4th Information Trust Institute Workshop
on Dependability and Security

Panel 2 — Systems

University of Illinois at Urbana-Champaign, USA — Friday November 30, 2007

Towards Computer Systems that are Powerful & Versatile and Dependable & Secure

Jean Arlat

(jean.arlat@laas.fr)

Facts, Trends and Issues

- **Increased Demand for Better Performance, Enhanced Functionality, Adaptivity, Awareness, …**
  - Evolution of Hardware Technologies & Chip Architectures and Reliability Issues (production and operation)
  - Openess of Computing Architectures in Embedded Critical Systems (coping with COTS Equipments and Software Components in Safety Critical Applications)
  - Adaptive Systems and Dynamic Configuration (Automotive: on-demand Services, Health: operation room, …)
  - Mitigating Demanding Security Requirements and Legitimate Privacy Concerns
  - …
- **Most Current Systems Fail to Meet — at the same time — Such Comprehensive Requirements**

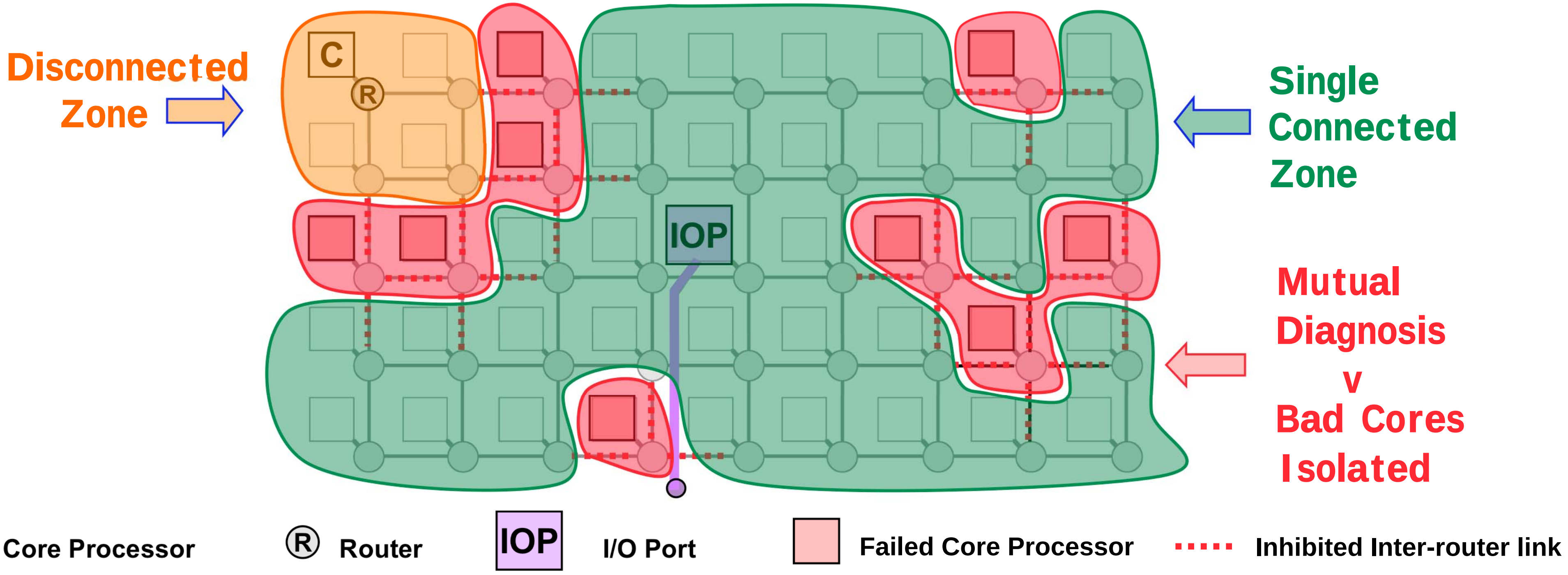
Technology Trend & Emerging Processor Chips

More Moore —> Low Yield,
Massively Defective Devices

HW Processor Chips
—> Large Multicore Architectures

On-line Reconfigurable (Gracefully Degradable) Multicore Chips

Example: 5x9-core Network — connectivity: 4, single IOP)



