

Ministry of Science and Technology of China  
*Forum on High-end Fault-tolerant Computers*  
Beijing, China — April 16, 2010

---

# Dependability Assessment of Computing Systems: Analytical Evaluation & Controlled-Experiments

Jean Arlat

[[jean.arlat@laas.fr](mailto:jean.arlat@laas.fr)]



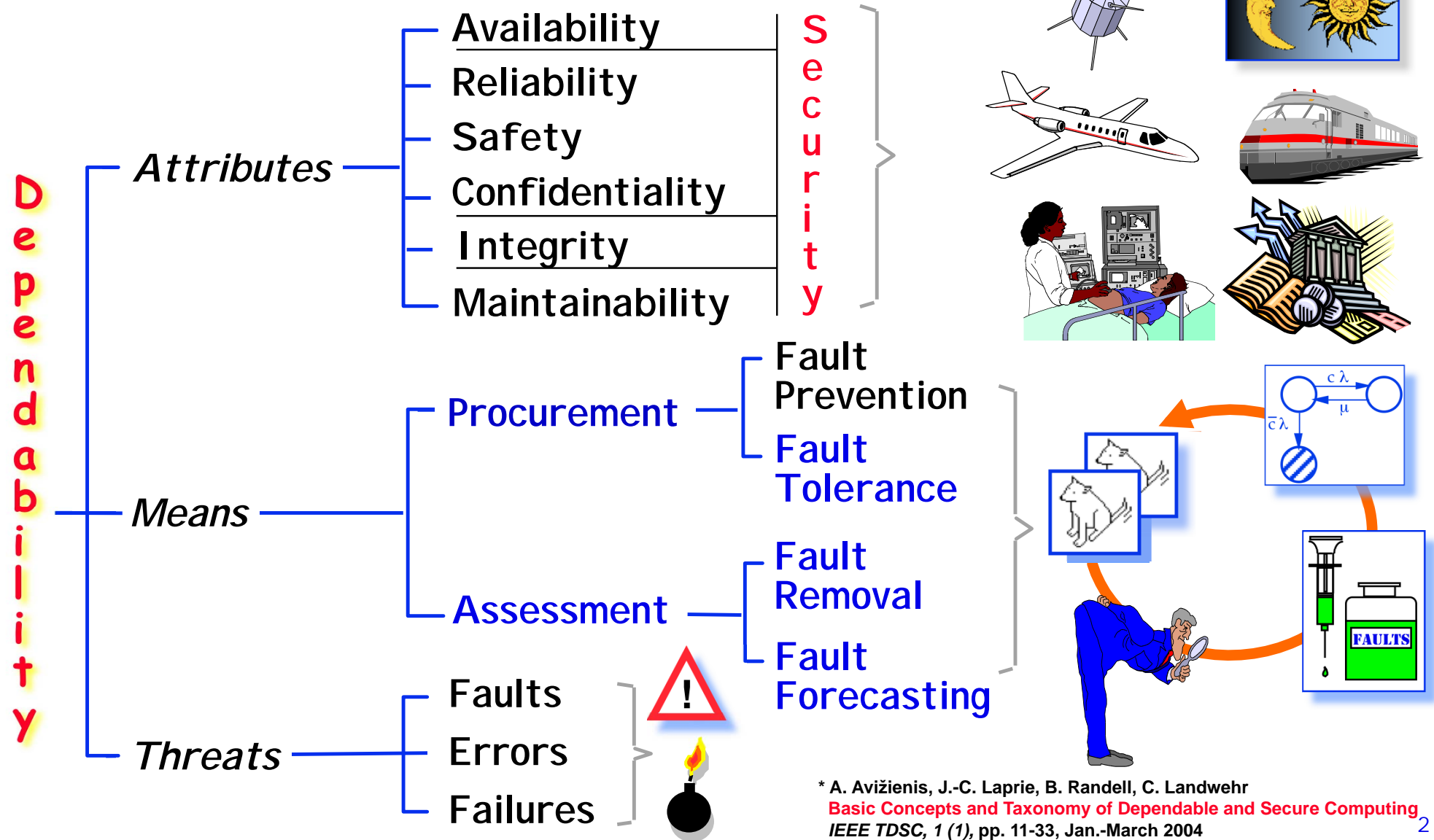
Université  
de Toulouse

---

LAAS-CNRS

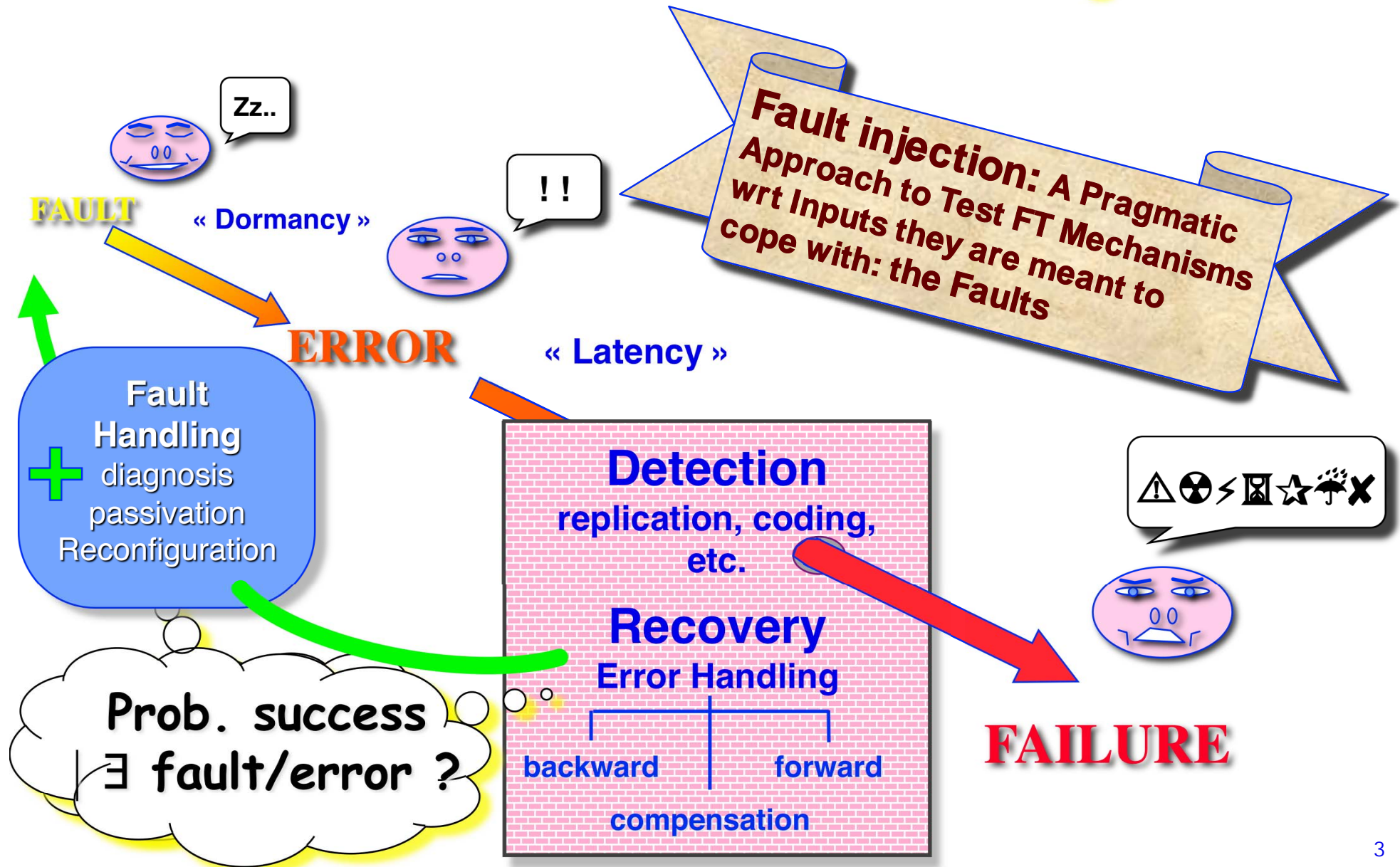
---

# The "Dependability Tree" \*

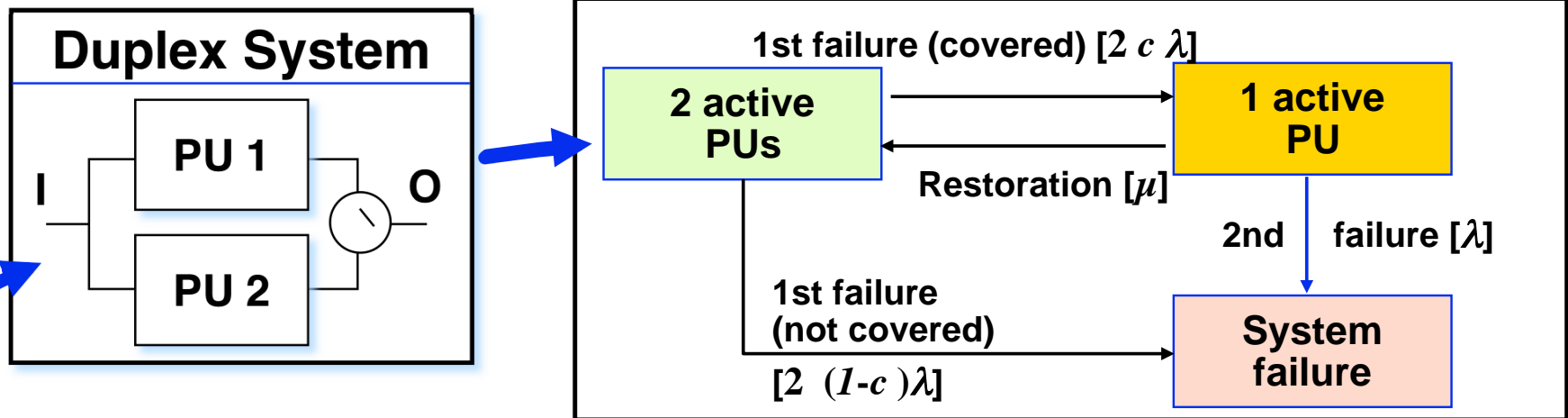


