41st IFIP WG 10.4 Meeting — 4-8 January 2002 — Saint John, US Virgin Islands

Workshop on "Challenges and Directions for Dependable Computing"

From Fault Injection Experiments to Dependability Benchmarking

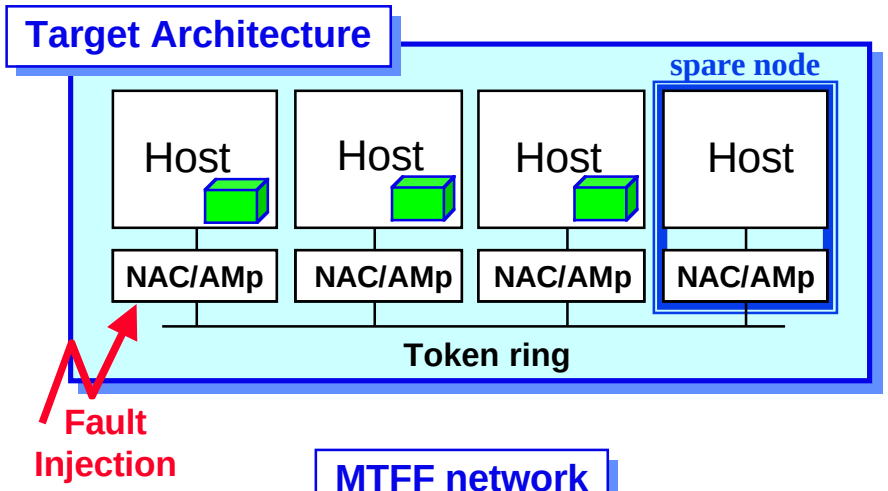
Jean Arlat
[arlat@laas.fr]

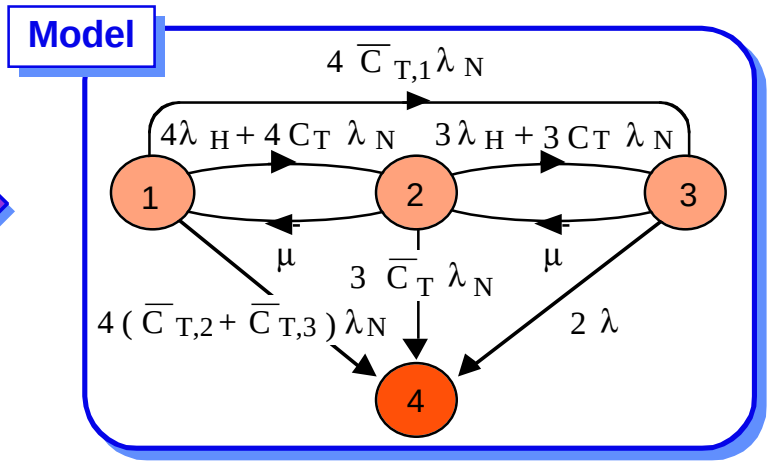
Fault Injection

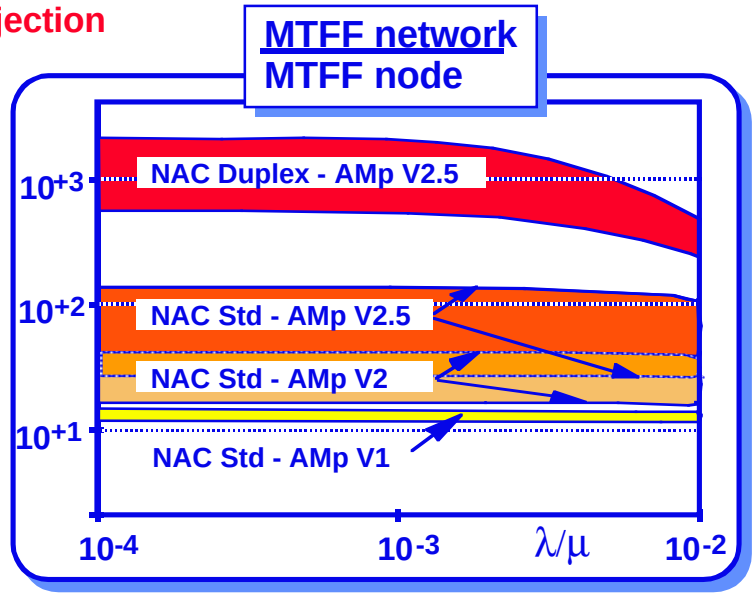
- Test and assessment of fault-tolerant systems & FT mechanisms
- Explicit characterization of faulty behaviors

Fault Injection as A Design Aid

[ESPRIT Project Delta-4]







