UNIVERSITY OF LEICESTER

# Fault Detection, Isolation and Recovery Schemes for Spaceborne Reconfigurable FPGA-Based Systems


Felix Siegle, PhD

Supervisor:

Prof Tanya Vladimirova

Department of Engineering, University of Leicester, UK

ESA Support:

J. Ilstad, M. Suess, C. Poivey

Airbus Support:

O. Emam


AIRBUS DEFENCE & SPACE

esa

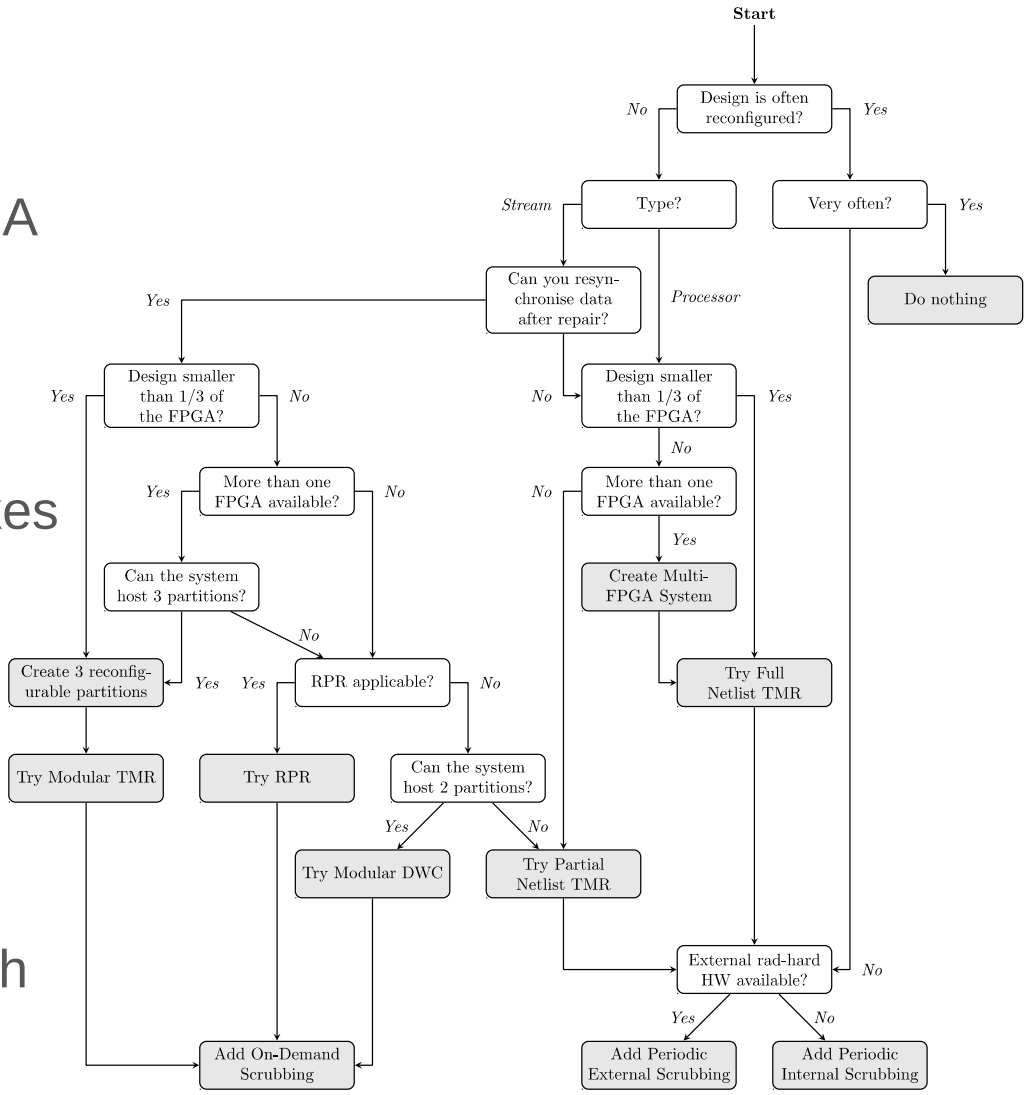

*Sponsorship from ESA under the NPI Programme, Airbus Defence and Space, UK and the University of Leicester.*

# Outline

- Literature Survey
- FDIR Hardware Framework: *Distributed Failure Detection*
- Availability Analysis Method
- Proton Irradiation Test Campaign
- Publications

# Literature Survey

- No FDIR scheme exists that specifically targets multi-FPGA systems.
- No availability analysis method exists for such an FDIR scheme, which also takes Block RAMs into account.
- Is on its own a novel contribution to knowledge.
- Together with the included design recommendations, it can serve as a tutorial for both scientists and engineers who are novices in this field.

