

Workshop on Fault-Tolerant Parallel and Distributed Systems — April 19, 2002

Int. Parallel & Distributed Processing Symp. (IPDPS-2002) — Fort Lauderdale, FL, USA

From Experimental Assessment of Fault-Tolerant Systems to Dependability Benchmarking

Jean Arlat



Work partially supported by project IST 2000-25425



DBench
Dependability Benchmarking

Dependability Assessment

■ Objectives

- ◆ Evaluation of Dependability Measures (Reliability, Availability, etc.)
- ◆ Verification of Properties
 - ◆ Nominal Service
 - ◆ Service in presence of Faults
- ◆ Characterization of Behavior in Presence of Faults
 - ◆ Failure modes
 - ◆ Efficiency of fault tolerance

■ Methods and Techniques

- ◆ Axiomatic
 - ◆ Stochastic processes
 - ◆ Model checking
- ◆ Empirical
 - ◆ Field measurement
 - ◆ Robustness testing
 - ◆ Fault injection

Fault Tolerance Validation

● Dependability

- FT mechanisms = human artefacts (not perfect)
- Calibration of models
- Formal approaches limits
- Threats = rare event



● Fault Tolerance (FT)

- Impact on dependability measures
- Estimation of FT efficiency
- Experimental approaches
- Controlled experiments

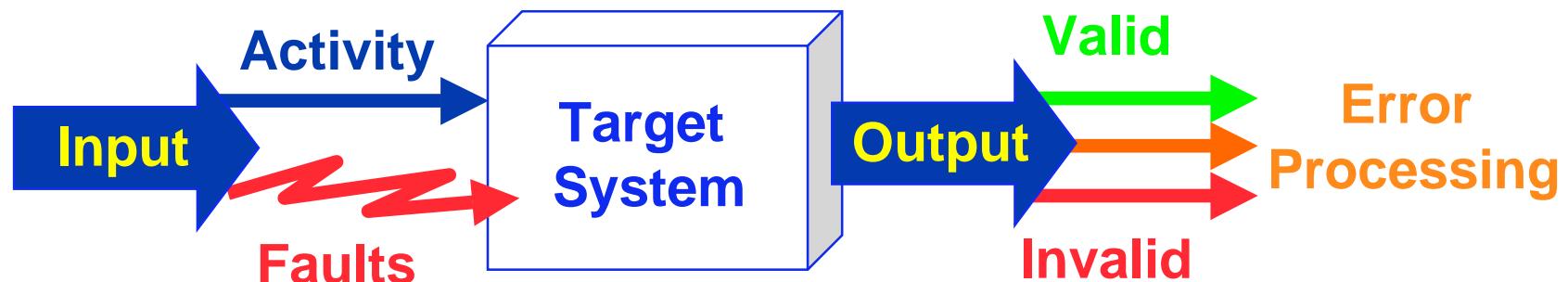


Fault Injection



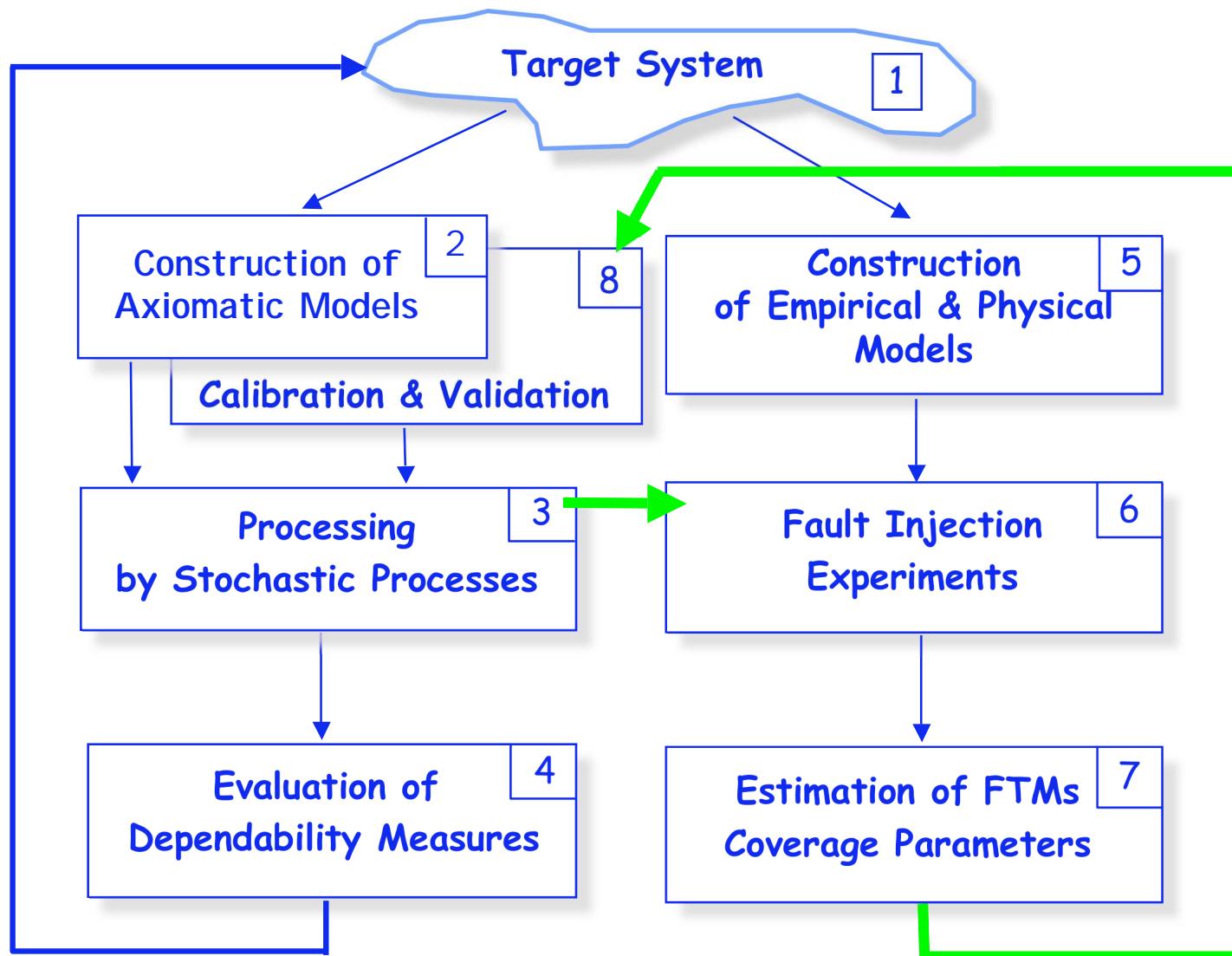
Validation of fault tolerance
wrt specific inputs it is designed to deal with: the faults

