2/21/03

John,

Many thanks for the opportunity to participate in discussing a subject that continues to fascinate me. Please feel free to forward this to any you deem appropriate.

As background, I have had a varied career in Military electronics, manufacturing engineering, systems engineering and of course Automatic Test Equipment (ATE) applied to both shipboard and aircraft maintenance. I am most recently semi-retired (quit actually, but too young to draw a retirement check <grin>) from Civil Service, working for Naval Aviation Systems Command supporting the F/A-18 aircraft since 1983. I have approximately 30 years of experience in ATE systems, spanning five generations of ATE system development. I am presently employed as a Senior Principal Systems Engineer with a well-known DOD Systems Integrator. 90 % + of our work is for the US Navy.

I have read the literature you were kind enough to provide, and all viewpoints are well taken, as far as they go. As I interpret the different writings, the intent seems to be to: 1) eliminate NFF wasted maintenance and increased risk hazards by more comprehensive testing, 2) pioneer and deploy enhanced testing techniques through parallel processing – to detect random, one-shot failures (my terminology), 3) as well as inject some insightful, realistic procedural rules in ground maintenance. Especially when considering AMR Flight 587's 12 previous sub-system failures with the rudder control system that failed to provoke a more in-depth review.)

In my years with the F/A-18 ATE, NFFs have robbed a significant amount of resources, causing needless maintenance actions on perfectly good (or so they seemed at the time) Avionics modules.

From my perception, there seems to be a major assumption by all that is in fact deeply flawed. Each of the respondents have presented their views, *seemingly based on the unspoken premise that aircraft power and control system design is an "Intrinsically Safe" system.*

In my opinion, it is not.

Indeed, the Emperor has no clothes.

Heresy you may ask? Not really. I say this because I know for a fact that many aircraft types do not generally employ design techniques *proven* to ensure integrity of control systems, i.e. computers. How then, could the basic design be considered safe?

You see, unappreciated by many aviation power system and control folks; computer systems, analog, hybrid, or digital, have been used on the ground for many years. Successfully, I might add. Land based computer systems have had more than their share of problems as well, actually with many similarities to aviation NFF issues. For instance, each time my home computer "locks-up" I just grit my teeth and reboot it. If I were an aircraft commander, I might reset the circuit breaker to hopefully clear a "glitch".

Over the years, the commercial computer industry has spawned an offshoot industry segment called "Power Quality" (PQ). PQ is concerned with the proper care and feeding of computer systems that our economy now depends upon. The PQ services and products market is an approximate $6B per year industry. Frost and Sullivan reported in January 2002 Power Quality Magazine, that PQ issues; voltage transients etc. cost industry $26B per year in losses. Well, they don't mention the aircraft industry, because there is no Power Quality as such to be found.

As the PQ industry matured, guides for recommended practice evolved. PQ had its early beginnings in the 1970s based on a Navy study concerning the causes of service outages at regional computer centers.

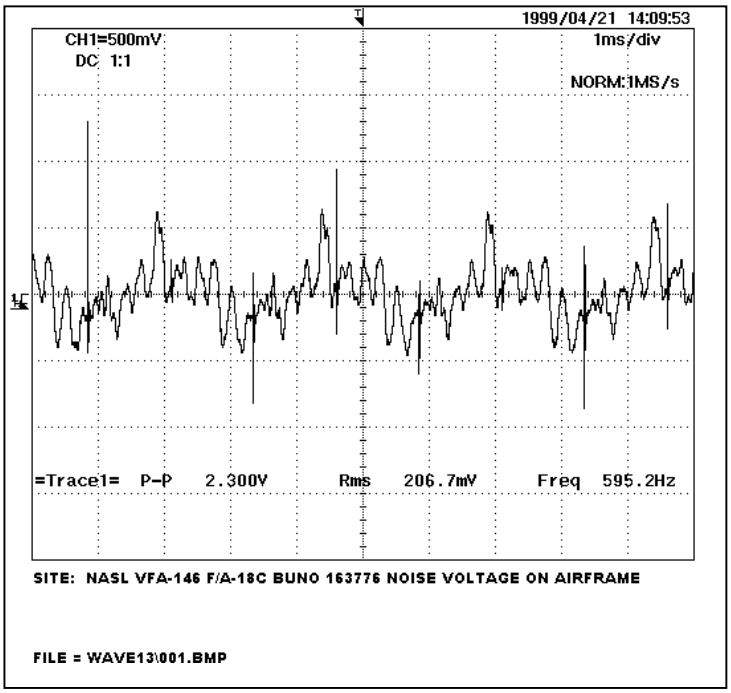
In 1983, the US Department of Commerce published the first generally accepted Federal guideline establishing newly recognized standards for the powering and grounding of sensitive electronic systems. It is the Federal Information Processing Standards Publication No. 94, known as FIPS PUB 94. Although now withdrawn, it did

