A Fault Tolerance Infrastructure for High-Performance COTS-Based Computing in Dependable Space Systems

Algirdas Avižienis
Vytautas Magnus University
Kaunas, Lithuania

Most high-performance COTS processors and other components of the current generation have limited error detection and relatively poor error containment. Internal error detection and recovery logic remain entirely unchecked. They also contain hardware design faults (called "errata") that are discovered after commitment to manufacturing and are listed in "specification update" publications [1]. A notable exception are the G5 and G6 processors from IBM that have very good error detection and containment. The COTS components also do not offer built-in hardware support for implementing fundamental fault tolerance techniques such as component duplexing, TMR voting, sparing, and design diversity for the tolerance of design faults. Such techniques are essential to assure long life and dependable operation of space-based computing systems.

A fundamental solution that allows the use of high-performance, but poorly checked processors in dependable space systems is the use of a generic, hierarchical, fault-tolerant hardware infrastructure (FTI) [2]. This FTI is a software-independent innermost defense for an autonomous, fault-tolerant long-life system that may also employ other, especially software-based , fault tolerance techniques. It is interesting to note that the attributes of the FTI are analogous to those of the human immune system when the analogies body = hardware and cognition = software are employed.

The elementary FTI of [2] is composed of four types of special-purpose ASICs called "nodes". Adapter (A) nodes are interfaces with the COTS processors; Monitor (M) nodes collect A-node inputs and issue recovery signals; S3 nodes control power-on and -off sequences of the system, generate fault-tolerant clock signals and provide nonvolatile storage; Decision (D) nodes provide comparison and voting services and provide communication links for COTS processors of the system. The entire FTI is fault-tolerant and contains no software, thus being immune to malicious software intrusions.

Biography Algirdas Avižienis is Research Professor at Vytautas Magnus University, Kaunas, Lithuania, and Professor Emeritus at UCLA, Los Angeles, CA, USA. He received his Ph.D. from the University of Illinois in 1960 and joined Caltech's Jet Propulsion Laboratory. There he initiated research on long-life interplanetary spacecraft computers that resulted in the concept of fault tolerance (1967) and US Patent No. 3517671, "Self Testing and Repairing Computer" in 1971 that described the JPL-STAR experimental computer. Dr. Avižienis joined the faculty of UCLA in 1962 and has supervised 31 Ph.D. dissertations and published over 150 papers on fault-tolerant computing and computer arithmetic. He has received numerous honors, including the NASA Apollo Achievement Award, the AIAA Information Systems Award, the NASA Exceptional Service Medal, and IFIP Silver Core. In 1985 he was awarded the degree "Docteur Honoris Causa" by the Institute National Polytechnique, Toulouse, France. He served as the Founding Chair of IEEE Computer Society TC on Fault-Tolerant Computing (1970-73) and of IFIP Working Group 10.4, "Dependable Computing and Fault Tolerance"(1980-85).

References

[1] Y. He and A. Avižienis, "Assessment of the applicability of COTS microprocessors in high-confidence computing systems: A case study," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2000)*, (New York, NY), pp. 81–86, June 2000.

[2] A. Avižienis, "A fault tolerance infrastructure for dependable computing with high-performance COTS components," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2000)*, (New York, NY), pp. 492–500, June 2000.

Proceedings of the 10th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'04)
0-7695-2076-6/04 $20.00 © 2004 **IEEE**