Fault Injection



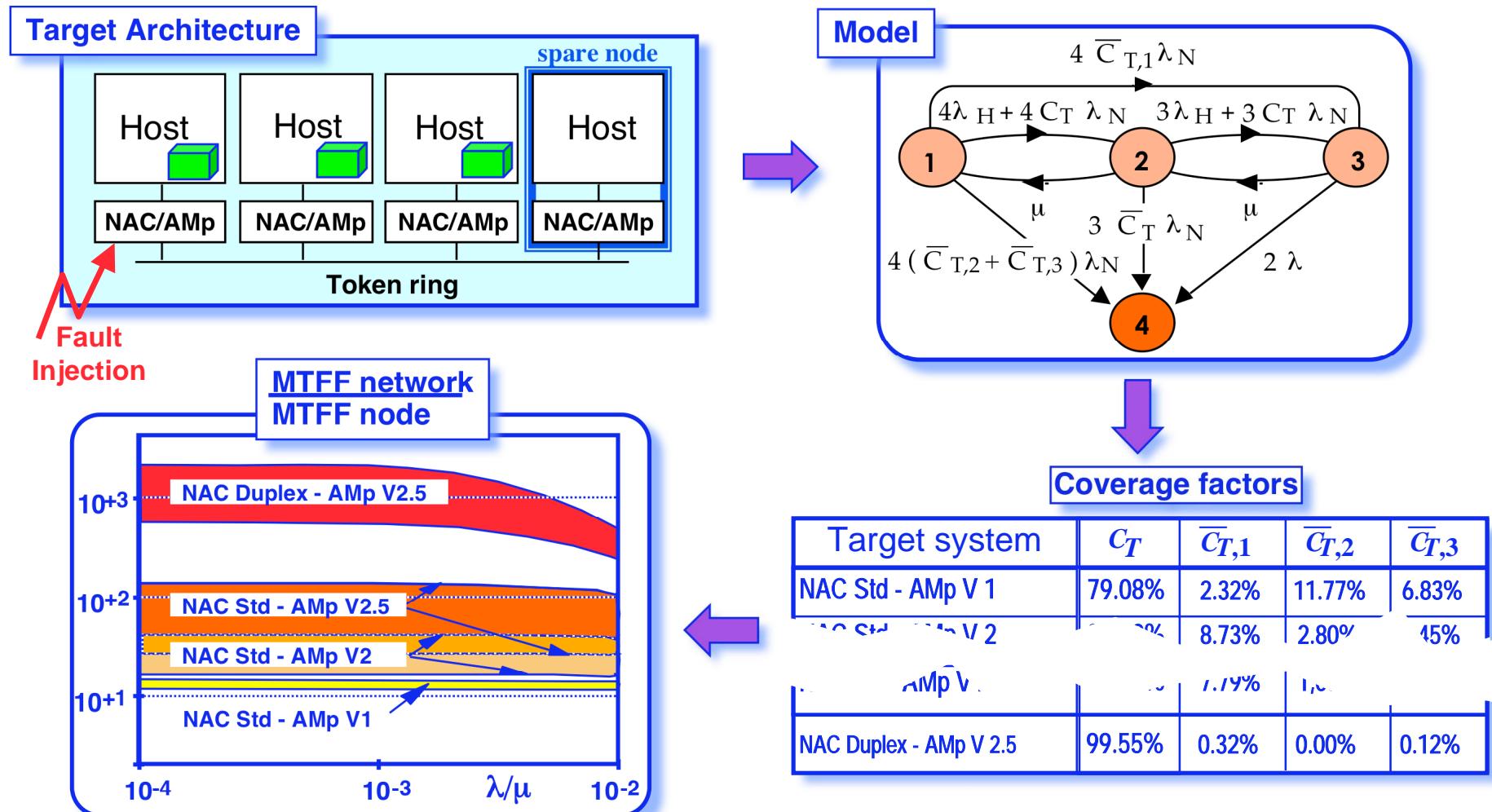
- Test and evaluation of fault-tolerant systems & FT mechanisms
- Explicit characterization of faulty behaviors

Analytical & Experimental Evaluations



Fault Injection as A Design Aid

[ESPRIT Project Delta-4]



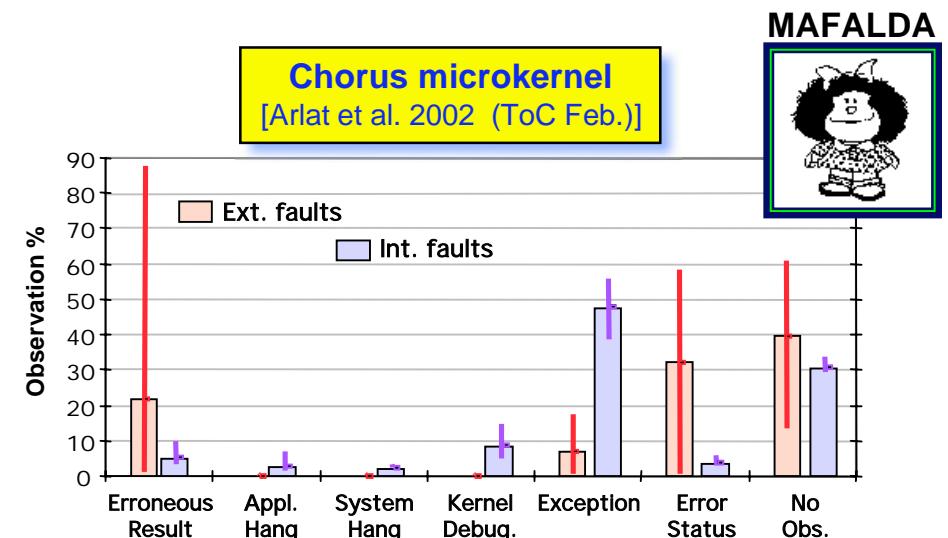
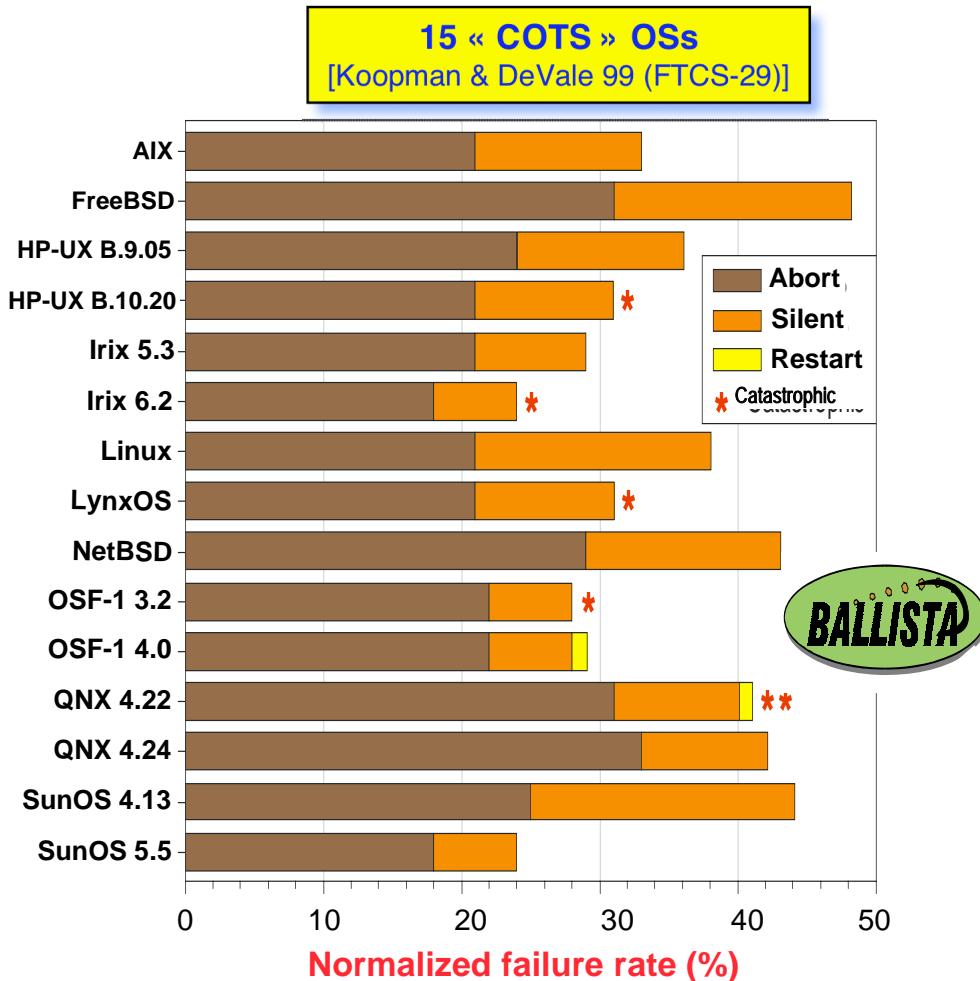
(Software) Component-based Development

- Integration of previously developed components (commercial or not)
 - ➡ **OTS** = either **COTS** or **OSS**
- Main advantages
 - ◆ productivity and time to market
 - ◆ incorporation of technology advances
 - ◆ compatibility with industry standards
 - ◆ quality (widely deployed components)

Applications Requiring High-level of Dependability

- Lack of observability and controllability : ? Dependability
- Global cost (development, validation, usage, etc.) ?

Fault Injection-based Dependability Characterization of COTS SW



Bit flips

- on parameters of kernel calls (ext.)
- in kernel memory space (int.)

Invalid parameters in system calls
at POSIX Interface

Fault Injection Well-Accepted by Industry as a Whole

■ Provider

- ◆ IBM, Intel, Sun MicroSystems,...

■ Integrator

- ◆ Ansaldo Segnalamento Ferroviario, Astrium, DaimlerChrysler, Saab Ericsson Space, Siemens, Technicatome, THALES, Volvo,...