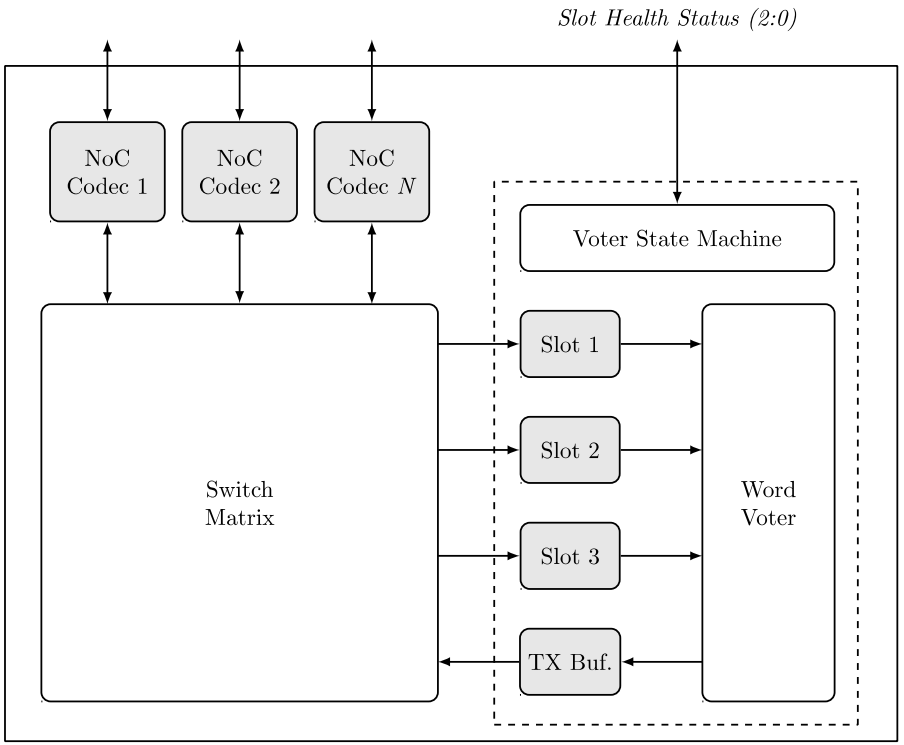


# Distributed Failure Detection

- Data is independently processed by “stream processors”.
- Data is provided via a Network-on-Chip (NoC)
- Based on modular redundancy + voting/comparison:
- Allows a real FDIR approach.
- Allows the distribution of redundant stream processors over several FPGAs.
- Redundant processors can be added / removed during operation, depending on the criticality of the current mission phase.

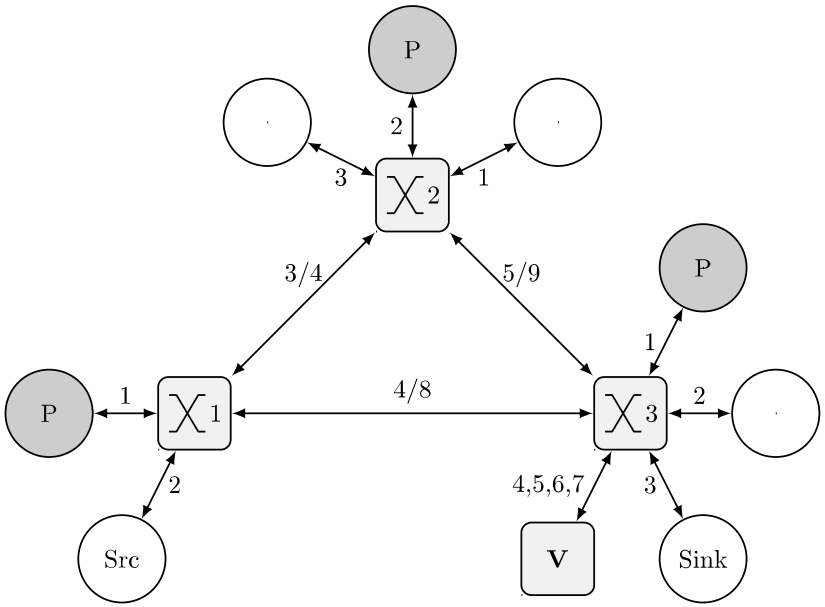
# Distributed Failure Detection

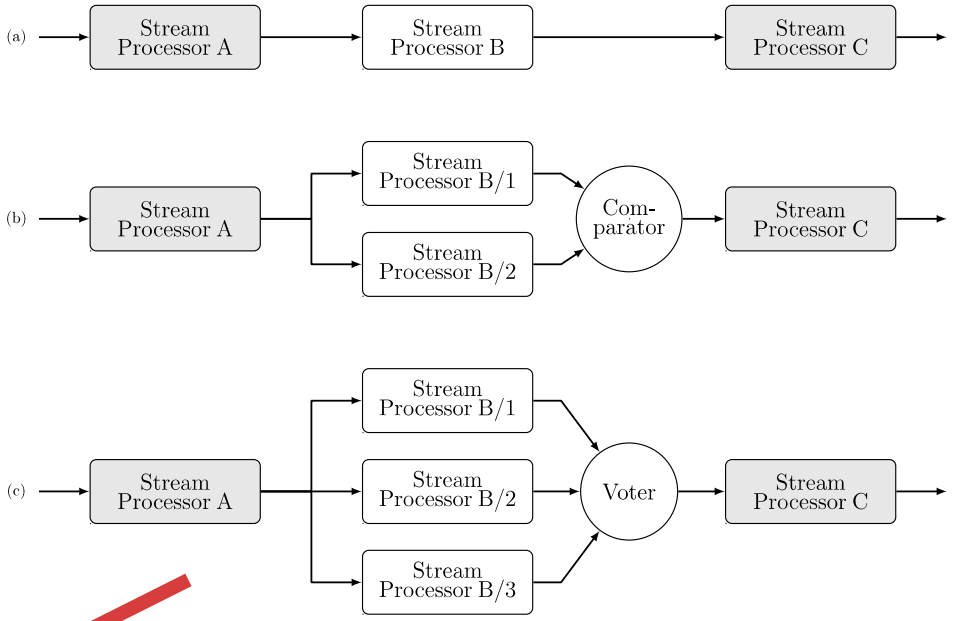
- Intercommunication is done via a switched fabric NoC architecture.
- Failure detection and isolation mechanisms are embedded into NoC switches.
- Compared to the state of the art, this approach scales much better with the size of the application.
- Can easily be applied to multi-FPGA systems.
- Is well suited for high-performance payload data processing.