\* A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr  
 Basic Concepts and Taxonomy of Dependable and Secure Computing  
 IEEE TDSC, 1 (1), pp. 11-33, Jan.-March 2004

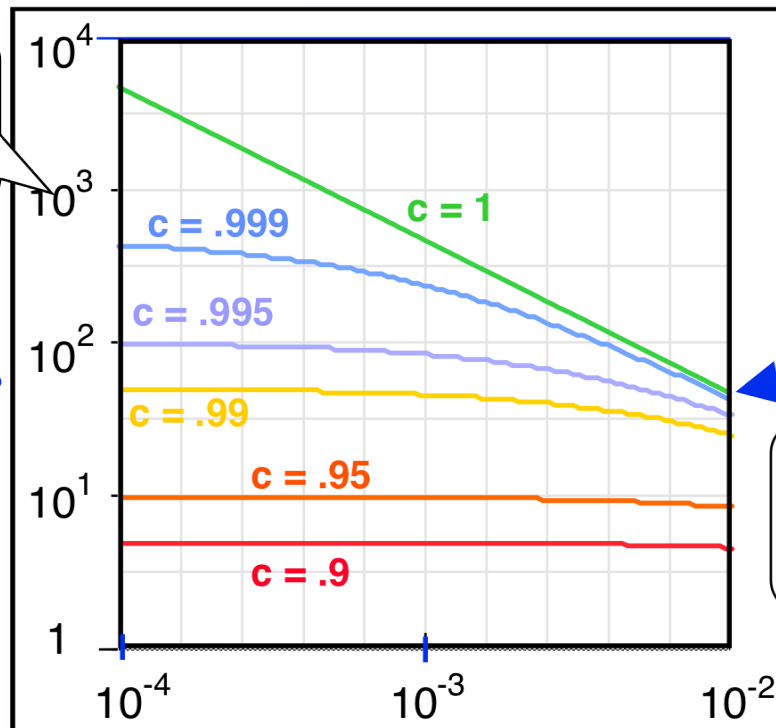
# Fault Tolerance ... and Coverage



# Impact of FT Coverage on Dependability

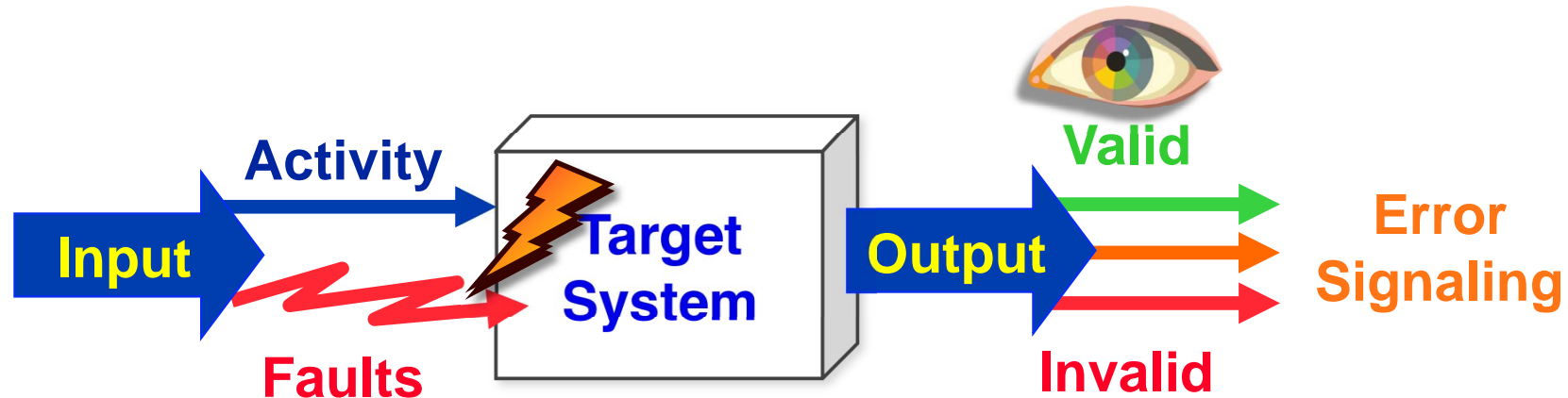


$$\frac{\text{MTTF}_{\text{DS}}}{\text{MTTF}_{\text{PU}}}$$



$$\frac{\text{MTTR}_{\text{PU}}}{\text{MTTF}_{\text{PU}}} \left( \frac{\lambda}{\mu} \right)$$

