1st SYMPOSIUM
SPACE EDUCATIONAL ACTIVITIES
PADOVA - 9/12 December 2015

# On Design for Reliability of Electronics in Nanosatellite

Olga Mamoutova (presenter)
Andrey Antonov

*Peter the Great St. Petersburg State Polytechnic University, Russia*
*Dpt. of Computer Systems & Software Engineering*
*Scientific-educational center “Embedded Microelectronic Systems”*

**1st Symposium on Space Educational Activities**

**Session 7: B – Nanosat Technologies** (Thursday, 11 December 2015, 11:30 – 13:00)

# Poly-sputnik & Polytechnic-Space 101

## Background

- Electronic and Computer Engineering
- VLSI Design Practices and Methodologies

## Objectives

- Methodology and Platform for Highly-Reliable Small Satellite Designs
- Hands-on Educational Course on Reliability

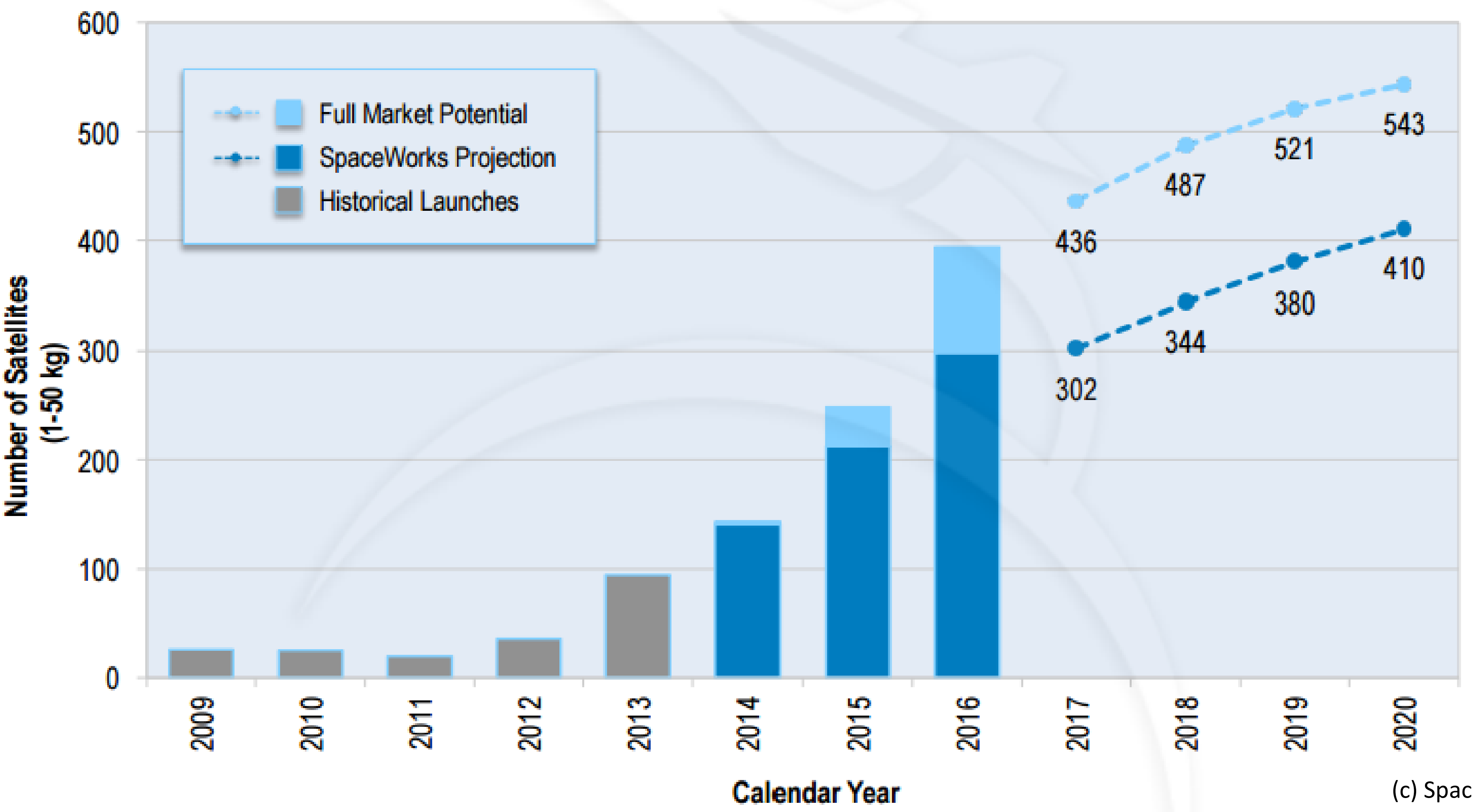
## Current Status

- Preliminary design phase

# Why Consider Dependability of a Nanosat?

## Nanosat technologies approach their maturity:

move from **dependability intentions** to **dependability plan**



(c) SpaceWorks

# Risk Analysis. Dependability & Security Specs

**Data-critical application**: Loss of valuable data = Failure

**Goal**: fail-controlled system with graceful degradation of functionality

| Fault | Factors/Reasons | Required Expertise |
|---|---|---|
| Mistakes | They are inevitable | Quality design |
| | Poor design practices | |
| | No standards for testing | |
| Bad design decisions | Strict budgets | |
| | Qualities of team | |