# Distributed Failure Detection

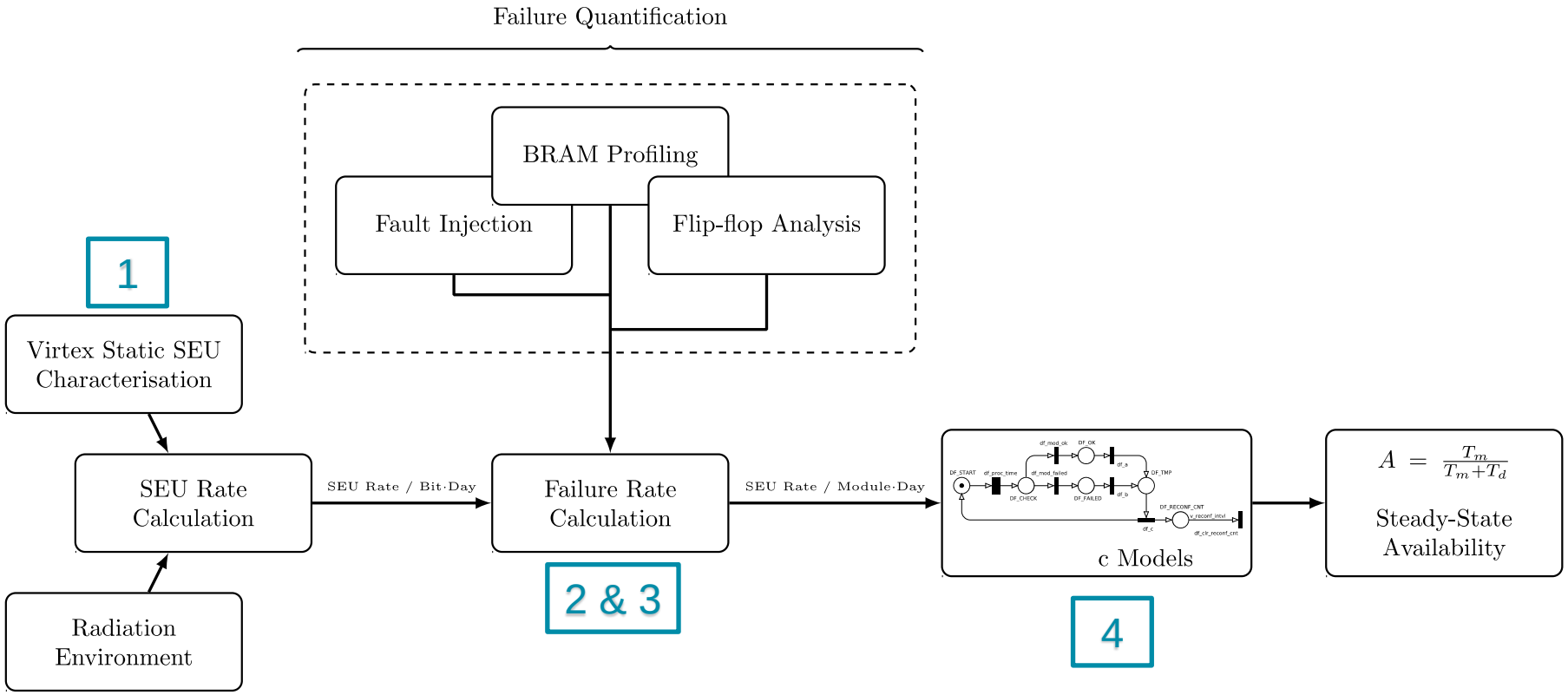
Example application and network topology:



# Availability Analysis Method

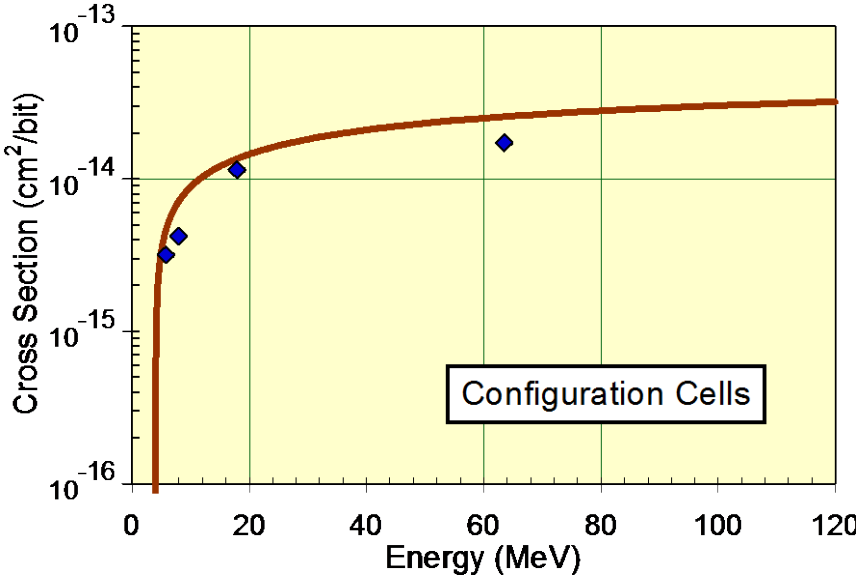
**Question: Which failure rates do we have to expect for a stream processor in a specific FDIR configuration in a specific radiation environment?**



# Availability Analysis Method

**Step 1: SEU Rate Calculation / Determination of MTBF**

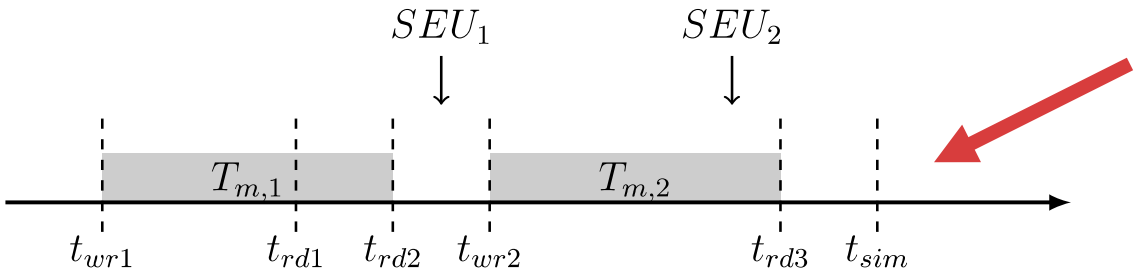
- Cross-sections (as provided e.g. from Xilinx/NASA) can be used to calculate the failure rates for a particular stream processor design in a particular orbit / radiation environment.
- Tools like OMERE simplify the computation according to ECSS standards.