Disconnected Zone

Single Connected Zone

Mutual Diagnosis
v
Bad Cores Isolated

C Core Processor

® Router

IOP I/O Port

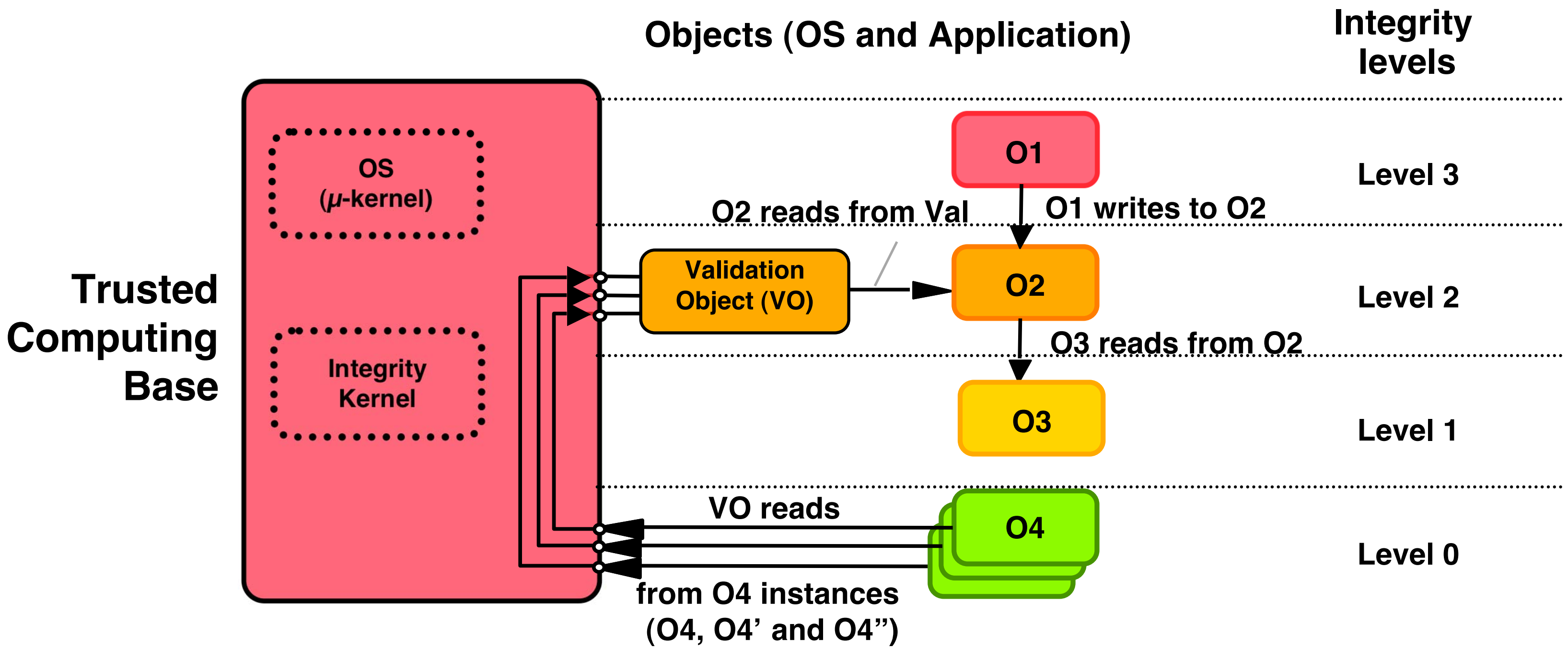
🟥 Failed Core Processor

▪▪▪▪ Inhibited Inter-router link

P. Zając, J. H. Collet, J. Arlat, Y. Crouzet, “Resilience through Self-Configuration in Future Massively Defective Nanochips”, Supplemental Volume DSN2007, Edinburgh, UK, pp.266-271, 2007