| Production defects<br>Physical deterioration<br>Environmental faults | Non-space qualified components | Dependability design |
| | Low-cost missions | |
| | Mission lifetime | |
| Reconfiguration faults | Erroneous control | Security design |
| Malicious intrusions | Protocol flaws | |

# Current Reliability Trends for Nanosats

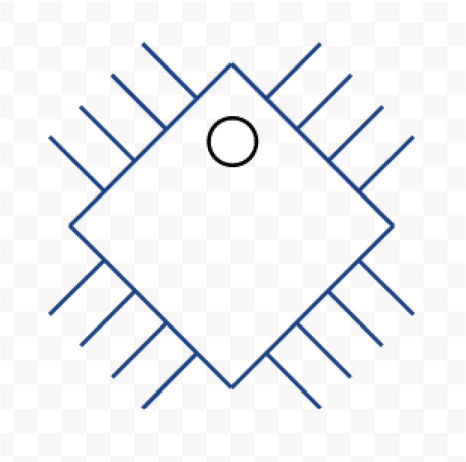
| Technology | Hardware & Software | | Design flow |
|---|---|---|---|
| Commercial-grade components | No single string designs | Distributed computing | Design methodologies |
| Industrial-grade components | Traditional fault tolerance techniq. | Simple SW | Testing strategies |
| Flight heritage | Reconfigurability | Modular SW | Open technical standards |
| Nanosatellite-class components | Generic multi-functional units | Security services | |
| | Reliable power | Mission redundancy | |

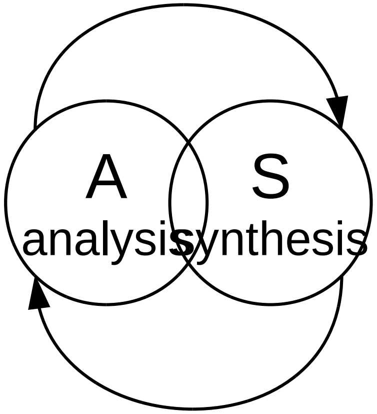
# Poly-sputnik. Focus Points of the Research

| Technology | Hardware & Software | | Design flow |
|---|---|---|---|
| Commercial-grade components | No single string designs | Distributed computing | **Design methodologies** |
| Industrial-grade components | Traditional fault tolerance techniq. | Simple SW | **Testing strategies** |
| Flight heritage | **Reconfigurability** | Modular SW | Open technical standards |
| Nanosatellite-class components | **Generic multi-functional units** | Security services | |
| | Reliable power | **Mission redundancy** | |

