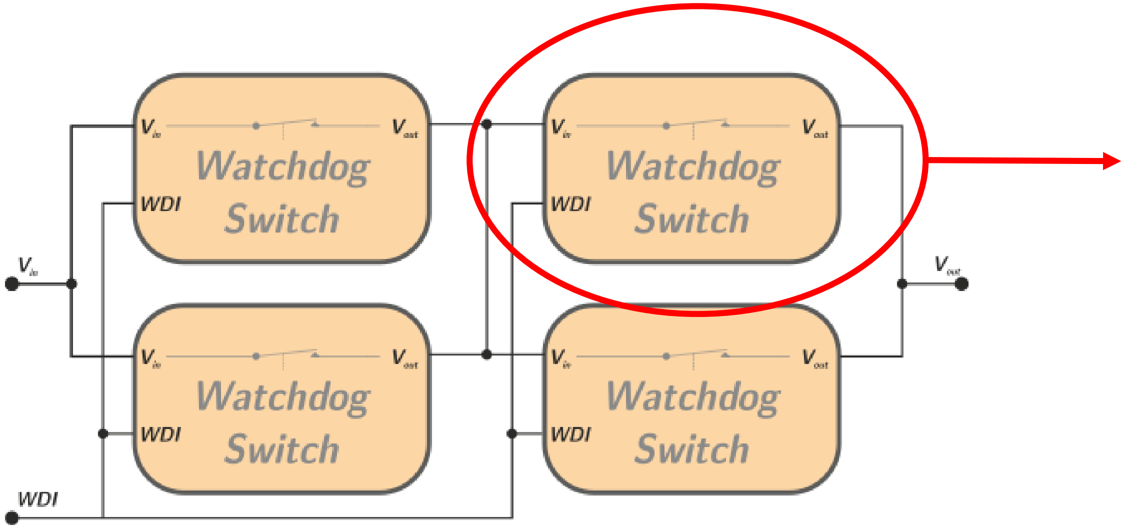


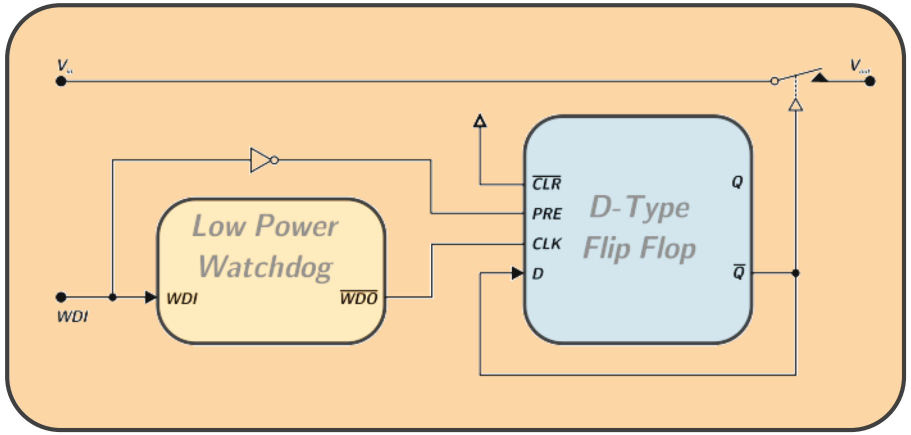
Robust and Efficient OBDH Core Module



- ❑ Power Cycling Unit (PCU)
  - loosely coupled redundancy
  - intrinsic majority voting
  - full isolation of CMOS devices

