Dependable Systems of the Future: What is Still Needed?

Algirdas Avižienis

Vytautas Magnus University
Kaunas, Lithuania

and

UCLA Computer Science Department
Los Angeles,CA, USA

WCC 2004 — Program Top 3 — 23 August 2004

A Contemporary Paradox

Computing systems provide protective infrastructures for critical infrastructures of modern society: electrical power, telecommunications, transportation,…

But,

These computing systems do not possess a protective infrastructure of their own!

My prediction:

A fully hardware-based fault-tolerant protective infrastructure for computing systems will evolve, because it is needed as systems progress toward ever higher complexity and speed of operation

Why a Hardware Infrastructure?

- **Because over the past half century hardware has not been adequately exploited to assure the dependability of computing and communication systems**

- **This “omission fault” needs to be corrected in order to better cope with proliferating threats to dependability and security**

The FT Defenses of Contemporary Systems

- **FT Defenses exist at four levels: component, board, platform, cluster.**
- **Weaknesses are found:**
  - **Components (processor, chip sets, etc.) have low error detection and containment coverage (except IBM's G5 and G6)**
  - **The presence of unprotected "hard core" elements, especially in the error detection and recovery management hardware and software**
  - **The commingling of hardware and software defenses: both must succeed in order to attain recovery**
  - **The absence of built-in support for multiple-channel computing that provides high coverage and containment, especially when design diversity is employed to attain design fault tolerance**

Desirable Properties of the Fault Tolerance Infrastructure

- **The FTI is generic, i.e., suitable for a variety of "client" systems**
- **The FTI is transparent to the client's software, but communicates with it**
- **The FTI is compatible with and able to support the client's other defenses**
- **The FTI is fully self-protected by fault tolerance, immune to the client's faults and to malicious software**

A Design Principle: the Immune System Paradigm

- **The desirable properties of the FTI are similar to those of the immune system of the human body**

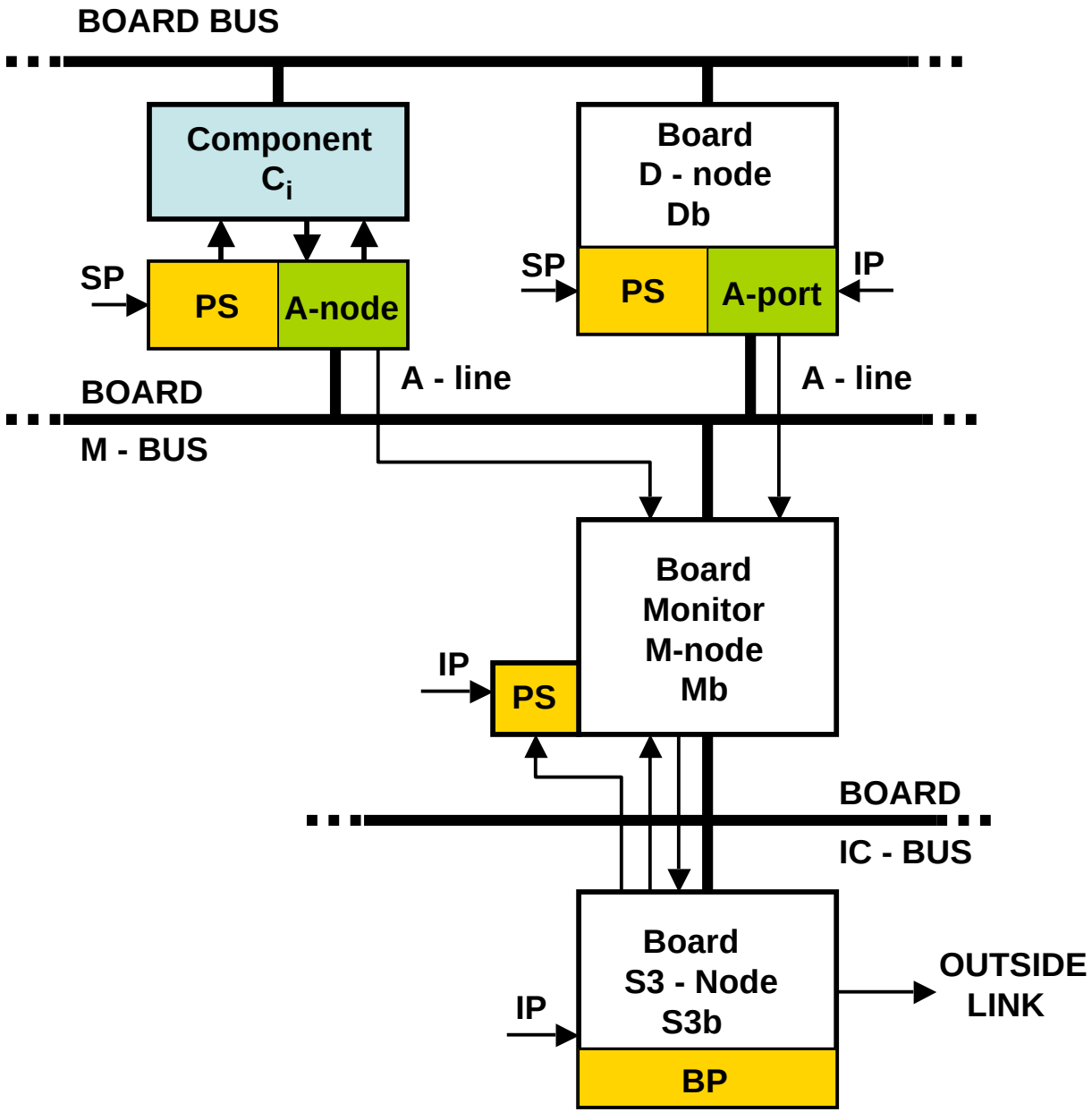
- **Use three analogies to explain the design principle of the FTI:**