Coverage factors

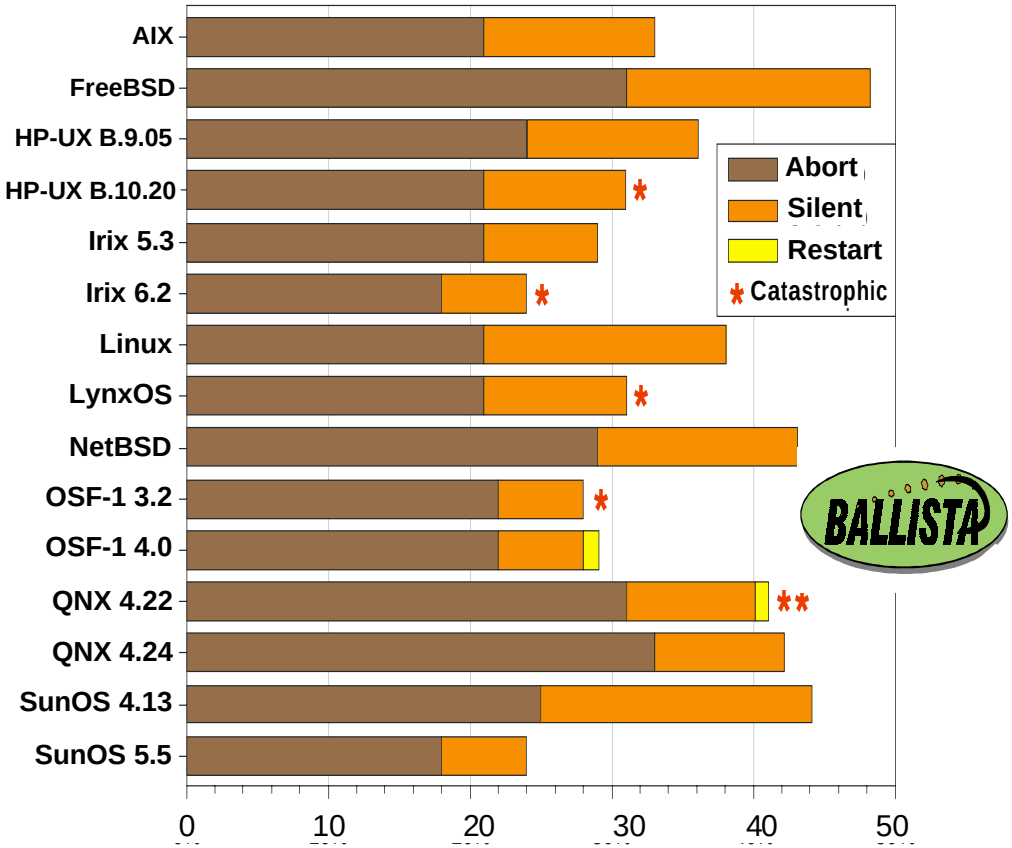
Target system	C_T	$\overline{C}_{T,1}$	$\overline{C}_{T,2}$	$\overline{C}_{T,3}$
NAC Std - AMp V 1	79,08%	2,32%	11,77%	6,83%
NAC Std - AMp V 2	[illegible]	8,73%	2,80%	45%
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
NAC Duplex - AMp V 2.5	99,55%	0,32%	0,00%	0,12%

Well-Accepted by Industry as a Whole

- **Provider**
  - IBM, Intel, Sun MicroSystems,…
- **Integrator**
  - Ansaldo Segnalamento Ferroviario, Astrium, DaimlerChrysler, SAAB Space, Siemens, Technicatome, THALES, Volvo,…
- **Stakeholder**
  - Electricité de France, ESA, NASA (JPL),…
- **Consultant**
  - Critical Software, Cigital,…

Fault Injection-based Dependability Characterization of COTS SW

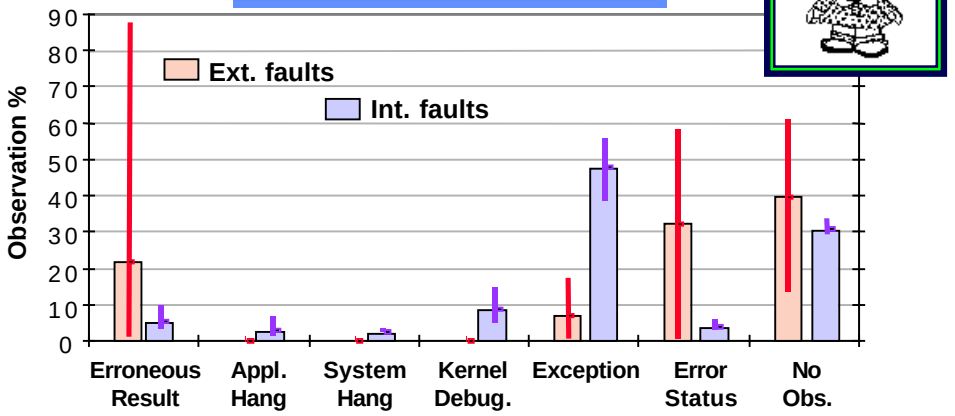
15 « COTS » OSs
[Koopman & DeVale 99 (FTCS-29)]