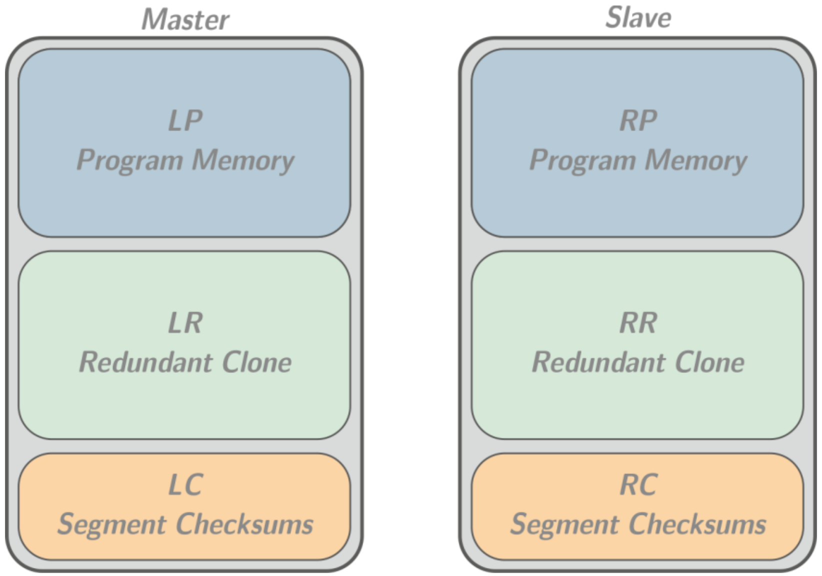


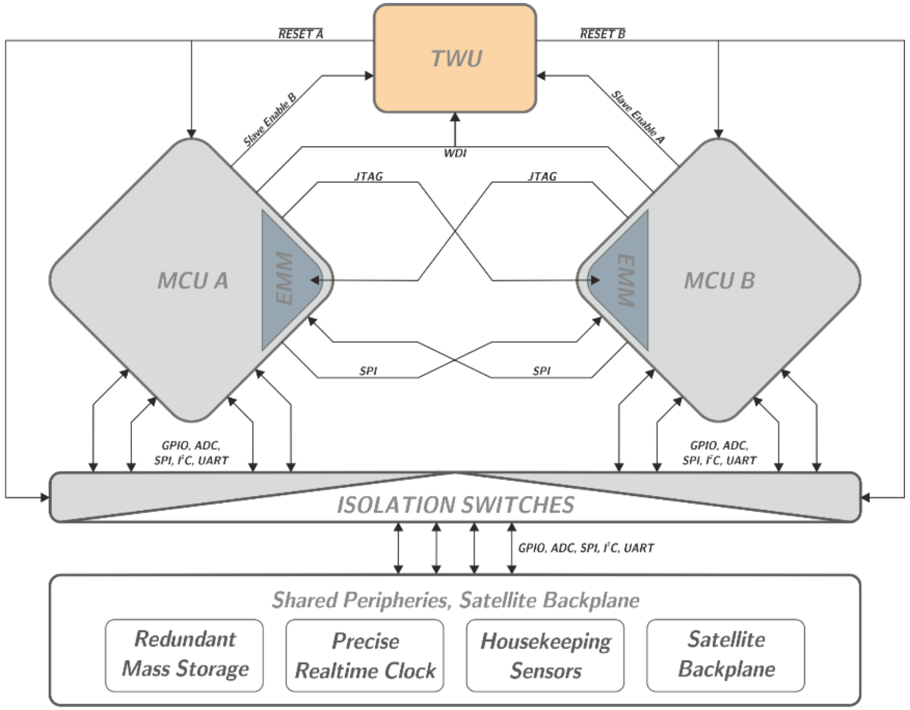




Robust and Efficient OBDH Core Module

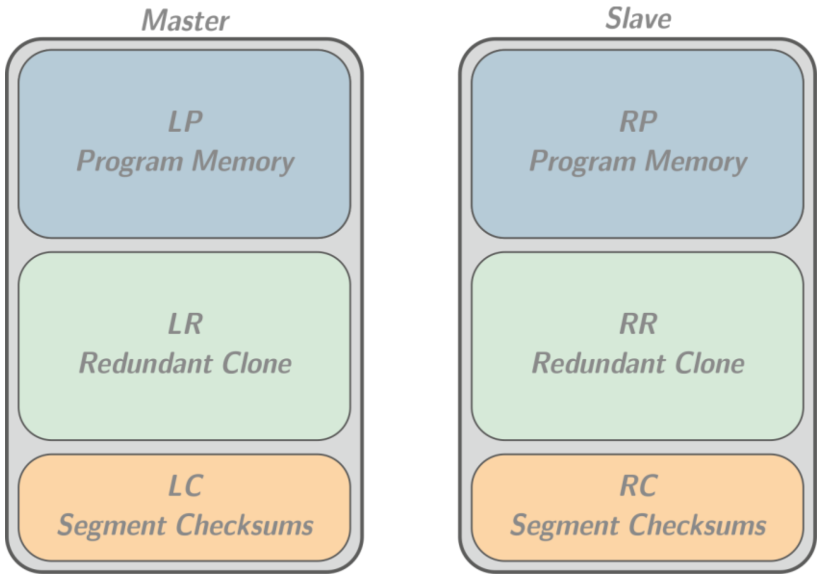
- Mutual MCU supervision and reconfiguration
  - redundant software images in local and remote unit
  - remote program memory supervision using rapid (<2s) pseudo signature analysis checksums PSA via JTAG/EEM hardware and bitwise-logic operators





Robust and Efficient OBDH Core Module

- Mutual MCU supervision and reconfiguration
  - redundant software images in local and remote unit
  - remote program memory supervision using rapid (<2s) pseudo signature analysis checksums PSA via JTAG/EEM hardware and bitwise-logic operators



not decidable		$\overline{RP}$		RP	
		$\overline{RR}$	RR	$\overline{RR}$	RR
$\overline{LP}$	$\overline{LR}$	0	0	0	x
	LR	0	x	x	1
LP	$\overline{LR}$	0	x	x	1
	LR	x	1	1	1

C1		$\overline{RP}$		RP	
		$\overline{RR}$	RR	$\overline{RR}$	RR
$\overline{LP}$	$\overline{LR}$	0	0	0	1
	LR	0	0	0	1
LP	$\overline{LR}$	0	0	0	1
	LR	1	1	1	1

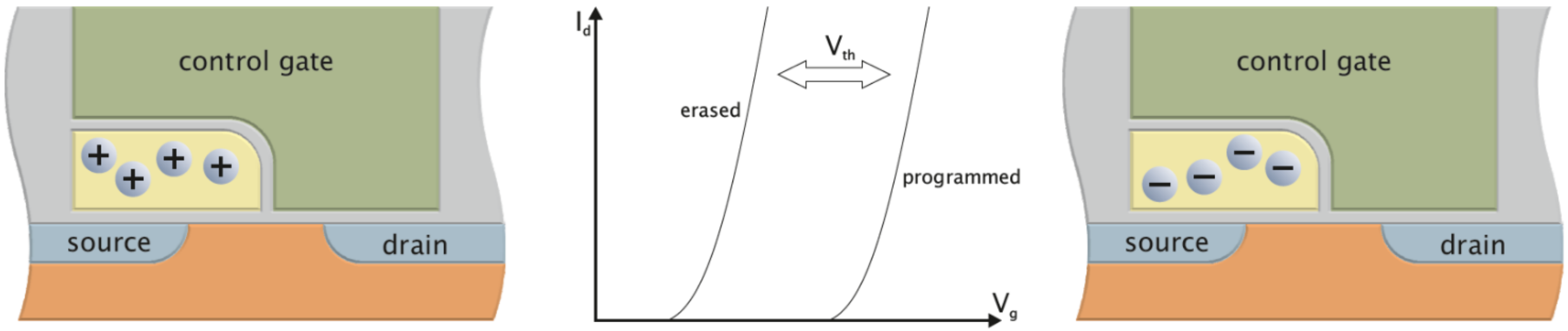
C1 = $(LP \wedge LR) \vee (RP \wedge RR)$

C2		$\overline{RP}$		RP	
		$\overline{RR}$	RR	$\overline{RR}$	RR
$\overline{LP}$	$\overline{LR}$	0	0	0	0
	LR	0	1	1	1
LP	$\overline{LR}$	0	1	1	1
	LR	0	1	1	1

