Ultra-Reliable Real-Time Control Systems – Future Trends

Robert C. Hammett
C.S. Draper Laboratory

INTRODUCTION

The last few decades have been revolutionary times in the development of control systems. Mechanical, hydraulic, and pneumatic control devices such as flyweight speed governors and integrating pistons and diaphragms have been replaced by electronic computers, sensors, and electrically operated actuation devices. Using complex real-time software algorithms, these controls can optimize the performance and efficiency of the system being controlled, and allow it to operate with minimal human supervision. This equipment has leveraged the huge computer electronics industry to provide these benefits at reasonable cost and with good reliability. Yet despite these benefits, designers of these systems must remain very cautious of the failure modes of these electronic controls. Unlike the mechanical devices they replaced, electronic components usually fail without warning and will rarely provide degraded operation after failure that is sufficient for the system to "limp home." Using redundant computers, sensors, and other components, it is possible to make these electronic controls completely dependable, but these systems are very costly. Only critical applications such as the Fly-By-Wire (FBW) flight controls used on commercial transport and military aircraft that demand the highest levels of reliability and are relatively insensitive to cost have been able to fully exploit the control advantages of electronics. Applying ultra-reliable but affordable controls to smaller and less expensive vehicles and other subsystems would have many benefits: their designers could reduce weight by using dependable controls to alleviate stress in lightweight structures too fragile to survive worst-case design load; dependable automatic controls could routinely pilot the vehicle and operate systems with reaction times beyond human capabilities; human operators that serve as back-up control systems can be eliminated and complex controls that enhance operating efficiencies can be depended on, reducing the need for safety fuel reserves. Examples of systems that could benefit from sophisticated, ultra-reliable, but affordable controls are: unmanned aircraft and spacecraft that can safely over-fly populated areas; autonomous spacecraft requiring minimal control from earth, but providing safety critical navigation or communications functions; marine ships that replace crew members with automation; drive-by-wire, auto-piloted ground vehicles that carry passengers and rely on sophisticated controls for safety. The challenge is to provide these ultra-reliable systems at an affordable cost.

ABSTRACT

Today's aircraft use ultra-reliable real-time controls for demanding functions such as Fly-By-Wire (FBW) flight control. Future aircraft, spacecraft and other vehicles will

Author's Current Address:
C.S. Draper Laboratory, MIT, 33-113, Cambridge MA 02139-4307, USA.

Based on a presentation at DASC '98.

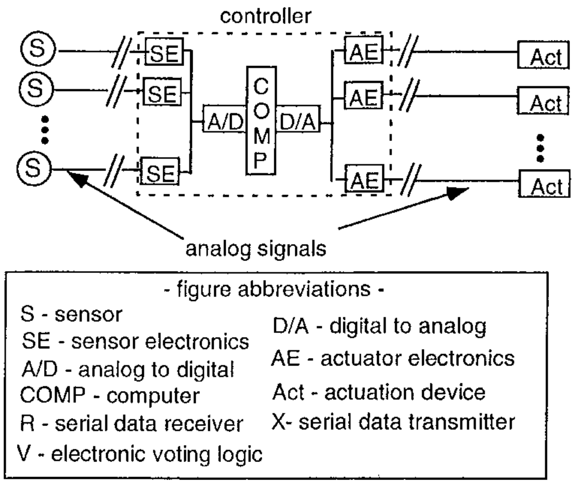

Fig. 1. Control System Using All Analog I/O Signals

require greater use of these types of controls for functions that currently are allowed to fail, fail to degraded operation, or require human intervention in response to failure. Fully automated and autonomous functions will require ultra-reliable control. But ultra-reliable systems are very expensive to design and require large amounts of on-board equipment. This paper will discuss how the use of low-cost sensors with digital outputs, digitally commanded fault-tolerant actuation devices and interconnecting networks of low-cost data buses offer the promise of more affordable ultra-reliable systems. Specific technologies and concepts to be discussed include low-cost automotive and industrial data buses, "smart" actuation devices with integral fault masking capabilities, management of redundant sensors, and the fault detection and diagnosis of the data network. The advantages of integrating the control and distribution of electrical power with the control system will be illustrated. The design, installation, and upgrade flexibility benefits provided by an all-digital and shared network approach will be presented. The economic benefits of systems that can operate following failure and without immediate repair will be reviewed. The inherent ability of these redundant systems to provide effective built-in-test and self-diagnostics capabilities will be described. The challenges associated with developing ultra-reliable software for these systems and the difficulties associated with exhaustive verification testing will be presented as will additional development hurdles that must be overcome.

