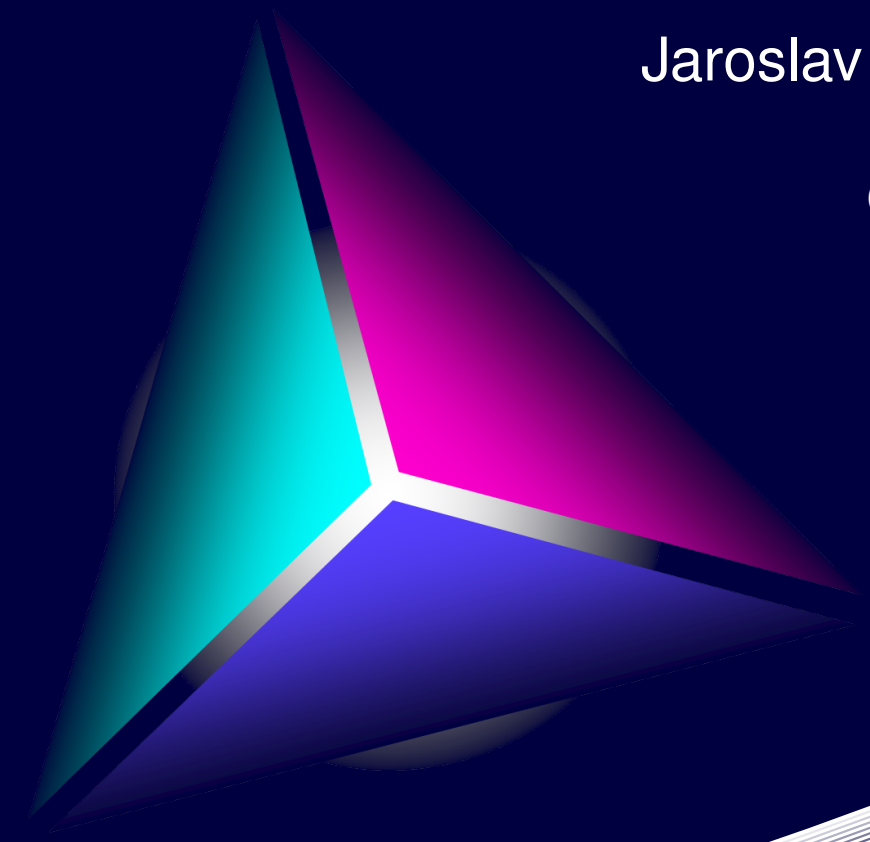
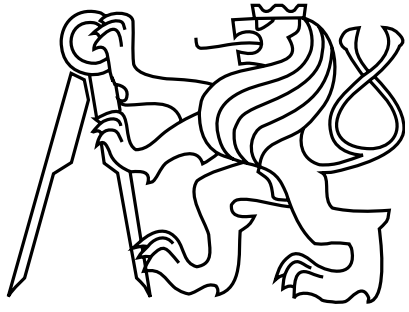
Fault Recovery Method of Modular Systems based on Reconfigurations

Jaroslav Borecký, Pavel Vít and Hana Kubátová

Czech Technical University in Prague
Faculty of Information Technology
Department of Digital Design