BALLISTA

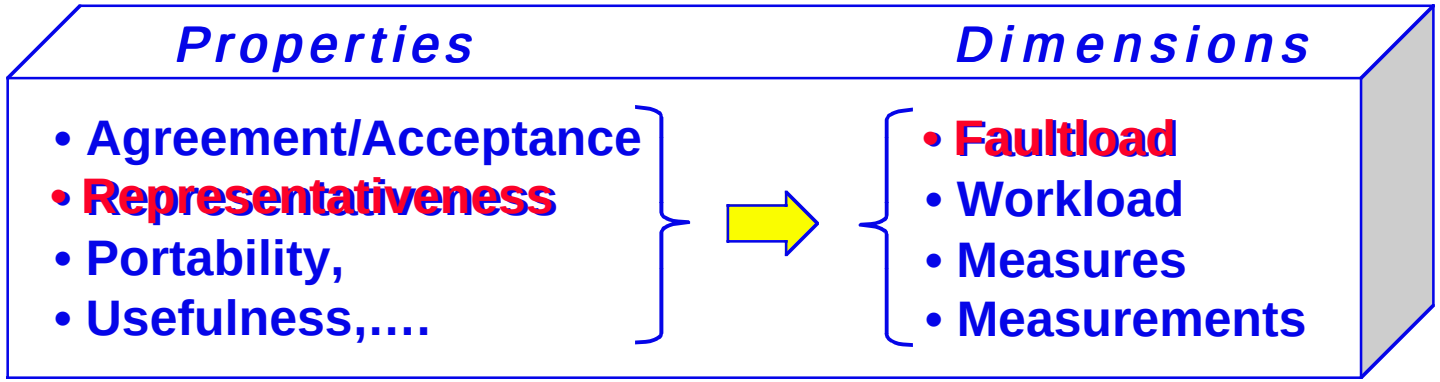
Invalid parameters in calls at POSIX Interface

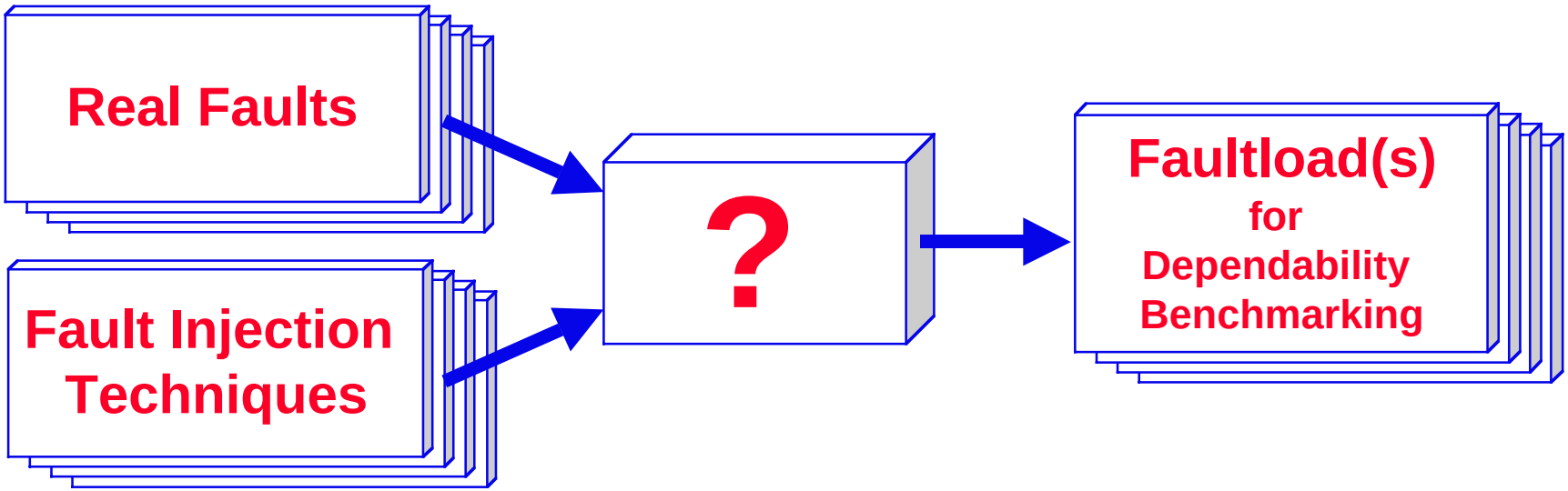
Chorus microkernel
[Fabre et al. 99 (DCCA-7)]



