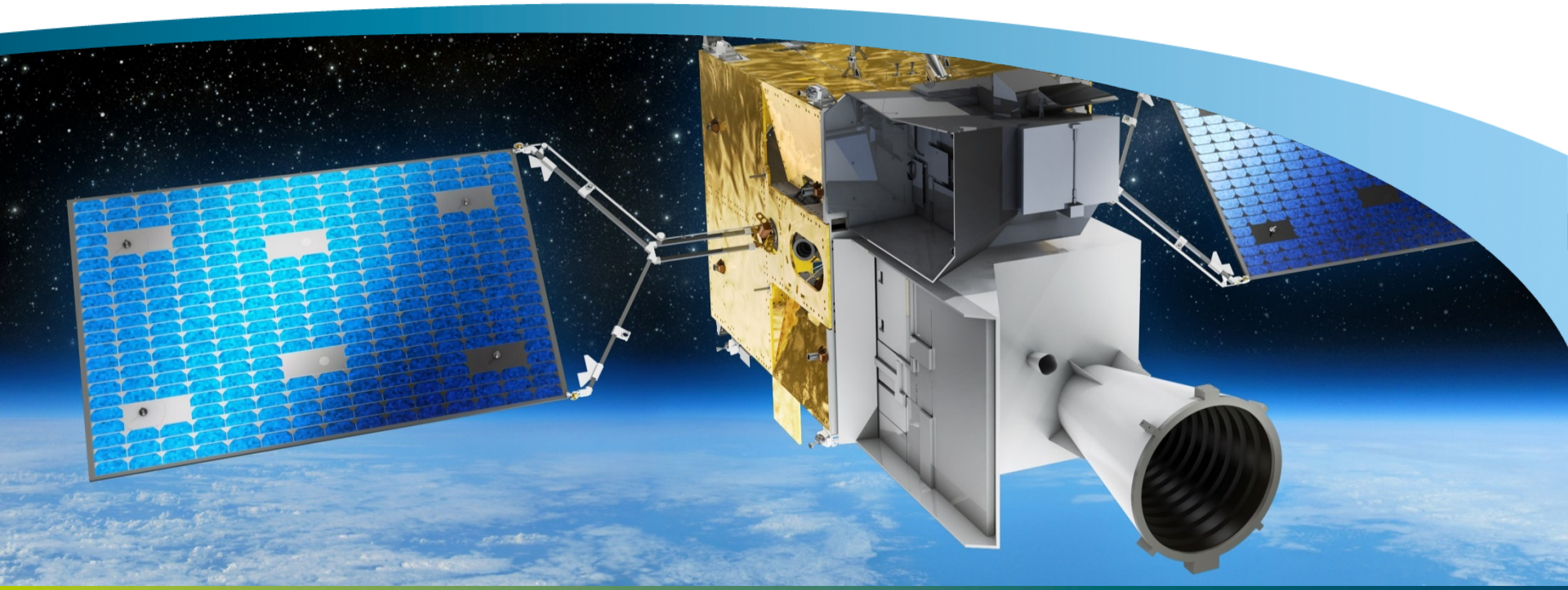
OHB System AG
Michael Brahm
21/10/2015, ESA-ESTEC



SPACE SYSTEMS

Decoupling FDIR Levels by Different Monitoring Frequencies to Reduce Software Complexity

We. Create. Space.