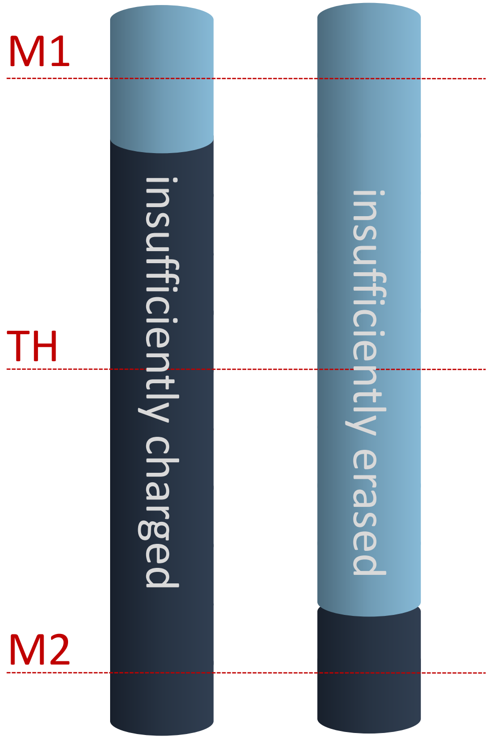
C2 = $(LP \vee LR) \wedge (RP \vee RR)$

Robust and Efficient OBDH Core Module

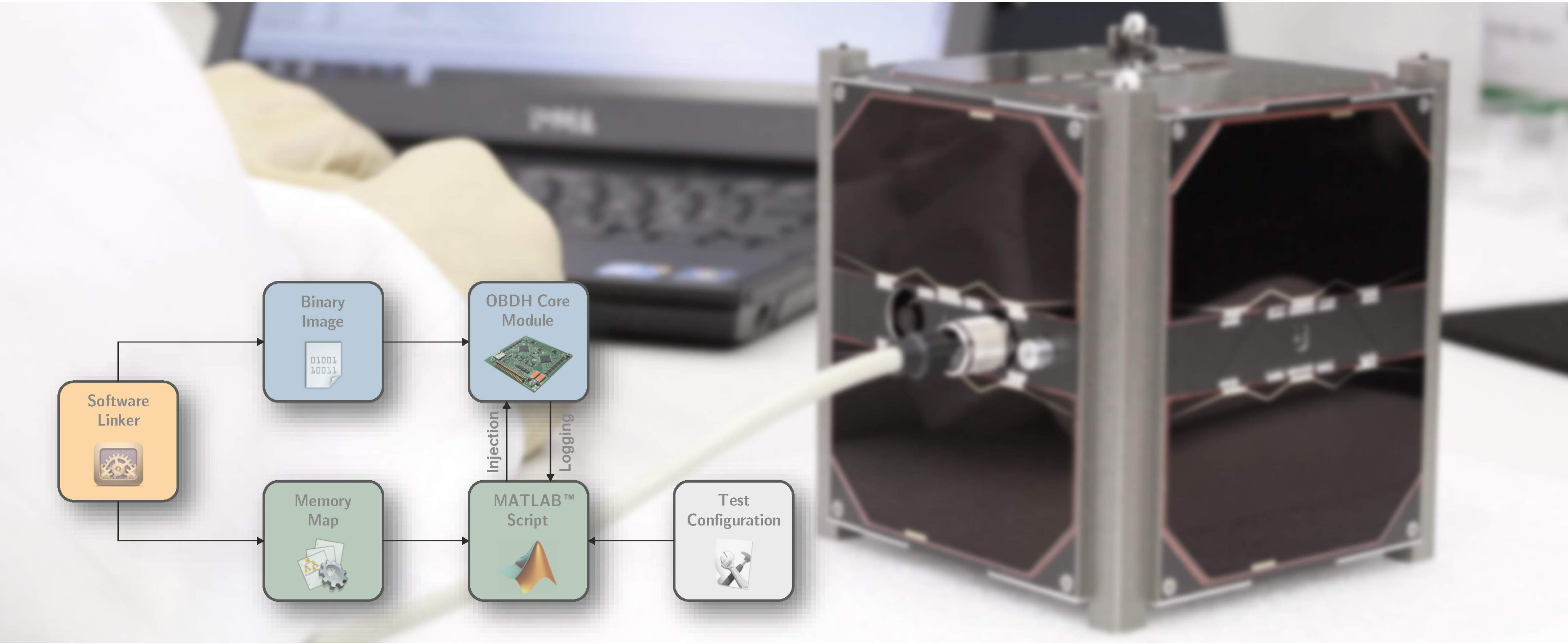
- Mutual MCU supervision and reconfiguration
  - redundant software images in local and remote unit
  - remote program memory supervision using rapid (<2s) pseudo signature analysis checksums PSA via JTAG/EEM hardware and bitwise-logic operators
  - early recovery by floating gate cell marginal read



Flash Memory Cell
Fill Level



Software Implemented Fault Injection (SWIFI)



Software Linker

Binary Image

Memory Map

OBDH Core Module

MATLAB™ Script

Test Configuration

Injection

Logging

Software Implemented Fault Injection (SWIFI)

❑ PER (periphery registers)
- illegal access violation
- hardware misconfiguration (e.g. clock, interfaces,…)

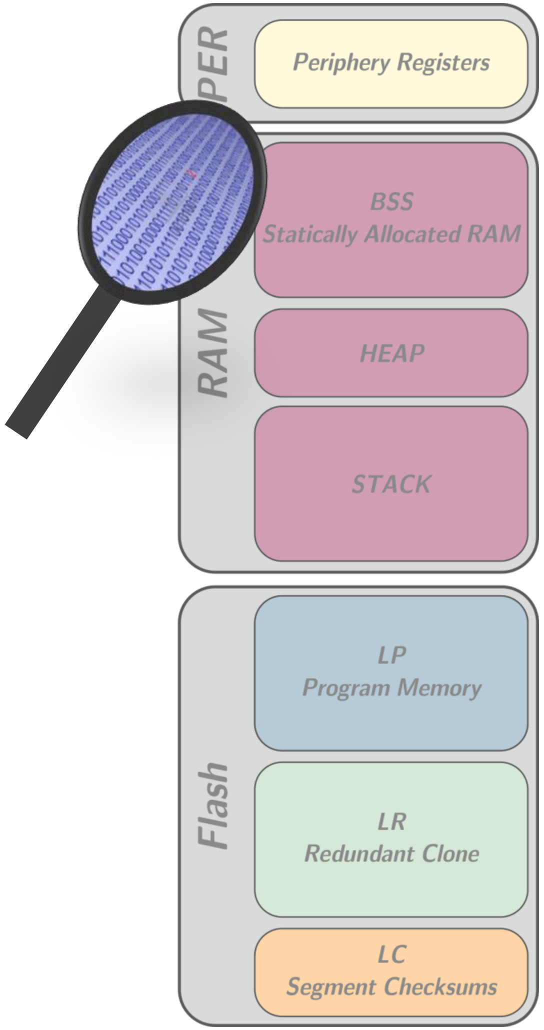
❑ BSS (statically allocated RAM)
- state corruption
- function pointer corruption

❑ STACK
- return pointer corruption

❑ HEAP (not used)