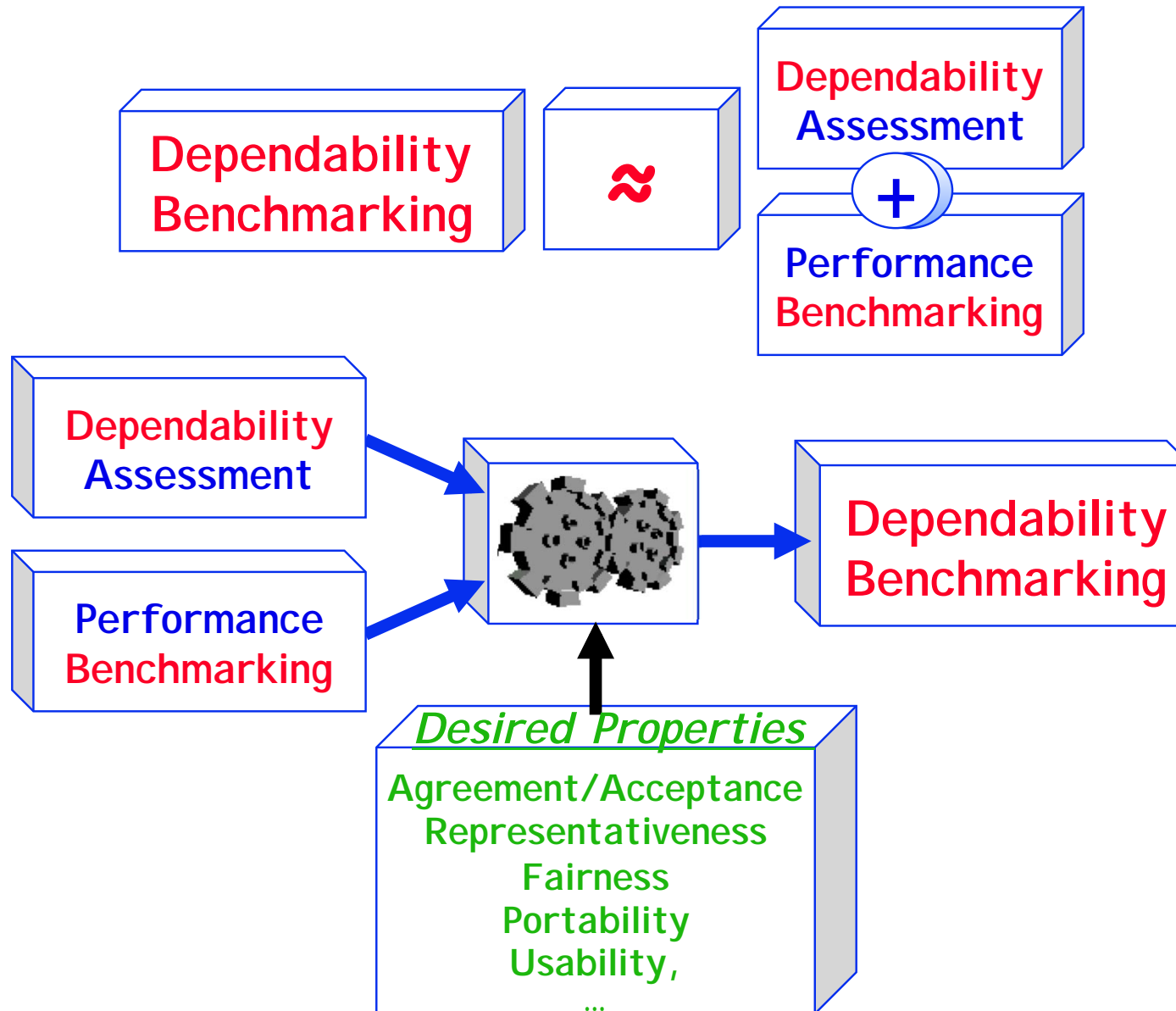
# Fault Injection-based Assessment



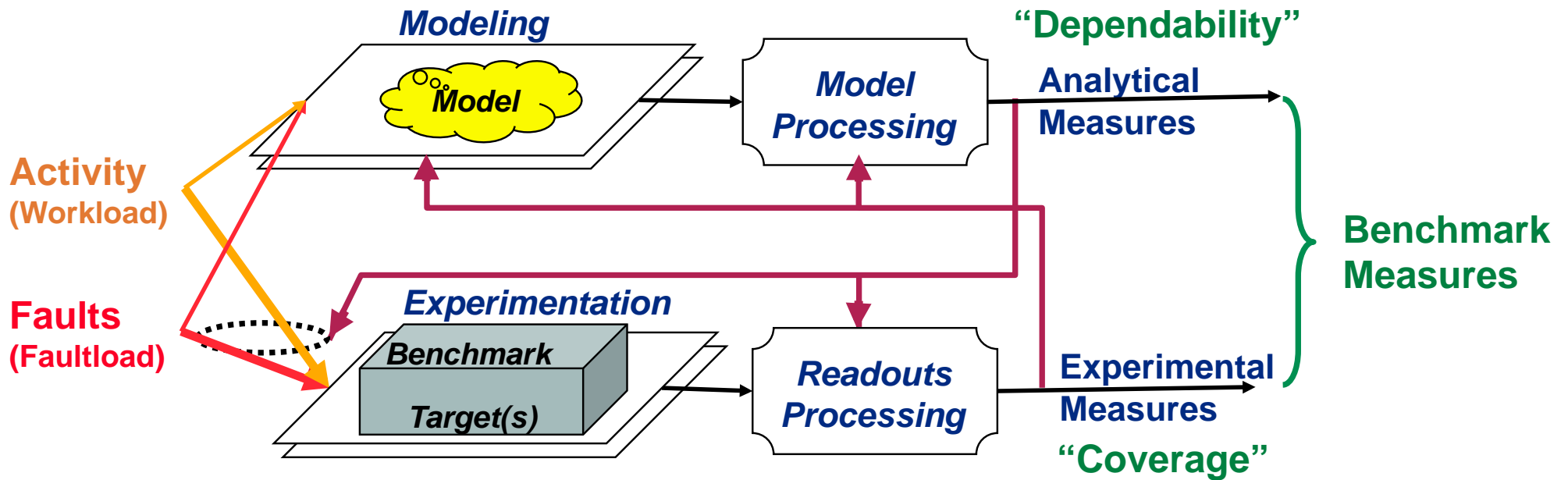
—> **Partial** dependability assessment:  
controlled application of fault/error conditions

- **Testing and evaluation** (*measurement*) of a fault-tolerant system and of its FT algorithms & mechanisms
- **Characterization** (*measurement*) of faulty behaviors and failure modes of **several** systems/components
  - > *Benchmarking*

# Dependability Benchmarking



# A Comprehensive Dependability Assessment Frame



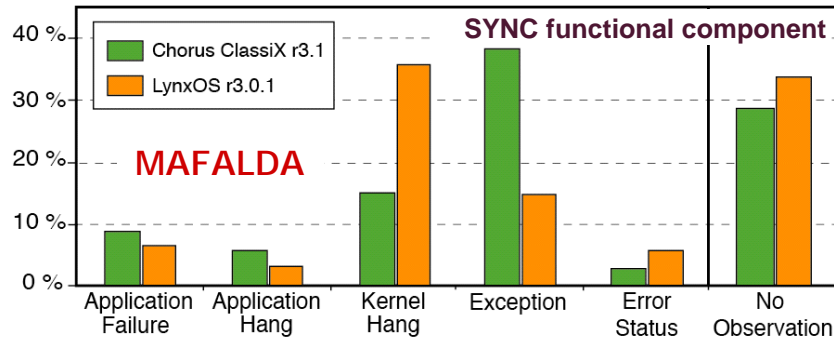
IST Project **DBench** (*Dependability Benchmarking*) — [www.laas.fr/DBench](http://www.laas.fr/DBench) and [www.dbench.org](http://www.dbench.org)



—> Minimal set of data needed from the Target System(s)  
(architecture, configuration, operation, environment, etc.)  
to derive actual dependability attributes?