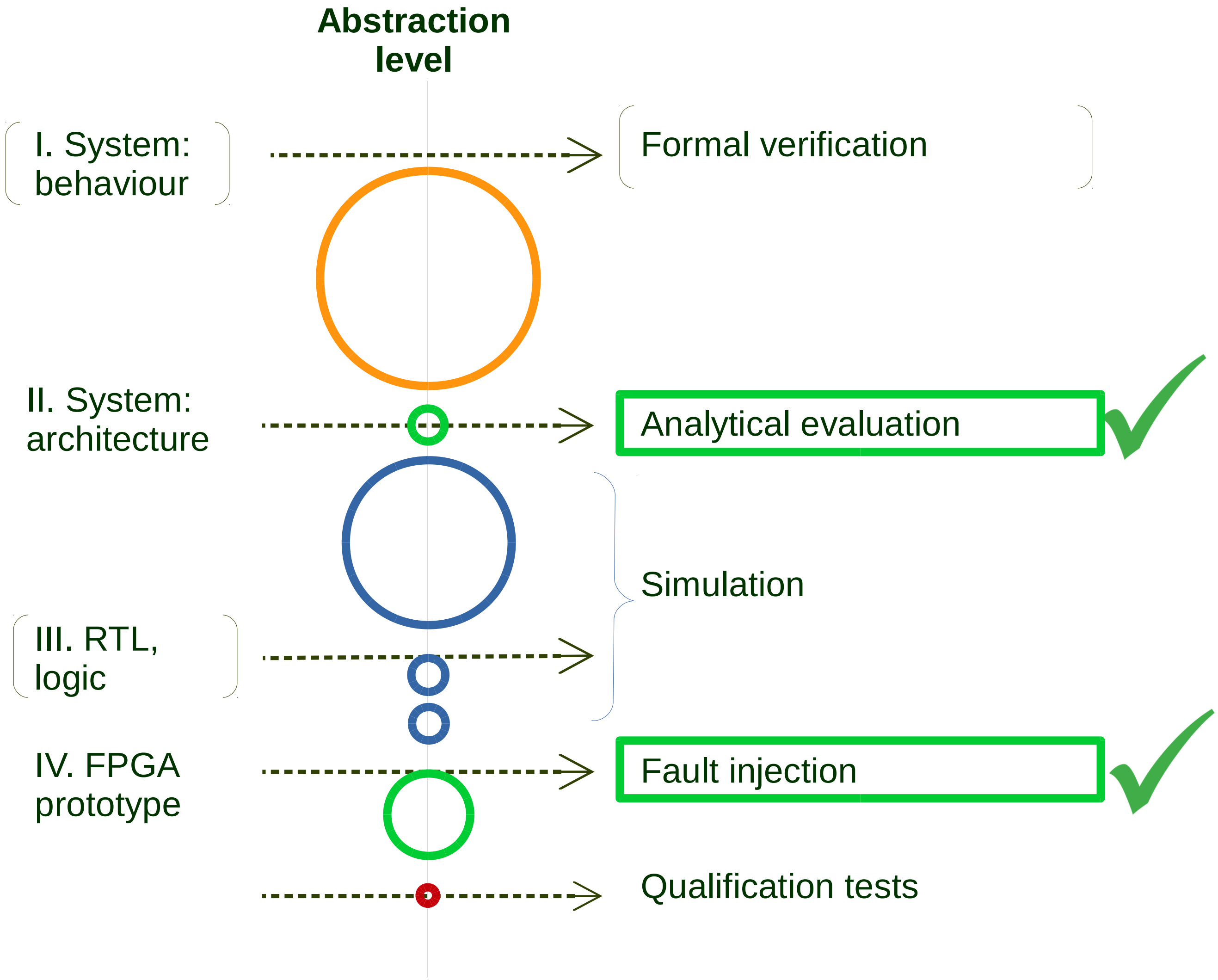
# Focus of the Research – Design Methodology

System-on-chip design



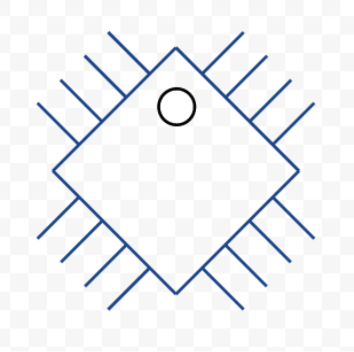


Gradual refinement of dependability specs:

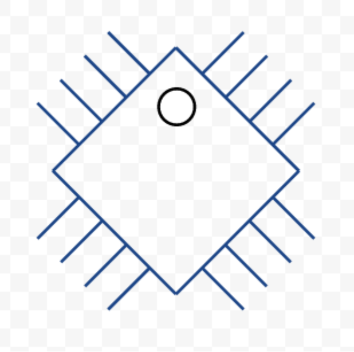


# Focus of the Research.
# Single Event Effects Experiment

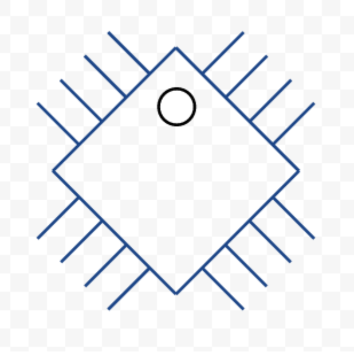
- Dependability life data collection
- Evaluate abilities of nanosat as a testbed for SEE analysis
- Compare SEE-sensitivity for several technologies:



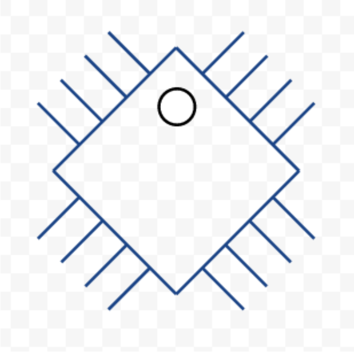
SRAM-based FPGA



Flash-based FPGA

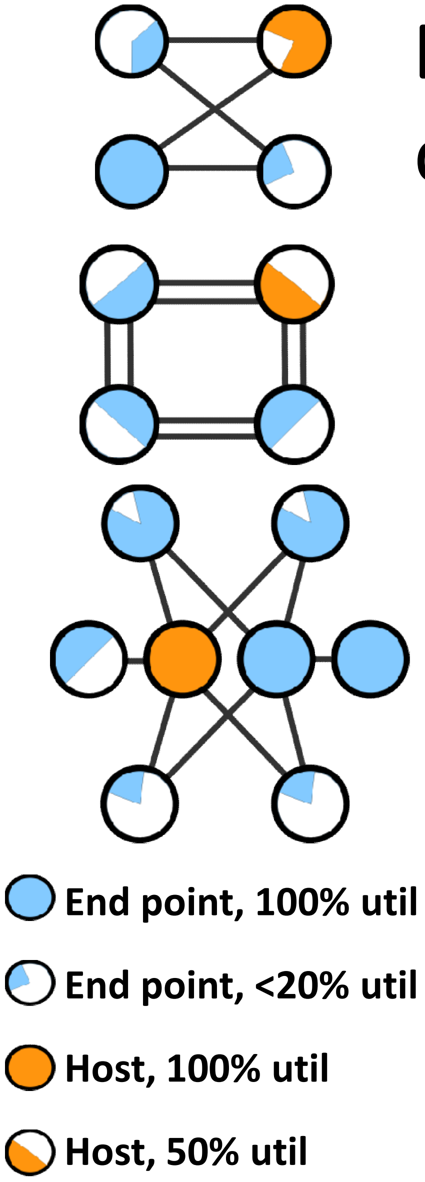


ASIC



ASSP

# Implementation. C&DH platform prototype



🔵 End point, 100% util

◔ End point, <20% util

🟠 Host, 100% util

◑ Host, 50% util

**Design task** – adapt plug-n-play platform concept of SpaceWire-based small satellites.

- **Ability** – provides resources for information processing
- **Flexibility** – those resources distinct in computing power
- **Customizability** – the module utilization can be tuned for particular task
- **Programmability** – the module can easily change its functionality
- **Networkability** – support of arbitrary network topologies and protocols

# Summary and Conclusions. Action List

1. **Dependability is an integral quality.**

   **todo:** practise strong team cooperation

2. **Design quality is crucial.**

   **todo:** practise deliberate design methodologies and develop standards

3. **Autonomy has a two-fold effect.**

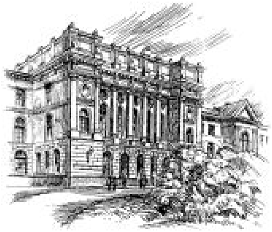
   **todo:** look for trade-offs between security and reconfigurability

