From Component Reliability to System Dependability:
A Modeling and Assessment Perspective

Jean Arlat

[jean.arlat@laas.fr]

LAAS-CNRS

INSTITUT CARNOT LAAS CNRS

cnrs dépasser les frontières

Université de Toulouse

Outline

- Moving Towards a New Paradigm
- From Fault Models to Error Models
- Faultload and Workload Dimensions
- Dependability Assessment
- Conclusions

Towards A “New” Paradigm in HW

- **“More Moore Trend” (Device size ↘):**
- **Manufacturing:** Process variations ↗; Costs (lithography, testing) ↗; Yield ↘ ; Prob. defects get undetected ↗ ; Impact of defects ↗
- **Operation:** Frequency ↗; Power dissipation ↗; Parameter variation ↗; Power supply voltage ↘; Soft Error Rate ↗
- **Correctness ↘; Testability ↘; Robustness ↘**
- **From: 100% Reliability**
  To: 100% Dependability/Resilience

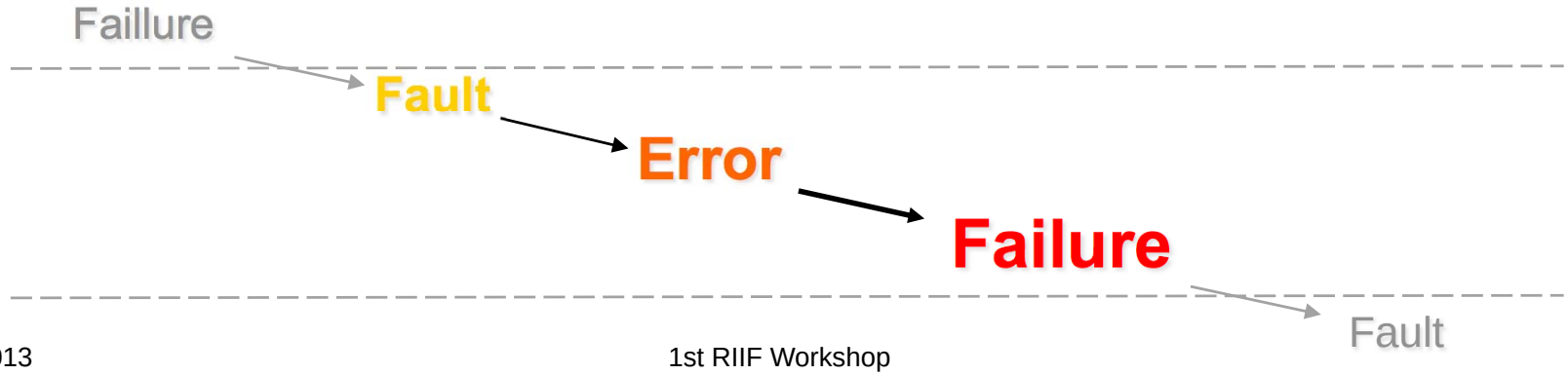
International Technology Roadmap for Semiconductors

- **Crosscutting Challenge 5: Reliability (2008 Update)**
  Reliability & Resilience (2009 Edition)
- **<u>2011 Edition/ 2012 Update</u>: Design for Reliability and Resilience confirmed as "new long-term *Grand Challenge*"**
  (together with design of concurrent software)

  "Design Technology for Resilience: A Fundamental Portion of DFM"
- **Quoting the Design Section** [http://www.itrs.net/Links/2011ITRS/2011Chapters/2011Design.pdf]
  - *Relaxing the requirement of 100% correctness for devices and interconnects may dramatically reduce costs of manufacturing, verification, and test*
  - *Such a paradigm shift will likely be forced in any case by technology scaling, which leads to more transient and permanent failures of signals, logic values, devices, and interconnects*
  - *In general, automatic insertion of robustness into the design will become a priority as systems become too large to be functionally tested at manufacturing exit*
  - *Potential solutions include automatic introduction of redundant logic and on-chip reconfigurability for fault tolerance, development of adaptive and self-correcting or self-healing circuits, and software-based fault- tolerance*

About Dependability Impairments

- **Failure**
  - deviation of the service from the accomplishment of the function of the system
    - *Function : what is the system meant for*
- **Error**
  - part of system state liable to lead to a failure
    - *Error affecting the service : evidence of failure occurrence*
- **Fault**
  - cause (attributed or supposed) of an error



