Challenges of Electronics Hardware Technology For High Integrity Aerospace Applications

Y. C. (Bob) Yeh
Boeing Commercial Airplanes
Flight Controls Systems
Ying.c.yeh@boeing.com

Hardware Component Obsolescence

Avionics Computer Architecture

Design for Testability

44th Meeting of IFIP WG 10.4, Monterrey, CA, June 28-29'03
Panel: Challenges, Opinions, Perspectives & Proposals
Y.C. (Bob) Yeh, Boeing Commercial Airplanes

Hardware Component Obsolescence

High Integrity Avionics Systems (such as FBW computer with a functional integrity requirement of 1.0E-10 per hour) generally takes at least 4-5 years to develop and certify.

Key electronics devices (e.g., Microprocessor), selected at the start of design cycle, would become obsolete before the host system is certified for safety critical application.

Continuous cycle of hardware redesign is a normal way of life for high integrity avionics systems.

The hardware technology (clock speeds, voltage, physics of failure) advances at faster speed than a design/redesign cycle of avionics systems. Components are used at lower stress levels (speed, voltage, current, power) for safe and reliable operations in airplane environments (temperature cycle, passive cooling-air, etc).

44th Meeting of IFIP WG 10.4, Monterrey, CA, June 28-29'03
Panel: Challenges, Opinions, Perspectives & Proposals
Y.C. (Bob) Yeh, Boeing Commercial Airplanes

Avionics Computer Architecture

It is desirable to configure a high integrity computer architecture that can be continuously redesigned with minimum cost and certification impacts.

Complex electronics hardware devices (with an exception of COTS processor) should be justified for its necessity.

Redundancy management function (core of a high integrity computer architecture) may preferably be implemented in software. Hardware devices, invoked for redundancy management, should be configured for simplicity and testability (commonly quoted as: 100% analyzable and testable).

44th Meeting of IFIP WG 10.4, Monterrey, CA, June 28-29'03
Panel: Challenges, Opinions, Perspectives & Proposals
Y.C. (Bob) Yeh, Boeing Commercial Airplanes

Design for Testability

Safety Analysis

Computer system/hardware design should facilitate testability of hardware monitors that are credited in safety analysis for exposure times of:

Continuous monitoring time period
Automatic self-testing per flight (exposure time =
one flight)
Manual initiated (scheduled) testing per 100/200/… hours
Production ATP (automatic testing procedure) (exposure time = MTBF)

Proof of Correctness

Proof of correctness for high integrity systems (such as FBW) are required for all aspects of (system, hardware, and software) design cycle: requirements, design, and implementation.

Hardware devices, designed for testability, can relieve complexity of high integrity system design for proof of correctness and for safety analysis.

44th Meeting of IFIP WG 10.4, Monterrey, CA, June 28-29'03
Panel: Challenges, Opinions, Perspectives & Proposals
Y.C. (Bob) Yeh, Boeing Commercial Airplanes