FUTURE CONTROL SYSTEMS MUST BE SOPHISTICATED BUT DEPENDABLE

As systems become more highly automated, autonomous, and totally dependent on their automatic controls, more control functions must remain fully operational for the vehicle or system to complete its mission, and do so safely. Vehicles and subsystems that today use simple controls will utilize digital controls to realize efficiency, weight and automation benefits, and will be totally inoperative without them. At the same time that the need for dependability is increasing, the level of control sophistication is also rising. New systems will use controls requiring more sensors and actuation devices to optimize efficiency and performance. Complex new sensor inputs, such as machine vision for obstacle avoidance, may be used and will perform critical functions. Sensors will be added to provide the automatic health monitoring and fault diagnostic capabilities that are in demand to reduce the maintenance costs. Highly sophisticated control and decision making algorithms will reside in ever faster control computers to manage these systems. Affordable, ultra-reliable control systems will find widespread application in future systems.

I/O CIRCUITRY IS THE KEY TO AFFORDABLE ULTRA-RELIABLE SYSTEMS

Consumer demand for ever faster personal computers, portable laptop computers, and hand-held equipment has made miniaturized, rugged, and low power microprocessor components available at low cost. Using these components, affordable Fault-Tolerant Processors (FTP) can be developed that will form the core of an affordable, ultra-reliable system. [1] But the FTP is only a fraction of the system. To realize affordable, highly dependable systems, a simple and cost-effective means to sense many different measurements and provide sensor redundancy for fault tolerance is needed. These systems will also require affordable, compact, lightweight and fault-tolerant means to operate control actuation devices.

The designers of existing FBW flight controls have already taken steps to manage I/O complexity. These designers soon realized that building large, highly redundant systems using all analog electronic signaling was impractical. Figure 1 illustrates a single-channel control system using all analog signaling and a centralized digital computer. Using this approach, long wire rims may be required to connect sensors and actuators to the control computer. To make this system ultra-reliable, the entire system must be replicated several times to form redundant channels. Making each analog signal redundant results in many independent wiring paths requiring separate connectors and introducing problems of signal accuracy and electro-magnetic interference.

To overcome these problems, data multiplexing was introduced. Figure 2, on next page, illustrates how multiplexing units and serial data buses are used to consolidate or multiplex many sensor and actuator command signals onto common wiring and transmit them to/from the central computer.

These systems use data multiplexer units located as near as possible to the sensors and actuators to minimize analog wire lengths. The data multiplexer amplifies and transforms the sensor analog signals into digital data and vice versa. Today's FBW systems use this approach,

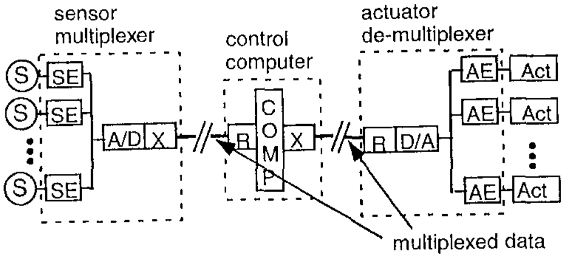

Fig. 2. Control System Using Data Multiplexing

replicating the data multiplexers into multiple channels to make the system redundant and ultra-reliable. Data multiplexing has helped reduce the amount of wiring and eliminate analog signal problems, but it also provides a standard interface between equipment from different manufacturers. But even with this data multiplexing, redundant systems remain very expensive and complex. The multiplexer and demultiplexer electronic units are expensive, heavy, require power and must be made redundant. Extensive wiring is still needed to connect the redundant analog sensors and actuation equipment to the data multiplexing units. Automatic fault detection and localization of failures in the remaining analog circuitry is difficult, limiting the effectiveness of built-in-test and system health monitoring. And given the relatively high cost of each I/O signal, even the most extravagant of today's FBW systems minimize redundancy by only applying it where demanded by safety. The software is complicated by the need to manage mixed levels of redundant I/O within one system.