# Examples of Benchmarking Results

## Bit-flips into code segment

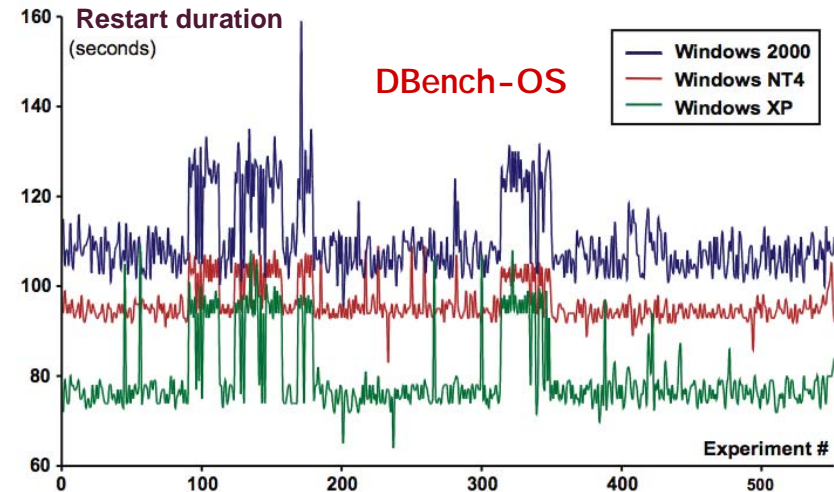


J. Arlat, J.-C. Fabre, M. Rodríguez, F. Salles

*Dependability of COTS Microkernel-Based Systems*

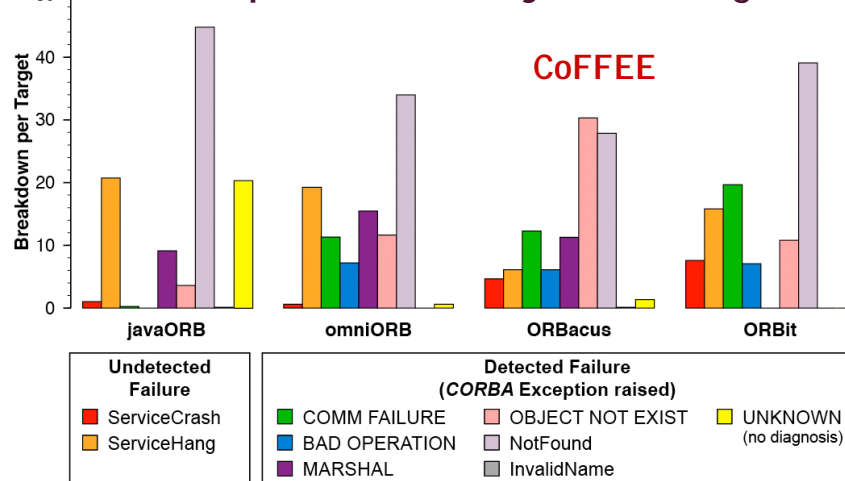
IEEE Trans. Computers vol. 51, no. 2, pp. 138-163, February 2002.

## System call parameter corruption at API



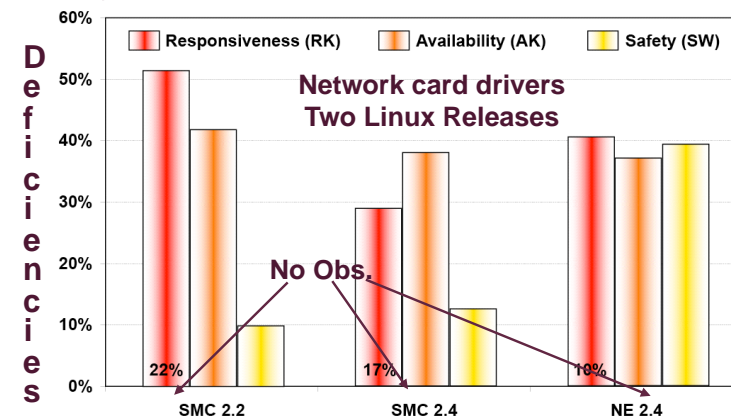
K. Kanoun, Y. Crouzet, A. Kalakech, A.E. Rugina, "Windows and Linux Robustness Benchmarks with respect to Application Erroneous Behavior", *Dependability Benchmarking for Computer Systems*, (K. Kanoun, L. Spainhower, Eds.), pp. 227-254, 2008

## Bit-flips into interobject messages



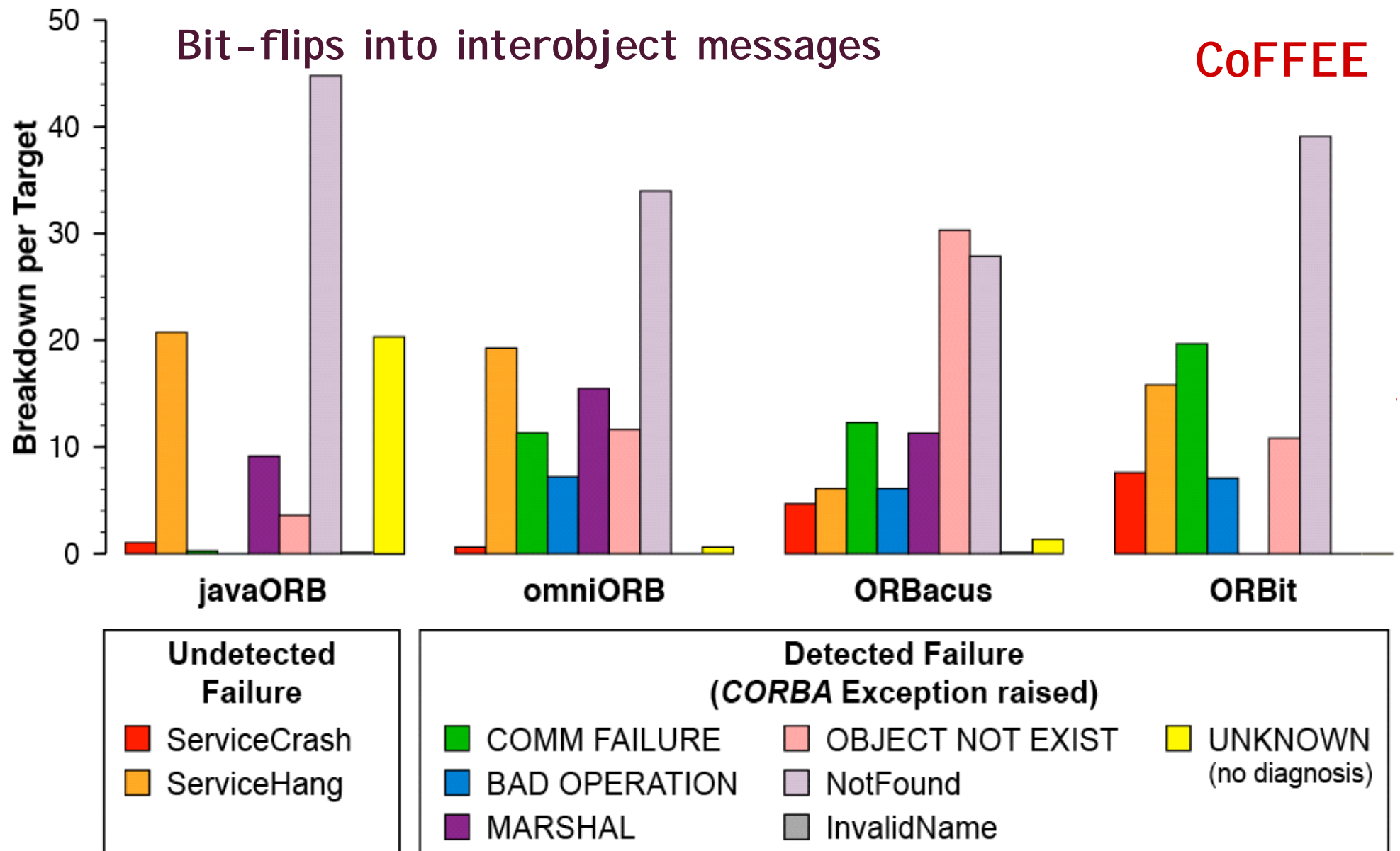
E. Marsden, J.-C. Fabre, J. Arlat, "Dependability of CORBA Systems: Service Characterization by Fault Injection," Proc. SRDS-2002, Osaka, Japan, 2002, pp. 276-285.