■ Stakeholder

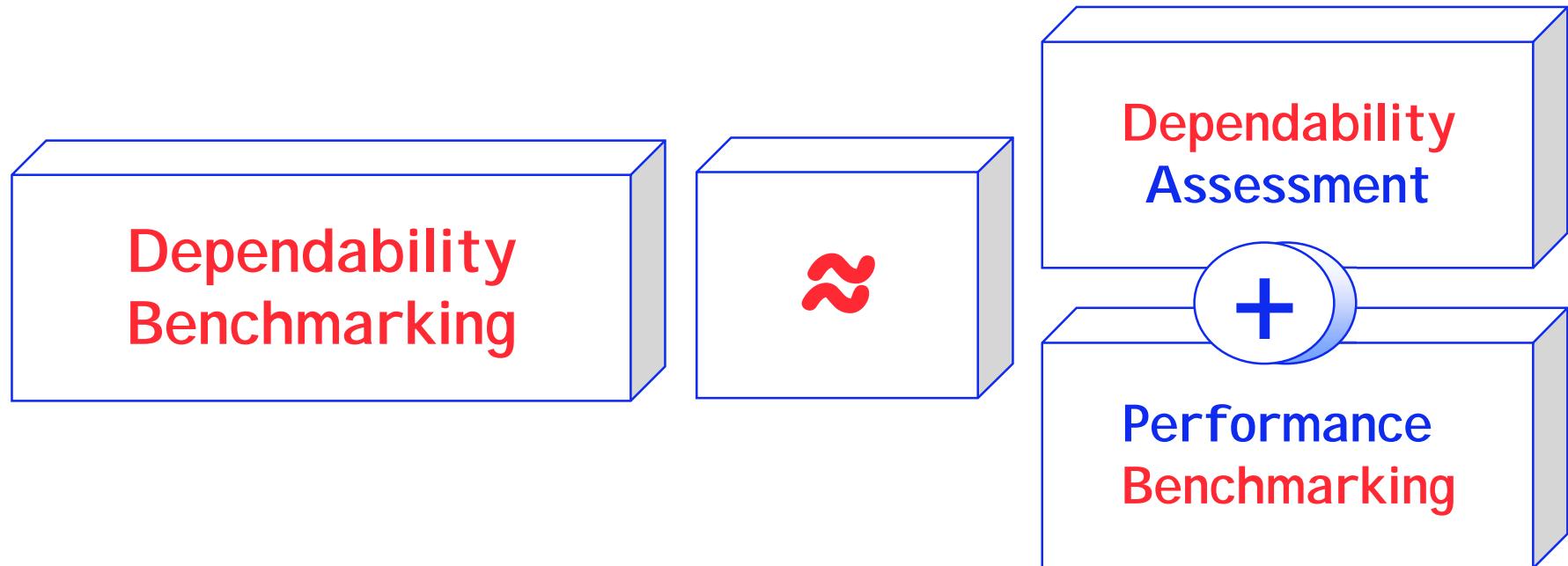
- ◆ Electricité de France, ESA, NASA (JPL),...

■ Consultant

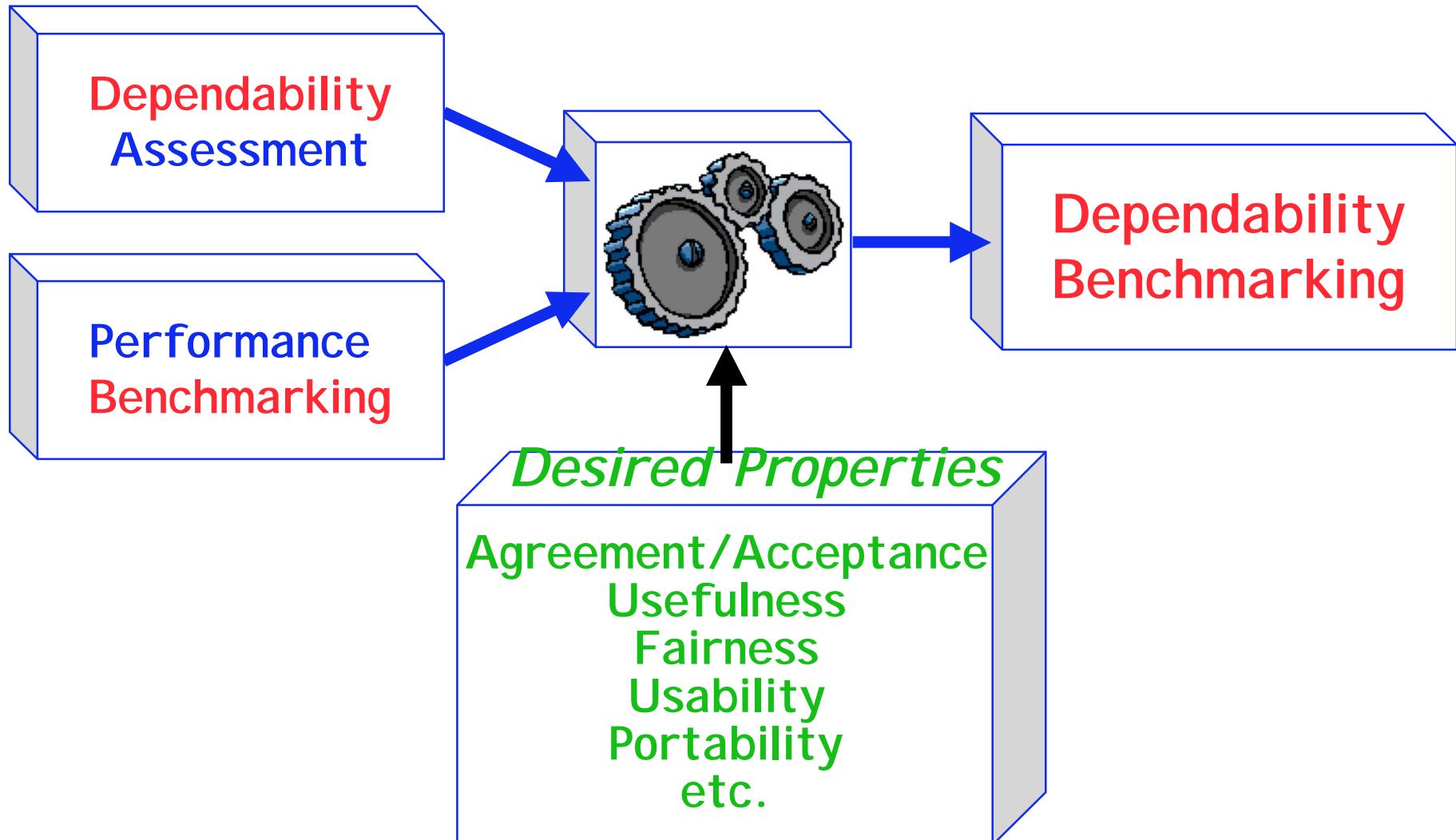
- ◆ Critical Software, Cigital,...

Dependability Benchmarking

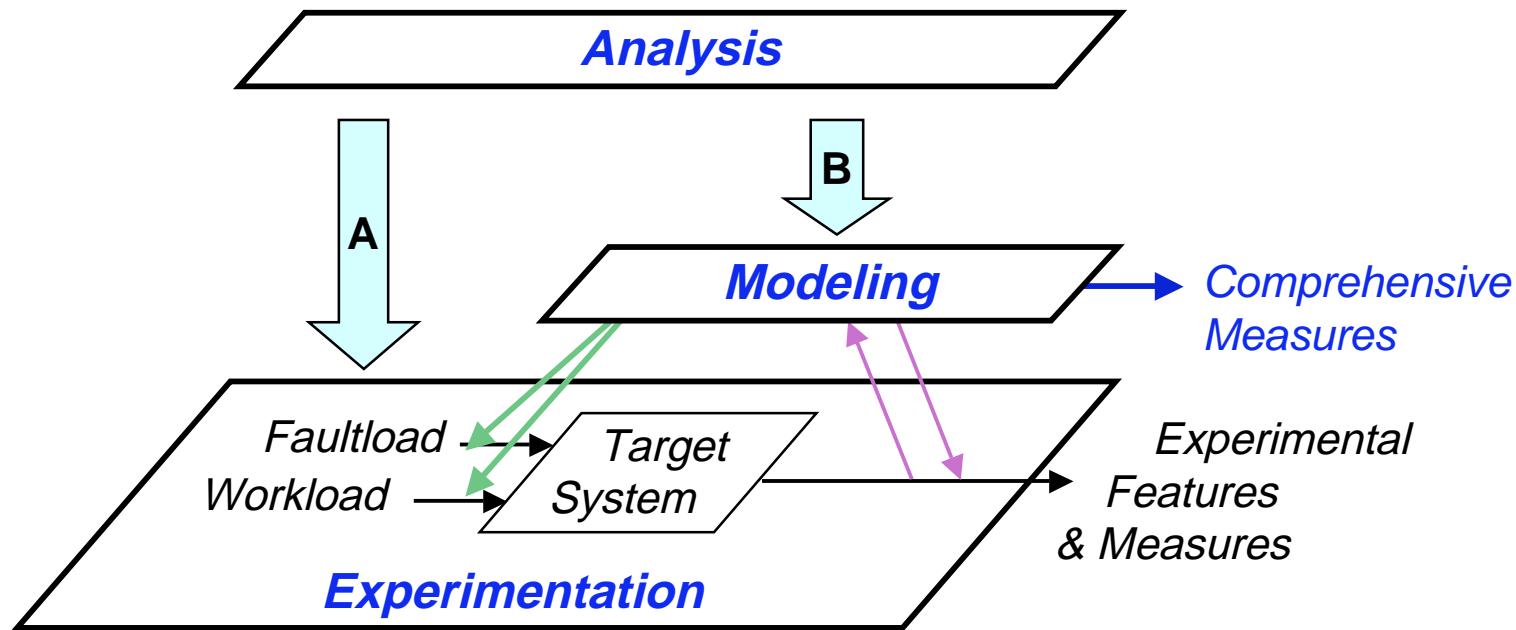
Naive View ... :-)