Openess of Critical Systems

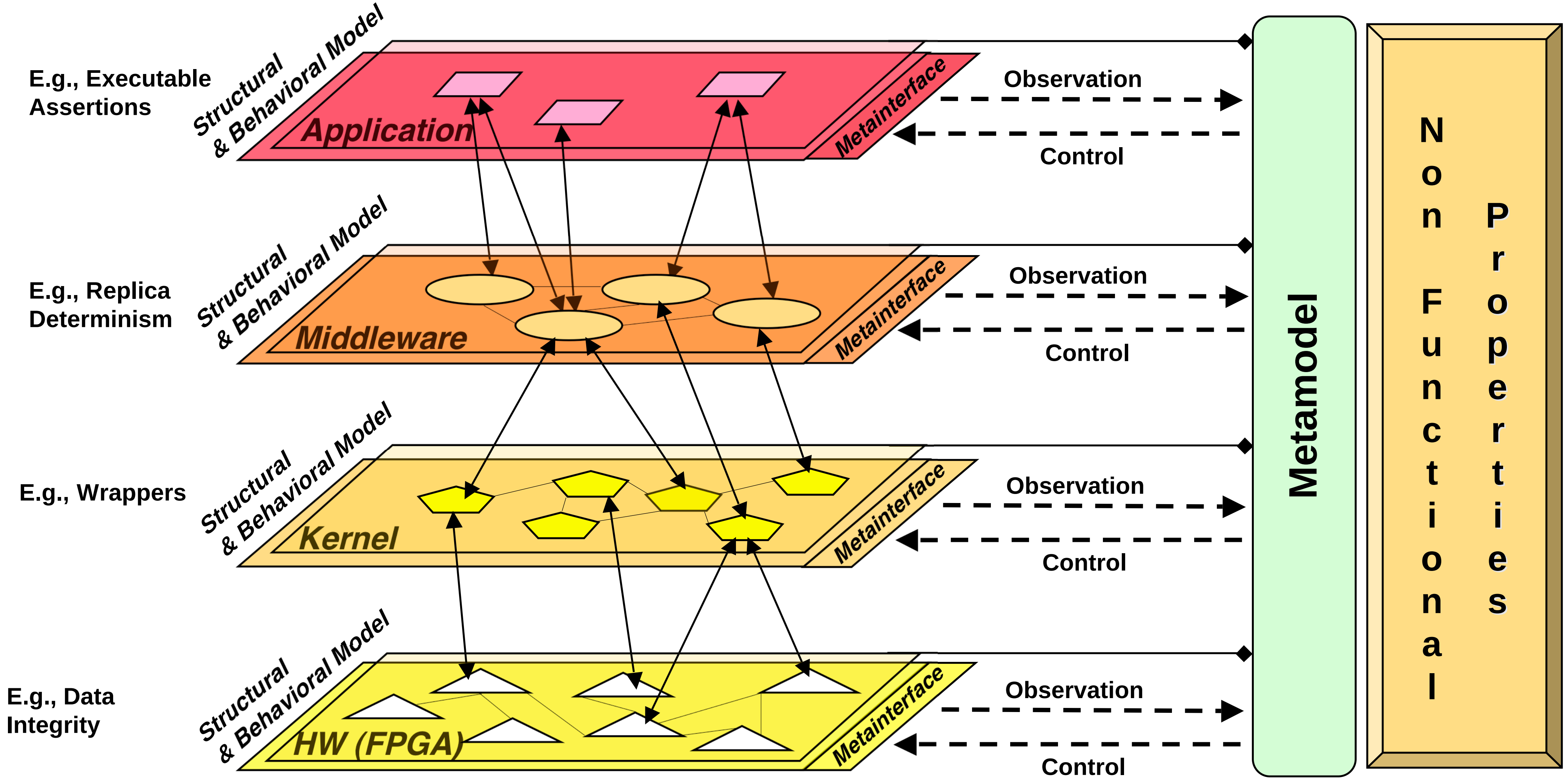
- Interactions between information infrastructures in critical embedded systems and other lower integrity level equipments (e.g., routine vehicle configuration and maintenance actions)
- Classically, High Integrity Systems rely on unidirectional static data flow control. Not sufficient to support flexible operation…



E. Totel, J.-P. Blanquart, Y. Deswarte and D. Powell, "Supporting Multiple Levels of Criticality", *Proc. FTCS-28,* Munich, Germany, pp.70-79, 1998.

—> A Basic Scheme to Mitigate Safety *and* Security Issues?

Multilayer Reflection Frame for Resilient Computing



F. Taiani, J-.C. Fabre, M.-O. Killijian, “A Multi-Level Meta-Object Protocol for Fault-Tolerance in Complex Architectures” Proc. IEEE/IFIP DSN-2005, Yokohama, Japan, 2005, pp. 270-279.

Still a Long Way to Go …

- **Scalability** of proposed resilience solutions is one of the major challenge to cope with **widely deployed, ubiquitous, open, interconnected** systems and infrastructures subjected to a **wide spectrum of faults and threats** (accidental and malicious)

- These **challenges** are **real and generic** enough to **deserve joint efforts** — academia (multidisciplinarity) and industry (multi application domains: automotive, aerospace, communications,…) to identify and promote suitable enabling technologies

- **From Resilience-Building to Resilience-Scaling Technologies: Directions** (ResIST NoE, Deliverable D13, Sept. 2007,130 p.)
  - Evolvability — Assessability — Usability — Diversity

Towards Safe and Secure

“Plug & Play” Systems …