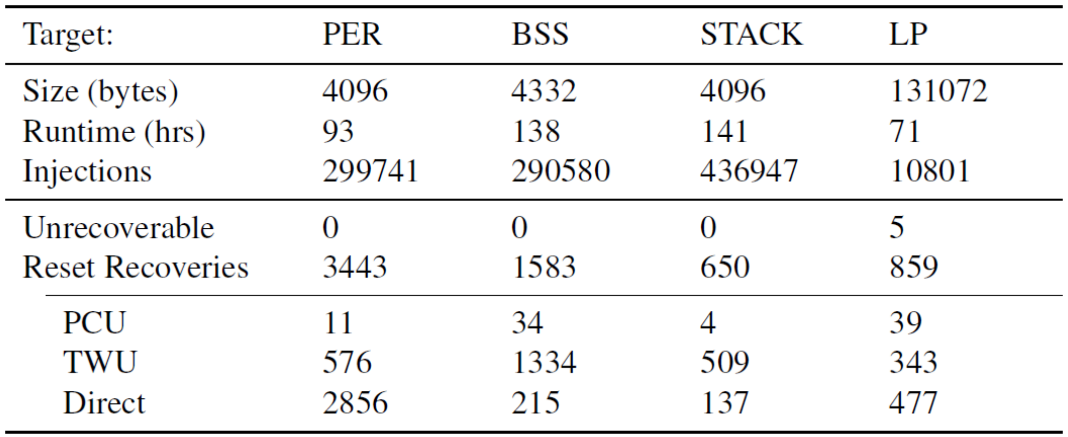
❑ Flash
- illegal instruction execution

→ fault → recovery

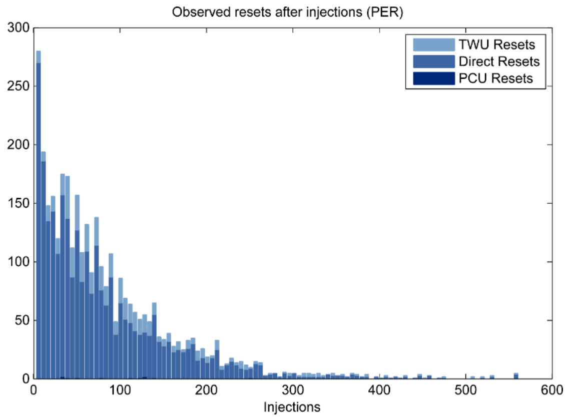


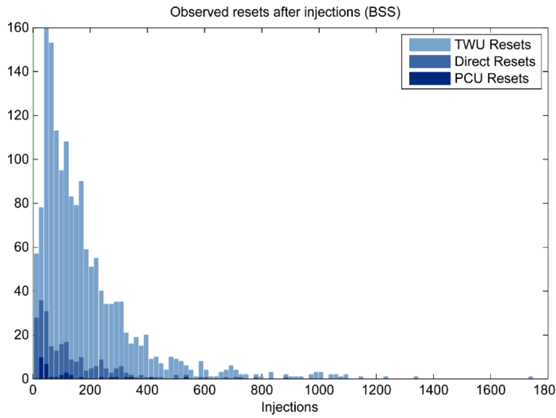
Software Implemented Fault Injection (SWIFI)

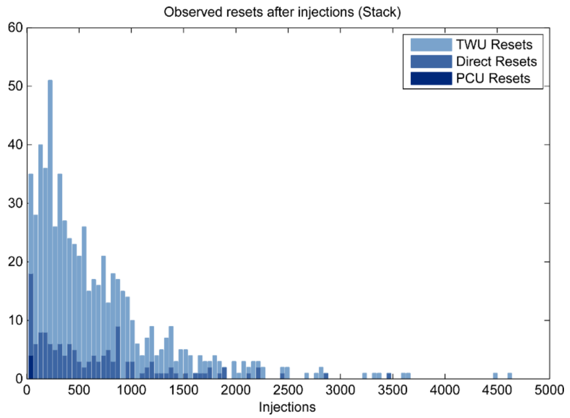
- ❑ runtime: 443 hours
- ❑ injections: 1.038.069
- ❑ recovered: 6490
- ❑ not-recovered: 5

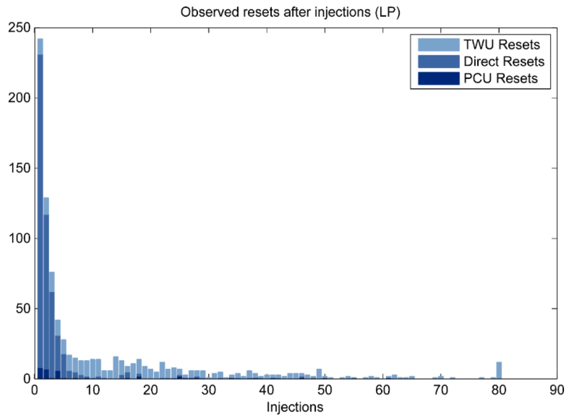


Target:	PER	BSS	STACK	LP
Size (bytes)	4096	4332	4096	131072
Runtime (hrs)	93	138	141	71
Injections	299741	290580	436947	10801
Unrecoverable	0	0	0	5
Reset Recoveries	3443	1583	650	859
PCU	11	34	4	39
TWU	576	1334	509	343
Direct	2856	215	137	477