## System call parameter corruption at DPI

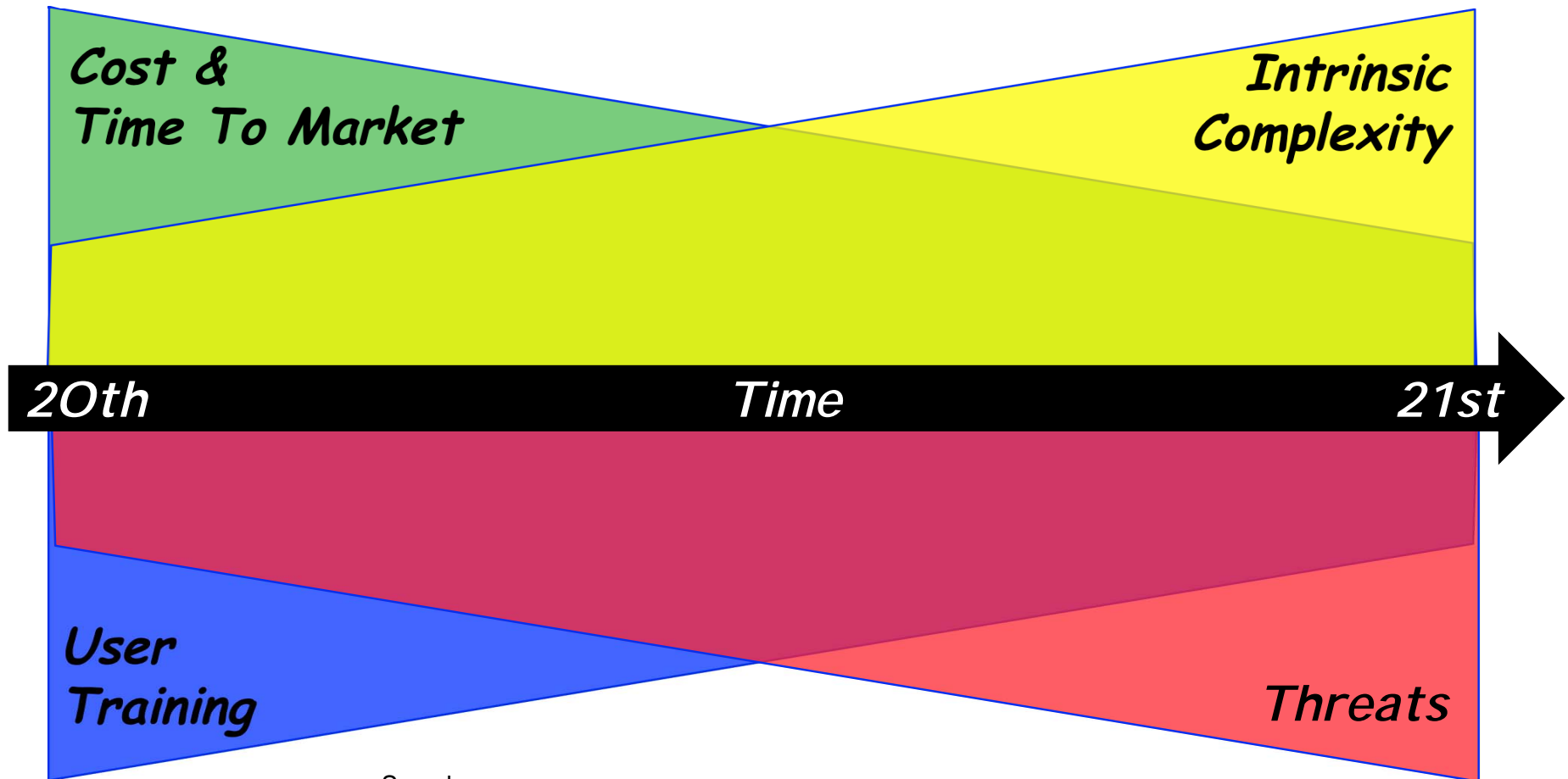


A. Albinet, J. Arlat, J.-C. Fabre, "Benchmarking the Impact of Faulty Drivers: Application to the Linux Kernel", *Dependability Benchmarking for Computer Systems* (K. Kanoun, L. Spainhower, Eds.), pp. 285-310, 2008.

# Examples of Benchmarking Results



# Looking Ahead: An Ever Moving Target



See also:

D. Siewiorek, R. Chillarege, Z. Kalbarczyk

*Reflections on Industry Trends and Experimental Research in Dependability*

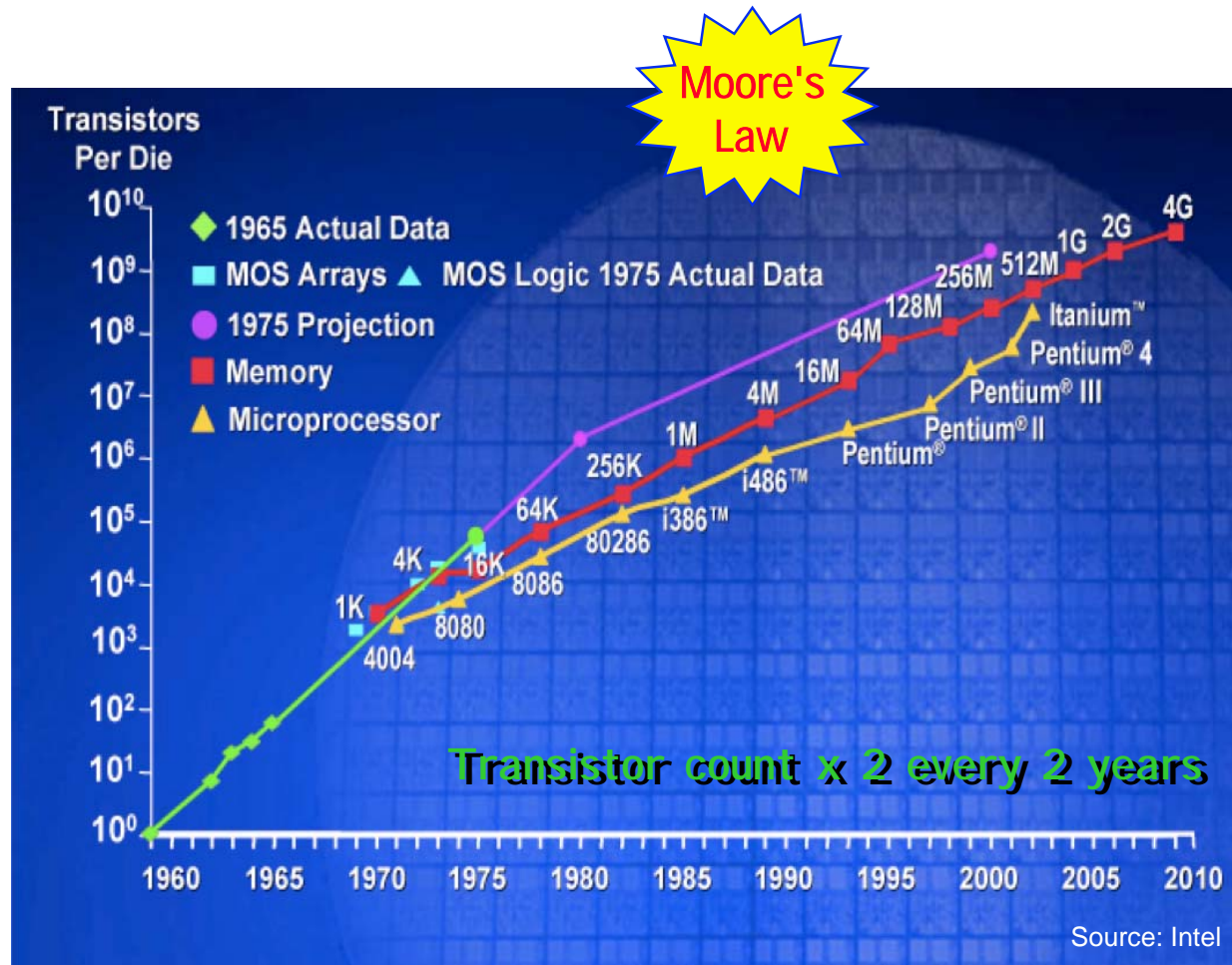
*IEEE TDSC*, Vol. 1, No. 2, April-june 2004, pp. 109-127.