Hardware Fault Pathology

Short-circuit in integrated circuit

Failure

↓

Fault

Stuck-at connection, modification of circuit function

|

Activation

Faulty component and inputs

↓

Error

|

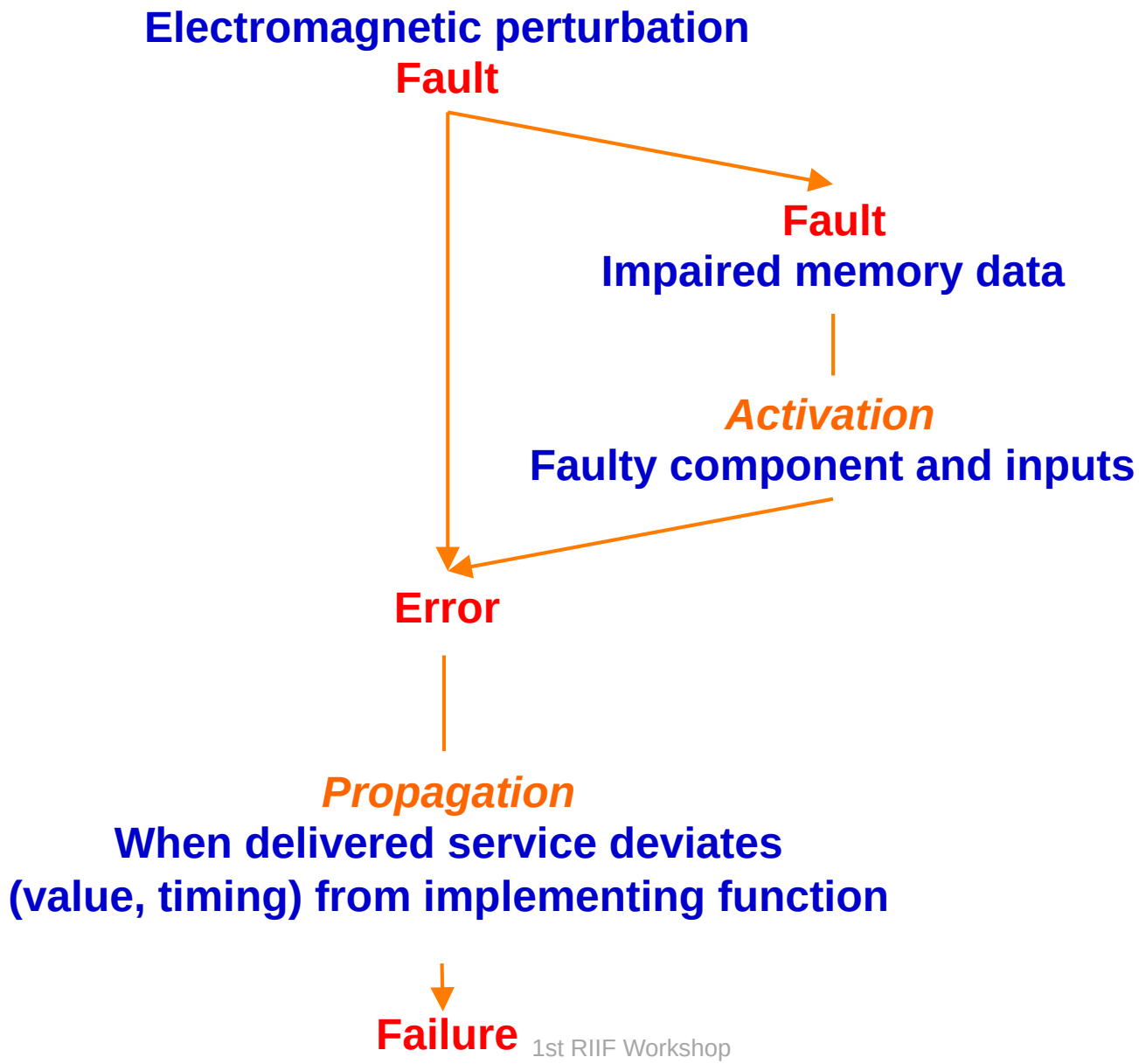