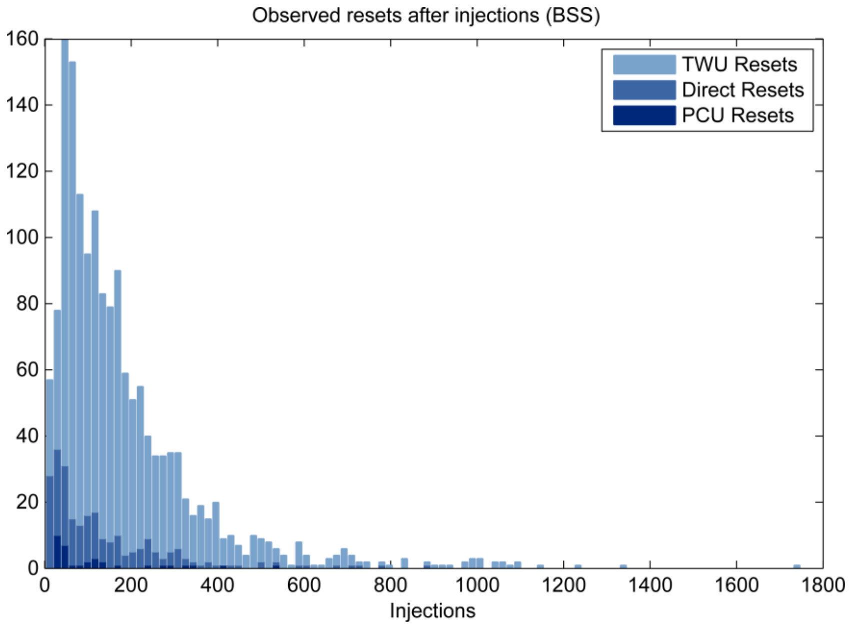


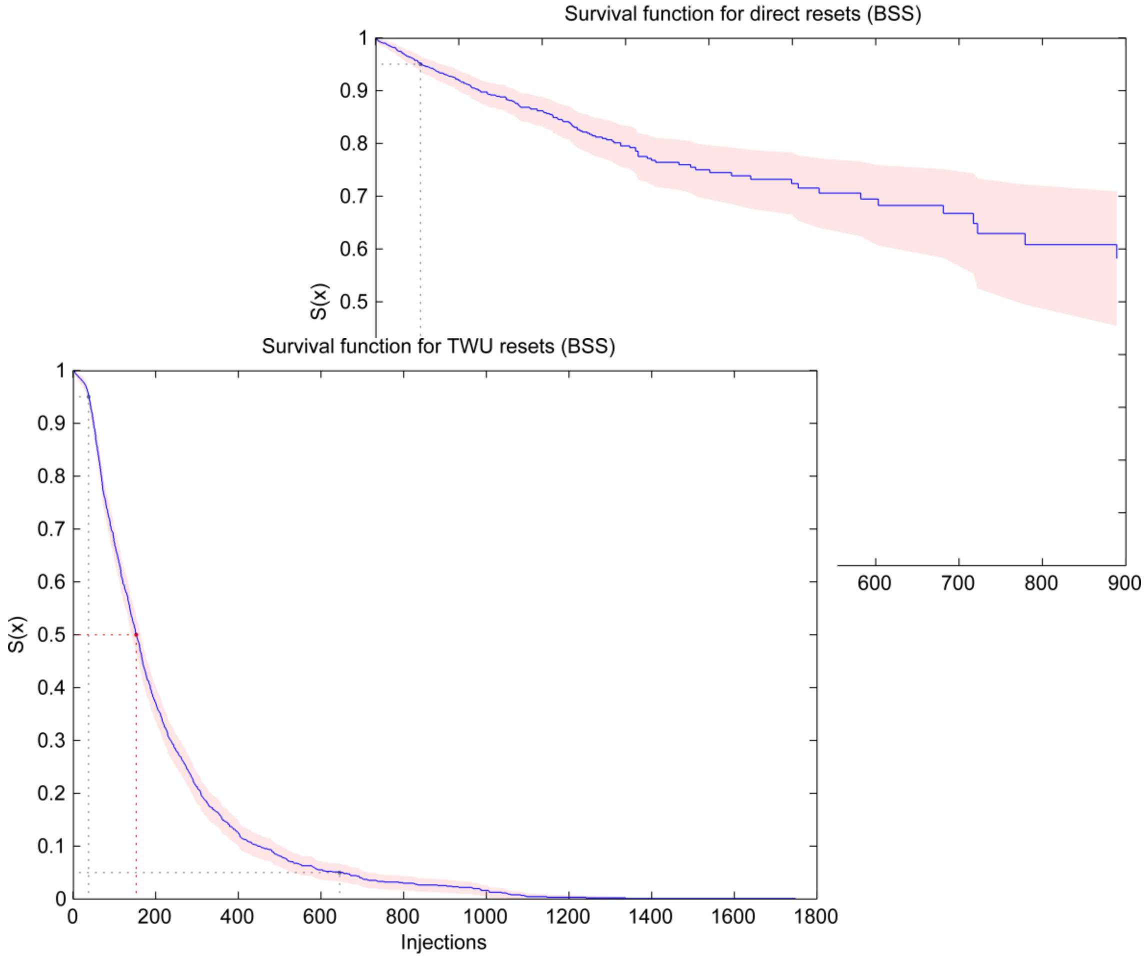






Survival Analysis (here BSS)