These systems remain too expensive and complex for all but the most critical of functions. The key to affordable, ultra-reliable systems will be to further reduce the size, weight, and cost of the I/O electronics.

FAULT MASKING ACTUATION DEVICES ALSO INCREASE COST

The need for fault-tolerant actuation devices is another contributor to the high cost of ultra-reliable systems. These systems need actuation devices that are themselves, fault tolerant, providing a means to reject a faulty command from any one channel of electronics. Today's FBW controls typically use specialized fault masking actuation devices as the final safeguard or "voting plane" to prevent system failure. As an example, a force sum voting hydraulic actuator, as illustrated in Figure 3, are used for critical functions such as to control the position of an aircraft aerodynamic control surface like an aileron or elevator. These devices serve to translate the multiple, redundant electrical command signals into a hydraulic actuator position that represents the consensus of these signals. In this way, the effect of an electrical failure does not result in incorrect motion of the surface and a loss of control. This is accomplished by a small three (or more) piston hydraulic actuator that sums the hydraulic forces from three electro-hydraulic servo valves to position a control valve. This valve in turn applies hydraulic pressure to one side of the actuation cylinder under control to move it to the desired position.

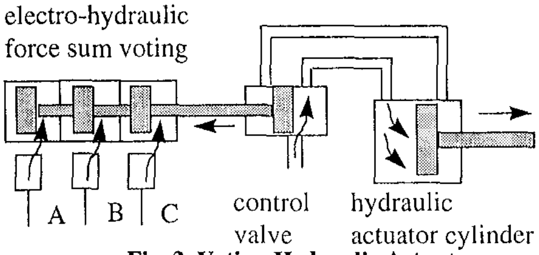
electro-hydraulic force sum voting
A
B
C
control valve
hydraulic actuator cylinder

Fig. 3. Voting Hydraulic Actuator

Bringing the benefits of ultra-reliable controls to a wider range of systems will require that affordable alternatives to these specialized voting actuators be developed. One promising approach is to minimize the complexity of the actuator, using redundant electric voting circuits instead of hydraulics. This also conforms to the current trend toward greater use of low-maintenance electrical actuation in favor of hydraulic actuation. Another type of actuation voting is also needed for ultra-reliable control systems. On or off (discrete) output types such as energizing solenoid valves, turning on or off sources of electrical power, firing pyrotechnic separation and ignition devices, and operating electric motors also require fault-tolerance. The Space Shuttle orbiter provides an example of the need for an ultra-reliable electrical actuation device. As part of the shuttle launch to orbit sequence, the avionics system is required to control the firing of the pyrotechnic devices that ignite the Solid Rocket Boosters (SRBs) and later control separation of the SRBs and external fuel tank. Either a failure to fire, or premature firing, would have catastrophic consequences for the shuttle. To ensure dependable operation, the shuttle uses special Master Event Controller (MEC) electronic units to vote on the consensus of computer commands to initiate these critical events. [2]. Conceptually, the MEC uses logic similar to the simple discrete voting logic illustrated in Figure 4, on next page.

Briefly, the discrete electronic voter uses electronically controlled series switches operated by channels A, B and C of the control system to switch power source Va, Vb or Vc to diode "or" logic. Should any two of the three channels issue commands to close the switches, the output will be energized (fired). No channel acting alone can fire or prevent the firing of the output. These types of devices also insure that failure of one source of electrical power, Va, Vb or Vc does not result in a loss of the function. Any approach directed toward making ultra-reliable systems affordable must not lose sight of the importance of these output voting devices and costs associated with them.