Propagation

When delivered service deviates (value, timing) from implemented function

↓

Failure

Environment Fault



Software Fault Pathology

Error of a programmer

Fault
Impaired instructions or data

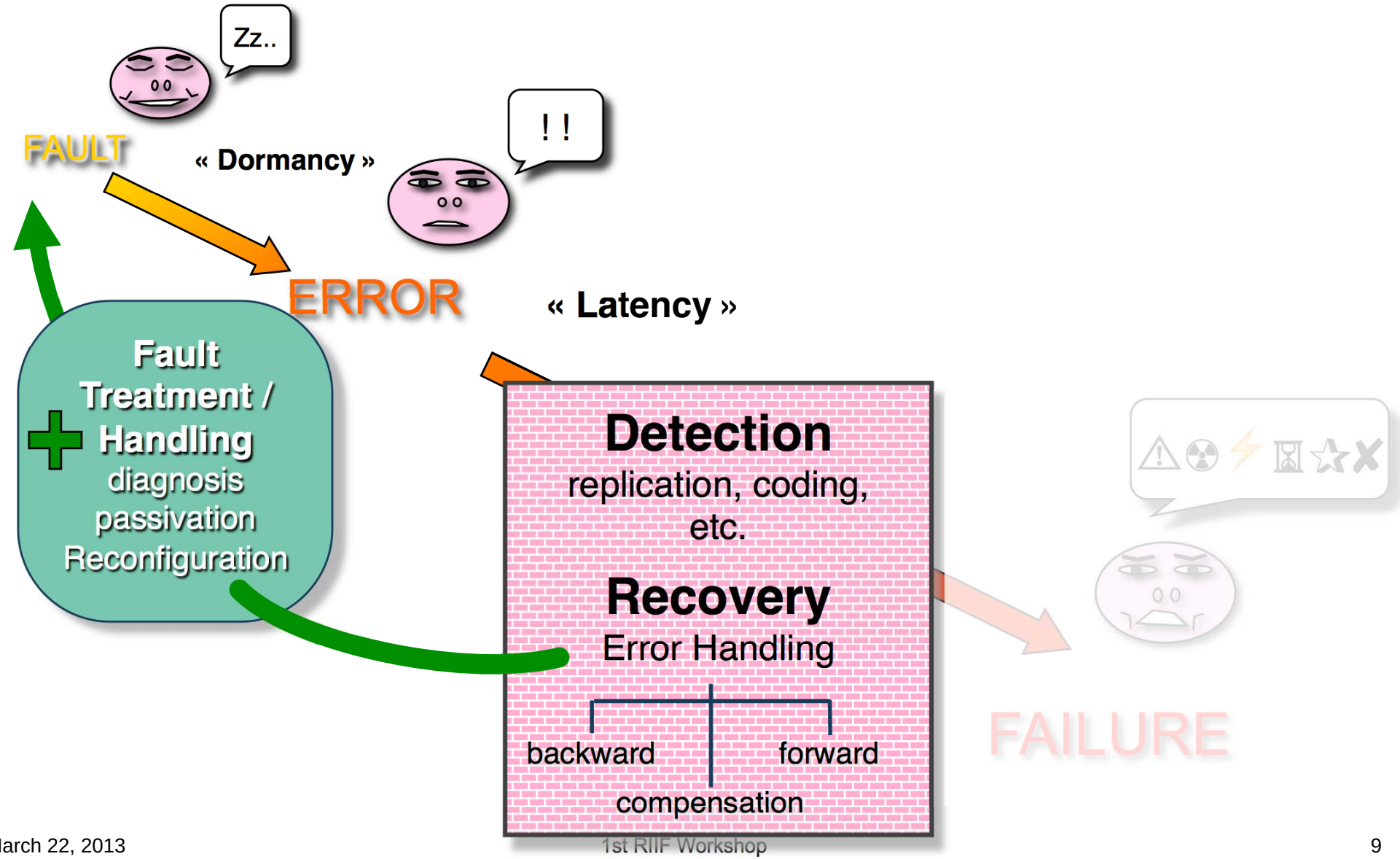
Activation
Faulty component and inputs

Error

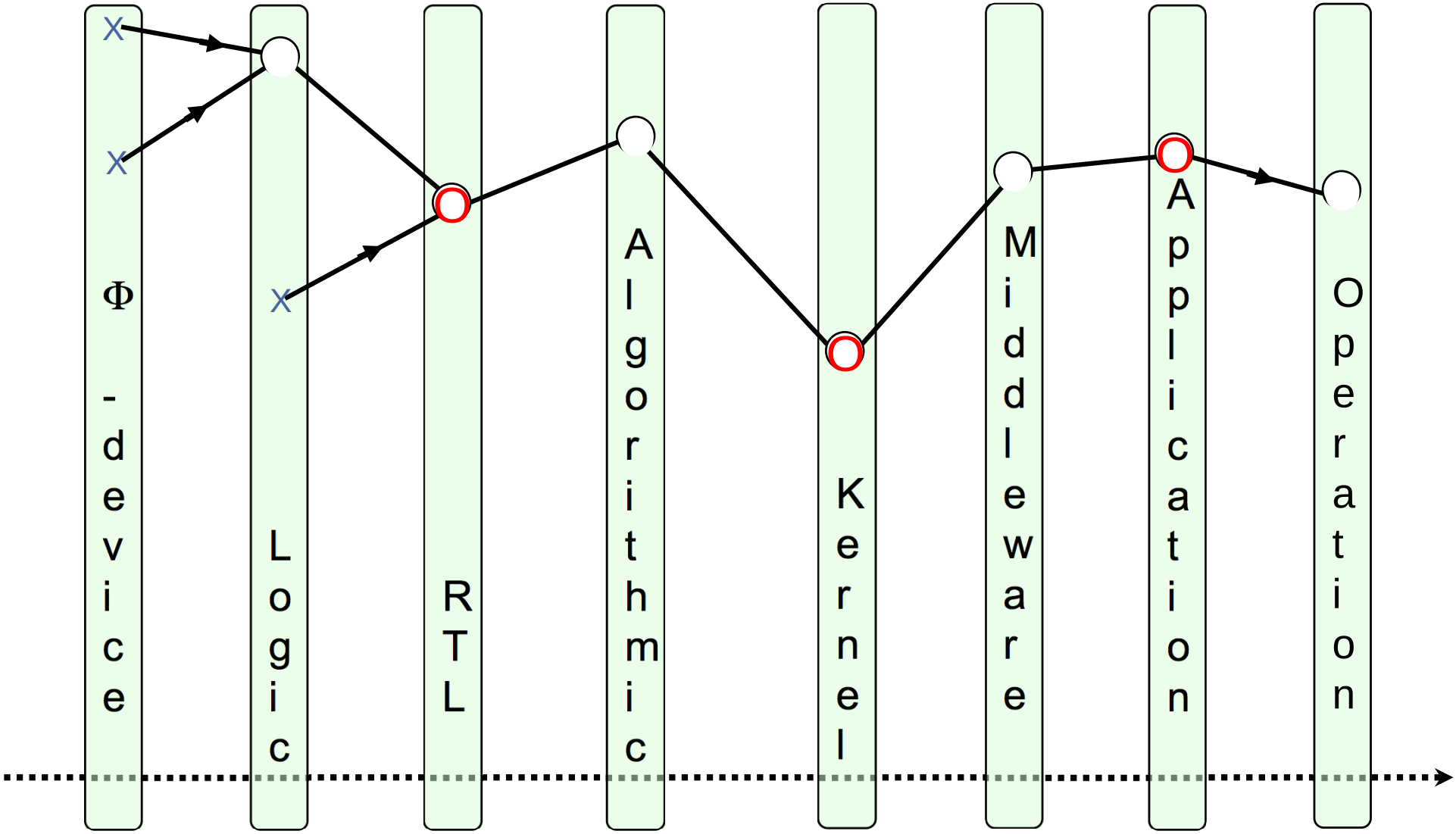
Propagation
When delivered service deviates (value, timing)
from implementing function