D. Siewiorek, X-Z. Yang, R. Chillarege, Z. Kalbarczyk

*Industry Trends and Research in Dependable Computing*

*Chinese Journal of Computers*, Vol. 30, No. 10, 2007, pp.1645-1661.

# Trend in Hardware Technology



- Performance ↗
- Clock frequency ↗
- ...

But:

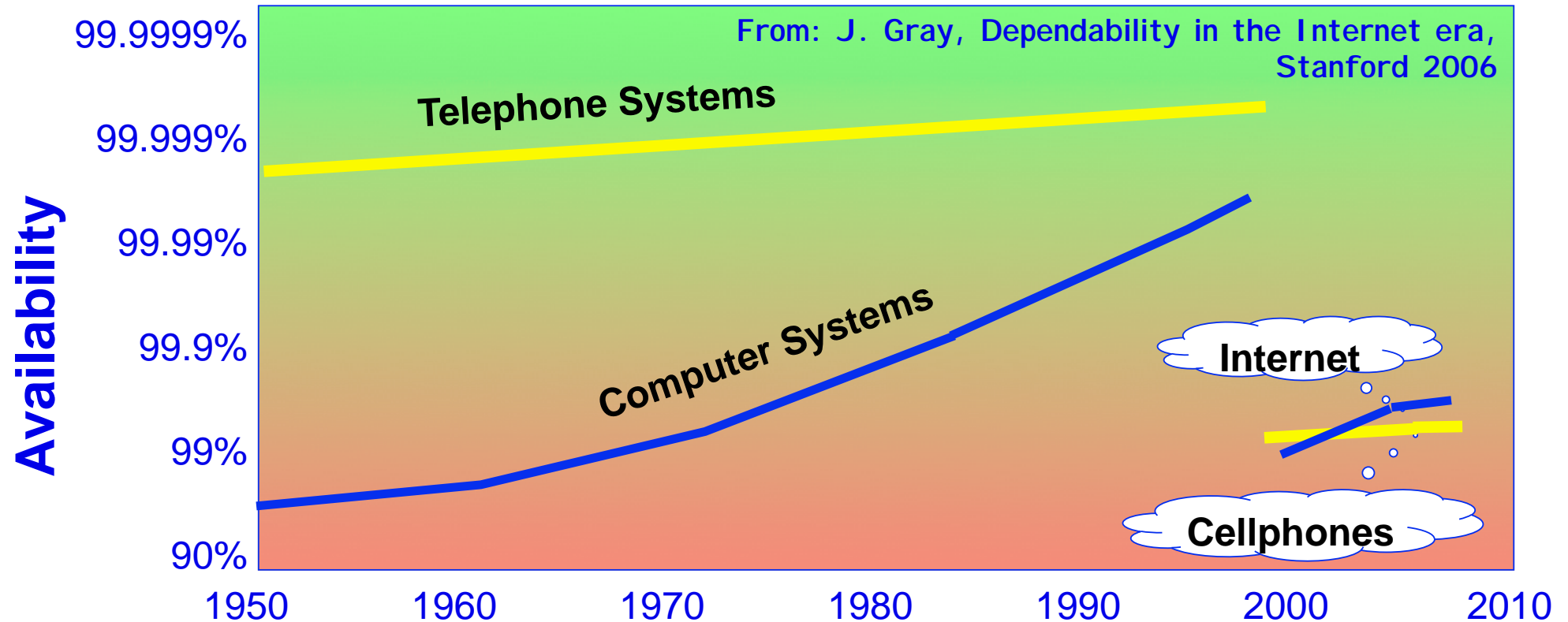
- Power dissipation ↗
- Process variations ↗
- Manufacturing costs ↗
- Yield ↘
- Prob. Defects undetected ↗
- Soft Error Rate ↗

Less than Perfect" Circuits (Manufacturing Defects and Transient Faults)

—> Resilience Achieved via Redundancy Techniques

See: International Technology Roadmap for Semiconductors — 2008 Update — Crosscutting Challenge 5: Reliability 11

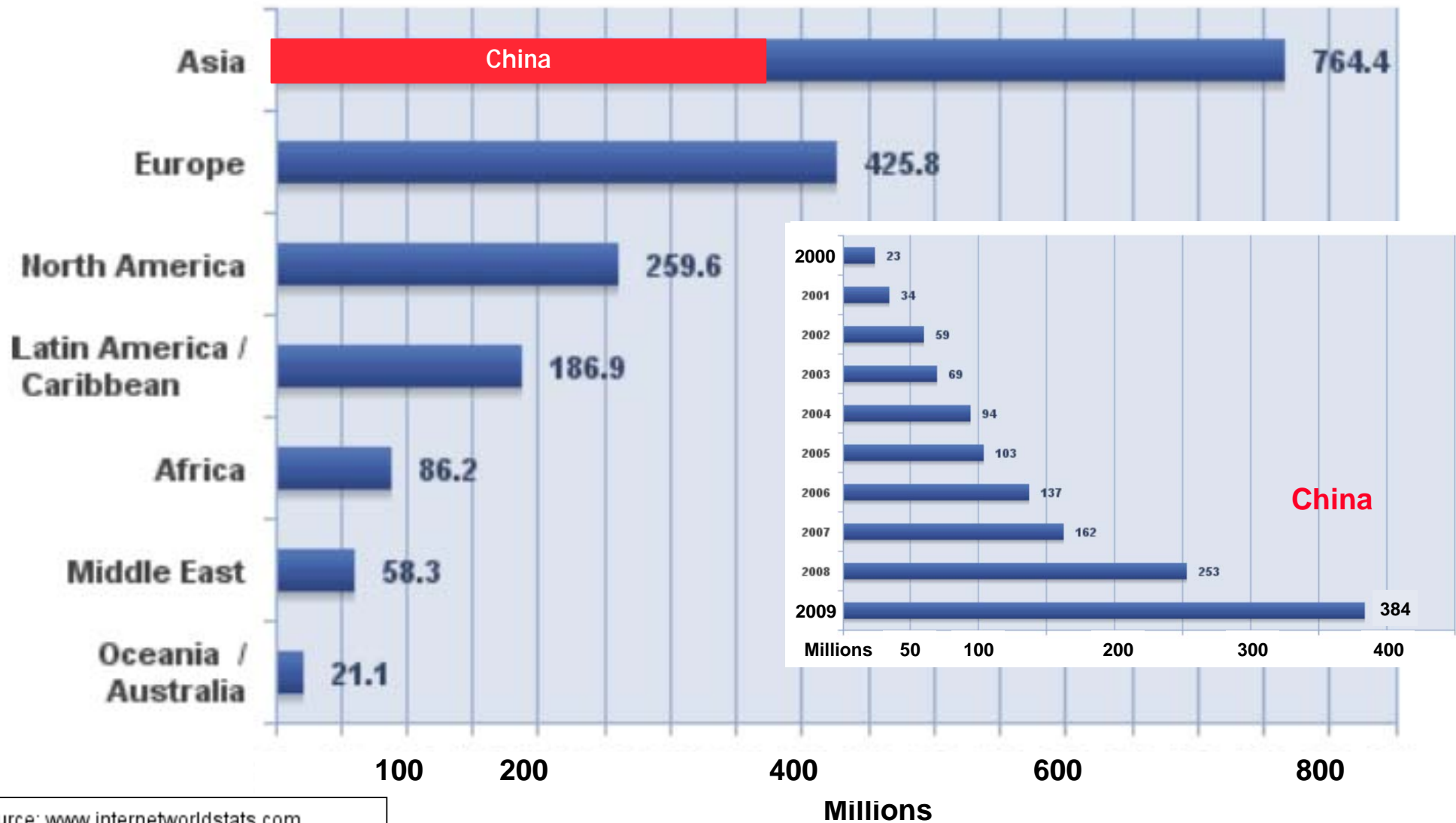
# Evolution of Information Infrastructures