Bit flips on parameters of kernel calls and in memory segments

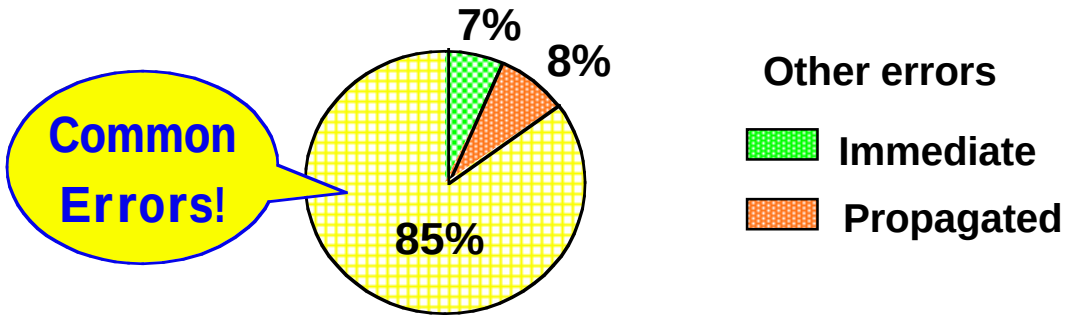
Dependability Benchmarking



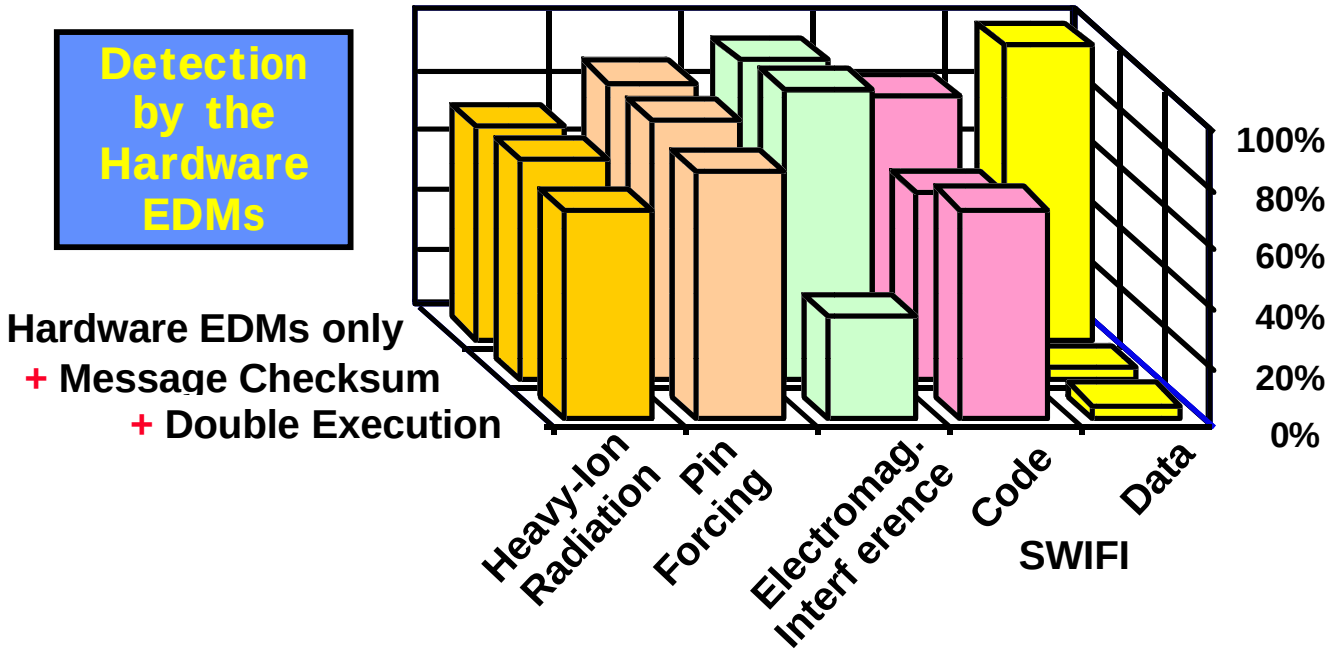