# Availability Analysis Method

**Step 2: Block RAM Profiling**

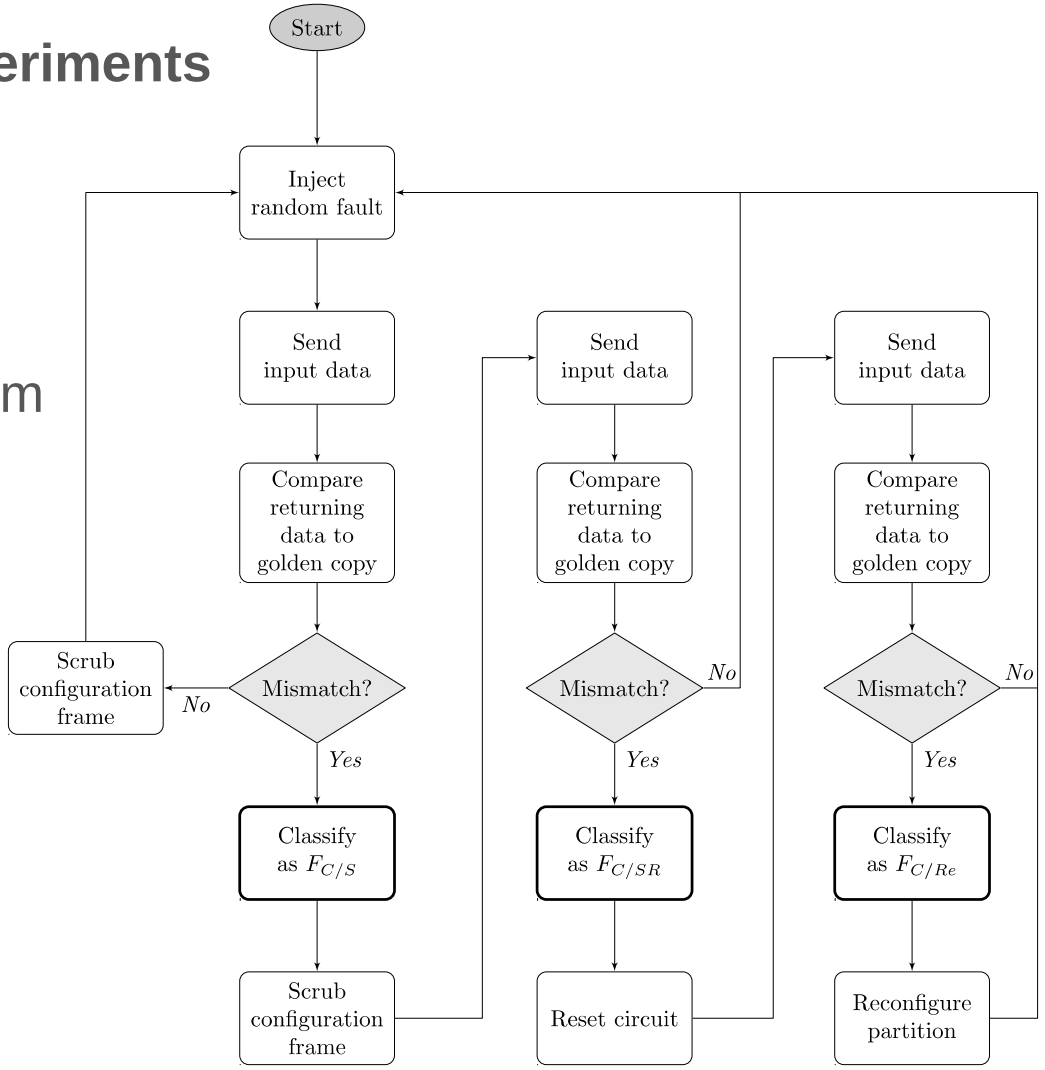
- Main novelty: Block RAM profiling tool.
- Allows a much better estimate of the number of susceptible Block RAM bits.
- It therefore increases the overall prediction precision of MTBF and availability figures.



