Dependable Computing in 2031—
Back to the Start?

H. Kopetz

June 2006

Structure of Systems

*If you look at automata which have been built by men or which exist in nature, you very frequently notice that their structure is controlled to a much larger extent by the manner in which they might fail and by the (more or less effective) precautionary measures which have been taken against their failure. . . . . .**There can be no question of eliminating failures or of completely paralyzing [i.e., neutralizing] the effects of failures.** All we can try to do is arrange an automaton so that in the vast majority of failures it can continue to operate.*

John von Neumann, Theory of Self-Reproducing Automata, Urbana, University of Illinois Press, 1966

The Causes of Failure in 2031

The three main causes for the failure of systems will still be the same:

- ♦ Physical Faults--Hardware
- ♦ Design Faults in Hardware and Software
- ♦ Improper User Interactions

However, a new fault pattern, the *unintended emergent behavior of a self-organizing system*, might justify the introduction of a new fault class.

Estimated Parameters of an SoC around 2025

	2004	2007	2025
Feature Size (nm)	90	65	<10
DRAM Mbits/mm^2	10	40	>500
SRAM Mbits/mm^2	0.2	.8	>10
Million transistors/mm^2	1	4	>50
Chip size mm^2	200	200	200
Frequency in GHz	2	8	>100
Cost/ mm^2 (in cents)	10	10	10
Cost per transistor (μcents)	10	2.5	<0.2
Number of CPUs/mm^2	5	20	>250
Cost (c) per CPU ARM 7 (200k)	2	0.5	0.04
MTTF/chip permanent (years)	1000	1000	100
MTTF/chip transient (years)	1	.8	<0.01

Significant Hardware Trends

- ♦ Hardware will get smaller and cheaper, but not as fast as in the past--*Moore's law* will slow down.
- ♦ Reliability per function will increase, but not at *Moore's speed* anymore--this has dramatic consequences for system design.
- ♦ Reliability per chip will decrease significantly, particularly w.r.t. transient faults (e.g., soft errors caused by cosmic radiation)
- ♦ Mitigation techniques for soft errors will be needed at different levels--material selection, cell design level, system design level.
- ♦ Hardware delivers only the *intrinsic reliability* for mass-market devices--reliability improvements for more demanding applications must be done at the system level.

Mitigation of Soft Errors by Architectural Means

Architectural means to mitigate the consequences of component failures might become a necessity when using the upcoming submicron devices, as stipulated in the latest *2005 International Roadmap of Semiconductors p.6:*

Relaxing the requirement of 100% correctness for devices and interconnects may dramatically reduce the costs of manufacturing, verification and test. Such a paradigm shift is likely ***forced in any case by technology scaling****, which leads to more transient and permanent failures of signals, logic values, devices and interconnects.*

FPGAs--Lose a Factor of 10, Gain a Factor of 100

The maturing of FPGA technology has a dramatic effect on system design

- ♦ Compared to a hardwired chip, FPGA loses a factor of 10 in most parameters (size, power, performance)
- ♦ Compared to a CPU implementation of an algorithm, FPGA implementations can gain a 100x performance improvement.
- ♦ FPGA chips are well-suited for mass production--Non -recurring costs (e.g., mask costs) can be distributed over high production volumes.
- ♦ FPGA-based design environments blur the difference between hardware and software design (e.g., *soft CPU* in an FPGA)

Significant System Architecture Trends

- Multi-core chips are the norm--Network-on-chips link the islands of synchronicity
- Component-based design technology has matured, since this is the only way to handle the complexity of the giga-scale SoCs
- Static and dynamic reconfiguration around faulty on-chip subsystems is widely deployed
- System design must consider both hardware and software aspects (e.g., power-aware algorithms).
- TMR structures are widely deployed at the system level to mask transient hardware failures and *Heisenbugs* in the software.

Software Trends

The reduction and management of the *cognitive complexity* of large systems are the key design drivers for the software:

- ♦ *Model-Driven Design Methods* have emerged to the point where the behavior of platform independent models (PIM) can be analyzed and the *transformation* to the desired platform-specific model (PSM) for a heterogeneous execution environment, meeting given non-functional requirements such as the required dependability, is tool supported.
- ♦ *Correct-by-construction system platforms* will facilitate the integration of components into a system.
- ♦ *Integrated diagnostic services* will detect the misbehavior of components and initiate fault-management activities autonomously.

Principles of Systematics

Gall states among the principles of Systemantics:

- *A complex system that works is invariably found to have evolved from a simple system that works.*
- *A complex system designed from scratch never works and cannot be patched up to make it work. You have to start over, beginning with a simple working system. (Translation for computer programmers: Programs never run the first time. Complex programs never run.)*

Amory Lovins, Brittle Power, p. 202

Robustness

The user-perceived services of the highly interconnected information infrastructure must be reliable, despite the failure of some subsystems, which will be the norm:

- ♦ Fault Masking and Reconfiguration must be autonomic without any explicit human interaction.
- ♦ Ambient intelligence will only succeed, if the fault-diagnosis is done by the system and physical repair--if needed-- can be performed by the average user.
- ♦ New design methods, such as *state-aware design*, are needed to simplify reconfiguration and repair.
- ♦ Even in a single system, different functions are designed to differing reliability levels (e.g., multimedia)

Safety-Critical Systems in 2031

- Certification is widely deployed, e.g., aerospace, automotive, medical, some process industries.
- The system architecture is determined, to a considerable degree, by dependability and certification requirements in order that it can be analyzed: see the quote from *von Neumann*.
- A shift from *process-oriented* to *product-oriented* certification will have taken based.
- Modular certification technology, where the certification arguments are strongly supported by architectural properties, has matured.

Conclusion: What Can we Expect 25 Years from Now?

- The concern for dependability will increase significantly, due to the deteriorating hardware base and the increased dependence of society on all types of computing systems.
- To me, the biggest challenge is in the field of education: bringing the concern for and the knowledge about dependability into the heads of the practicing engineers.
- I do not expect *revolutionary new methods* to enter the mainstream of dependable computing in the next twenty-five years.
- **We started work on our Time-Triggered Architecture (TTA) in 1979--more than 25 years ago--and only today we see some industrial uptake.**

Power Blackout on August 14, 2003

A valuable lesson from the August 14 blackout is the importance of having time-synchronized system data recorders. The Task Force's investigators labored over ***thousands*** *of data items to determine the sequence of events, much like putting together small pieces of a very large puzzle. That process would have been significantly faster and easier if there had been wider use of synchronized data recording devices.*

U. S. - Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations P.173

Power Blackout on June 22, 2022

A valuable lesson from the June 22 blackout is the importance of having time-synchronized system data recorders. The Task Force's investigators labored over ***millions*** *of data items to determine the sequence of events, much like putting together small pieces of a very large puzzle. That process would have been significantly faster and easier if there had been wider use of synchronized data recording devices.*

U. S. - Canada Power System Outage Task Force, Final Report on the June 22, 2022 Blackout in the United States and Canada: Causes and Recommendations P.888