NAVY FAULT TOLERANT VALIDATION EFFORTS

Timothy P. Monaghan

The Naval Air Warfare Center, Aircraft Division, Warminster
PO Box 5152 Warminster, PA 18974-0591

ABSTRACT

This paper describes two 6.3 and 6.4 efforts that are attempting to clarify the Navy's management of the design of complex, computer based, weapon and avionic systems. The 6.3 effort, the Advanced Avionics Technical Demonstration (AATD) Fault Tolerance Demonstration is focused on the fault tolerant specifications, validation techniques and acceptance tests of any future Naval Avionic system and the 6.4 effort, the Next Generation Computer Resources (NGCR) Fault Tolerant Task Group is concerned with the fault tolerance features of the Navy's next generation open system computer standards.

MOTIVATION

As the Navy enters the 21st century, the decreasing defense budget, the increasing costs of ownership, and increasing complexity of avionic systems is causing a paradigm shift in the way the military acquires and maintains its next generation of avionic systems. Traditionally performance was the primary design force and dependability was an afterthought. With the increasing complexity of systems and the high costs of ownership performance, dependability and contained life cycle costs are all equal drivers from the initial specification to the final design and implementation of modern, Navy, computer based, weapon systems. The Navy does not design the avionics but provides the specifications, standards and acceptance tests the contractors use to design the systems. Without clear specifications and acceptance tests that can be validated by the government, and standards that adequately support dependable and fault tolerant systems, the costs of ownership (Maintenance Man Hours per Flight Hour (MMH/FH), spares usage, and frequent degraded modes of performance) will continue to spiral and seriously undermine our future defense capabilities.

The Rand Corporation has studied the military's process of acquiring weapon systems and has concluded: (1) there is no meaningful set of management measures for Reliability and Maintainability (R&M), (2) there is no adequate process for setting rationally based R&M goals for future systems, and (3) there are no strong assurances that needed levels of R&M will be delivered. The Rand report concluded that R&M has many dimensions, it is not an easily quantified attribute, and that the elusive quality of R&M will grow more elusive as system complexity grows. [1,2]

The Rand corporation based its findings on an in-depth examination of two critical radar systems the APG-66 on the F-16 A/B and the APG-63 on the F-15 C/D. During a six month period, June to December 1984, Rand had a contractor team interview the crew and maintenance personnel after 16,077 flights. The data collected was thus raw field experience of users of the systems, not data filtered through the official collection sources. 50% of the requested flight line maintenance

actions resulted in a isolated faulty part. Of the 50% of the boxes found to be faulty on the flight line and sent back to the shop for repair, the shop fault isolation efficiency was 68% (board level) and of those 68% sent back to the depo for repair 80% of the time the problem was isolated to the chip level and repaired. Thus, of the overall pilot-reported anomalies, the overall fault removal efficiency was 27%. $(0.50 \times 0.68 \times 0.80)$

The interview data also showed that the pilots were reporting anomalies at a rate of about one in every five flights in which they actually experienced a problem. Thus pilots had built up a threshold of faults they would put up with due to past inefficient fault removal. Pilots reported anomalies in cockpit only 20% of the time, when these anomalies reached a certain "headache" threshold.

Thus the combined fault removal efficiency of the poor fault isolation $(0.51 \times 0.68 \times 0.8)$ and pilot reported degraded mode threshold $(1 \text{ in } 5 \text{ or } 20\%)$ equals a total fault removal efficiency of $0.27 \times 0.20 = 0.05!$

This field experience leads to two conclusions: (1) because modern avionics has a difficult fault isolation problem pilots are complaining less often and flying frequently in degraded modes of mission performance, (2) when cockpit anomalies reach a certain threshold and the pilot does complain, the fault isolation problem eats up large amounts of Maintenance Man Hours per Flight Hour (MMH/FH) and high spares usage. [3]

The most critical task of a program office interested in developing a dependable avionic system with contained life cycle costs are the fault tolerance, testability, and reliability specifications, acceptance tests and the required Mil Standards in the Request For Proposals (RFP) and Statement Of Work (SOW) package. The government does not design an avionic system or give direct supervision of the ongoing work. The government's role is to *specify* and *validate* the work. The SOW contains the governments specifications and the validation testing that will verify that the specifications are met. These packages must call for specific information as deliverables in reports. The design review meetings will focus on this deliverable information to ensure that the contractors are producing a system that will meet the specifications. The courts have generally held any ambiguities in the SOW against the government. Thus for the government to ensure a dependable computing system it is essential to have accurate dependability and fault tolerance specifications and validation methods.