Failure

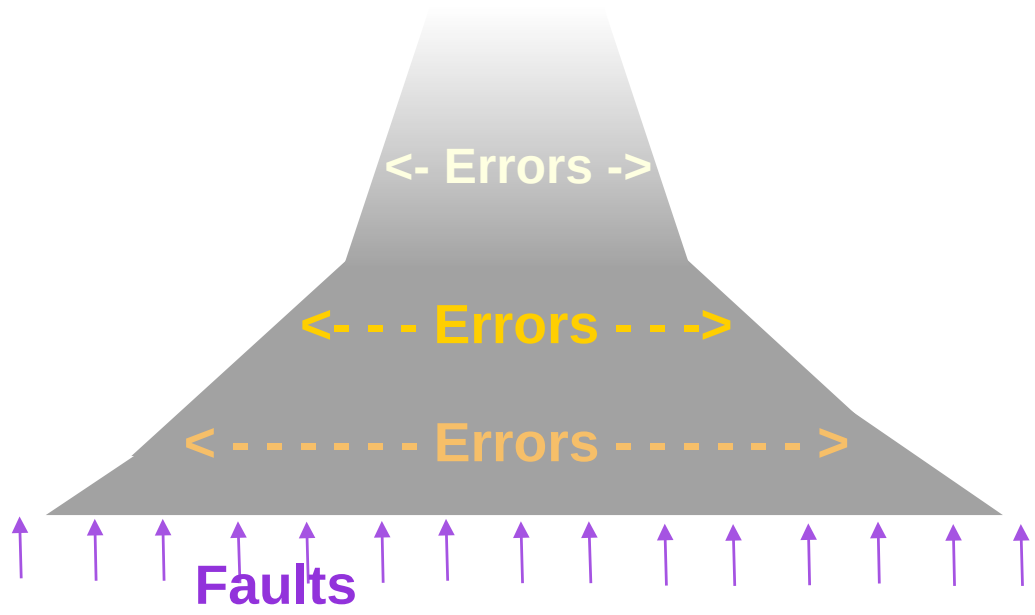
Fault Tolerance



System Levels … and Fault Pathology



The Fault/Error Cone



- **Fault Equivalence**
- **Fault Collapsing**

=> Manage Errors rather than Faults…

Dependability Assessment

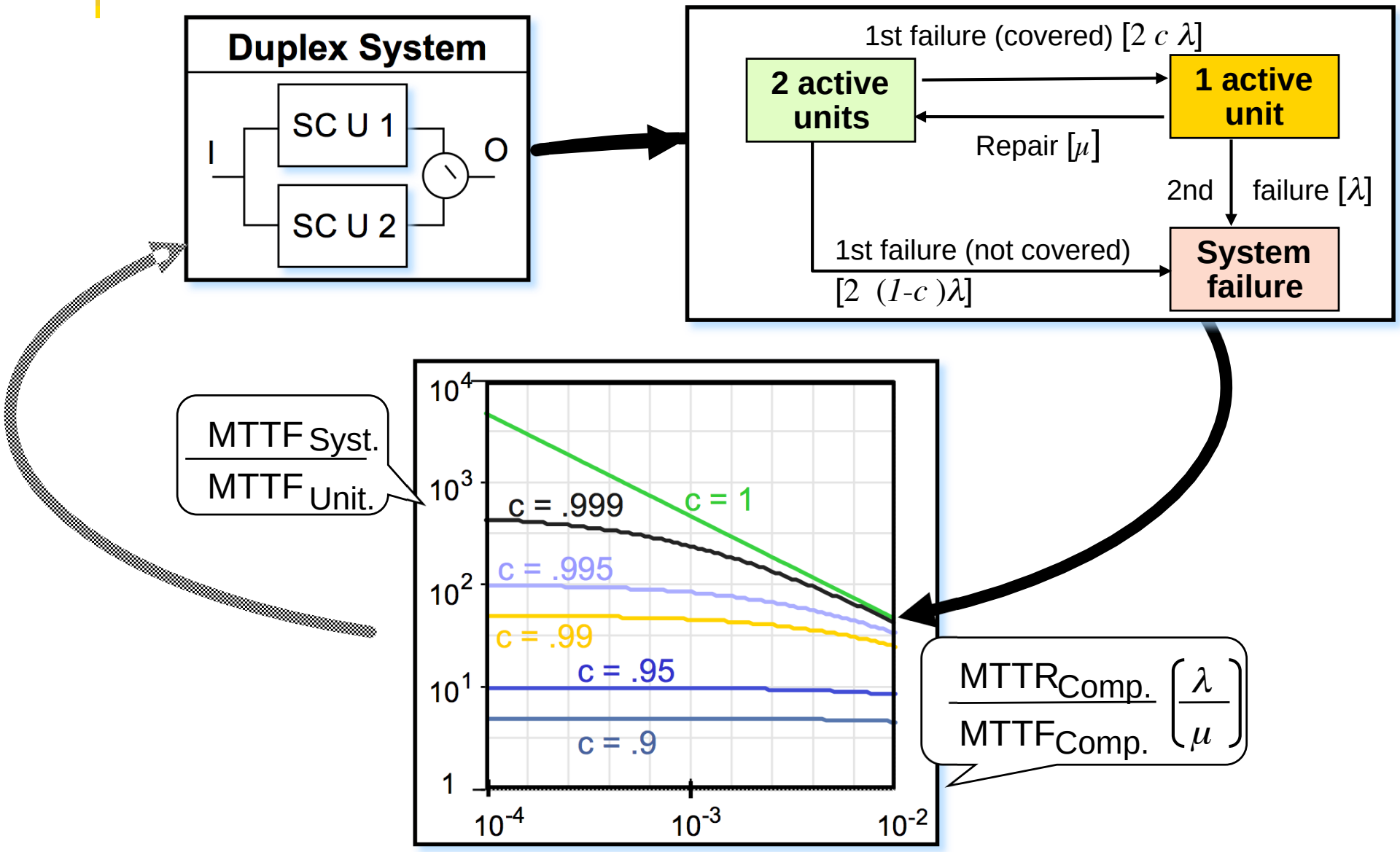
- **Objectives**
  - **Evaluation of Dependability Measures (Reliability, Availability, etc.)**
  - **Verification of Properties**
    - Nominal Service
    - Service in presence of Faults
  - **Characterization of Behavior in Presence of Faults**
    - Failure modes
    - Efficiency of fault tolerance
- **Methods and Techniques**
  - **Axiomatic**
    - Static analysis
    - Model checking
    - Stochastic processes
  - **Simulation**
    - Functional
    - Fault
  - **Empirical**
    - Field measurement
    - Robustness testing
    - Fault injection