Agenda

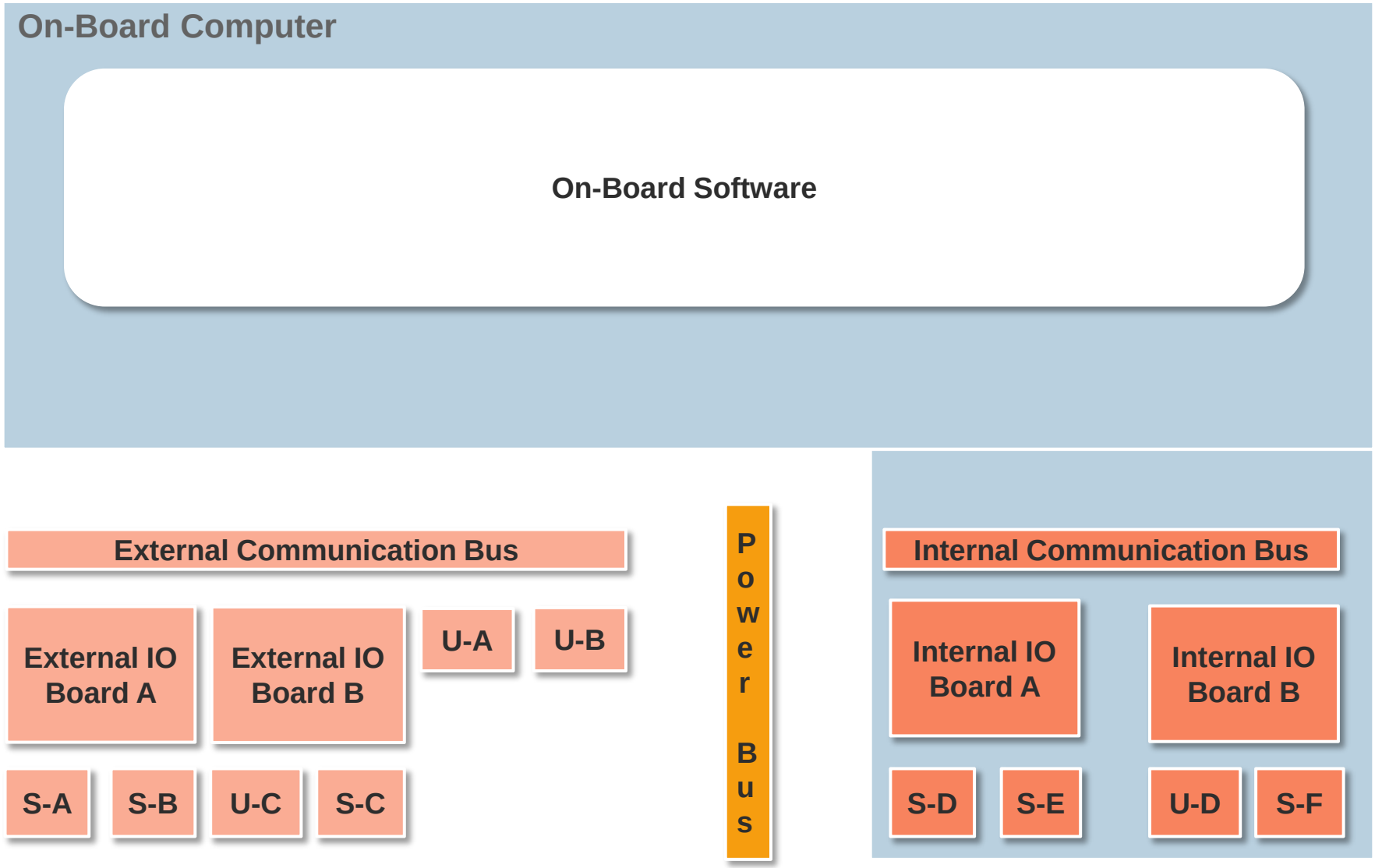
- Basic Constraints & Assumptions
- FDIR Levels & Failure Propagation
- FDIR Level Dependencies & Timing
- Benefits & Constraints