NAVY FAULT TOLERANCE RESEARCH

Funds for the research, development, transition and insertion of new technologies into the fleet are divided into 6.1, 6.2, 6.3A and 6.4 funds. The 6.1 and 6.2 funds are focused on exploring the feasibility of new technologies. The 6.3 funds are aimed at demonstrating those technologies so that program office's can specify them with confidence. These general stages and their metrics of success are shown in figure 1. In 1990

ONR's 6.1 research started the Ultradependable Multicomputers and Electronic Systems Research Initiative. This research initiative is in a wide ranging number of fault tolerance topics including measurement and modeling of expected system fault modes, fault injection, simulation and modeling techniques, software fault tolerance approaches, as well as compiler, algorithm and hardware based fault tolerance techniques. ONT's 6.2 exploratory development, computer block has an effort called the "Engineering of Complex Systems Technology" whose aim is to explore the entire design and development of advanced real-time systems. The fault tolerance portion of the block plan is aimed at integrating fault tolerance into the design process of complex systems.

FAULT TOLERANT SPECIFICATIONS AND ACCEPTANCE TESTS- ADVANCED AVIONICS TECHNICAL DEMONSTRATION (AATD) FAULT TOLERANCE DEMONSTRATION

There is no comprehensive DoD or IEEE fault tolerant computer system validation standard. The dependability of current systems depends on the individual emphasis of the various contractors in-house design teams and their in-house awareness of the practice of dependable and fault tolerant system design. The government should take the lead in bringing about this coordination and consensus develop contractual requirements that will ensure reasonable Life Cycle Costs (LCC) and dependable system operation.

The government must provide clear fault tolerant metrics throughout the contractors design of the avionic system. These metrics are crucial to enable the government to evaluate the

Figure 1

The Advanced Avionics Technical Demonstration (AATD) Fault Tolerance Demonstration is a 6.3A project to take the 6.2 Engineering of Complex Systems effort the next step and demonstrate the fault tolerance metrics and acceptance tests at each stage of an evolving contractors design. The AATD work will also transition some of the ONR 6.1 developed tools (Fault injection, fault tolerance benchmarks and fault tolerance simulation techniques). The AATD effort is working in close coordination with the tri-service Dependability Working Group (DWG). The DWG is a group of leading researchers and industry developers of fault tolerant systems who, under the leadership of the DoD, are addressing the topic of the dependability validation of complex computer-based, weapon systems. The goal of the DWG is to coordinate industry and the research community to come to a consensus on the necessary and sufficient dependability validation criteria. The AATD Fault Tolerant Demonstration will demonstrate these fault tolerant metrics for the Navy and also document the specifications of a testbed to carry out these metrics.

design and provide the contractor with feedback on the evolving design. In the Systems Requirements Review (SRR) the performance and fault tolerance requirements are set and applicable architectural approaches are identified. In the System Design Review (SDR) a architectural approach and fault tolerance strategy has been selected and the relevant trade studies are presented which provide the rationale for that choice. In the Preliminary Design Review (PDR) and Critical Design Review (CDR) a simulation of the design in VHDL will grow in detail and testing. A prototype design is then tested in the final TEST phase of the design.

Initially the government provides quantitative and qualitative fault tolerant specifications. The quantitative specifications include terms like fault recovery times, MTBF, reliability and availability, and fault detection latency requirements. The qualitative requirements include terms like no single point of failure, fail operational/ fail safe, specified fault containment regions, and the preservation of critical state information.

A fault set is a key part of a fault tolerance specification. Faults in the fault set might include: permanent, transient, coincident, timing and synchronization faults. In the subsequent stages of the design the quantitative specifications will become more precise and the qualitative specifications will become more detailed as they are verified with the fault set against the evolving design. In the VHDL and breadboard stages the government needs to provide clear acceptance tests for the fault tolerant validation of the design. These acceptance tests will be in the form of the specified fault set, mapped to critical parts of the hardware and software. The fault tolerant features of the system are thus verified by observing the systems response to these injected faults. Also at this stage the initial abstract modeling of the system will be verified as a design integrity check. The output of the AATD Fault Tolerant Demonstration are the complete set of these careful fault tolerant and dependability validation checks throughout a contractors design. Figure 2 shows the approximate stage of the contractors design mapped against the various design reviews and parallels the Naval Air Warfare Center (NAWC) fault tolerant validation lab capabilities.