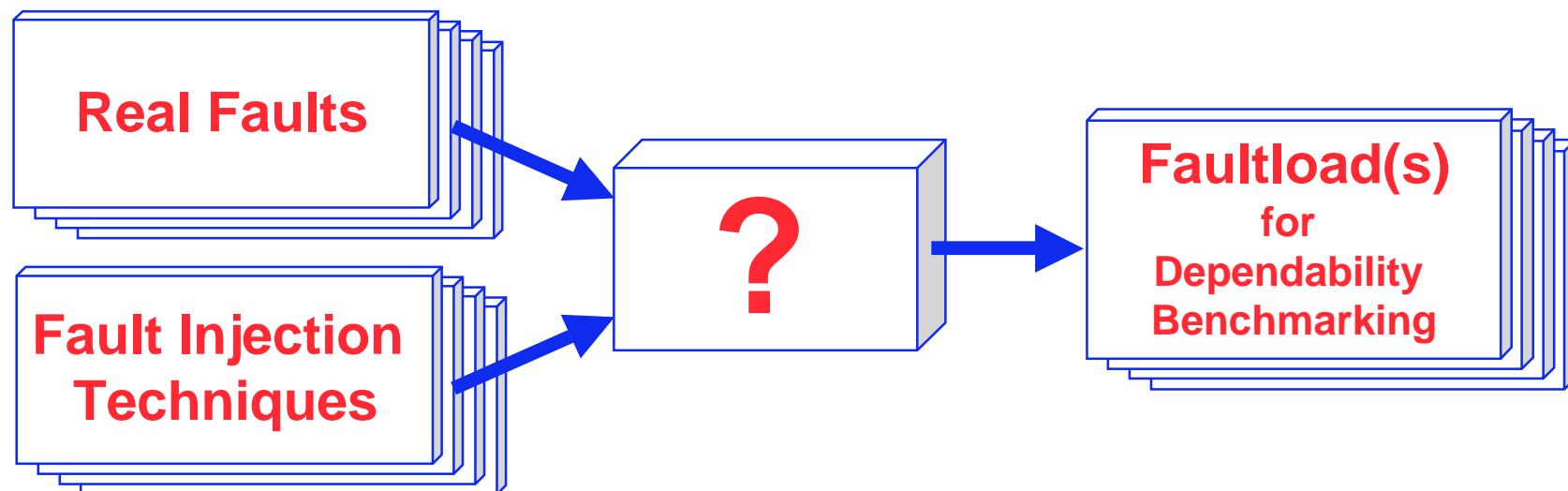
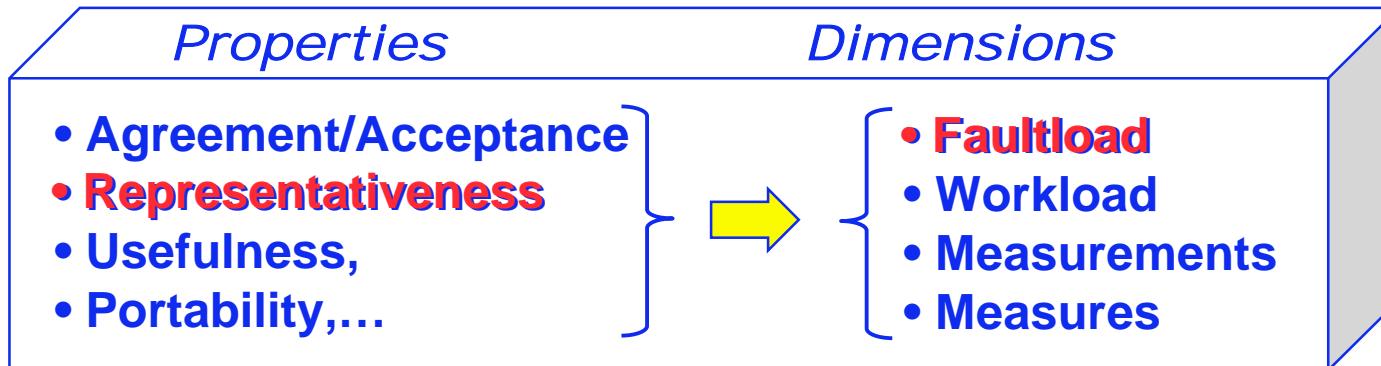
More Realistic View