On Fault Representativeness

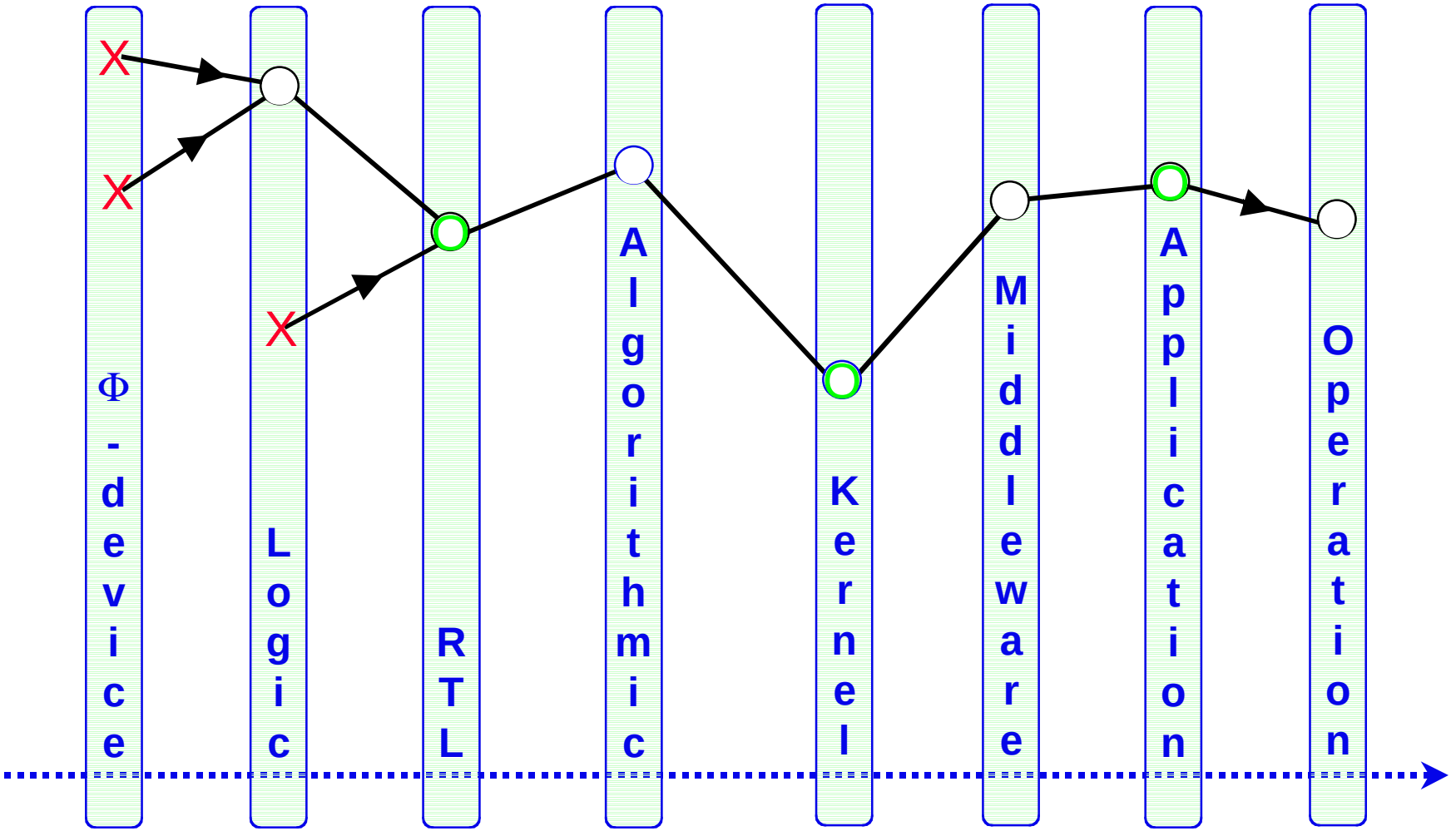
- **Software:**
  - **Comparison of Mutations**
  - **wrt Real Faults**
  - [Daran & Thévenod-Fosse 1996]