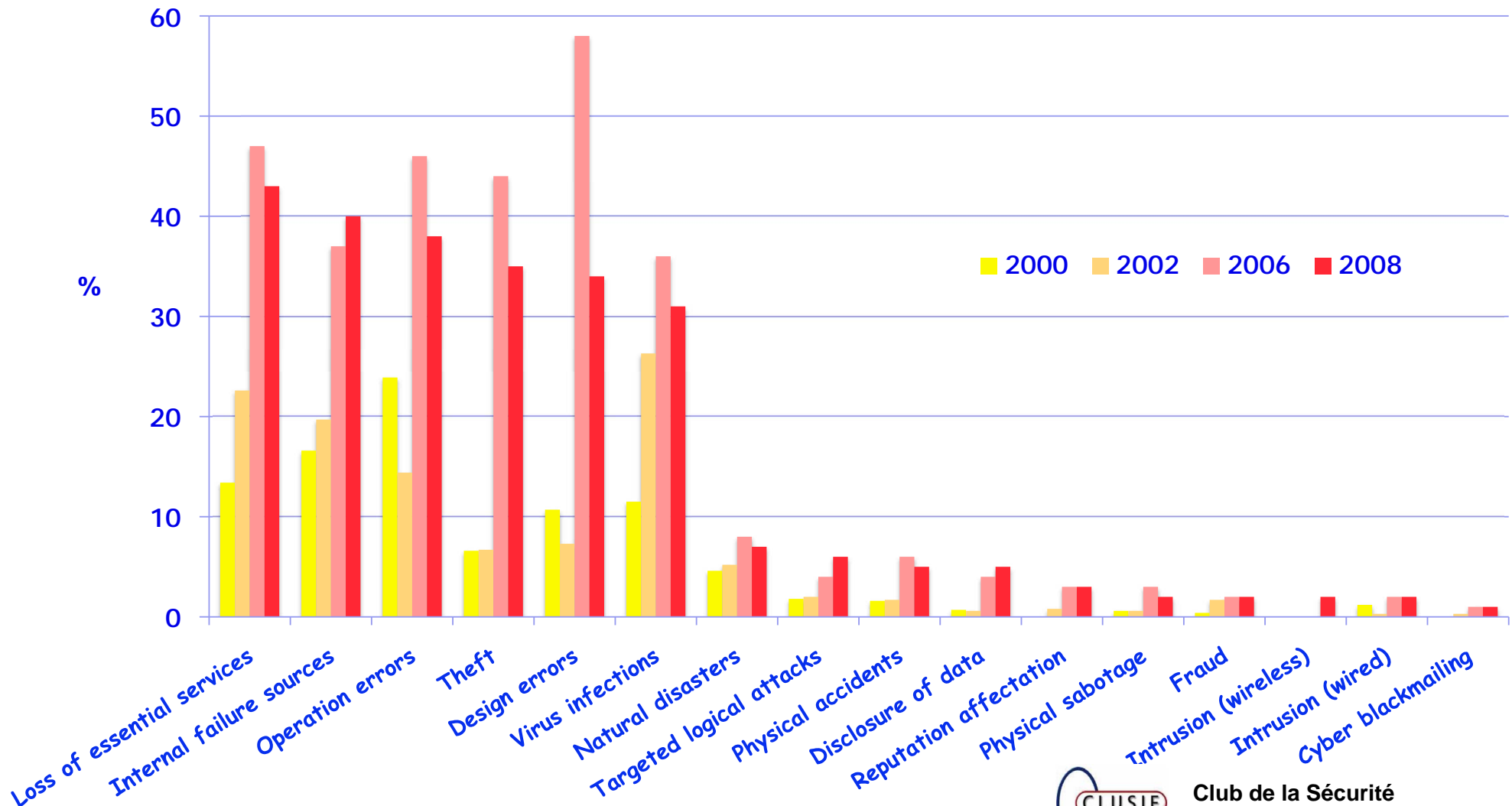
- Enhanced Functionalities and Complexity
- Economic Pressure → reuse (COTS components)
- Intrusions, Attacks,...

Availability		Unavailability per year
6 x '9'	0,9999999	32s
5 x '9'	0,999999	5mn 15s
4 x '9'	0,99999	52mn 34s
3 x '9'	0,9999	8h 46mn
2 x '9'	0,99	3d 16h
1 x '9'	0,9	36d 12h

# Internet Users ( $\approx 1.8 \cdot 10^9$ — end 2009)

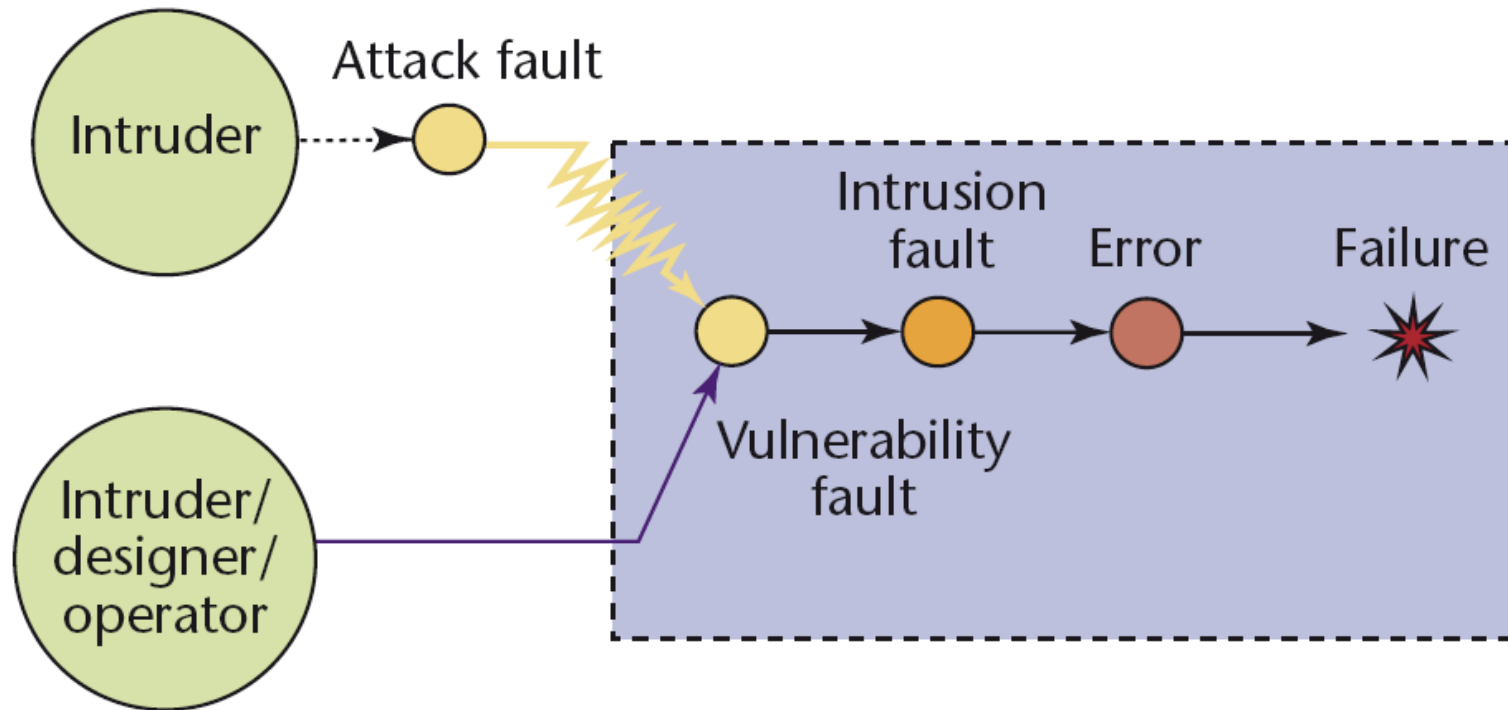


# Reported Security Incidents in Companies (F)



# Attack/Vulnerability/Intrusion Model\*

(The MAFTIA IST Project)