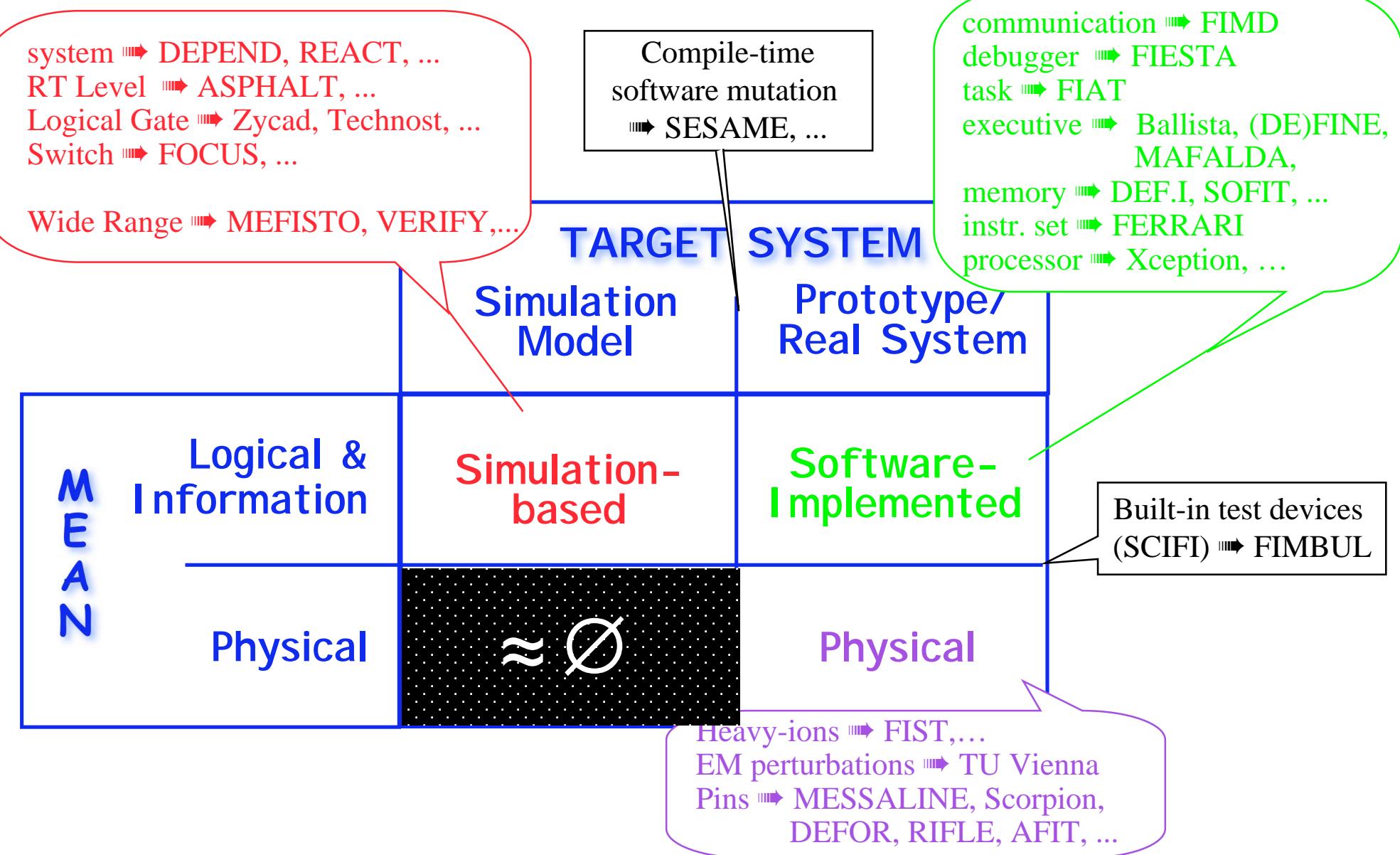
Dependability Benchmarking Framework



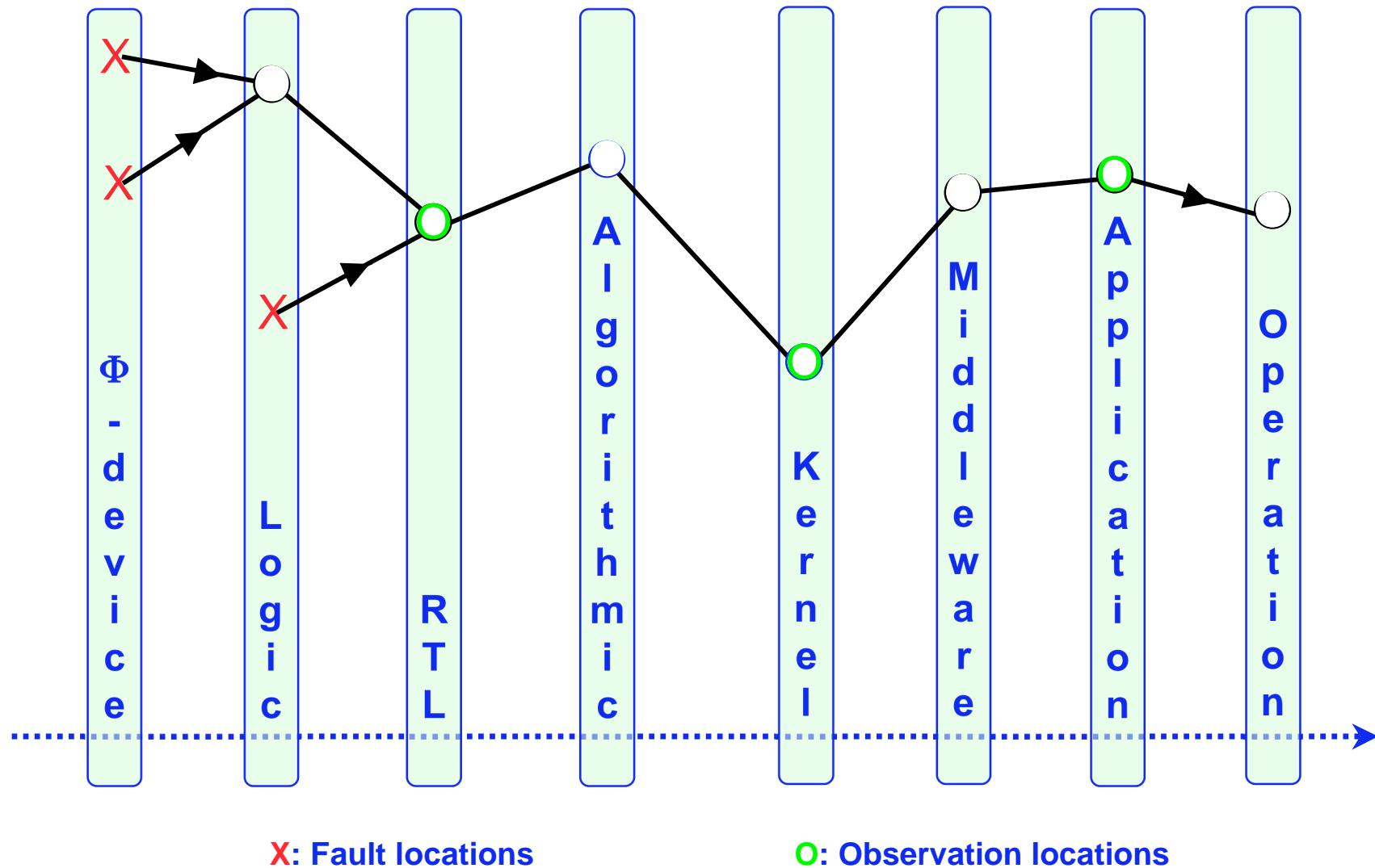
Challenges



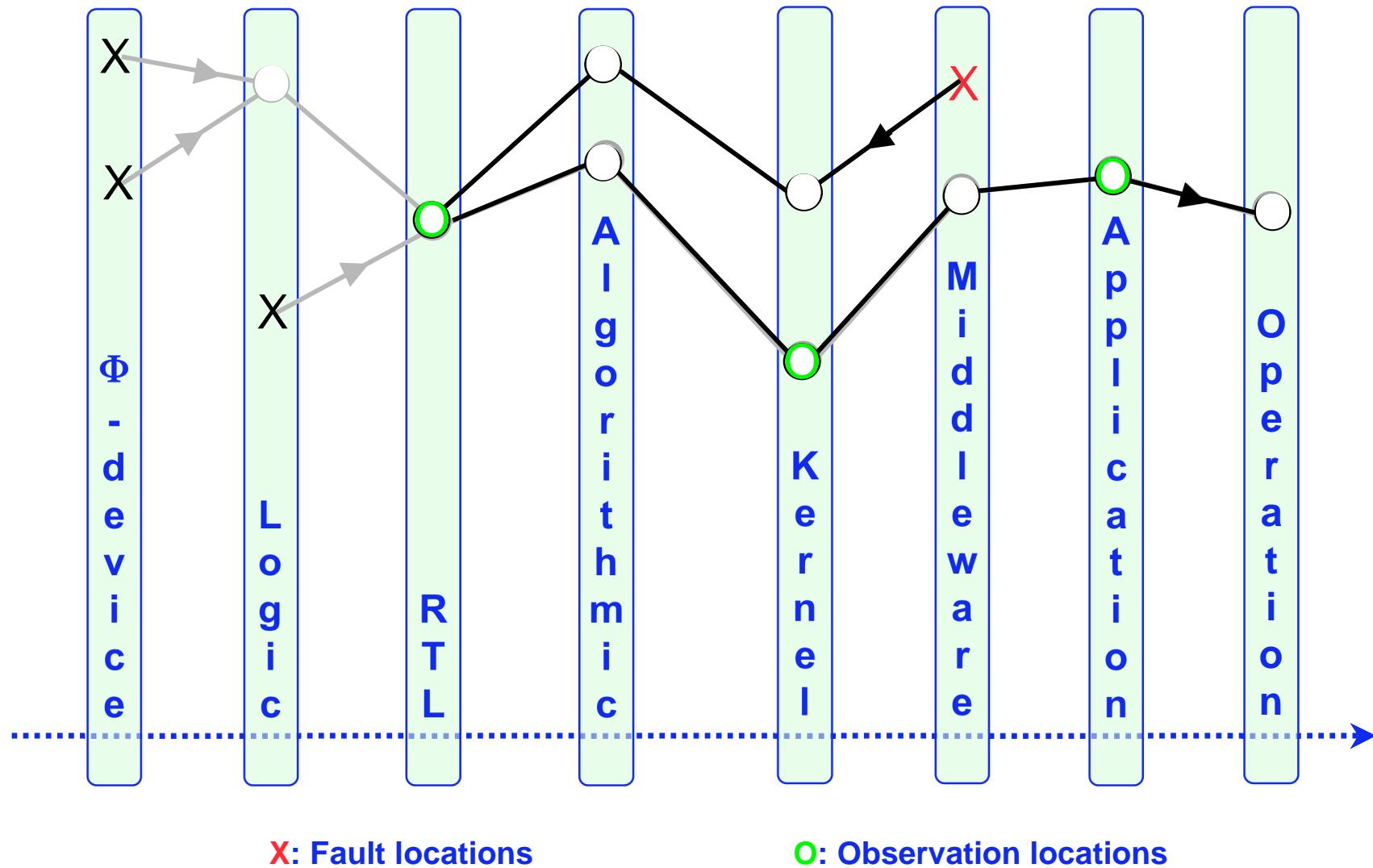
The Fault Injection Techniques



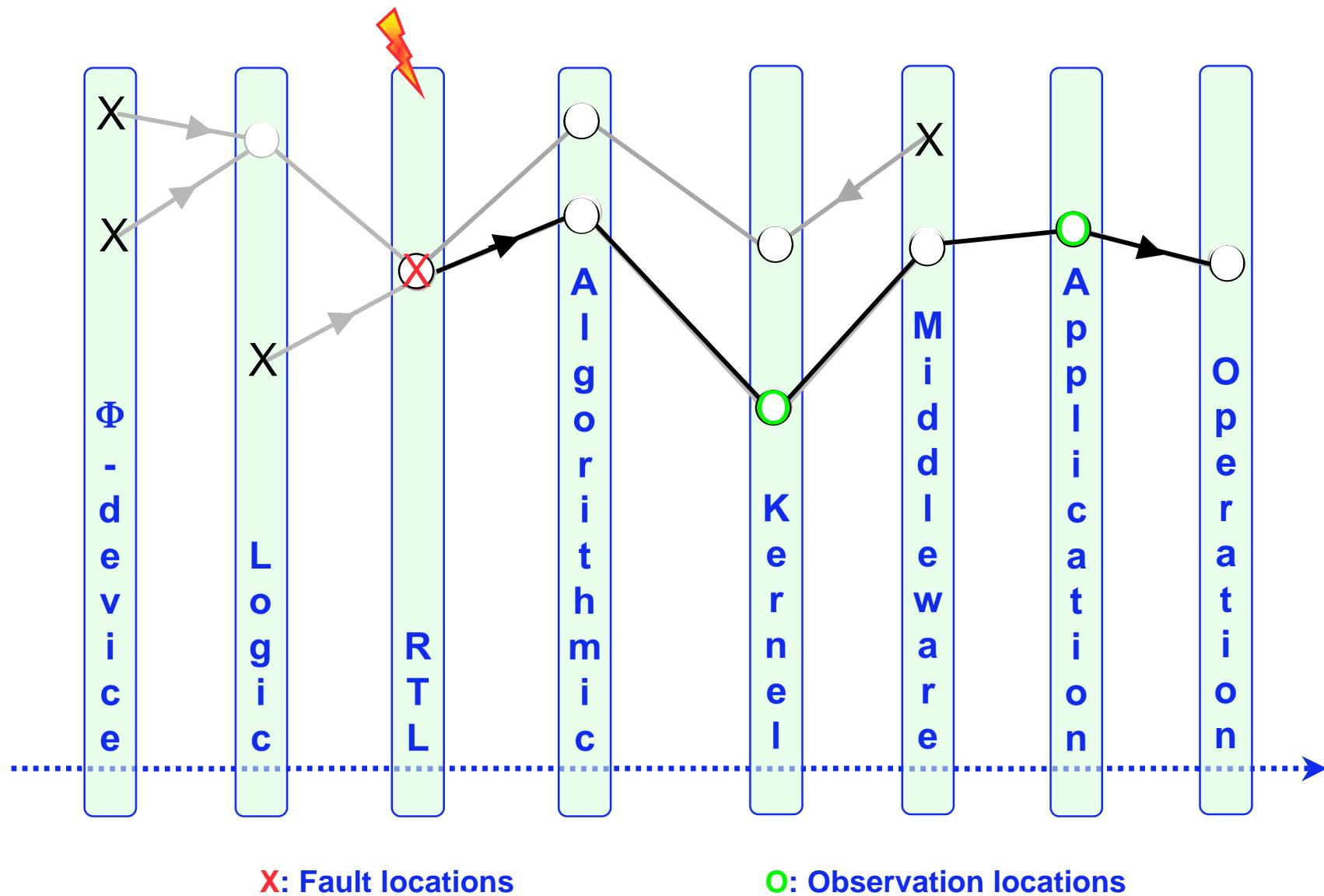
Target System Levels & Fault Pathology



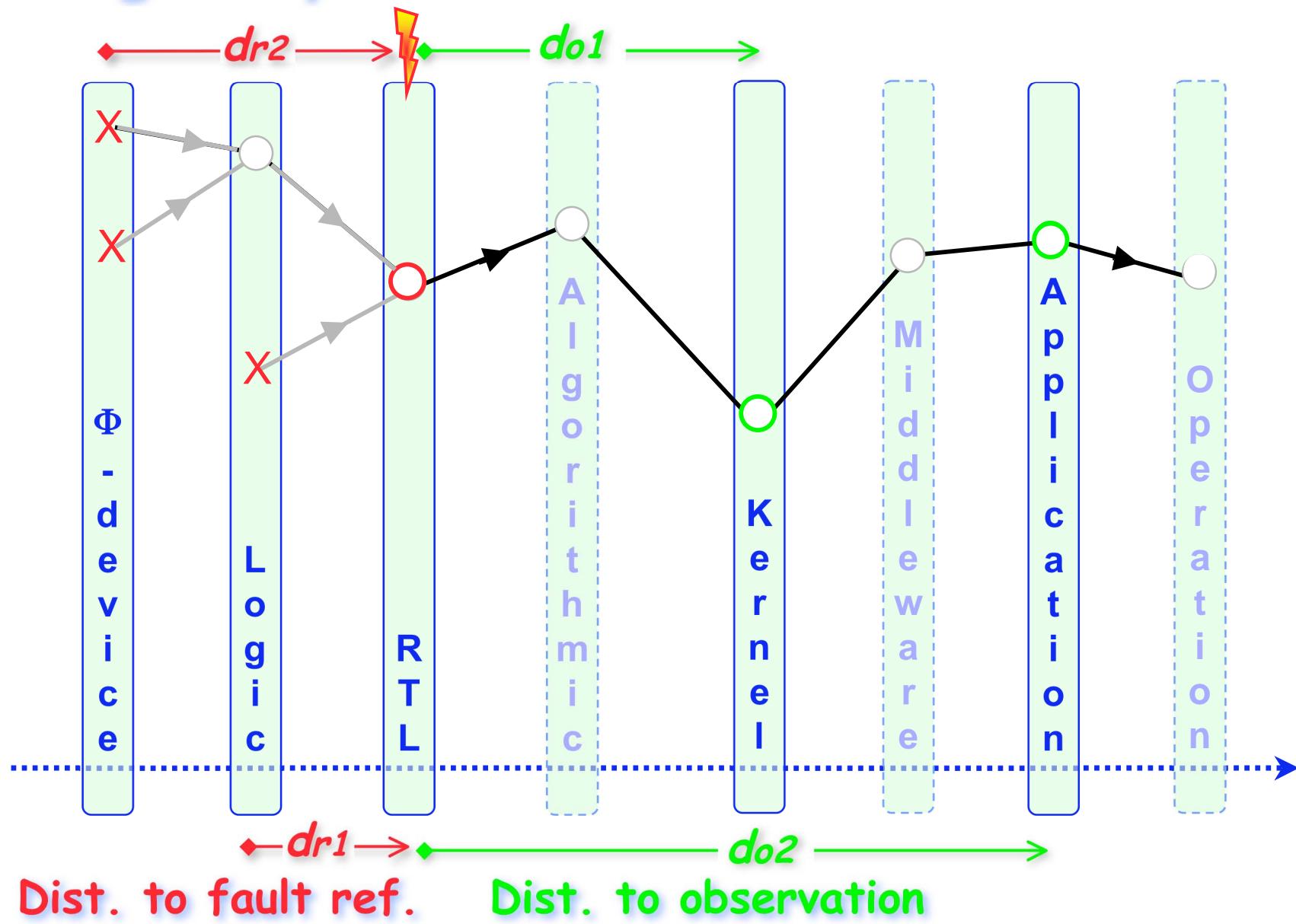
Target System Levels & Fault Pathology



Target System Levels & Fault Pathology



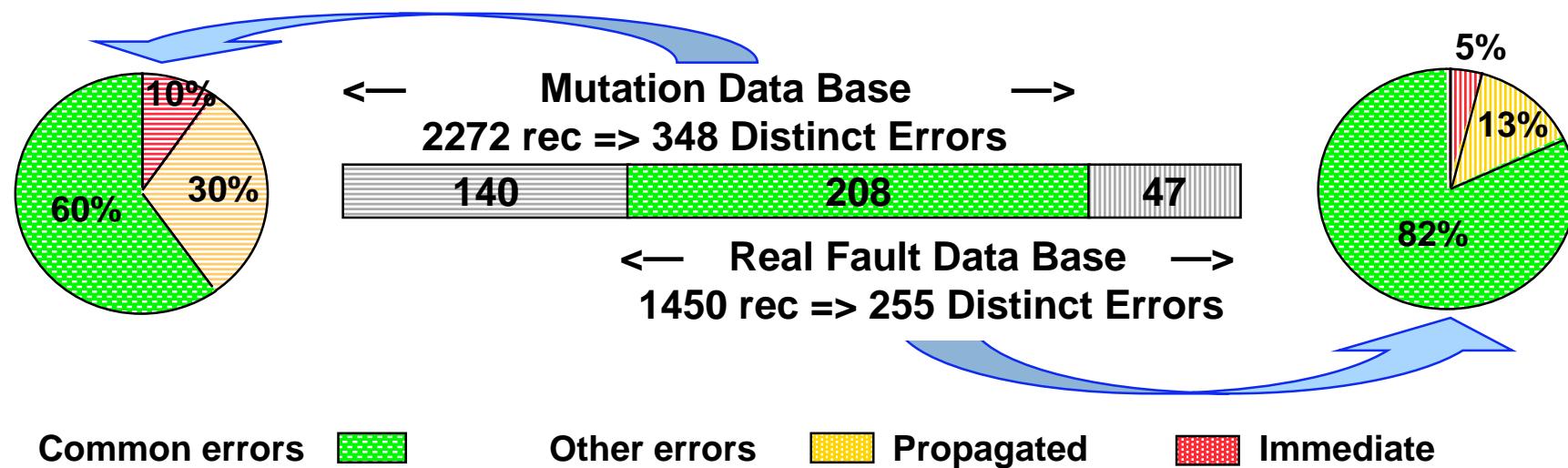
Target System Levels – Ref. & Obs. dist.