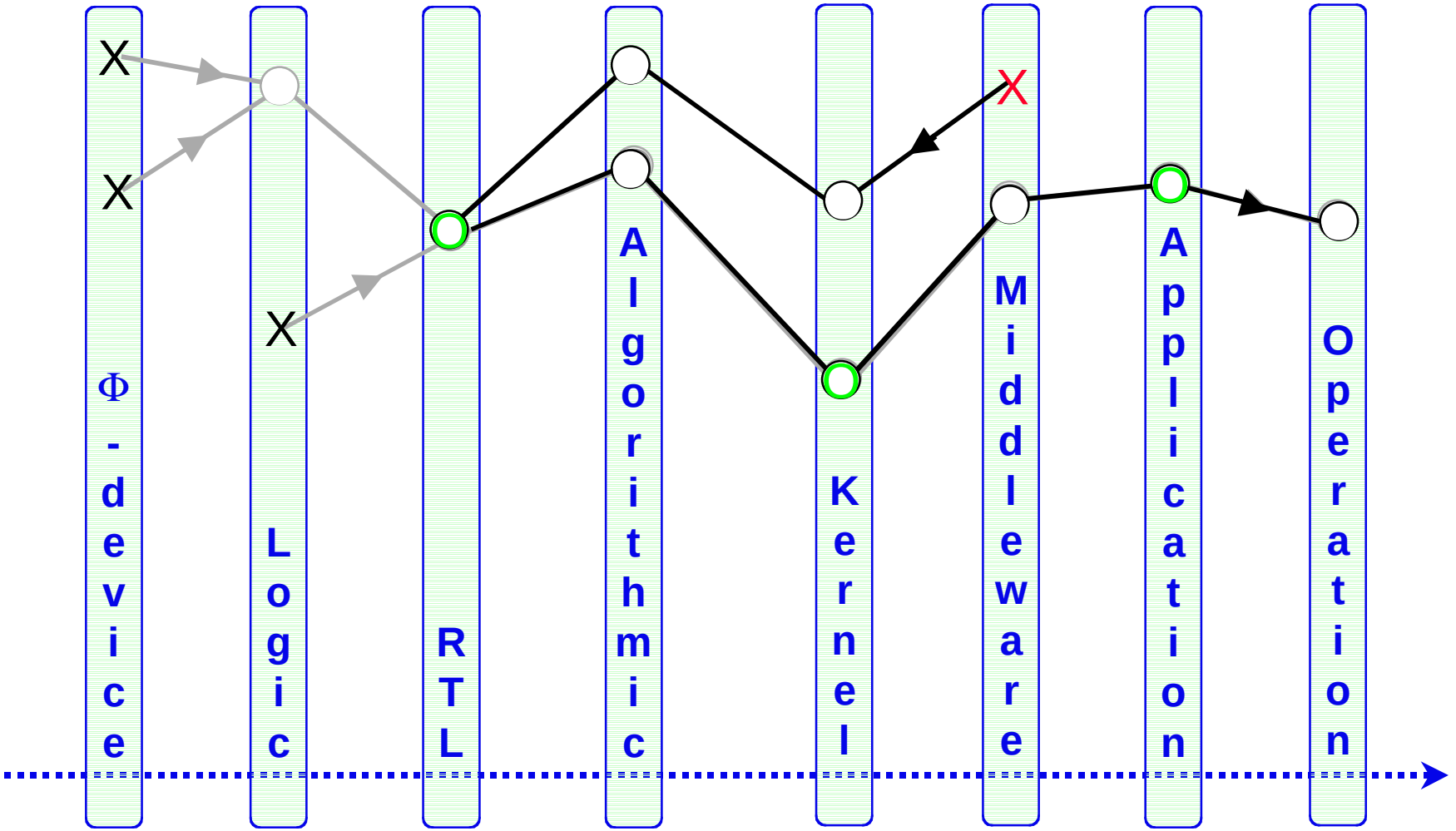
- **Hardware:**
  - **FI Experiments on the MARS FT & RT Architecture**
  - [ESPRIT Project PDCS]