# Availability Analysis Method

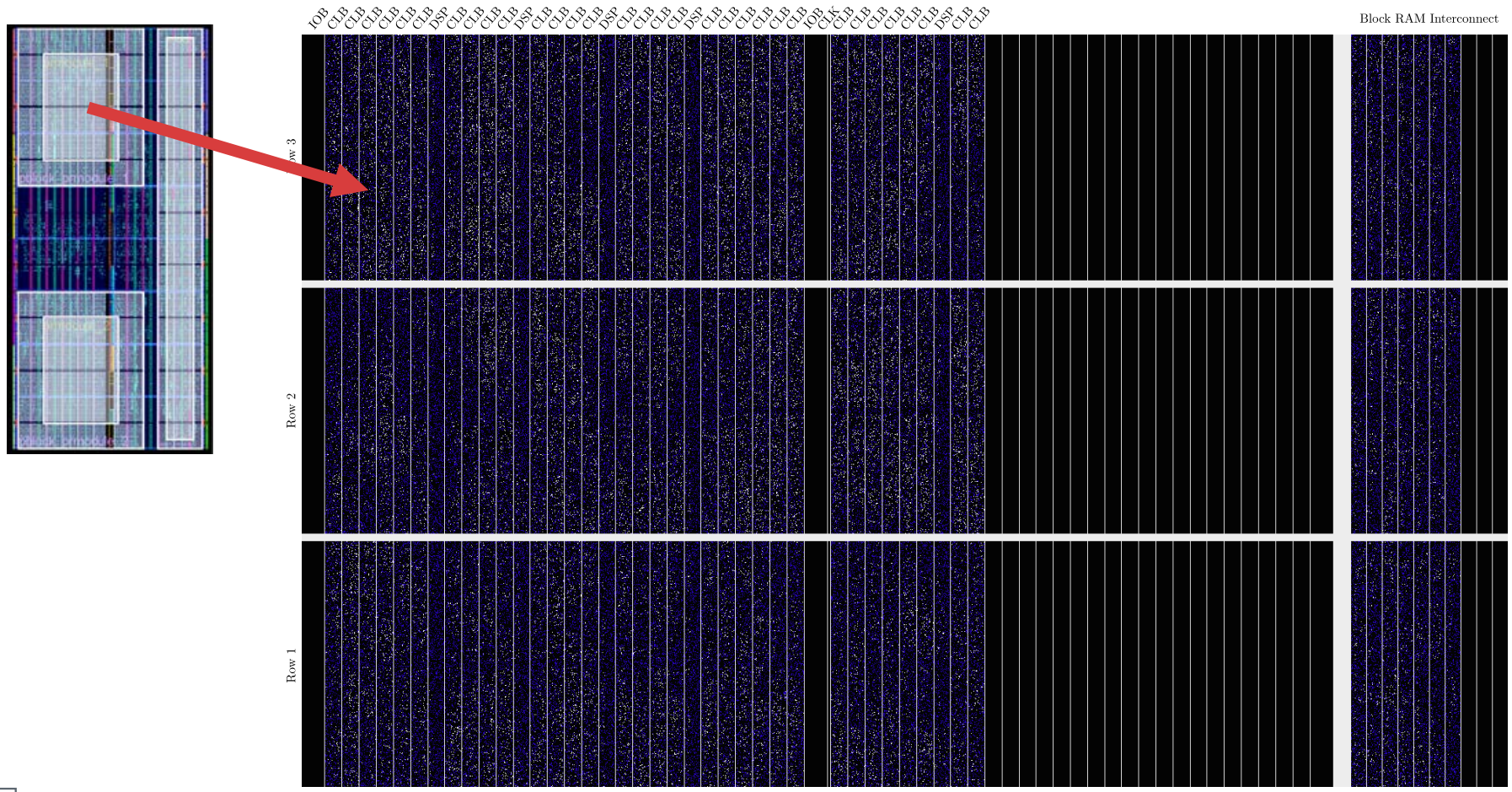
## Step 3: Fault Injection Experiments

- Second novelty:
  Fault injection algorithm.
- Can classify sensitive bits depending on how a system can recover from failures triggered by upsets in these bits.
- Allows more advanced availability models.



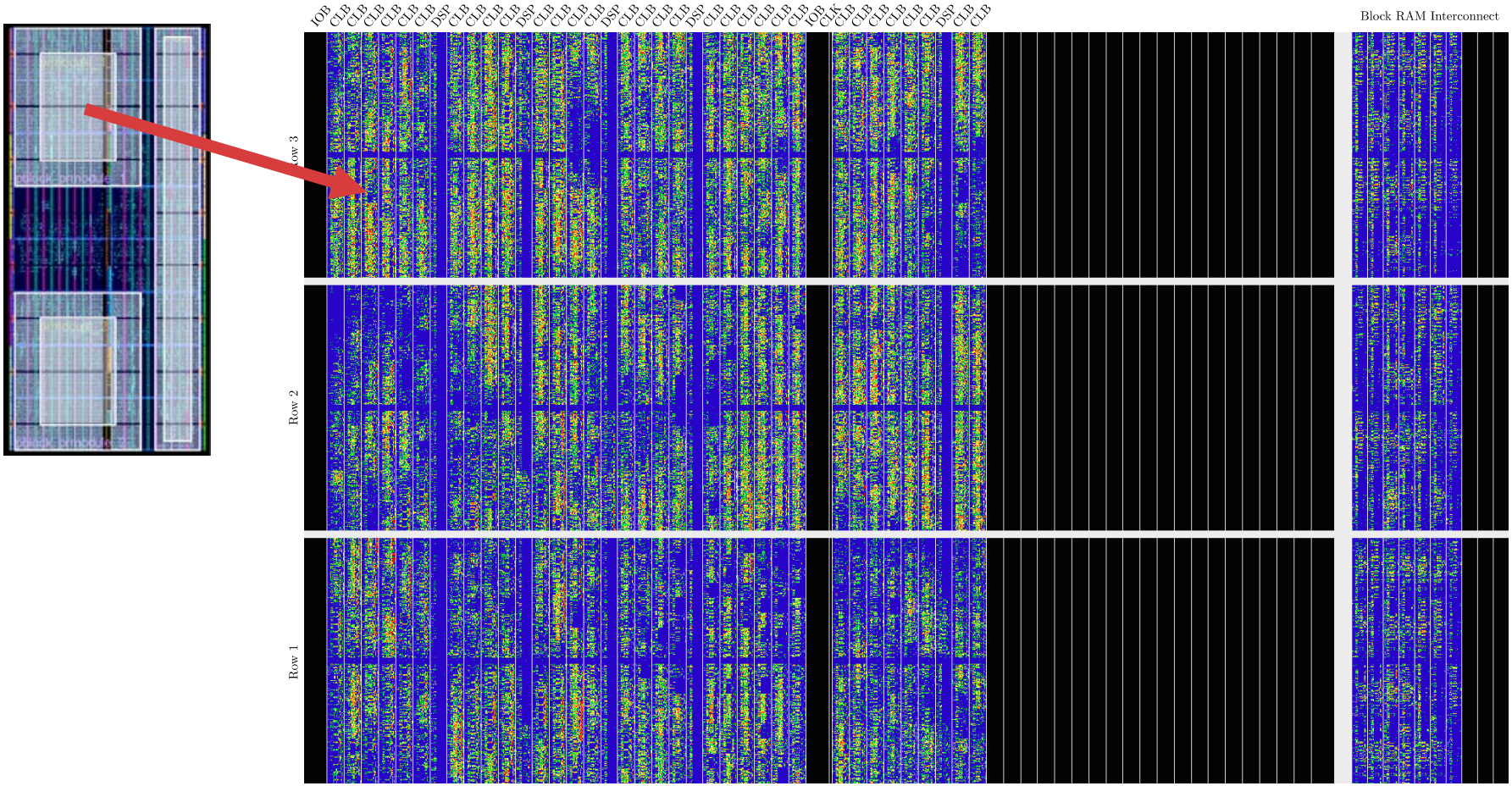
# Availability Analysis Method

Random fault injection can provide accurate results



# Availability Analysis Method

Random fault injection can provide accurate results



# Availability Analysis Method

Random fault injection can provide accurate results

- SEU rate per bit-day is known. Thus, we need to determine the number of sensitive configuration memory elements.
- Random fault injection preferred, full campaign would take too much time.

| # Tested | # Sensitive | 95% confidence interval | |
|---|---|---|---|
| 1,000 | 134 | 11.35% | 15.67% |
| 10,000 | 1,382 | 13.15% | 14.51% |
| 100,000 | 13,899 | 13.69% | 14.11% |
| **150,000** | **20,870** | **13.74%** | **14.09%** |
| 3,735,264 | 523,543 | 14.02% | |