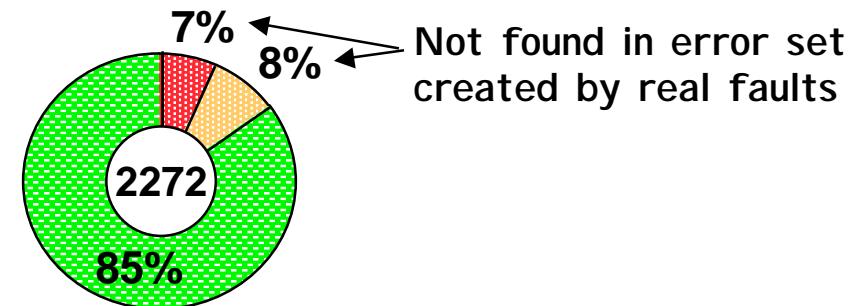
Mutation vs. Real Software Faults

[Daran & Thévenod-Fosse 1996 — ISSTA'96]

- Critical software from civil nuclear field - 12 programming faults
- Sets of Errors Provoked => 395 distinct errors



- Impact of the Mutation Experiments (wrt Real Faults)



SWIFI vs. Software Faults

■ SW Fault Classification (ODC)

- ◆ Assignment
 - ◆ Checking
 - ◆ Interface
 - ◆ Timing
 - ◆ Algorithm
 - ◆ Function
- 
- Can be (easily) emulated by SWIFI