Program Office Support Needs
(Risk Reduction Studies, Independent Performance & Dependability Evaluations)

Figure 2

STANDARDS - NEXT GENERATION COMPUTER RESOURCES (NGCR)

The RFP/SOW package includes Mil Standards that the contractor must use in the design. The Navy's Next Generation Computer Resources (NGCR) is defining the Navy's next generation of military computer standards. NGCR is a 6.4 program that is seeking to adapt commercial hardware and software standards for military use. In the overall world of electronics the military is a small player. Thus the motivation of NGCR is to leverage commercial standards to keep pace with the rapid changes in electronics and maintain this edge at reasonable costs.

NGCR is developing ten interface standards, six in the hardware area and four in the software area:

- LAN standards
 - (1) SAFENET
 - (2) High Performance LAN -- TBD

- Backplane standards
 - (3) Backplane Bus -- Futurebus+
 - (4) High Performance Backplane Bus -- TBD
 - (5) Switch Network -- TBD

- Software
 - (6) Network Operating System -- Based on POSIX
 - (7) Network Data Base Management System -- TBD
 - (8) Programing Support Environment -- TBD
 - (9) Graphics Language/Interface -- TBD

The Navy will assess these standards for military needs such as:

- (1) Real Time Performance and Dependability
- (2) Fault Tolerance
- (3) Built In Test
- (4) Module Fault and Stress History Logging

- (5) Module Revision History
- (6) Multi-Level Security

NGCR FAULT TOLERANT TASK GROUP (NFTG)

The NGCR Fault Tolerance Task Group (NFTG) is an FY92 start. The NGCR Fault Tolerant Task Group (NFTG) was formed to investigate the system wide fault tolerant issues of the NGCR standards. Are the standards adequate to design fault tolerant systems? Do the fault handling assumptions of one standard fit with the fault handling assumptions of the other standards? The group has been tasked to:

- (1) Define the Mission Critical Computing Resources (MCCR) fault tolerance requirements and policy
- (2) Investigate the fault handling across standards
- (3) Investigate current open systems that implement fault tolerance
- (4) Make recommendations for the resolution of key fault tolerance issues to the standards working groups
- (5) Conduct laboratory fault injection experiments on the standards as they become available (FY93 Futurebus+)

Such a system wide fault handling analysis of the NGCR standards is a unique problem. The analysis is not focused on a particular design nor is the analysis itself designing a system. Thus, the fault tolerance evaluation of a NGCR open system evaluates the NGCR *interface* standards. It evaluates specific vendor designs to identify the types of fault handling done *between* standards and gauges the impact of these types of fault handling on the NGCR standards. Will the fault handling assumptions of one standard fit the fault handling assumptions of the other given the types of vendor specific designs that will be between the standards? (The discussion and figures that follow will clarify this point).

A system's architecture can be described as the structure of interconnecting parts in the system. The specifications of these component interactions describe the details of the interface among interoperating components. Traditionally this architecture, the components and their interfaces, have been proprietary. The user purchases all components and future upgrades from one vendor. An open system is one in which the system components and their interfaces are specified in a non-proprietary environment and thus the interfaces are widely available, widely accepted and standardized. Layered models of architectures are used to hide implementation details from unrelated components. The functionality of the system is divided into layers with each layer depending only on the interface of the layer below it. Thus the interface of that lower layer is public or open to the higher layer and its implementation details are private and the overall system can be built from different, competing vendors components.[4]

Figure 3

Fault tolerant system analysis maps a specified fault set onto a systems error containment region and gauges the systems ability to protect the system state against that specified fault set. [5] For the purpose of the NGCR fault tolerance task group the fault containment region would be the vendor specific "black boxes" of the system with the public interfaces being the NGCR standards.

Fault Tolerant System Analysis

Specified Fault Set

ex/ stuck-at-0
stuck-at-1
transient
coincident
pwr & timing
interaction
synchronization
consistency

Mapped onto Fault Containment Regions

System Impact:

fault/error containment
mission function protection
recovery time

As an example of this type of analysis consider Futurebus+ and POSIX in some future NGCR fault tolerant system.