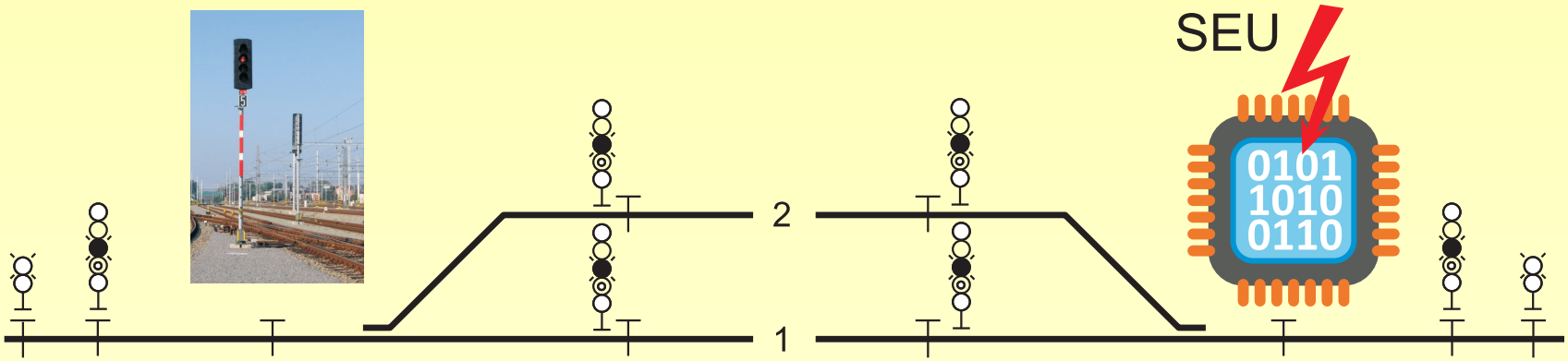


Outline

Introduction

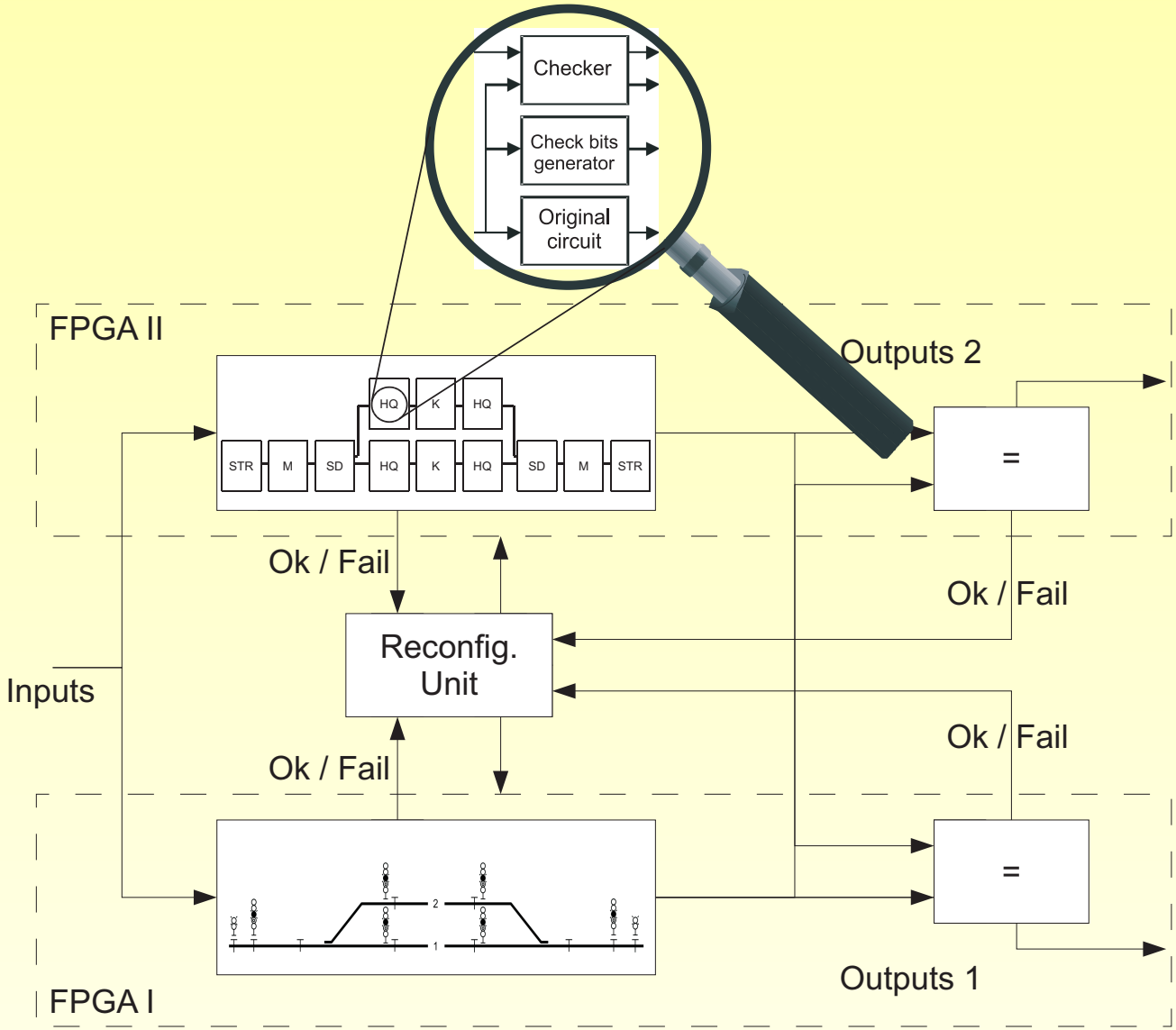
- Mission critical applications
  - Space missions
  - Public transport
- SRAM-based FPGAs are sensitive to the radiation (SEU)
- Undetectable by off-line tests
- Design a high reliable modular system on unreliable components