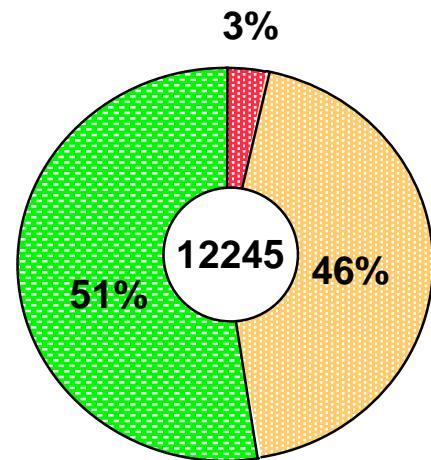
-> Main open issues are related
to fault-trigerring conditions?

SWIFI Bit-flips vs. SEUs

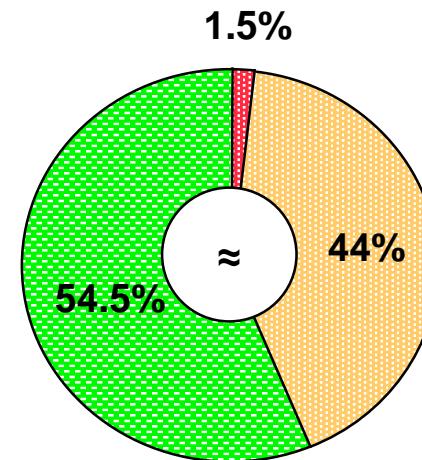
[Velazco *et al.* 2000 — IEEE ToNS Dec. 2000]

- Computerized system (80C51 μ controller)
- Activity: 6x6 matrix multiplication

SWIFI Bit-flips



SEUs Radiation



Tolerated



Erroneous result



Sequence loss

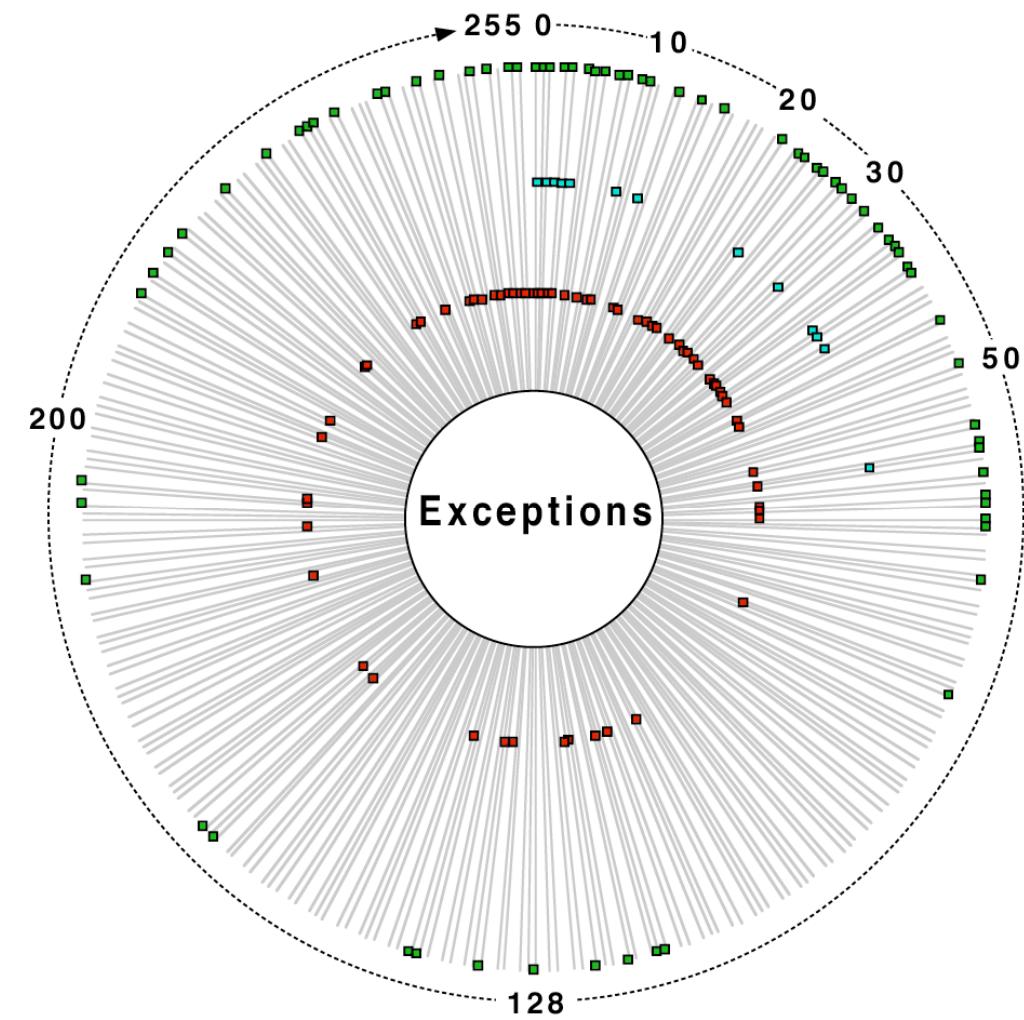


Several Φ FI techniques

[Karlsson *et al.* 1998 — DCCA-5]