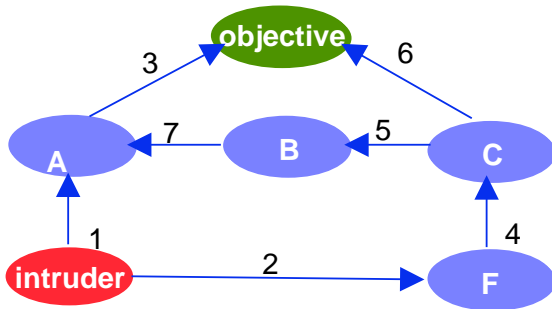
Malicious-and Accidental-Fault Tolerance  
for Internet Applications

<http://research.cs.ncl.ac.uk/cabernet/>  
[www.laas.research.ec.org/maftia/](http://www.laas.research.ec.org/maftia/)

\* P. Verissimo, N. Neves, C. Cachin, J. Poritz, Y. Deswarte, D. Powell, R. Stroud, I. Welch  
*Intrusion-Tolerant Middleware: The Road to Automatic Security*  
IEEE Security & Privacy, 4 (4), pp.54-62, July-August 2006

# Quantitative Assessment of Security

## Vulnerabilities Modeling "privilege graph"

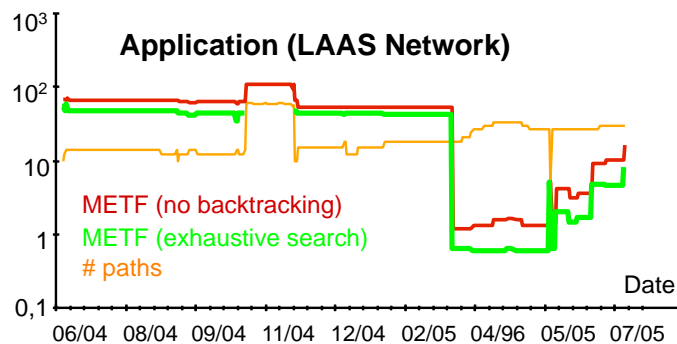


Node = set of privileges

Arc = vulnerability class

Path = sequence of vulnerabilities that could be exploited by an attacker to defeat a security objective

Arc weight = effort to exploit the vulnerability



R. Ortalo, Y. Deswarte, M. Kaâniche

Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security, IEEE Trans. Soft. Eng., 25 (5), pp.633-650, 1999

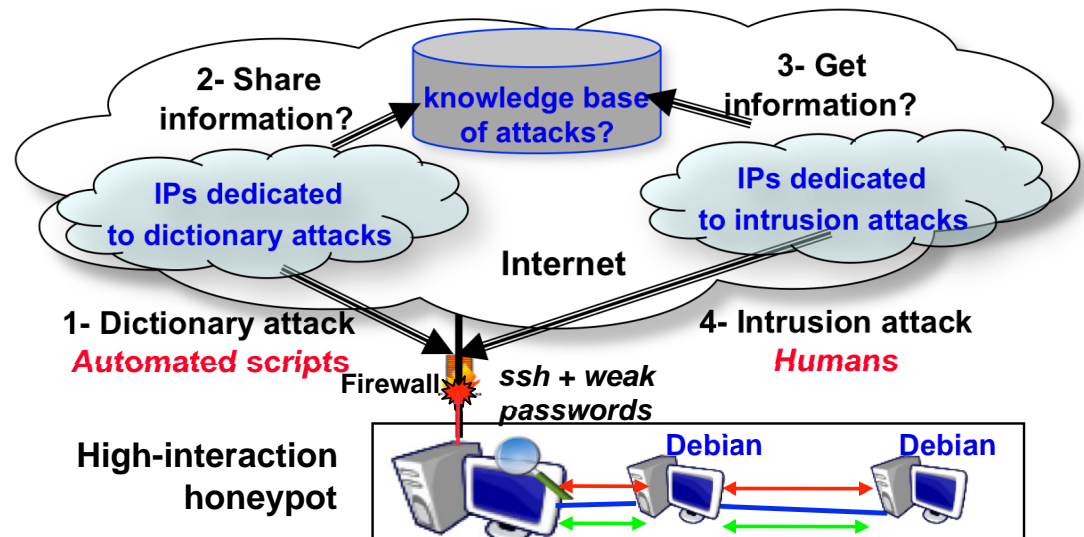
## -> Questions?

- Is such a model valid in the real world?
- Considered behaviors (no backtracking/exhaustive) are two extreme ones; what would be a "real" attacker behavior?
- Weight parameters are assessed arbitrarily (subjective?)

## -> Wanted ! Real Data

CADHo project: "Collection and analysis of Attack Data based on Honeypots (Eurecom, LAAS-CNRS, Renater)

- Both low- (35 worldwide) and high-interaction honeypots
- Typical behavior:



E. Alata, V. Nicomette, M. Kaâniche, M. Dacier

Lessons Learned from the Deployment of a High-interaction Honeypot  
Proc. EDCC-6, (Comibra, Portugal), pp.39-44, IEEE CS Press, 2006.

# The Integration of Information Processing into Everyday Objects and Activities



Ubiquitous & Pervasive Computing



Ambiant Intelligence



Internet of Things

- Everyware, Haptic Computing, Things that Think, Cyber-Physical Systems,

...

Main challenge wrt classical transaction systems  
—> Managing dynamics, time, and concurrency  
in networked computational + physical systems

So ... Let's be:  
Flexible, Adaptive,  
Inclusive and ...  
Tolerant about  
Terminology! ; -)

Calls for  
**Resilient  
Computing  
& Proactive  
Assessment**

## Thanks to...

- Colleagues of the Dependable Computing and Fault Tolerance research group at LAAS-CNRS
- Many partners of Delta-4, PDCS, DeVA & DBench projects, members of IFIP WG 10.4, and of the "FTCS-DSN" community

## To Probe further

- A. Benso, P. Prinetto (Eds.), Fault Injection Techniques and Tools for Embedded Systems Reliability Evaluation, Frontiers in Electronic Testing, #23, 245p., Kluwer Academic Publishers, London, UK, 2003.
- SIGDeB: IFIP WG 10.4 on Dependable Computing and Fault Tolerance Special Interest Group on Dependability Benchmarking  
[[www.dependability.org/wg10.4/SIGDeB](http://www.dependability.org/wg10.4/SIGDeB)]
- DeBench: Dependability Benchmarking Project (IST-2000-25425)  
[<http://www.laas.fr/DBench>]
- K. Kanoun, L. Spainhower (Eds.), Dependability Benchmarking for Computer Systems, 362p., Wiley-IEEE CS Press, 2008.
- ReSIST: Resilience for Survivability in IST - EU Network of Excellence  
[[www.resist-noe.org](http://www.resist-noe.org)]

# Thank you for your Attention!

