Safety of Fly-by-Wire Systems

Herbert Hecht, Ph. D.
SoHaR Incorporated
Culver City, California

The glass cockpit and fly-by-wire systems have in many ways made air travel safer and more comfortable. But they also have created a new class of safety concerns that requires new methods of analysis. Because these systems are flight critical they must meet the requirement of FAR 25.1309 that "the occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable." A single string implementation obviously does not meet that requirement and thus redundancy is used in all practical systems. Usually software is employed to monitor the failure conditions and to activate an alternate.

This software is carefully verified by the developer and reviewed by a certifying body, the FAA Aircraft Certification Office. But in spite of these safeguards glitches are found, such as the following that are excerpted from the FAA Airworthiness Directives referenced at the end of each description.

> It has been found that some "caution" messages issued by the Flight Guidance Control System (FGCS) are not displayed on aircraft equipped with [certain] QQQ software load[s]. Therefore, following a possible failure on one FGCS channel during a given flight, such a failure condition will remain undetected. If another failure occurs on the second FGCS channel, the result may be a hardover command by the autopilot. An unexpected hardover command may cause a sudden roll, pitch, or yaw movement, which could result in reduced controllability of the airplane. (AD 2008-17-11)

> We have received reports of in-flight unannunciated shifts of computed position in airplanes with XXX navigation and YYY integrated avionics computers serving Flight Management Systems (FMSs). The computed position shift, attributed to a software design error induced during a previous software modification, occurs when the number of inertial reference units (IRUs) supplying data to the FMS degrades from 3 to 2 or from 2 to 1, or increases from 2 to 3 or from 1 to 2. If the FMS system is coupled to an autopilot or flight director system, this shift in the FMS computed position could result in uncommanded deviations from the intended flight path of the airplane and, if those deviations are undetected by the flight crew, compromised terrain/traffic avoidance. (AD 2007-07-12)

> We received a recent report of a significant nose-up pitch event on a ZZZ airplane while climbing through 36,000 feet altitude. The flight crew disconnected the autopilot and stabilized the airplane, during which time the airplane climbed above 41,000 feet, decelerated to a minimum speed of 158 knots, and activated

> the stick shaker. A review of the flight data recorder shows there were abrupt and persistent errors in the outputs of the inertial reference unit. These errors were caused by the operational software using data from faulted (failed) sensors. This problem exists in all software versions … While these versions have been installed on many airplanes before we issued AD 2005-10-03, they had not caused an incident until recently, and the problem was therefore unknown until then. Software using data from faulted sensors, if not corrected, could result in anomalies of the fly-by-wire primary flight control, autopilot, auto-throttle, pilot display, and auto-brake systems, which could result in high pilot workload, deviation from the intended flight path, and possible loss of control of the airplane. (AD 2005-18-51)

The ultimate correction in each of these conditions involved a software change but that does not imply that the problems were the fault of the software developers. They were most likely due to lapses in the analysis and formulation of system requirements. The aircraft involved as well as the subsystems that caused the problems were produced by responsible organizations and had undergone multiple levels of testing. The problems were not found because the tests did not cover the specific conditions that caused the failures. The lack of test coverage implies incomplete requirements because compliance with every stated requirement must be established by at least one test.

At this point it must be admitted that it is very difficult to write requirements for all anomalous situations that an aircraft or a control system may encounter. Single failure modes that arise within the subsystem are usually well understood by the designer. But multiple failures happen, and they can lead to unexpected and dangerous results. Also, the subsystems don't operate in a cocoon; there are multiple interactions with other subsystems. Close reading of the above examples shows initiating events that were not classical computer or sensor failures but interactions between anomalous states in several subsystems. These interactions occur much less frequently than conventional failures but they do occur and are therefore not "extremely improbable". A requirement for testing of every exception state of a flight critical system with each of the possible exception states of every interfacing function may be prohibitively expensive but a systematic approach must be found for assessing the criticality of possible interactions of anomalous states across systems and functions.

As an example of a systematic approach we list these operational interfaces of a typical civil transport flight control system (zonal interfaces are excluded here):

- Electric power
- Environmental control
- Communication (aircraft buses)
- Thrust control
- Outer loop functions (navigation, collision avoidance)
- Real time monitoring (cockpit annunciation)
- Non-real time monitoring (maintenance)

Each of these interfaces can then be further partitioned into functional threads. A hypothetical example of functional threads at the interface between electric power and flight controls is:

- Duration of transients or interruptions during reconfiguration of the power system
- Required/desired reconfiguration of the flight controls under emergency power (e. g., disabling redundant channels, reversion to minimum fly-by-wire system)
- Uninterruptible power for minimum flight control configurations
- Temperature control of flight control components
- Concise and prioritized annunciation of multiple anomalies

For each of these threads a criticality level can be established and those of the highest criticality can be further decomposed into testable requirements. Decomposition is not a solution by itself but it reduces the likelihood that significant interactions are overlooked and it opens redundancy management requirements to detailed review. The minutes of working groups that assign criticality levels and that formulate the testable requirements can form the starting point of an improved approach for certification of flight critical systems.

BIOGRAPHICAL SKETCH
HERBERT HECHT

Herbert Hecht is Chief Engineer of SoHaR Incorporated, an R&D and consulting company for high dependability systems. The name of the company is a contraction of Software and Hardware Reliability. In addition to his managerial duties he supervises technical work in hardware and software reliability analysis, sneak circuit analysis and safety analysis. His current research interests include causes of failure of software intensive systems and economical methods of software verification. Prior to joining SoHaR he was employed at The Aerospace Corporation, El Segundo CA and Sperry Flight Systems, Phoenix AZ.

Hecht's professional activities include a term on the Board of Governors of the IEEE Computer Society, service as Visitor in Computer Engineering for ABET, and membership in standards working groups of the IEEE, the AIAA, and the ISA. He is currently participating in IEEE/AIAA Project 1633 "Recommended Practice for Software Reliability Prediction". He is the author of *System Reliability and Failure Prevention* published by Artech House, 2004 and chapter author for Reliability in several volumes of the *Space Mission Analysis and Design (SMAD)* series edited by James Wertz and Wiley Larson and in *Fault-Tolerant Computing* edited by D. K. Pradhan. He has over 100 papers in refereed journals or conference proceedings and holds 12 patents in the field of highly reliable control systems. He is licensed as a Professional Engineer in Control Systems Engineering by the State of California.

Hecht received a Bachelor of Electrical Engineering degree from City College, New York, and an MEE from Polytechnic Institute of Brooklyn (now part of Polytechnic University). In 1967 he received a Ph. D. in Engineering from the University of California at Los Angeles, with a dissertation on Economics of Reliability for Space Launch Vehicles.