- MARS fault-tolerant distributed system
(prior version of TTP architecture)

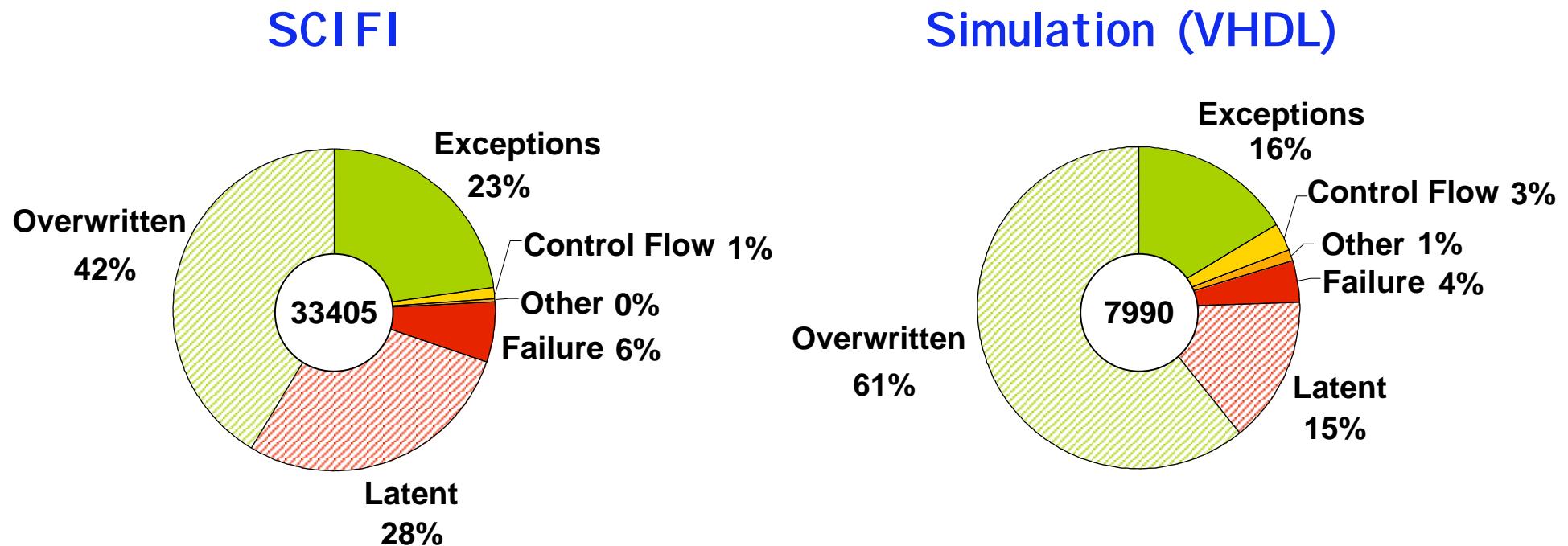
- Heavy-ion radiation
- Electromagnetic interferences
- Pin-level (forcing)



Scan Chain- Implemented Fault Injection vs. Simulation

[Folkesson *et al.* 1998 – FTCS-28]

- 32-bit Processor (Saab Ericsson Space)
- Control program

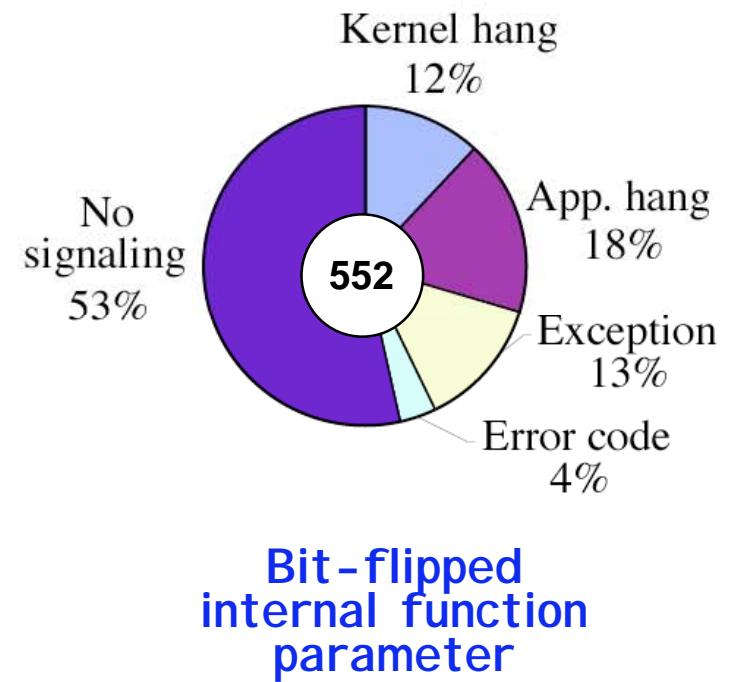
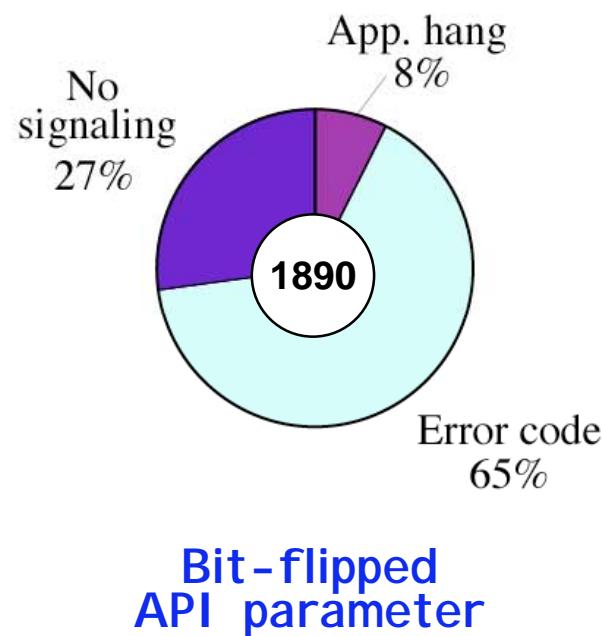
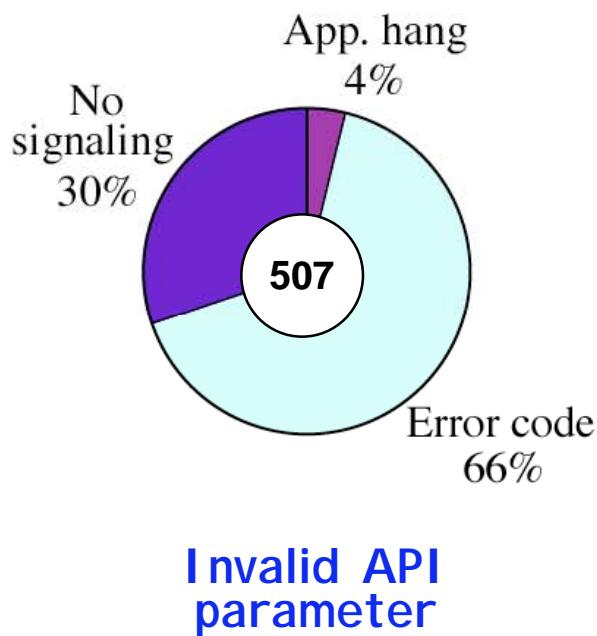


Comprehensive & Coordinated Study

- **Physical Faults** (VHDL Simulation and SWIFI)
- **Software Faults**
 - ◆ Application (Mutation, Controlled-SWIFI)
 - ◆ OS (Bit-flips on system call parameters, Invalid system call parameters, Bit-flips on internal function calls, real faults)
- **Operator & Maintenance Administrator Faults**
(emulation scripts, real faults from field data and interviews)

Software Faults in OSs

- Target:
 - ◆ Linux OS
 - ◆ Scheduling component



More information

- **DBench – Dependability Benchmarking**
[IST Project 2000-25425]
-> <http://www.laas.fr/dbench/>

- **IFIP WG 10.4 – SIGDeB**
Special Interest Group on Dependability Benchmarking
-> <http://www.dependability.org/wg10.4/SIGDeB>