**Random fault injection can provide accurate estimates!**



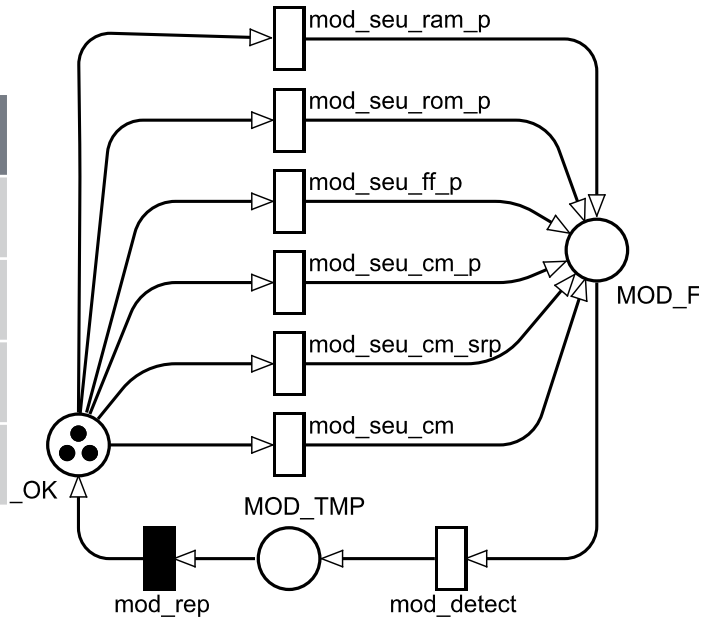
$$F_C = 0.1409 \cdot 3735264\text{bits} = 526299\text{bits} \approx 526300\text{bits}$$

# Availability Analysis Method

**Step 4: Stochastic modelling to determine availability for different redundancy configurations (Duplication with comparison, TMR)**

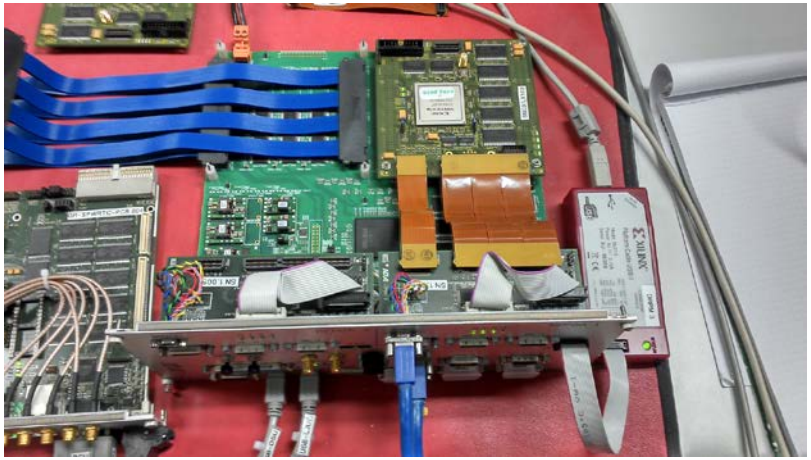
- The steady-state availability gives an indication of how much downtime must be expected.
- It is also a good figure to compare different FDIR approaches.
- Stochastic Petri nets are used for modelling, which can analytically be solved by the TimeNET tool.

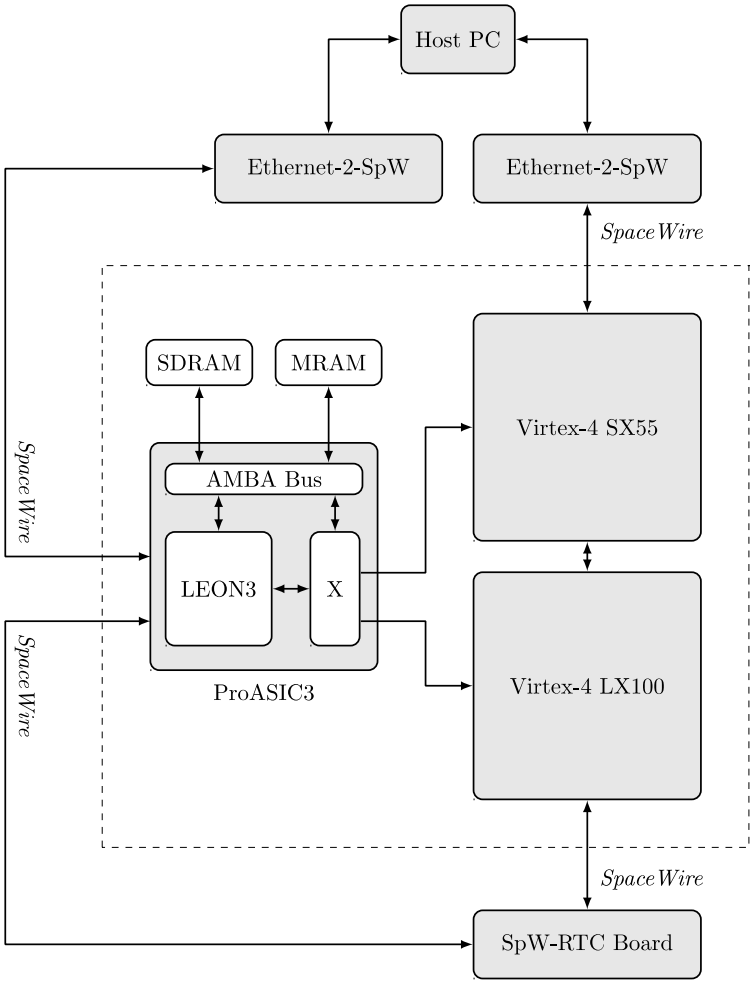
| Mission | DWC | TMR |
|---|---|---|
| Sentinel-3 | 0.999996 | 0.999999999... |
| Sentinel-3 (SPE) | 0.998 | 0.9999998 |
| Galileo | 0.999998 | 0.999999999... |
| Galileo (SPE) | 0.995 | 0.999998 |



# Demonstration System

- Complex demonstration system comprising hardware, embedded software and workstation software components.
- Very similar to flight systems since most components are available as space-qualified versions.