Figure 5

Consider a mission avionics scenario - a medium attack fighter is on air to ground mission, it sweeps inland hugging the landscape then pops up to take a SAR map and jam a few SAM sites simultaneously. This combined SAR Map and jamming scenario is a high stress benchmark for the AX, the Navy's next generation medium attack fighter. The mission processor will be at or near maximum throughput. In this scenario, during the jamming time slice, the Futurebus+ starts to experience difficulty with repeated parity errors on the AD[], the multiplexed address and data lines. Figure 6 shows the rich amount of fault handling information that is available from a Futurebus+: the byte the parity error occurred at, the retry threshold and whether the threshold was exceeded, the time of the error, and the address of the error. The Futurebus+ Control Status Registers (CSR) can be set to react to errors: the number of retrys, the time between retrys, and the Built In Testing (BIT) to perform on that error condition. The between interface analysis then asks what implication this Futurebus+ error information and actions have on the POSIX application interface. There are two options: (1) Fault tolerance is strictly a hardware and operating system kernel issue. (The application doesn't concern itself with computer system fault tolerance. The hardware and kernel will provide the

uninterrupted service needed.) But will all implementations of POSIX on military systems have a massive hardware (Trimodular Redundant) requirement or will many have lesser fault tolerance requirements yet still require fault tolerance. For these systems will the current POSIX panic routine, buffer flush and system reboot be adequate? (2) How could an application use some of the information and actions available in Futurebus+? (see figure 6) In the SAR and jamming scenario the applications programmer might want to know if the system can recover from the fault with out a system reboot and reconfiguration based on startup BIT. Can the fault has been localized to a bad unit, the utilization of the new hardware configuration estimated and a new loading prioritized (continue the jamming). The application might want to be able to choose between data availability (keep some jamming going at all costs) or data integrity (reboot and reconfigure and ensure the highest data integrity). The application might also want to fine tune the error handling for that application and thus want a fuller error report than a POSIX bus error signal, and utilize that information in the applications own error handling routine.

Figure 6

The NGCR Fault Tolerant Task Group will proceed along this type of inquiry between standards, between Futurebus+ and POSIX and SAFNET and the emerging database, High Performance Network (HPN) and switched network standards, and ensure that a wide variety of future fault tolerant Mission Critical Computer systems can be designed with the NGCR standards.

CONCLUSION

The Navy does not design or build avionic systems. The Navy specifies and validates the system it is purchasing is adequate to support the Navy's needs. In order for these systems to be dependable, fault tolerant and provide quick fault isolation and repair, the Navy must provide clear and detailed specifications of what the Navy means by "fault tolerance" and "dependable" systems and adequate metrics for each stage of the evolving systems design. Also the Navy must ensure that it's next generation of open system computer standards adequately support fault tolerance. This paper described two related 6.3 and 6.4 efforts that are attempting to clarify the Navy's management of the design of avionic systems. The Advanced Avionics Technical Demonstration (AATD) Fault Tolerance Demonstration is focused on the fault tolerant specifications, validation techniques and acceptance tests to be specified in the RFP/SOW package. These specifications will clarify the fault tolerance metrics for each design review for future Navy avionic systems regardless of the standards used (JIAWG, NGCR, or others). The Next Generation Computer Resources (NGCR) Fault Tolerant Task Group is concerned with the fault tolerance features of the Navy's next generation open system computer standards. This effort will ensure that future designers are able to adequately implement the AATD fault tolerance specifications using the NGCR standards.

REFERENCES

- [1] J. R. Gebman, "Needed reforms to the Defense System Management of Avionics Acquisition and Support," The RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138.
- [2] J.R. Gebman and H.L. Shulman, "A Strategy for Reforming Avionics Acquisition and Support," July 1988, A Project Air Force report prepared for the United States Air Force R-2908/2-AF, The RAND Corporation, 1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138.
- [3] *Naval Aviation Maintenance Material Management (3-M) Summary for December 1989*, Navy Maintenance Support Office, Mechanicsburg, PA.
- [4] G.L. Nutt, "Open Systems," Prentice Hall Series in Innovative Technology, 1992
- [5] G. Gilley, "Validation of Fault Tolerant Designs," IEEE/AIAA 10th Digital Avionics Systems Conference, October 1991.