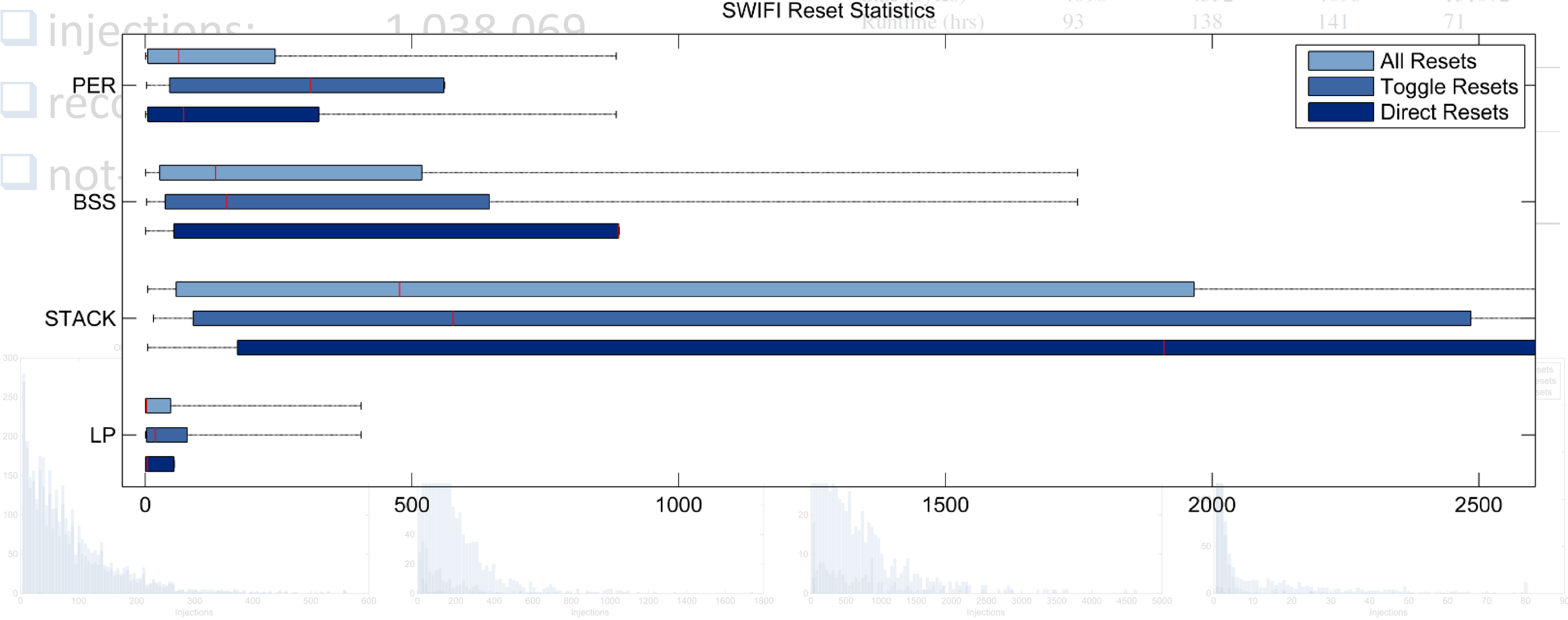


Survival Analysis

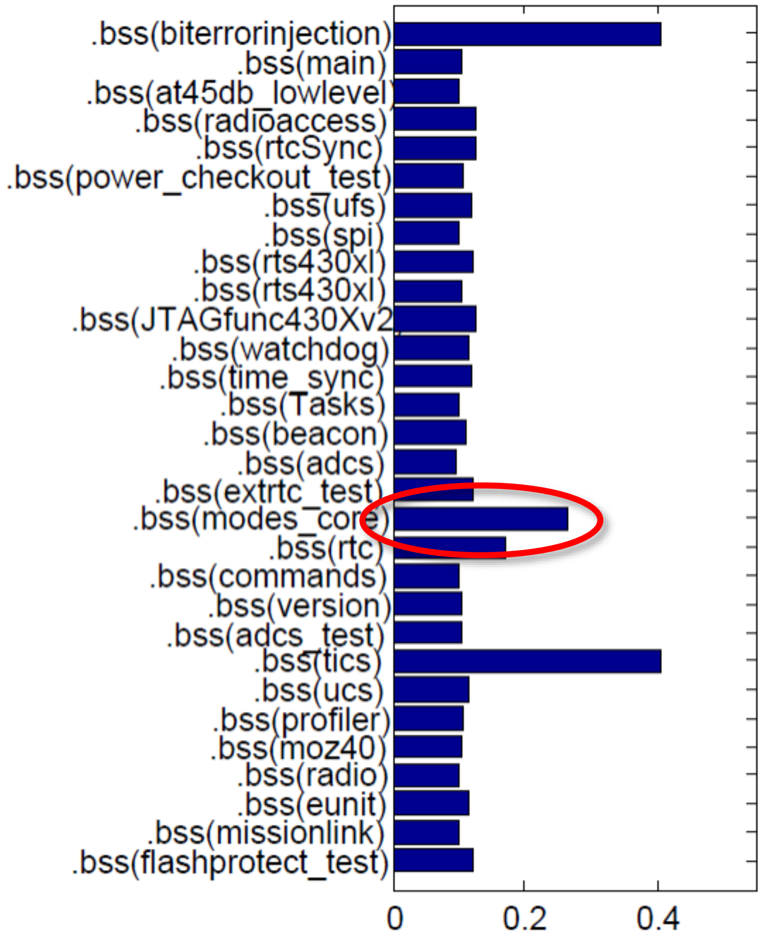
- ❑ runtime: 443 hours
- ❑ injections: 1,038,069
- ❑ reco
- ❑ not-

Target:	PER	BSS	STACK	LP
Size (bytes)	4096	4332	4096	131072
Runtime (hrs)	93	138	141	71

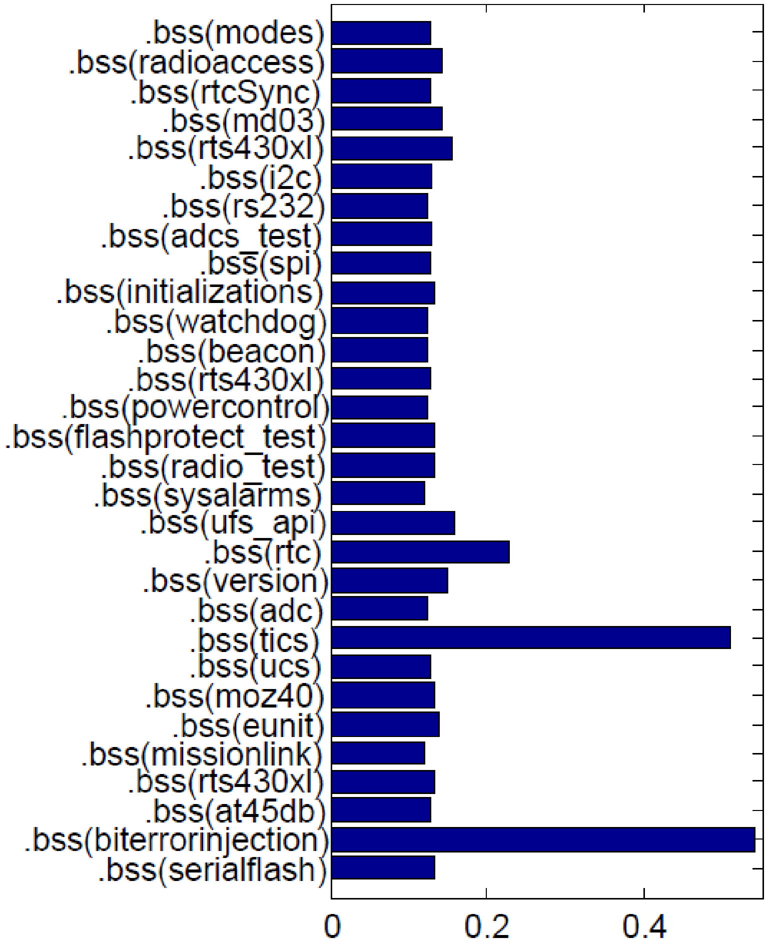
SWIFI Reset Statistics



Sensitivity Analysis



selective code hardening



In-Orbit Operation

Various SEEs in first months after launch

- 10^{-6} bit^{-1} day^{-1} SEU in RAM
- 1 latchup (+ 50mW on 20.04.2014)
- several TWU recoveries and direct resets