Simple Railway Station Safety Device



- Inovation of a czech railway station safety device
- Converted from modular system of relays into modular system in one FPGA

Modified Duplex System – initial design



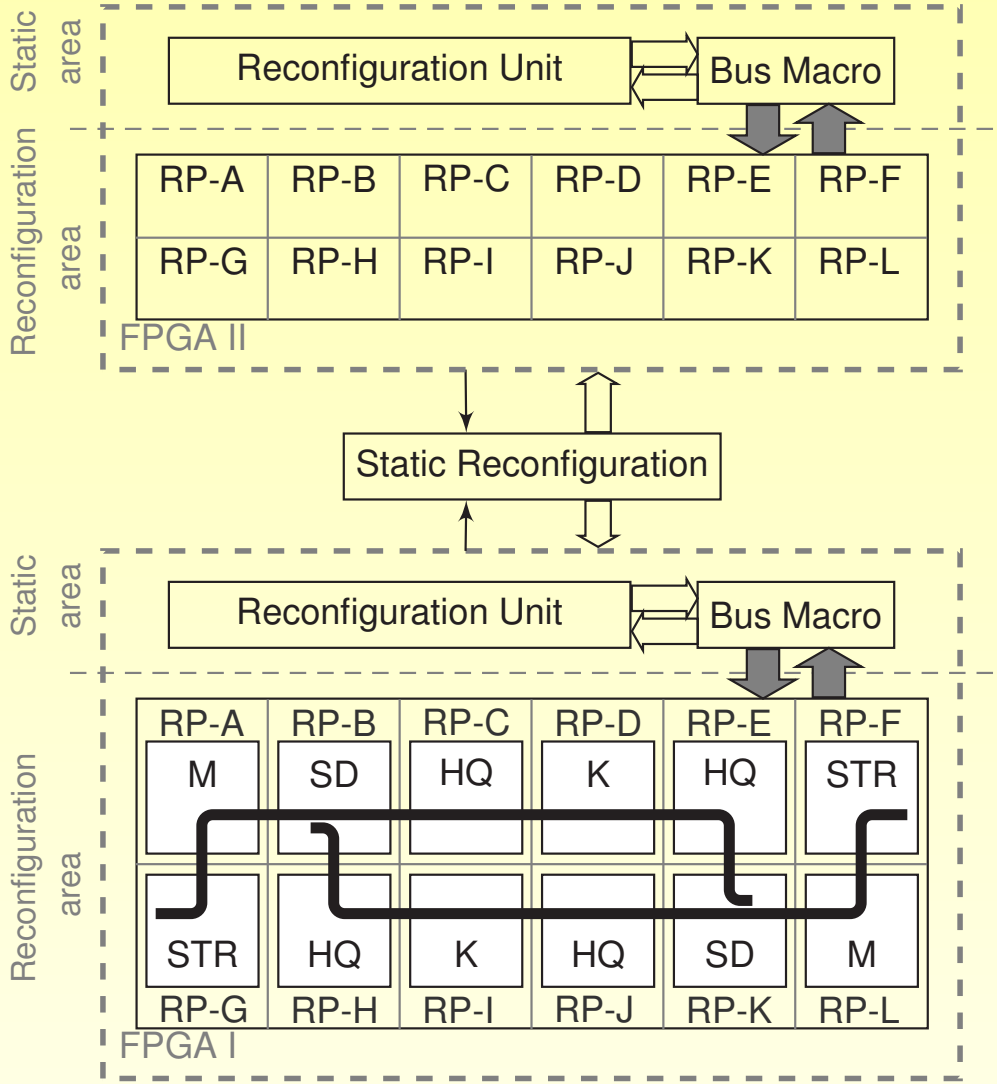
Modified Duplex System – properties

- Uses two same FPGA boards with the same design
- Error is detected by TSC block and/or by comparators, which initiate reconfiguration
- Static reconfiguration of whole FPGA
  - Full reconfiguration is a time demanding process
- Lower area overhead in comparison with TMR