Body	**<—>**	**Hardware**
Consciousness	**<—>**	**Software**
Immune System	**<—>**	**Fault Tolerance Infrastructure**

Four Key Properties of the Immune System

- **It functions (i.e., detects and reacts to threats) continuously and autonomously, independently of consciousness**
- **Its elements (lymph nodes, other lymphoid organs, lymphocytes) are distributed throughout the body, serving all its organs**
- **It has its own communication links – the network of lymphatic vessels**
- **Its elements (cells, organs, and vessels) themselves are self-defended, redundant and in several cases diverse**

The Board Fault Tolerance Infrastructure



Legend:

SP: System Power

IP: Infrastructure Power

BP: Backup Power

PS: Power Switch

C_i: Board Component i

A: Adapter Node

D: Decision Node

M: Monitor Node

S3: Startup, Shutdown, Survival Node

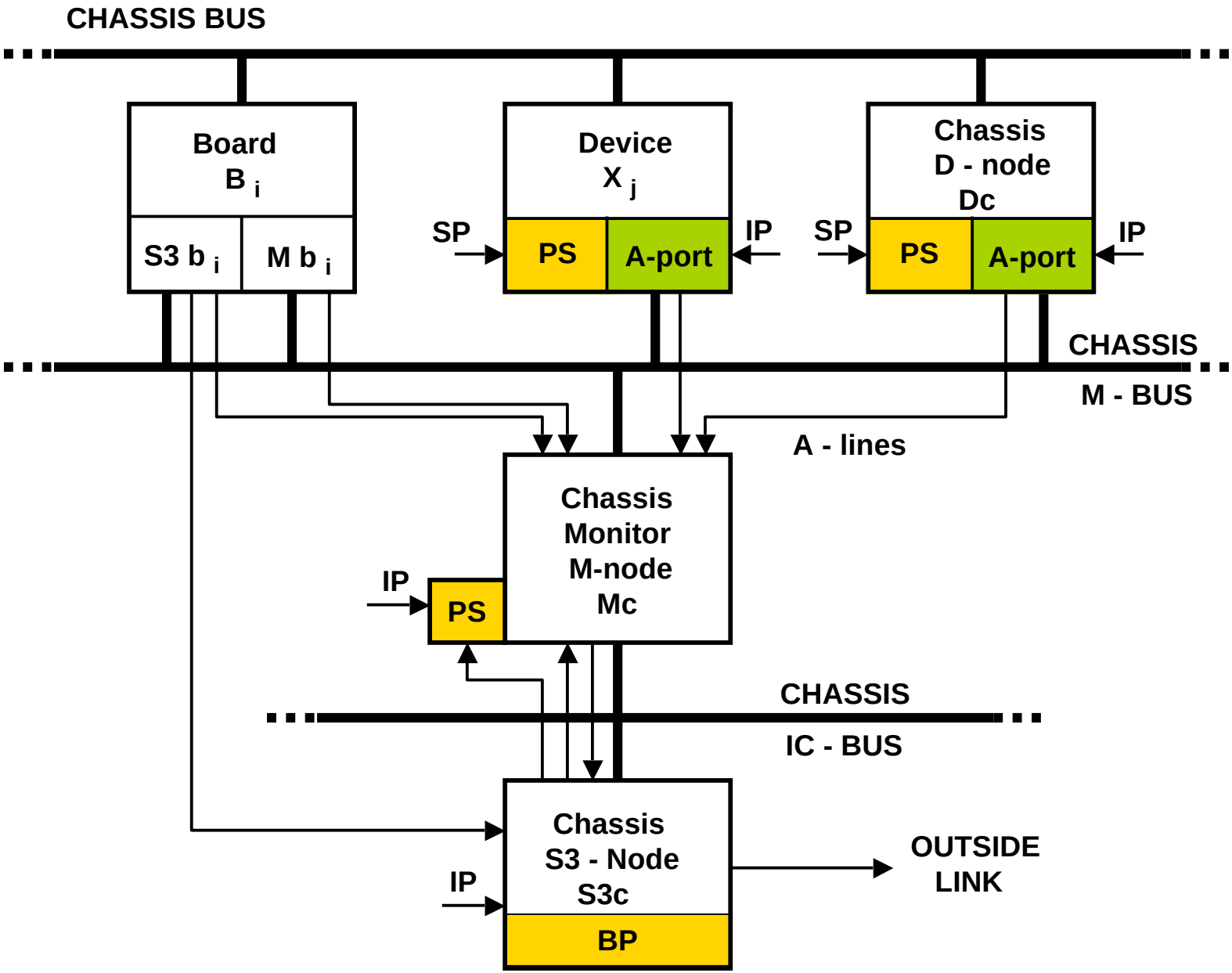
Evolution of the FTI

1- Replace A-nodes by A-ports in board components

2- Build an on-chip simplified FTI whose M and S3 nodes serve as the A-port of the chip

3- Develop an FTI hierarchy: board FTI, chassis FTI, cluster FTI…
Constraint: Dedicated A-lines and M-buses are needed at each level