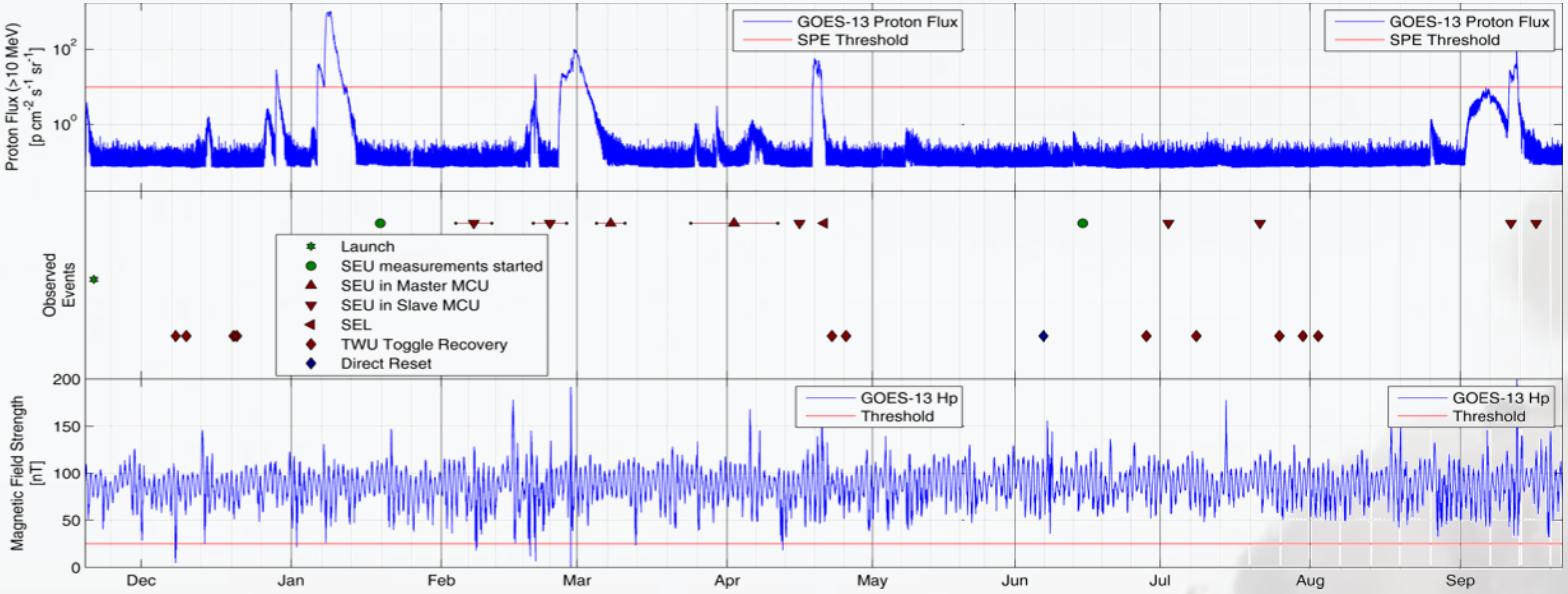


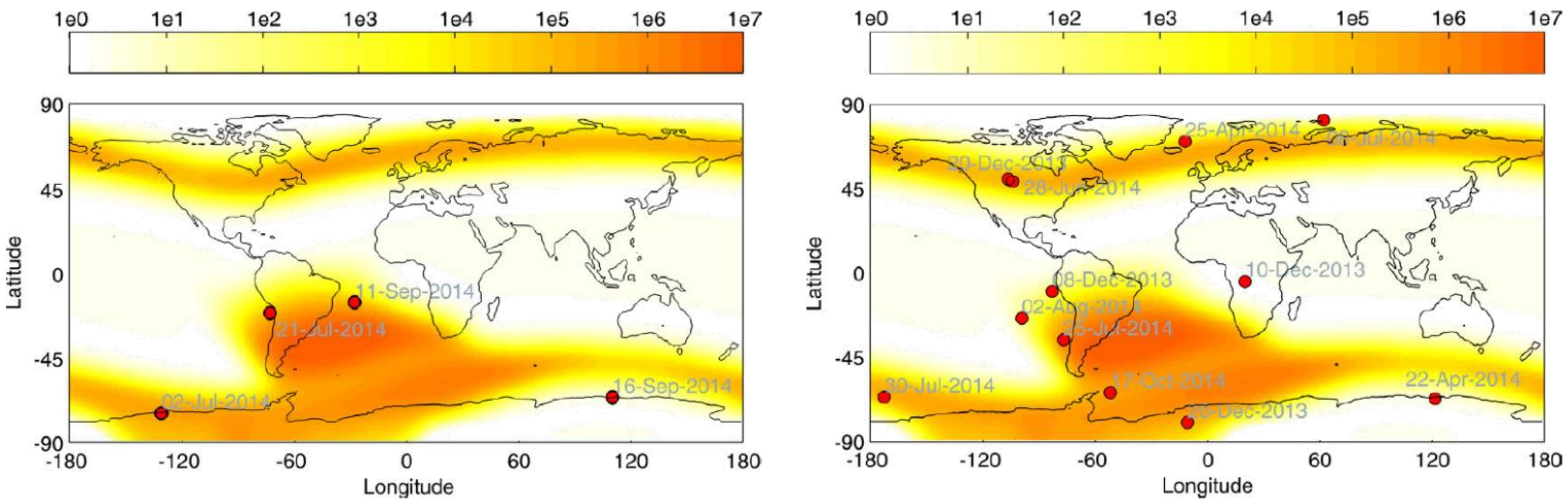
Image credits: Kosmotras

In-Orbit Operation

- ❑ Clear correlation of observed SEE with position in orbit

SEU in monitored section

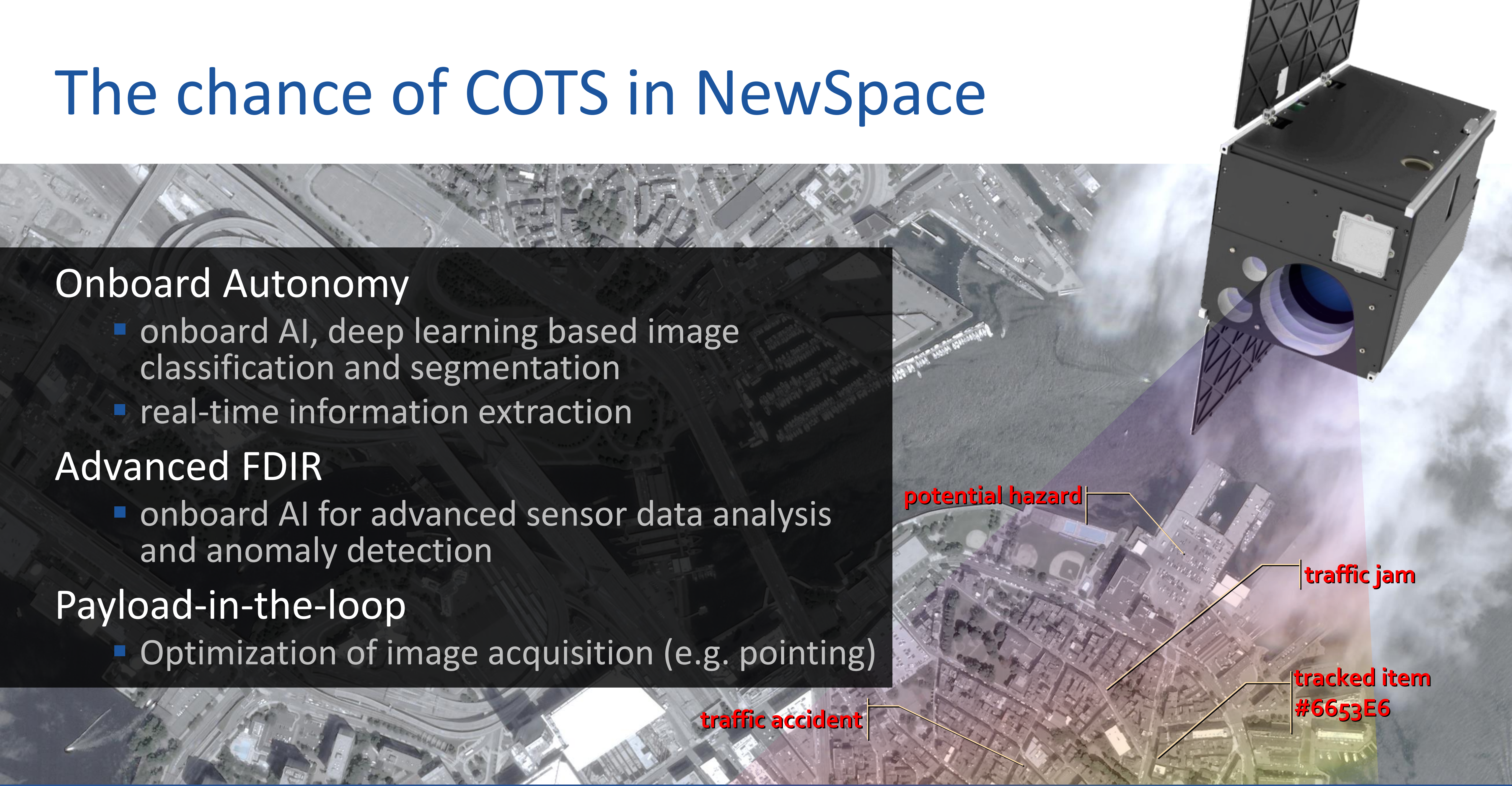
TWU recovery



SEE locations for SEU detection and TWU recoveries with two minute scan interval. Overlay on Electron (> 0.04MeV) and Proton (> 0.1MeV) MAX Integral Flux (cm−2s−1) according to AE-8/AP-8 models as simulated with SPENVIS for the UWE-3 orbit

On the Horizon

The chance of COTS in NewSpace



Onboard Autonomy

- onboard AI, deep learning based image classification and segmentation
- real-time information extraction

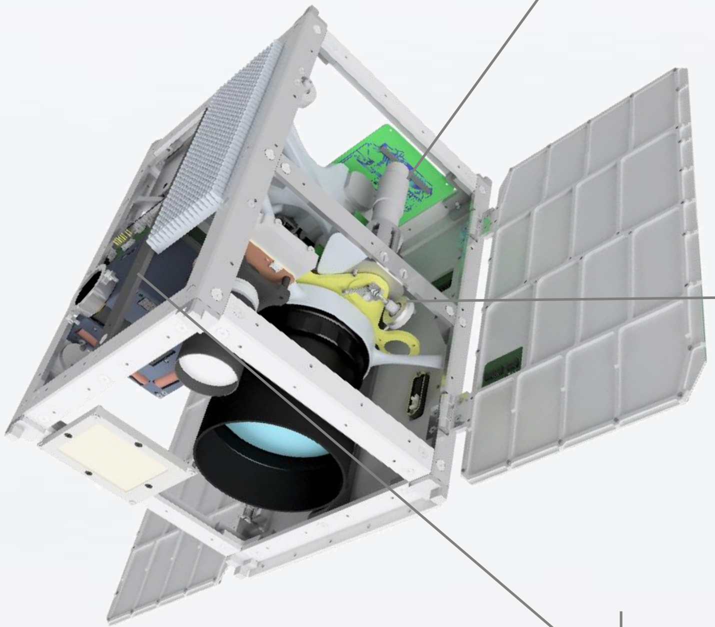
Advanced FDIR

- onboard AI for advanced sensor data analysis and anomaly detection

Payload-in-the-loop

- Optimization of image acquisition (e.g. pointing)

Fraunhofer Advanced Nanosatellite



High Performance Data Processing Unit

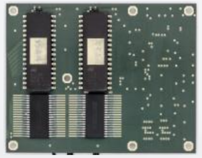
- COTS SoC ZynqMP Ultrascale+
- various camera interfaces
- image processing pipeline
- hardware AI accelerator
- mass storage

Cryo Cooled Detector

- 1280 × 1024px HgCdTe detector
- Cryogenic Stirling Cooler (95K)
- 8 channel filter wheel
- 2.5-5µm MWIR

Radiation Sensor (Fraunhofer INT)

- SEE (calibrated SRAM)
- TID (preconditioned EEPROM)



[Schimmerohn et. al., 2022]