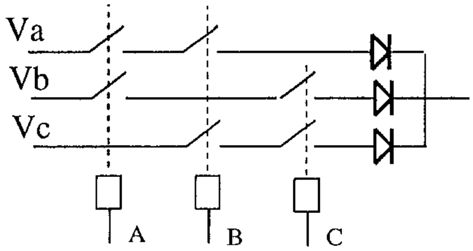

Fig. 4. Discrete Electronic Voting

APPLYING AUTOMOTIVE AND INDUSTRIAL ELECTRONICS TO ULTRA-RELIABLE CONTROLS

A promising approach for reducing the cost of I/O for affordable but dependable systems can be found in components being introduced into automobiles and industrial control systems. These industries have made a large investment toward making data multiplexing available for cost sensitive applications. Two popular approaches are the Controller Access Network or CAN bus and the Echelon Corporation LonWorks bus. The CAN bus, originally developed by Robert Bosch GmbH for the automotive market, has also been adapted to industrial control applications. The LonWorks bus has been primarily applied to industrial controls. Either bus, and other similar buses, offer great potential for developing affordable, dependable controls. In today's automobile and industrial controls, these buses are applied primarily to allow two control computers to communicate. For future systems, the advantage that the automotive/industrial approach offers is that the data multiplexing electronics become small, inexpensive, rugged and low enough in power to be embedded directly into the sensor or actuation device. Ideally, a single "chip" is integrated directly with the sensor or actuator, allowing that device to directly interface to a shared I/O data bus without need for analog signal connections as shown in Figure 5. Further miniaturization and cost reductions could be realized by integrating the data multiplexing electronics with single chip sensor or by combining them with Micro Electro Mechanical Systems (MEMS) sensors.

Using these "smart" sensors and actuators that directly produce digital outputs, data multiplexing units are eliminated, along with the analog signals and associated wiring. The CAN and LonWorks buses both offer data rates as high as 1 million bits per second, allowing potentially hundreds of sensors and/or actuators to share the same bus wires. Using this I/O bus approach, the cost and complexity associated with the redundant sensors and multiple input, voting actuation devices needed for ultra-reliable systems is made manageable. Figure 6 illustrates an ultra-reliable, redundant system architecture constructed using the I/O bus approach.

For the actuation devices, electronic circuits that provide the voting function are also embedded into the actuator, interfacing directly to the automotive / industrial demultiplexer electronics. At Draper Laboratory, experimental testing of a breadboard system using the CAN bus and integral electrical voting planes has demonstrated these concepts. Low-cost multiplexing and integral electrical voting plane architectures holds great promise for making ultra-reliable systems affordable. There are also many other benefits of this approach.

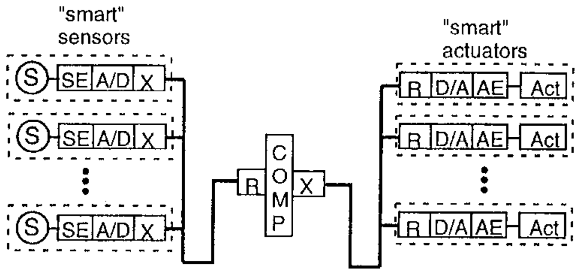

Fig. 5. Control System Using Automotive / Industrial I/O Bus

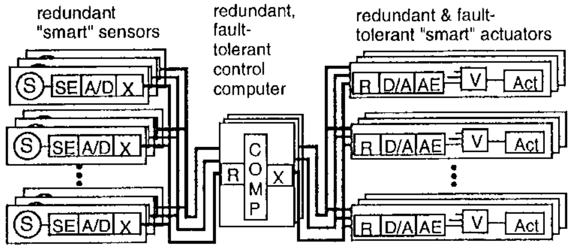
redundant "smart" sensors
redundant, fault-tolerant control computer
redundant & fault-tolerant "smart" actuators
S
SE
A/D
X
R
C O M P
X
R
D/A
AE
V
Act