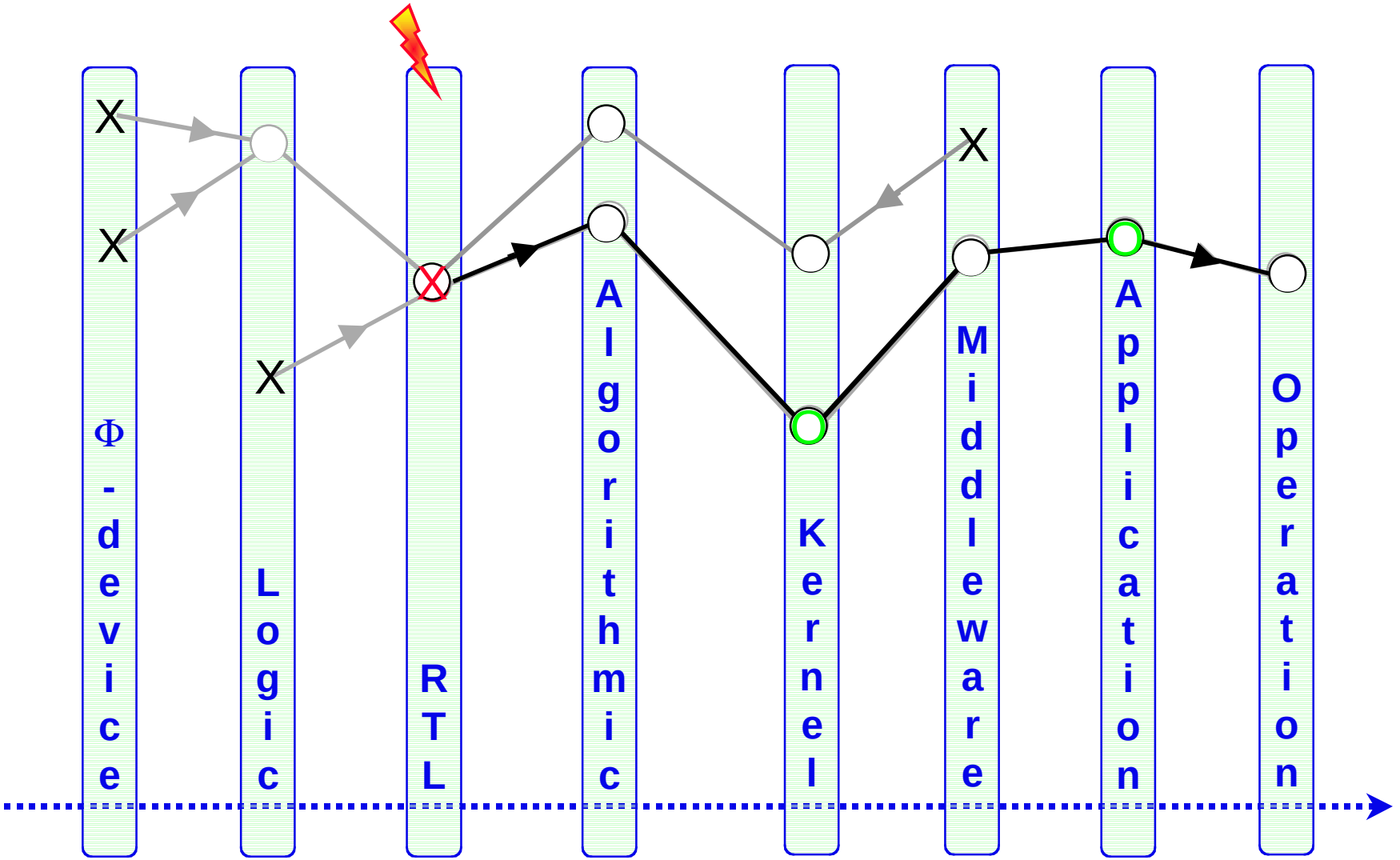
Target System Levels & Fault Pathology



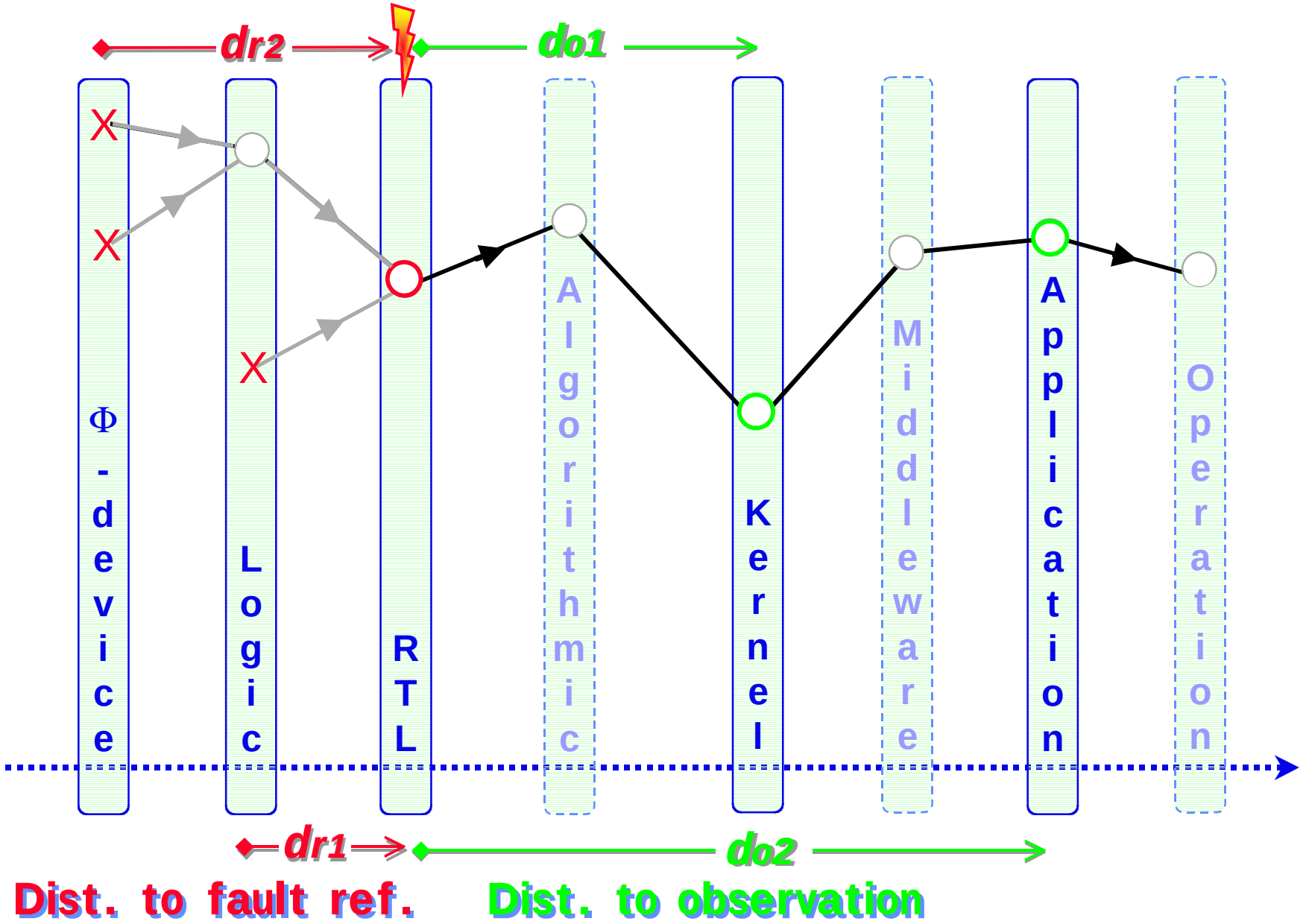
Target System Levels & Fault Pathology



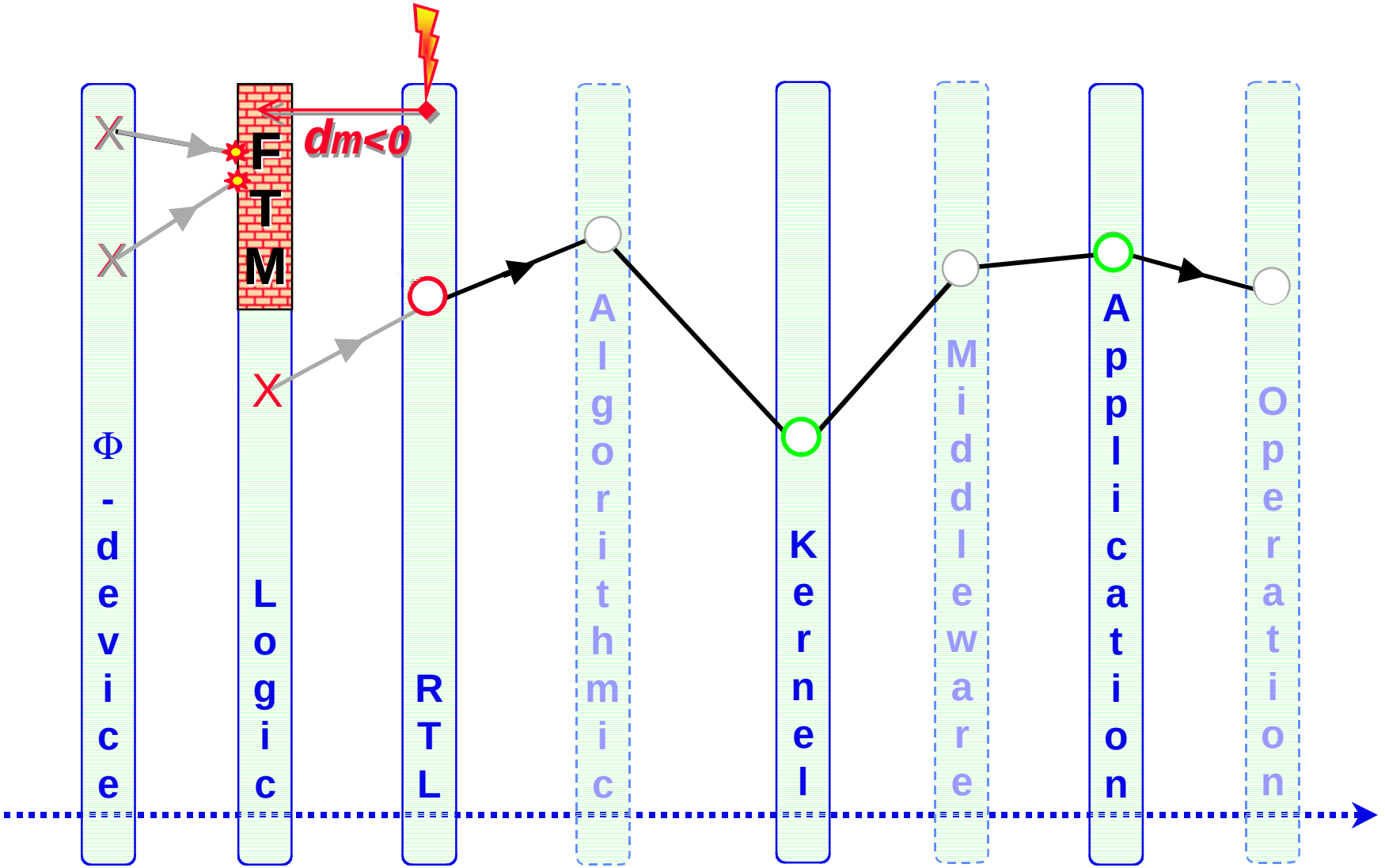
Target System Levels & Fault Pathology



Target System Levels — Ref. & Obs. dist.



Target System Levels & FT Mechanisms



Some Scenarios and Challenges...

- Impact on the Certification Process:
  - From process to product -> Agreed/Accepted Dependability Benchmarks
- Coordinated Research Actions (Academia + Industry)
  - WG SIG 10.4, IST DBench and Beyond...
- Human-related faults (either Accidental or Malicious)
- Combination of Faults:
  e.g., Technical Accidental and Malicious Faults
- Large Scale Communication Infrastructures and CHI (Computerized-Human Interferences)
- ...