References

References

[Busch, 2016] Busch, S. *Robust, Flexible and Efficient Design for Miniature Satellite Systems*. Würzburger Forschungsberichte in Robotik und Telematik, Band 11., Universität Würzburg, 2016, URN: urn:nbn:de:bvb:20-opus-136523

[Schimmerohn et. al., 2022] Schimmerohn, M., Horch, C., Busch, S., Ledford, N., Schäfer, K., Maue, T., Schäfer, F., Kappe, K., Weber, M., Schweitzer, C., Höffgen, S., Paape, A., *ERNST: Demonstrating advanced infrared detection from a 12U CubeSat*, 36th Small Satellite Conference, Logan UT, 6-11 August, 2022, SSC22-WKVIII-03

[Maurer et. al., 2008] Maurer, R. H., Fraeman, M. E., Martin, M. N., and Roth, D. R. (2008).; *Harsh Environments: Space Radiation Environment*, Effects, and Mitigation. John Hopkins APL Technical Digest, 28(1):17–29.

[Höffgen, 2021] Stefan K. Höffgen; *Radiation environment and Effects*; Fraunhofer INT, Spacecraft System Analysis Lecture for Satellite Technology Program, Würzburg, 2021

[Kuvaiskii et. al., 2016] Kuvaiskii, Dmitrii; Oleksenko, Oleksii; Bhatotia, Pramod; Felber, Pascal; Fetzer, Christof; *Triple Modular Redundancy usingIntel Advanced Vector Extensions*, 2016/04/02

[Abaffy et.al., 2010] Abaffy, J. and Tibor Krajcovic.; *Software support for multiple hardware watchdog timers in the Linux OS.;* 2010 International Conference on Applied Electronics (2010): 1-3.