4. **Power budgets are limited.**

   **todo:** search for breakthrough in power supply technologies

5. **There's a need for statistically meaningful reliability data.**

   **todo:** perform life data collection and analysis



**Our contacts:**

Olga Mamoutova mamoutova@kspt.icc.spbstu.ru
Andrey Antonov a.a.antonov.aivt@gmail.com

**Web:** http://kspt.icc.spbstu.ru/EMS-center

# Additional slides

# Polytechnic-Space 101. Study Plan

**Target:** master’s degree and PhD students

**Course agenda:** 72 hours + plus hands-on training

**Modules:** adopted to a nanosatellite design flow

1. Basic terms of reliability

2. Risk analysis

3.1. Fault prevention

3.2. Fault tolerance

3.2. Fault removal

4. Fault forecasting at design phase

5. Design for reliability

**Result:** dependability and security spec artifacts

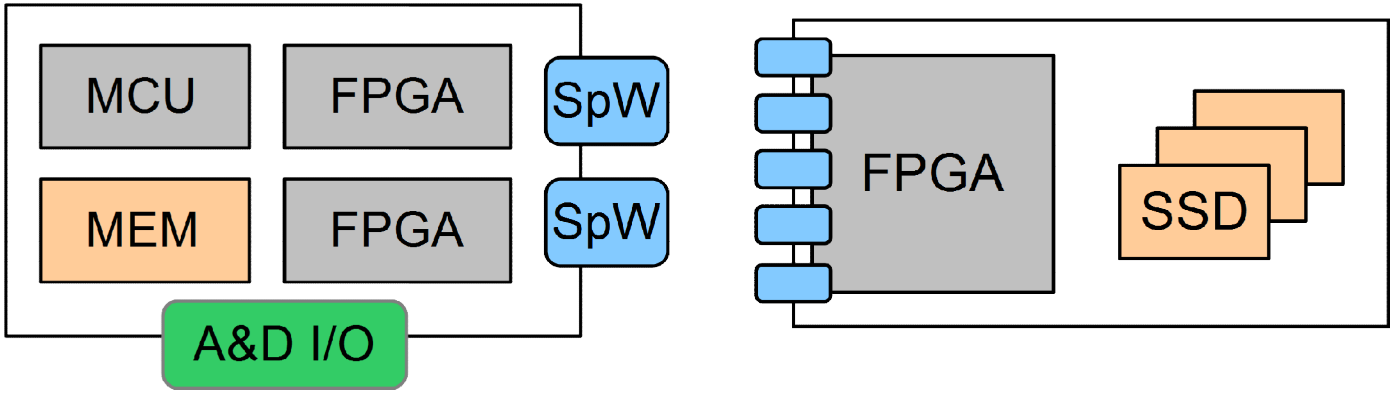
# Command and Data Handling in small satellite

## C&DH – State of the art:

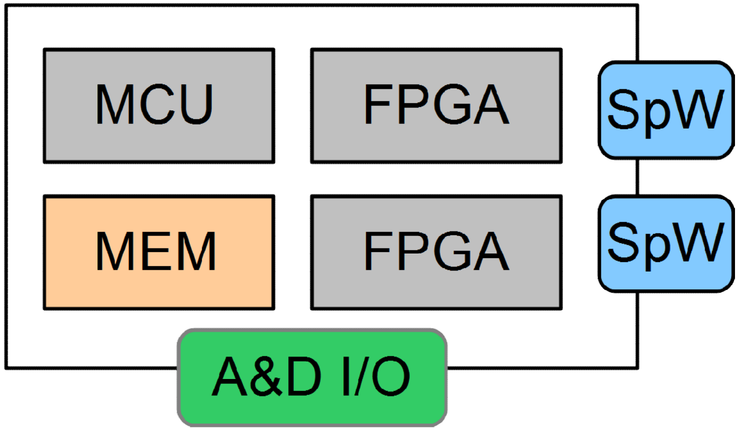
- Computer network
- Distributed information processing
- Plug-and-Play network architectures
- **Hardware architecture diversity – Problem!!!**