Impact of Fault Tolerance

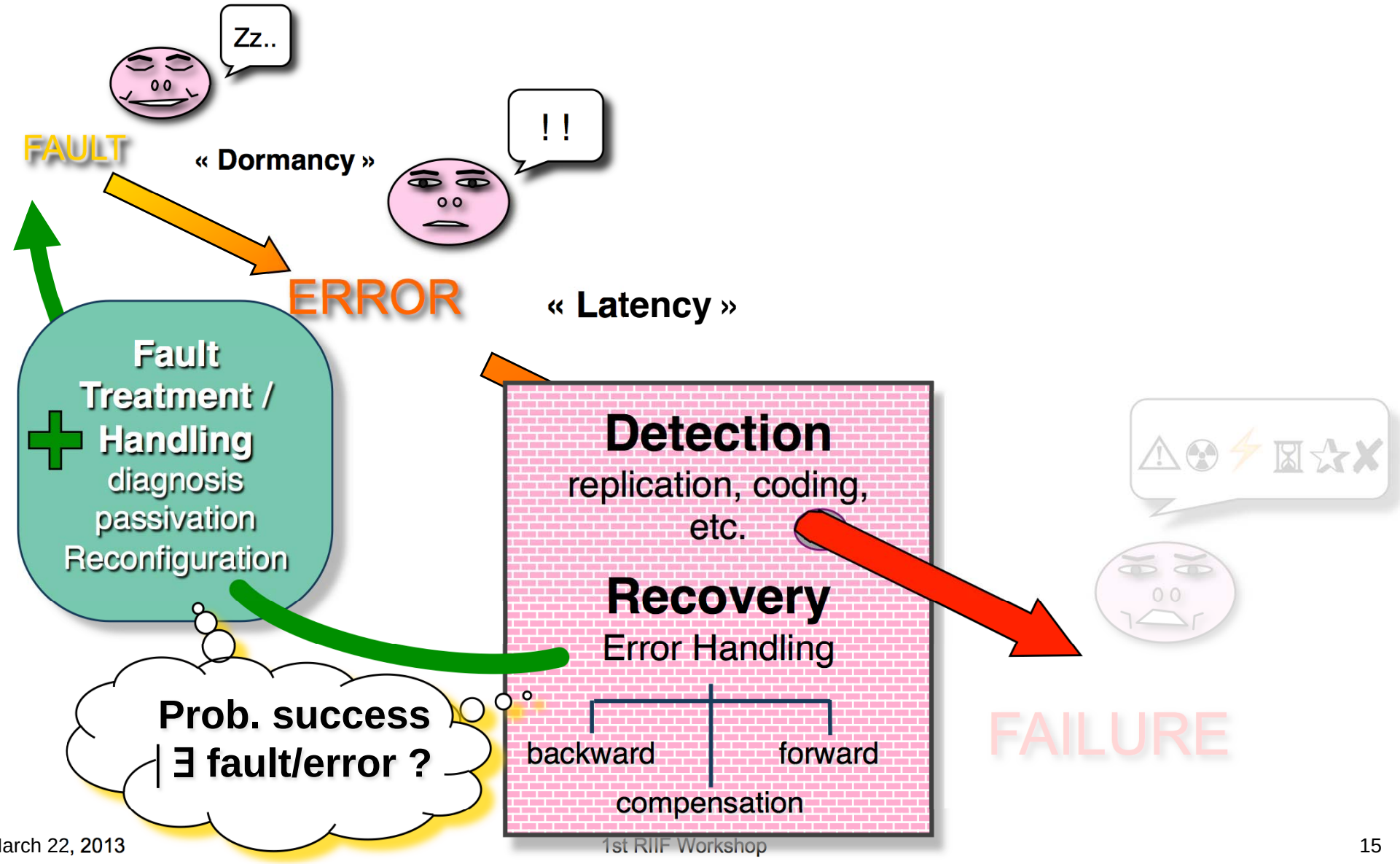
Dependability ≈ 1 - Pr{fault} × Pr{error/fault} × Pr{failure/error}

↓ System Impairments →	Fault	Error/Fault	Failure/Error
Non Fault-Tolerant (NFT)	$Pr_{NFT}\{fault\}$	$Pr_{NFT}\{error/fault\}$	$Pr_{NFT}\{failure/error\}$
	∧	∧	∨
Fault-Tolerant (FT)	$Pr_{FT}\{fault\}$	$Pr_{FT}\{error/fault\}$	$Pr_{FT}\{failure/error\}$