Fig. 6. Ultra-Reliable System Architecture Using the I/O Bus Approach

FLEXIBILITY OF THE 110 BUS APPROACH

The design of the electronic control system has a significant impact on the cost and schedule associated with developing new systems. The design effort is significantly increased if ultra-reliability is a goal, owing to redundancy requirements and attention to common mode failure concerns. In today's FBW systems, the addition of a new sensor or actuator, or the relocation of equipment can substantially impact the design of wiring and the number and location of data multiplexing units. Changing the allocation of analog sensor signals and actuation power signals that are bundled together in wiring requires a reevaluation of electromagnetic interference and grounding issues. Spare I/O channels must be allocated in anticipation of growth or change. Exceeding the anticipated growth can require major redesign. Software must be designed or redesigned with knowledge of the physical path between computers and I/O devices. A significant development advantage can be obtained by using an I/O bus approach. With a method to easily connect sensors and actuators to the bus, sensors and actuation devices can be added or moved easily, with few restrictions on growth. The use of digital signals minimizes concerns about signal interference. Software can be written to interface with sensors and actuators by logical address only, independent of physical location. The system can easily grow, without weight, power or size penalties for carrying spare I/O capacity.

AFFORDABLE HARDWARE REDUNDANCY SIMPLIFIES REDUNDANCY MANAGEMENT

The development of Fault Detection, Isolation, and Reconfiguration (FDIR) software for ultra-reliable systems is difficult and expensive. Somewhat counter-intuitively, much of this difficulty stems from too little, rather than too much, hardware redundancy. The process of detecting sensor faults from three redundant sensors is straightforward. The well established approach of middle value selection and majority signal voting can be applied, and the designer can be confident in the ability to detect and recover from even subtle sensors failures. The problem becomes much more difficult when less then three redundant sensors are used: sensors and electronics must be designed to provide easily recognizable failure signals; to increase assurance that all failures are detected, complex mathematical models are often included into the real-time software to provide a comparison to the sensor readings. Similarly, for outputs, utilizing triple redundant command signals with a hardware voting plane at the actuator is very effective for detecting and masking the effects of failures. When only two outputs are available, some form of an active/standby arrangement is needed, with complex and critical software needed to determine when switchover from the active output to the back-up is required to accommodate failure. The use of the I/O bus approach makes a straightforward triple redundant with output voting architecture small and affordable. This eliminates the incentive to use less redundancy that results in complex redundancy management software.

ULTRA-RELIABLE SYSTEM ARCHITECTURES OFFER INHERENT HEALTH MONITORING AND DIAGNOSTIC CAPABILITIES

The need for I/O redundancy to allow the system to fail operational is obvious. An additional benefit associated with redundant sensing and actuation is that it can greatly enhance the performance of automated Vehicle Health Monitoring (VHM). The availability of redundant measurements improves the ability to detect failures, minimizes false alarm fault reporting, improves the ability to automatically isolate faults to a single unit, and eliminates ambiguities in deciding if a failure is mechanical or electrical [3]. Effective VHM can reduce maintenance costs and ensures that back-up redundancy is ready to operate when needed.

ULTRA-RELIABILITY ALLOWS FOR DEFERRAL OF MAINTENANCE

The ability of an ultra-reliable system to provide uninterrupted operation following failure not only provides the high operating reliability needed by autonomous systems, but can greatly simplify maintenance logistics. Instead of requiring immediate, unscheduled maintenance to restore the system, repair personnel have the option to postpone the repair until parts or service personnel are available, the system has arrived at an appropriate repair depot, or the system is shut down for other routine scheduled maintenance. The ability to operate following failure is made possible by a combination of redundancy and confidence in the ability to detect, correctly isolate, and contain the effects of a failure. Affordable redundancy brings this benefit to more systems.

BENEFITS OF INTEGRATED ELECTRICAL POWER CONTROL

Because of concerns for common mode failures and the high cost of providing fault-tolerant switching of electrical power, previous systems have avoided integrating the control of electric power with other control functions. In systems such as the Space Shuttle, the control of electric power is performed manually by the crew. Placing control of electric power under the control system computer offers many advantages: system power-up and shut down can be automated; electric power load monitoring and management can be fully automated; electrical power can be automatically rerouted using power bus cross ties in response to failures; automatic cutoff of electric power can be used as a means of securing failed equipment to provide safe operation following failures and power wiring and manually operated switches and circuit breaker panel hardware are reduced. The redundant I/O bus approach, complemented by other advances in low-cost power switching devices, makes it practical to provide affordable, fault-tolerant power switching and control, allowing power control to be fully integrated with other control system functions.