Basic Constraints & Assumptions

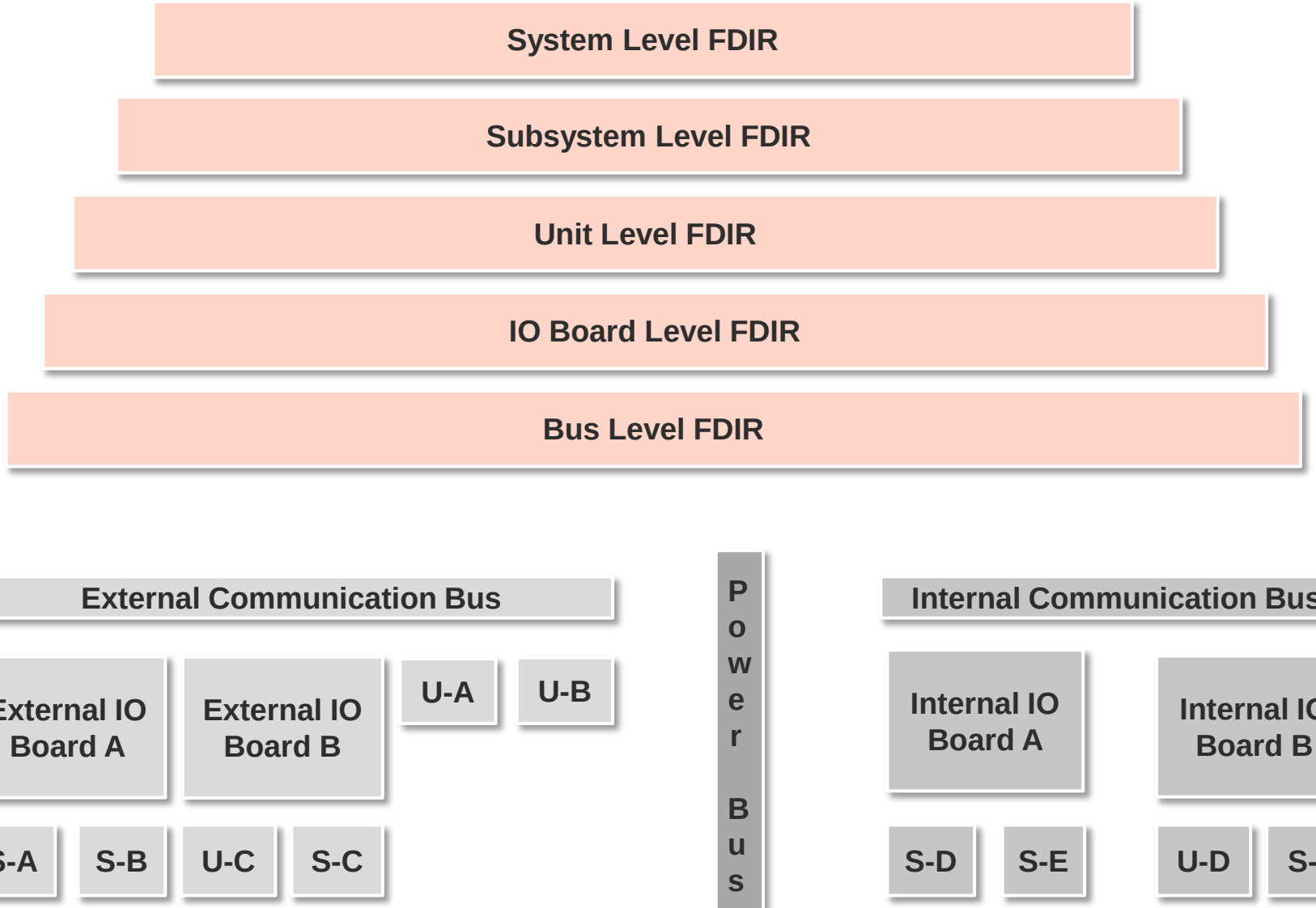
- Goal: Single Fault Tolerance
- Goal: Satellite Survival
- Goal: High Service Availability
- Goal: Fault Isolation (no false alarms!)
- Goal: Robustness (don’t be too nervous!)
- Assumption: Immediate Unit Damage is prevented by HW measures (e.g. LCLs)