Impact of Coverage on Dependability



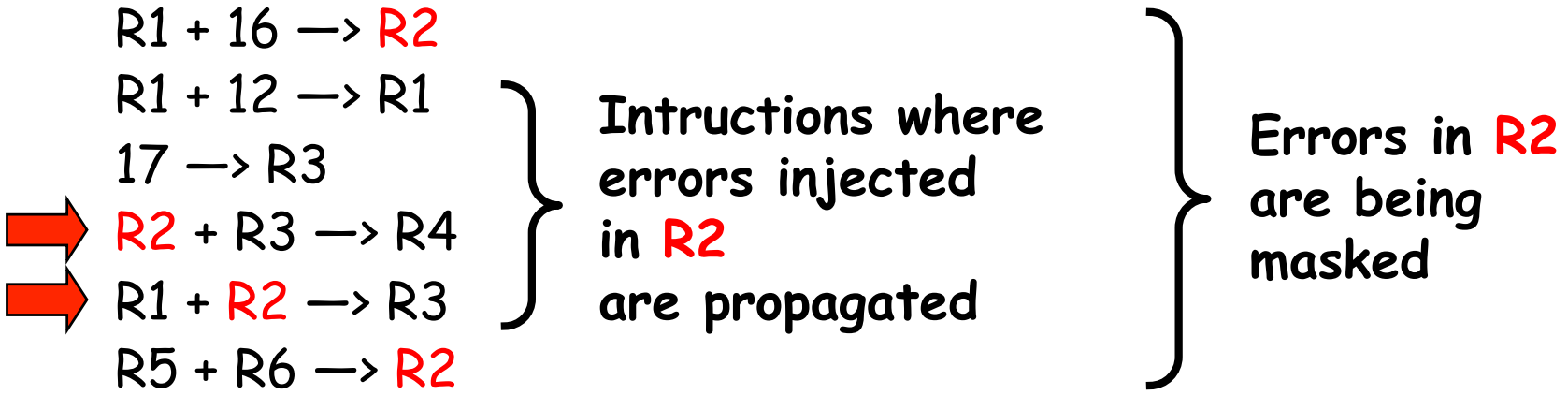
Fault Tolerance … and Coverage



The Dual Perspective

- **Dependability Assessment based on Hardware Reliability Modeling Only —> Conservative Measures**
- **Fault-effect "Masking"**
  - The fault affects an idle resource
  - The error created is erased
- **In addition to Faults (and related technological and environmental parameters), another essential facet is the Activity dimension**
- **Faultload + Workload => "Errorload"**
- **Resource allocation (fault activation), Data processing (error manipulation)**
- **=> The Software!**

Impact of Software on Hardware Faults



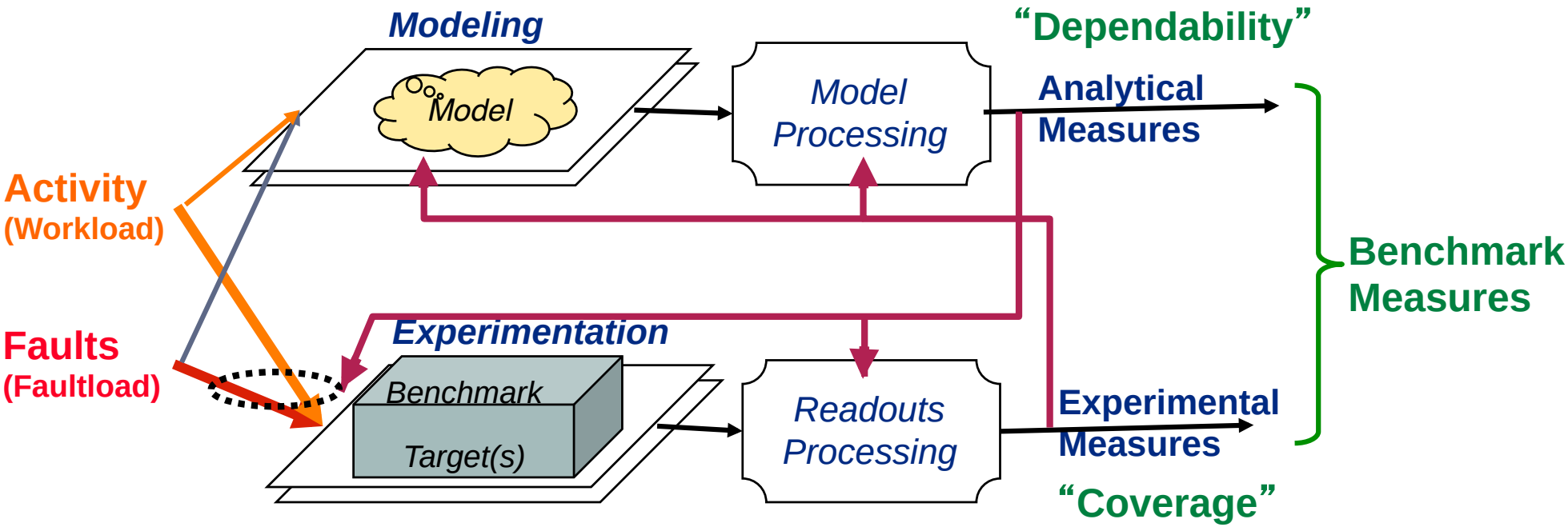
The Fault Injection perspective :

- Increase of 1 order of magnitude in the "effectiveness" of faults
- Reduction of the *F* set: 2 orders (CPU reg.); 4-5 (data mem.), still with similar estimation of coverage

R. Barbosa, J. Vinter, P. Folkesson, J. Karlsson
Assembly-Level Pre-injection Analysis for Improving Fault Injection Efficiency
EDCC-5, Budapest, Hungary, 2005

=> The dependability assessment perspective

A Comprehensive Dependability Assessment Frame



IST Project DBench (*Dependability Benchmarking*)

Dependability Assessment Perspective

- **High-level models of a complex component (e.g., a microprocessor) — Area-based**
- **Accounting explicitly for processing (operators) and storage (data) resources and their activation**
  - Fault Injection (in Simulation) Experiments for Consolidation and Validation => Very similar results
  - Much less conservative figures than usual raw reliability evaluation

=> Necessary and highly promising

A. Savino, S. Di Carlo, G. Politano, A. Benso, A. Bosio, G. Di Natale
Statistical Reliability Estimation of Microprocessor-Based Systems
IEEE Trans. on Computers, Vol.61, no11, Nov. 2012, pp. 1521-1534