The Chassis Fault Tolerance Infrastructure

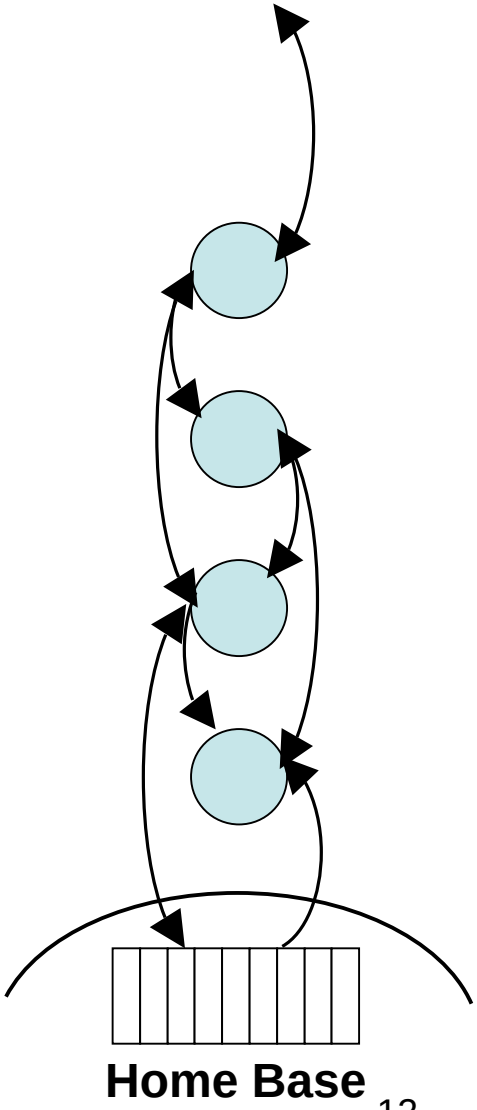


Some Interesting Applications

- **Projected device failure rate of 10 FITS gives:**
  Device MTBF of 10^8 hours = 11,400 years
  R(simplex) = .99 at 114 years or R(s) = .90 at 1140 years
  R (1 active, 3 spares) = .9989 at 1140 years (coverage c=.99)
- **The FTI will provide survival capability wrt design faults and transient catastrophic faults (temporary power loss, heavy radiation, etc.)**
- **Build a system for the 1000-day manned mission to Mars with the dependability of a 12-hour flight of an airliner**
- **Build a fault-tolerant relay chain of low cost DiSTAR spacecraft for an interstellar mission**

A Spacecraft Relay Chain for Interstellar Missions

1. **Launch a low cost DiSTAR spacecraft every N years; the design can evolve continuously**
2. **Use the chain of spacecraft to relay communications to Earth and back to the original spacecraft**
3. **Introduce redundancy at spacecraft level: every spacecraft can dependably communicate to M = 2, 3, or more, closest neighbors; then the loss of M-1 adjacent spacecraft is tolerable**
4. **Slow down all spacecraft ahead of the gap to repair the chain**
5. **Never stop launching better and better DiSTAR spacecraft!**



My Thanks for 50 Years of Friendship, Learning, Teamwork and Shared Achievement to

- **My mentors at the U. of Illinois: Prof. David Muller and the late Prof. James E. Robertson**
- **The ILLIAC 2 team at the Digital Computer Lab. of UI**
- **My role model at the Computer Society - Prof. Ed McCluskey**
- **The STAR team and fellow engineers at the Spacecraft Computers section at the Jet Propulsion Laboratory (JPL), especially George Gilley, Frank Mathur, Dave Rennels and John Rohr**
- **My faculty colleagues and 31 PhD winners at the UCLA Computer Science Department, especially Jerry Estrin, Milos Ercegovac, John Kelly, Liming Chen, Ann Tai, Kam-Sing Tso and Yutao He**
- **My "UCLA Club" of visiting scholars: Tom Anderson, Jean Arlat, Jean-Paul Blanquart, Y.T. Chen, Per Gunninberg, Ragnar Huslende, Jean-Claude Laprie, Takao Sasaki, Lorenzo Strigini, Pascal Traverse, Udo Voges and others**

My Thanks for 50 Years of Friendship, Learning, Teamwork and Shared Achievement to

- **My many friends in the IEEE-CS TC-FTCS and IFIP WG 10.4, especially those with whom we started those teams: Alain Costes, the late Bill Carter, John Meyer, Jacob Abraham, Jean-Claude Laprie, Hermann Kopetz, Yoshi Tohma, Hiro Ihara, Luca Simoncini, Mike Morganti, Dan Siewiorek, Brian Randell, Ravi Iyer and many more…**
- **My Lithuanian colleagues with whom we restarted Vytautas Magnus University in Kaunas, city of my birth and childhood, especially Rector Vytautas Kaminskas, who was my right-hand man from day one on**
- **All authors of the papers being presented here**
- **Jean Arlat, who organized this event with great care and dedication**
- **And most of all, thanks to my wife Jurate, and my sons Rimas and Audrius for patiently and lovingly sharing the sometimes frantic life of a restless academic competitor**