Partial Reconfiguration

- Only small part of FPGA – short time
- Repairs detected soft error
- Higher availability of whole system
- Rest of the FPGA still properly works
- Easy synchronization of the reconfigured part

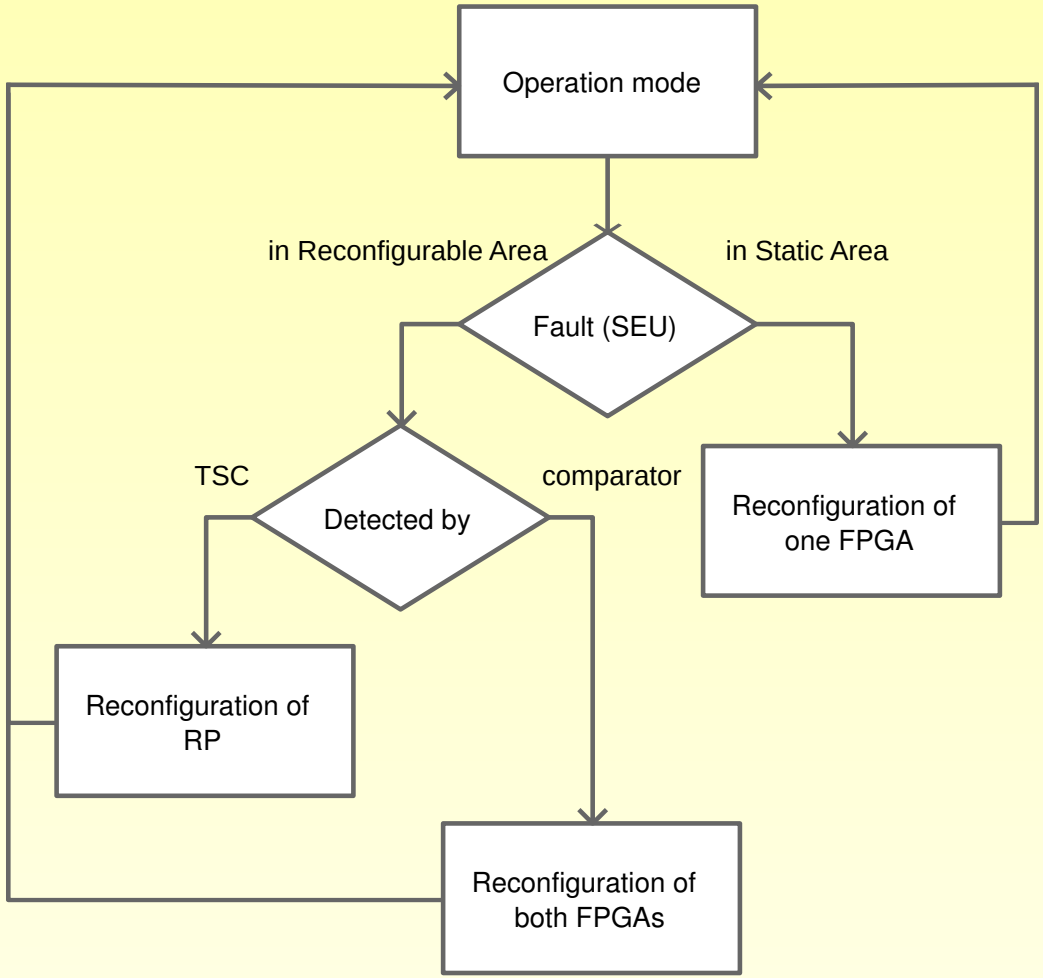
Schema of UMDS



Description

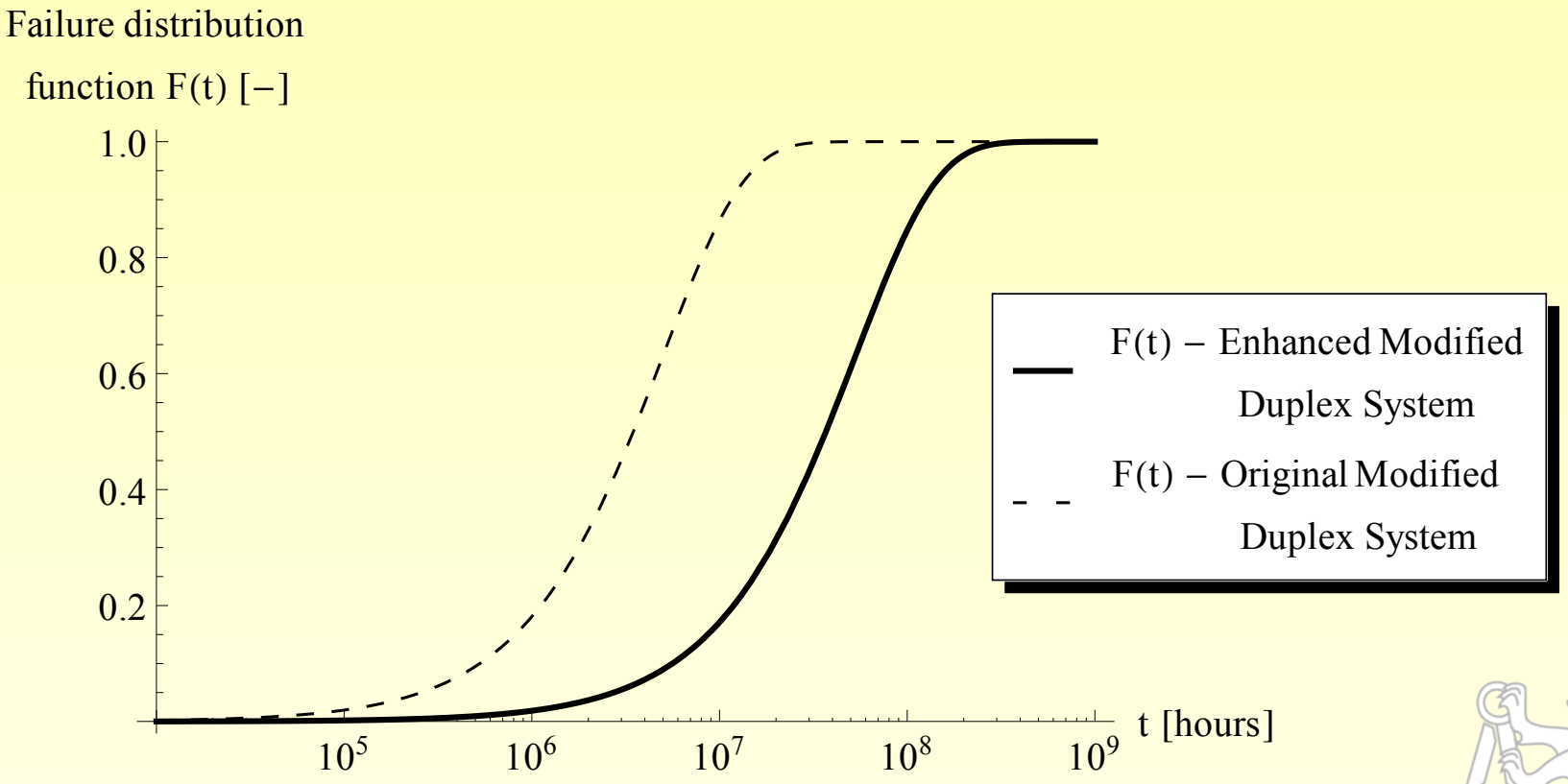
- Reconfiguration area (RA)
  - Divided into Reconfiguration Partitions (RP)
  - Partitions areas are able to perform partial reconfiguration
  - The number of RP depends on used application
  - The size of one RP depends on the specific architecture of an FPGA
- Static area
  - The Reconfiguration Unit controls the status of each TSC block in the RA
- Static reconfiguration
  - Performs reconfiguration of the whole FPGA
  - The reconfiguration is initiated by comparators