SOFTWARE ERRORS WILL REMAIN A PROBLEM

Even with an ultra-reliable hardware architecture, software errors remain as a common mode of failure. Techniques such as N-versions of dissimilar software in each channel can be applied, but this approach is expensive and introduces new concerns. For now, the widely accepted approach appears to be a tightly controlled software design process and exhaustive verification to eradicate software errors. As previously described, the I/O bus architecture can simplify the redundancy management software, at least provide some simplification to the verification of these software functions. Hopefully, new techniques for software development or formal methods for verification will be developed that provide a better solution.

REALIZATION OF AFFORDABLE, ULTRA-RELIABLE CONTROLS

The I/O bus architecture approach described is very promising, but would be difficult to produce today. Few sensors are available that can directly interface to a low cost bus. Those that are were designed for industrial applications where weight, power or rugged design are not as great of a concern. For some applications, the temperature range that some sensors and actuators must operate in is too severe for off-the-shelf automotive or industrial parts. There is limited consensus on bus standards that would open the door for greater availability of off-the-shelf sensors and actuators. Few industrial control applications demand ultra-reliability and as a result, off-the shelf fault-tolerant actuators are not available. But it seems likely that demand for these types of systems will prevail. Parallel developments in single chip sensors, high temperature electronics, MEMS and power switching semiconductors will all contribute toward making the approach practical. Visionary developers will build these systems, at first using custom designed sensor and actuation components. Later, these custom components will evolve into off-the shelf equipment, with the development of standards to allow for interchangeable components from different manufacturers. The availability of completely dependable but affordable control systems will free system designers to use controls to extract greater performance and efficiencies from tomorrow's systems.

SUMMARY

The case has been made that future systems will require controls that are as sophisticated and dependable as today's FBW Systems, but must be much smaller, lighter, lower in power and less expensive. The difficulty of meeting this need with today's system architectures has been described. An approach that eliminates analog signaling and separate multiplexing units by embedding data multiplexing devices directly into sensors and actuators has been described. The benefits that this provides both in terms of increased reliability and indirect benefits of increased flexibility during development, improved fault diagnostic capability, simplified redundancy management software and integral control of electric power were described. The need for visionary developers to take steps toward building such systems was discussed.

REFERENCES

[1] Prizant, J., November 1998,
High Speed Communicator for Real Time Fault Tolerant Systems,
Digital Avionics Systems Conference, Seattle, WA.

[2] Hanaway, J. and Morehead, R.,
Space Shuttle Avionics Systems,
NASA publication SP-504, TL3025.H36.

[3] Hammett, R.C., November 1996,
Seawolf Ship Control Performance Monitoring Provides Fault Tolerance and Simplified Maintenance,
ASNE Intelligent Ship Symposium, Philadelphia, PA.

Systems Magazine Situations Wanted Column

As part of the Board of Governors ongoing effort to assist AESS members who are unemployed, or soon to be unemployed, we offer the opportunity to run a single paragraph, *"Situation Wanted"* ad in ***Systems Magazine***. The ads should be sent to: ***IEEE AESS Systems Magazine***, 4500 North Park Avenue, Chevy Chase, Maryland 20815; ATTN: D. Dobson, or fax (301) 657-0209. Ads will run for two months at no charge.

Below is a sample format. Ads are strictly limited to a 60 word maximum. Names are optional: include a telephone and/or fax number where you can be reached by interested parties. If you have questions, contact Tim Grayson at the address on Cover 2.

SAMPLE FORMAT: Electrical Engineer seeking Systems Engineering position, BSEE, graduate work in computer science. 14 years experience in the development of both military and commercial avionics. Extensive experience in the negotiation, development and allocation of system requirements. Familiar with both Military and FAA specifications. Proficient with PCs. Good verbal and written communication skills. Will relocate. Call (101) 234-5678.