Concluding Remarks

- **Reliability-aware frameworks such as the one proposed by RIIF Initiative are very much needed and useful**
- **Dependability Assessment requires a System-level viewpoint that should accommodate Hardware and Software issues**
- **Both Modeling/Analytical and Experimentation/ Empirical dimensions are to be considered**
- **Probably, link to be made with Fault Injection and Dependability Benchmarking Initiatives?**

About Dependability Benchmarking

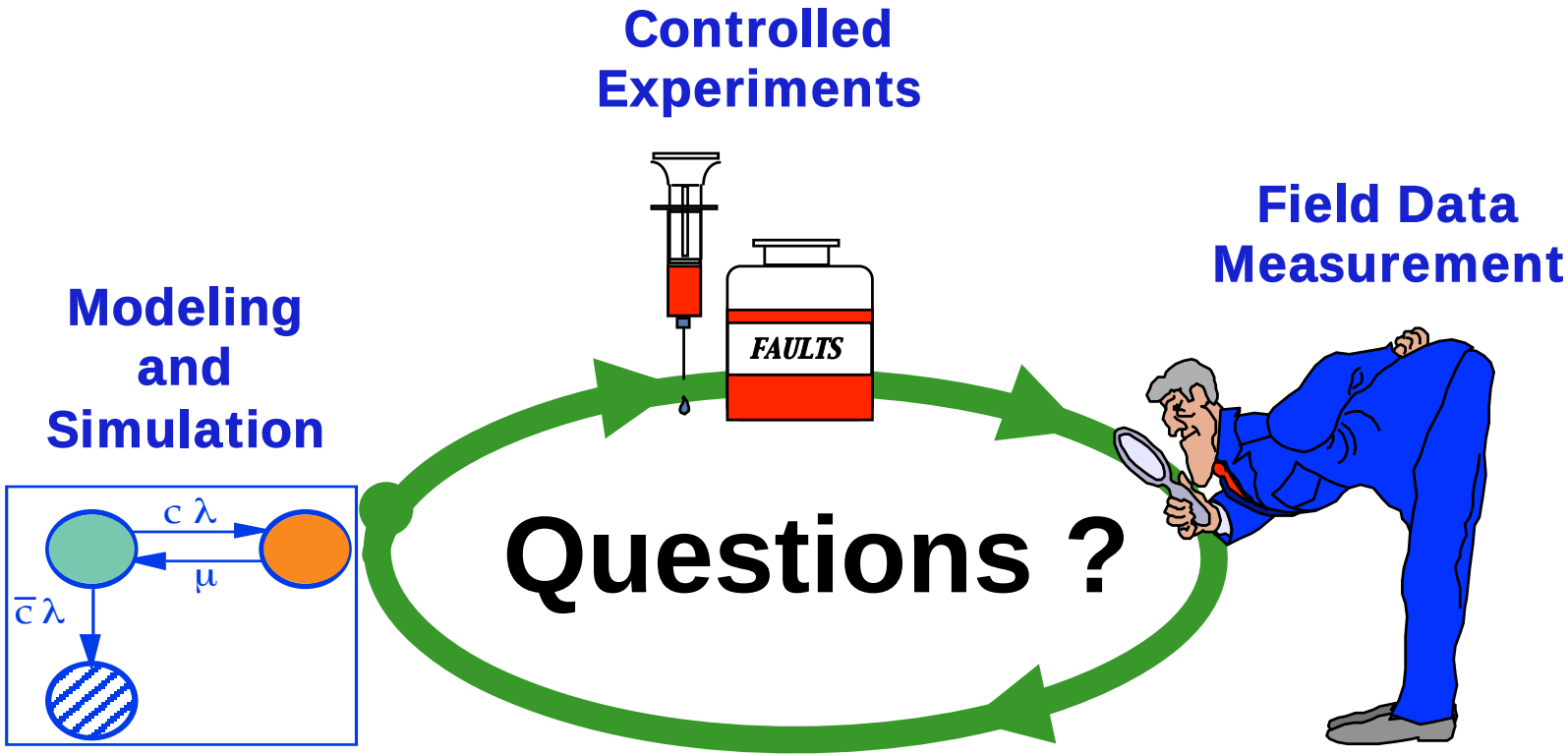
- IST Project ***DBench (Dependability Benchmarking)***
  www.laas.fr/DBench and www.dbench.org

- ***IFIP WG 10.4 SIG on Dependability Benchmarking***
  http://homepages.laas.fr/kanoun/ifip_wg_10_4_sigdeb/

- **K. Kanoun and L. Spainhower, Eds.**
  Dependability Benchmarking for Computer Systems**,**
  IEEE CS Press and Wiley, 2008

- ***IST CA AMBER - Assessing, Measuring, and Benchmarking Resilience***
  http://amber-dbserver.dei.uc.pt:8080/repository/main.action

Thank you!


Controlled
Experiments
Field Data
Measurement
Modeling
and
Simulation
FAULTS
Questions ?
c λ
μ
c̄ λ