Behavioural Model



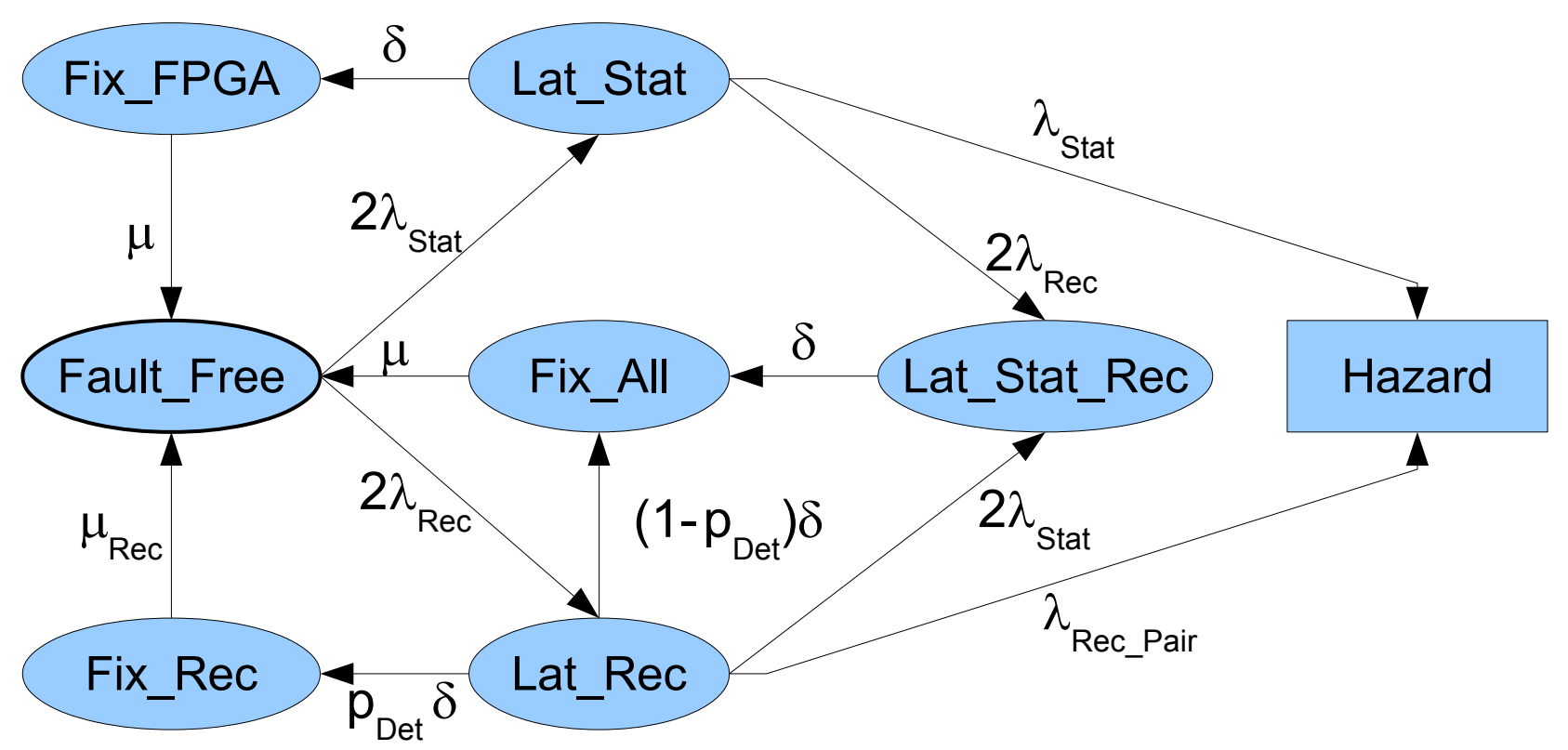
Failure Distribution Function

- Failure distribution function was calculated using Markov model



Failure Distribution Function

- Dependability model used to calculate the failure distribution function.



Conclusions

- Two independent FPGA boards with the same design
- Whole system is reconfigurable and repairable from soft errors
- Static area checks failure signals and repairs errors
- Ability of faster detection and correction of faults
- Availability and security were increased
- Method designed with respect to minimal area overhead
- Both FPGAs load same design, the systems development time was reduced