SW FDIR does not need “very” fast response times

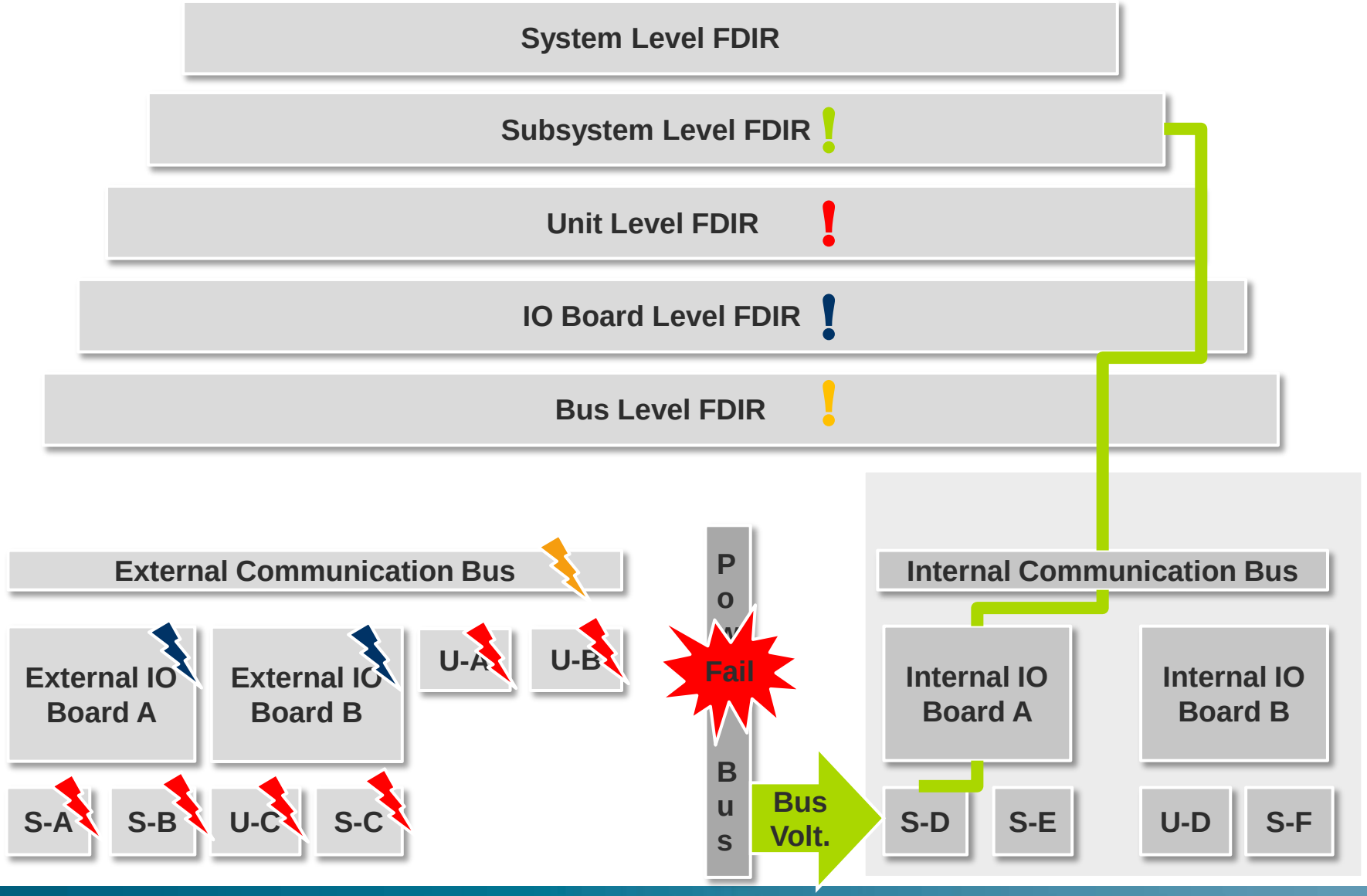
Typical Satellite Architecture



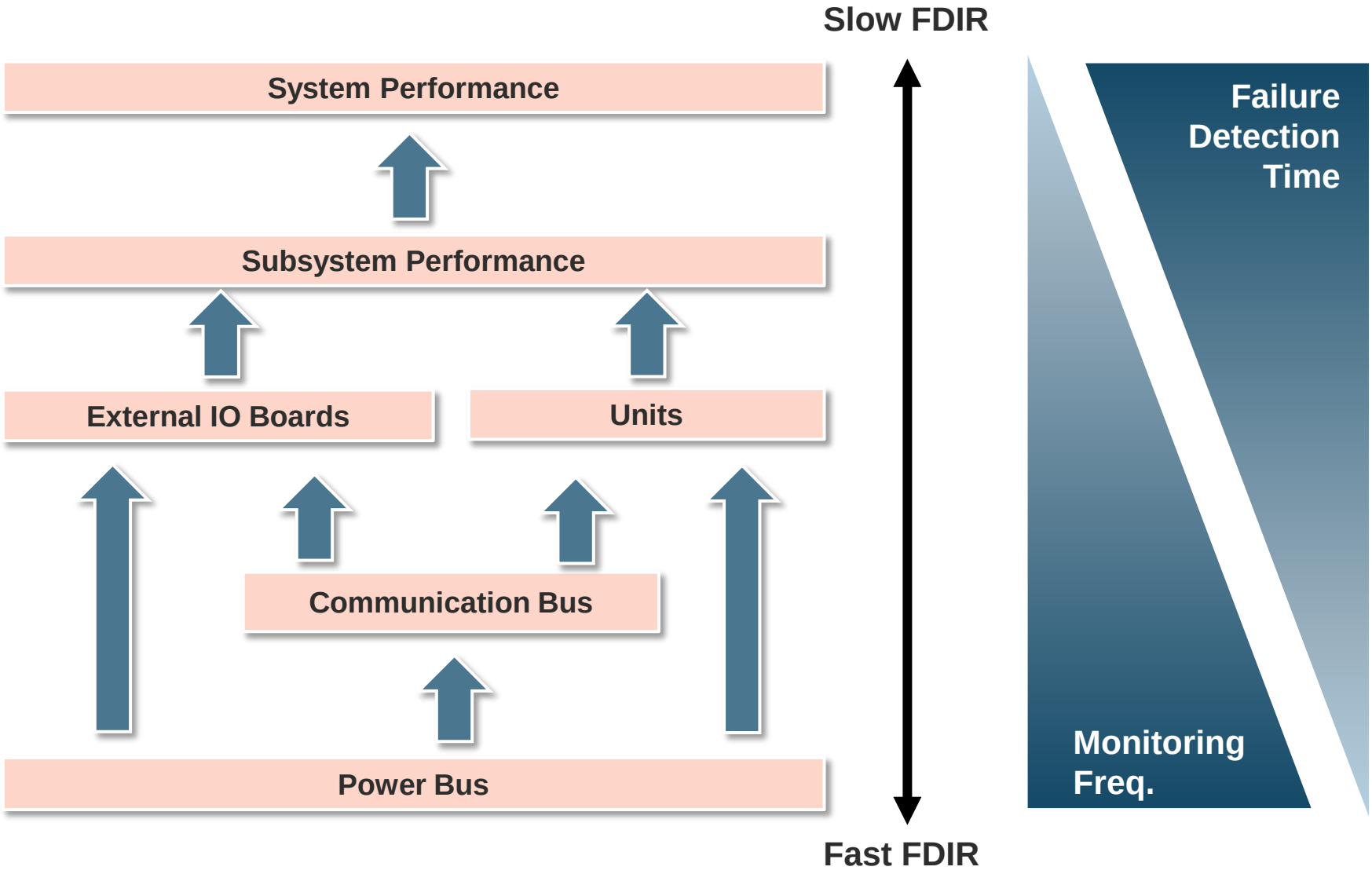
Respective FDIR Levels



Failure Propagation Examples



FDIR Level Dependencies & Timing



FDIR Level Dependencies & Timing Example

- Bus Power Failures before Communication Bus Failures
- Communication Bus Failures before I/O Board Failures & Unit Failures
- Unit Failures before Subsystem Failures
- Subsystem Failures before System Failures

Failure	Reaction Time	Failure Detection
Power Bus	< 1s	Bus Voltage Level
Communication Bus	< 2s	Packet Error Counter
Units/IO/Boards	< 5s	Board Voltage Level
Subsystem (e.g. Thermal)	< 10s	Temperature
SW Watchdog Failure	1s *	HW Alarm

* there are still failures that have no relationship to others, which can be handled immediately

Benefits & Constraints

Benefits:

- Concept can be realized using the PUS Services
  - Monitoring Service, Event-Action Service
- No complex SW logic necessary

Constraints:

- Perform recovery action before higher level failure is detected
- During recovery, related failure detections must be ineffective
  - E.g. disable FDIR globally during recovery
  - E.g. declare related monitored data invalid

Thank you for your kind attention!

Contact:

- **michael.brahm@ohb.de**