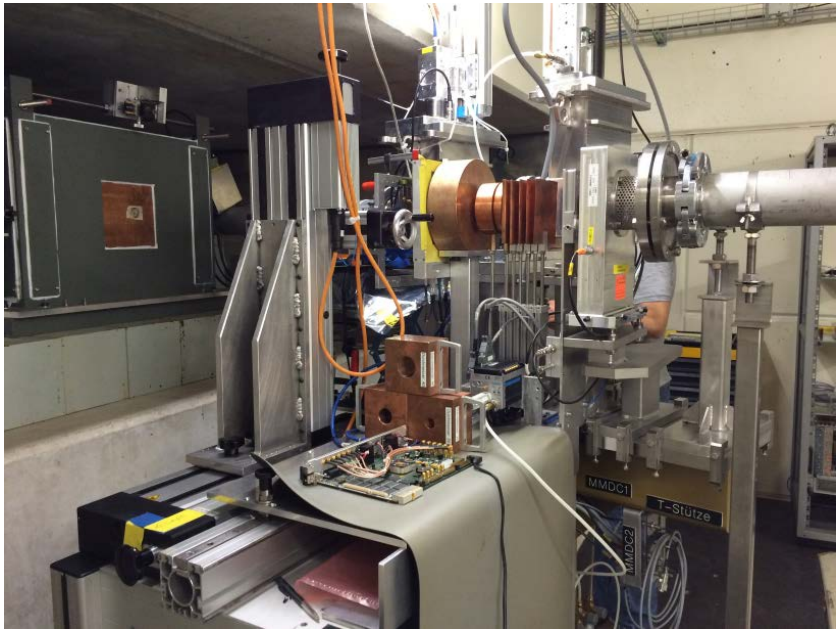




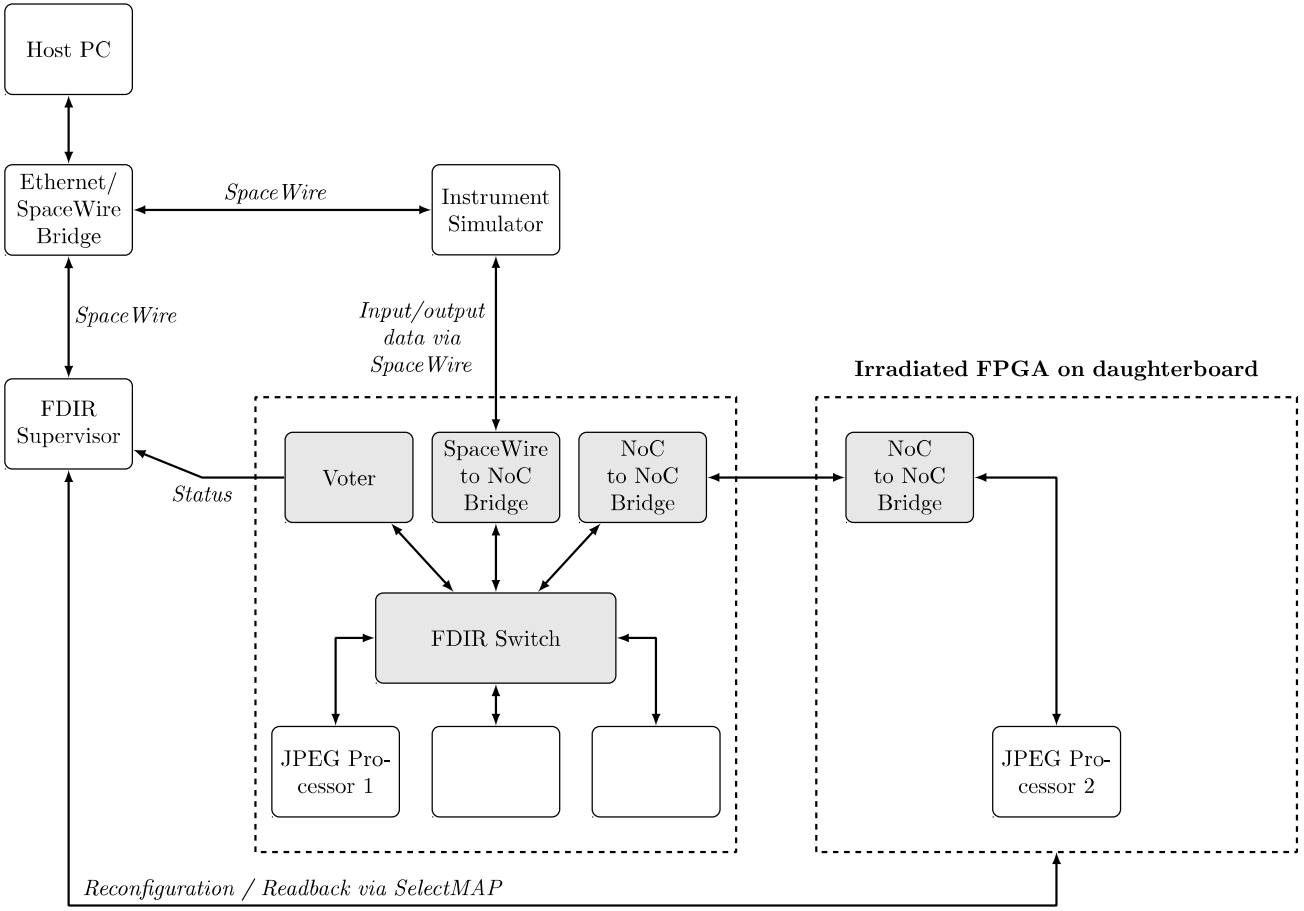
# Proton Irradiation Test Campaign

**Validation of both FDIR Hardware Framework and Availability Analysis method.**

- Test campaign was conducted at PSI.
- Three experiments:
  - 4.2E+06 p/cm$^2$-s @ 200 MeV
  - 8.3E+06 p/cm$^2$-s @ 200 MeV
  - 8.5E+06 p/cm$^2$-s @ 100 MeV
- DUT: Virtex-4 SX55.