## Our solution: **UMoMI**

**U**niversal
**Mo**dule for
**M**anaging the
**I**nformation

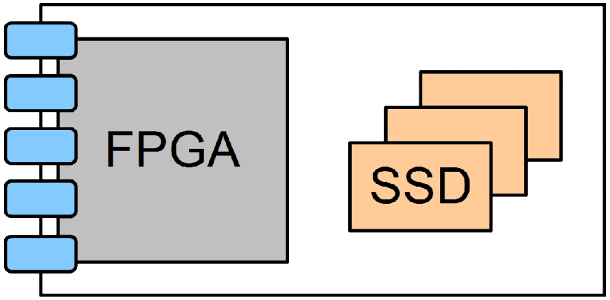


# UMoMI – command and data processing



- **Service FPGA** – basic interface and control
- **Main SpaceWire** interface (duplicated)
- * **FPGA** – DSP tasks + duplicates service FPGA
- * **Secondary SpaceWire** interface (duplicated)
- * **Microcontroller** – computations and control
- * **Memory** array – MCU support + data buffer
- * **Analog and digital I/O** – interface to instruments and payload

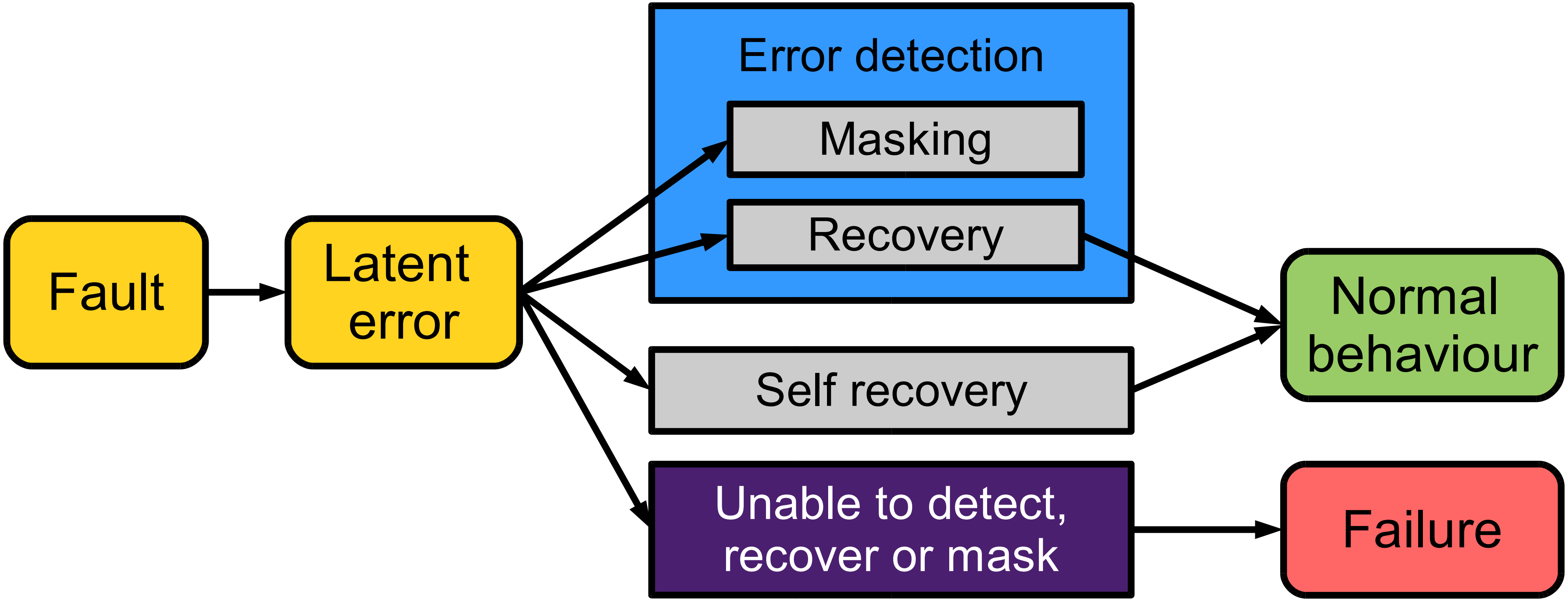
# UMoMI-R – router/mass memory



- Extended number of **SpaceWire interfaces**
- **Service FPGA** – network routing + control
- * **SSD array** – mass memory

* – Optional components

# Dependability and Security: Basic Terms



Since mid 1960s:

**Established armory of reliability engineering methods and techniques for computing systems**