# Proton Irradiation Test Campaign



# Proton Irradiation Test Campaign

**First interesting outcome: Static cross-sections also gained during dynamic testing by reading back the bitstream after each failure detection.**

| Experiment | Fluence[1] | Runtime | SEUs | X-Section / bit[2] |
|---|---|---|---|---|
| 200 MeV /A | 3.82E+10 | 9,176 s | 10,728 | **1.83E-14** |
| 200 MeV /B | 2.67E+10 | 3,207 s | 7,472 | **1.83E-14** |
| 100 MeV | 3.42E+10 | 4,028 s | 8,052 | **1.54E-14** |

Cross-sections: Configuration memory

| Experiment | Fluence[1] | Runtime | SEUs | X-Section / bit[2] |
|---|---|---|---|---|
| 200 MeV /A | 3.82E+10 | 9,176 s | 6,225 | **3.69E-14** |
| 200 MeV /B | 2.67E+10 | 3,207 s | 4,290 | **3.64E-14** |
| 100 MeV | 3.42E+10 | 4,028 s | 4,808 | **3.19E-14** |

Cross-sections: Block RAMs



1 [p/cm2]
2 [cm2/bit]

# Proton Irradiation Test Campaign

**Dynamic Test Results #1 (@ 200 MeV)**

- **Measured during beam test:**
  - Failures detected and recovered: 439
  - Average proton flux: 4.16E+06 p/cm$^2$-s
  - Average Mean Time Between Failures (MTBF): 20.23 sec
- **Estimation:**

$$3.69 \cdot 10^{-14}\ \mathrm{cm^2/bit} \cdot (67858 + 27351)\ \mathrm{bits})]^{-1} = 18.275\ \mathrm{s/p}$$

$$300\ \mathrm{bits} +$$

- **Error:** 9.7%

# Proton Irradiation Test Campaign

**Dynamic Test Results #2 (@ 200 MeV)**

- **Measured during beam test:**
  - Failures detected and recovered: 343
  - Average proton flux: 8.31E+06 p/cm$^2$-s
  - Average Mean Time Between Failures (MTBF): 9.147 sec
- **Estimation:**

$$\mathrm{MTBF} = [8.31 \cdot 10^{6}\,\mathrm{p/cm^2 \cdot s} \cdot (1.83 \cdot 10^{-14}\,\mathrm{cm^2/bit} \cdot 526300\,\mathrm{bits} + 3.64 \cdot 10^{-14}\,\mathrm{cm^2/bit} \cdot (67858 + 27351)\,\mathrm{bits})]^{-1} = 9.185\,\mathrm{s/p}$$

- **Error:** 0.4%

# Proton Irradiation Test Campaign

**Dynamic Test Results #3 (@ 100 MeV)**

- **Measured during beam test:**
  - Failures detected and recovered: 309
  - Average proton flux: 8.48E+06 p/cm$^2$-s
  - Average Mean Time Between Failures (MTBF): 12.518 sec
- **Estimation:**

$$\mathrm{MTBF} = [8.48 \cdot 10^{6}\,\mathrm{p/cm^2 \cdot s} \cdot (1.54 \cdot 10^{-14}\,\mathrm{cm^2/bit} \cdot 526300\,\mathrm{bits} + 3.19 \cdot 10^{-14}\,\mathrm{cm^2/bit} \cdot (67858 + 27351)\,\mathrm{bits})]^{-1} = 10.586\,\mathrm{s/p}$$

- **Error:** 15.4%

# Proton Irradiation Test Campaign

## Availability Prediction (based on stochastic Petri nets)

| Experiment | TX Img | RX Img | Availability |
|---|---|---|---|
| 200 MeV /A | 80,724 | 77,621 | 0.9616 |
| 200 MeV /B | 28,586 | 26,266 | 0.9188 |
| 100 MeV | 35,845 | 33,741 | 0.9413 |

Measured availability during beam test

| Experiment | Availability (Error) *using measured MTBF* | Availability (Error) *using predicted MTBF* |
|---|---|---|
| 200 MeV /A | 0.9639 (0.2%) | **0.9602 (0.1%)** |
| 200 MeV /B | 0.9235 (0.5%) | **0.9238 (0.5%)** |
| 100 MeV | 0.9429 (0.2%) | **0.9332 (0.9%)** |

Predicted steady-state availability using Petri nets

# Proton Irradiation Test Campaign

**Summary:**

- It was demonstrated that the proposed FDIR framework withstands a real radiation environment.
- It was shown that the availability analysis method could predict the measured MTBF value with a maximum error of 15.4% and the availability figure with a maximum error of only 0.9%.
- Static cross-sections at 200 MeV were measured for the Virtex-4 SX55 device (NASA/Xilinx documents only provide data up to 60 MeV).

# Publications


- F. Siegle, T. Vladimirova, O. Emam, and J. Ilstad, “Adaptive FDIR strategy for FPGAs hosting partial reconfigurable modules,” in Workshop on Reconfigurable Computing (WRC), HiPEAC Conference, Jan. 2013
- “Adaptive FDIR framework for payload data processing systems using reconfigurable FPGAs,” in Proc. of 8th NASA/ESA Conference on Adaptive Hardware and Systems, June 2013
- “New voter design enabling hot redundancy for asynchronous network nodes,” in Proc. of 9th NASA/ESA Conference on Adaptive Hardware and Systems, July 2014
- “Fault detection, isolation and recovery techniques for SRAM-based multi-FPGA systems,” in Proc. of the Military and Aerospace Programmable Logic Devices (MAPLD) Workshop, May 2014
- “FDIR techniques for payload streaming applications using SpaceWire-based networks,” in Proc. of the International SpaceWire Conference, 2014
- *“*Mitigation of radiation effects in SRAM-based FPGAs for space applications,” *in ACM Computing Surveys, 2014*
- *“*Availability analysis for satellite data processing systems based on SRAM FPGAs*,” in IEEE Transactions on Aerospace and Electronic Systems, 2016*
- F. Siegle, T. Vladimirova, C. Poivey, and O. Emam, “Validation of FDIR strategy for spaceborne SRAM-based FPGAs using proton radiation testing,” in Proc. of the Conference on Radiation Effects on Components and Systems (RADECS 2015), 2015

- Thank you -