serve as an excellent guideline to define the Facility or PLATFORM INTERFACE necessary to support sensitive electronic systems operations. FIPS PUB 94 defined all aspects of power systems anomalies, including types of upsets, and particularly the requirements for a stable voltage reference system.

In 1992, the Institute of Electrical and Electronics Engineers published IEEE Recommended Practice for Powering and Grounding Sensitive Electronic Equipment, IEEE STD 1100-1992. This standard provided a consensus of recommended practices for powering and grounding electronic equipment in commercial and industrial environments. The 1100 STD is also known as the EMERALD book in the IEEE Color Book Standard series. In 1999, the IEEE published a greatly expanded update.

Central to published PQ recommended practice, is the concept of circuit separation. I group all circuits into three categories, Signal, Power, and Voltage Reference. The rule of thumb I have learned by experience and observation, is never combine unlike circuits! A very common PQ error for ground computer platforms/facilities is two or more power Neutral bonds to the ground plane. This combines the voltage reference (Ground) with a power circuit (Return). The result in chaos from a control standpoint. It allows power currents to flow on the chassis of computers, disrupting the voltage reference plane. This is identical to aircraft design in which AC Neutral or DC currents are allowed to return via the airframe. IEEE Std 1100-1999, paragraph 6.4.1.1.1 “Improper, extraneous neutral-ground bonds are a relatively common problem that not only create shock hazards for operating personnel, but can also degrade the performance of electronic equipment." While MIL-STD-461 does allow this in certain cases, the UK EMI standard, Defense Standard 59-41, does not.

The airframe is not a -0- Volt plane. Here is a picture of an F/A-18 airframe with ground power applied and Avionics running systems checks.



It’s interesting to note that the Ground plane Interference EMI Specification for the FA-18 is < 1 volt RMS above 500 Hz. This is to avoid damage to the Avionics, I learned in a phone call to a Boeing expert.

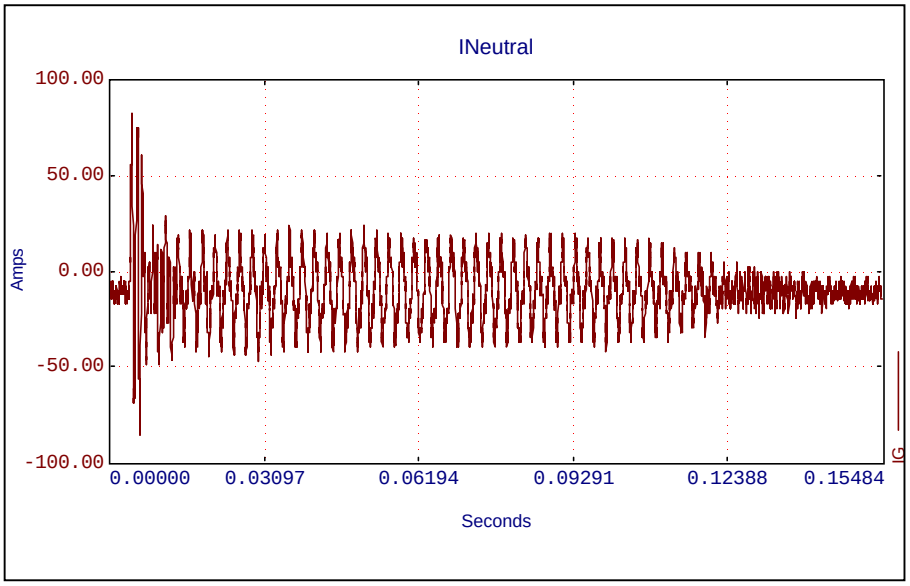
Voltage transients propagated via the ground plane can force truth table violations of integrated circuits. When these violations occur, three things can happen: Type I, Signal-Data Disruption; Type II, Gradual Hardware Stress

and Latent Failures; Type III, Immediate Hardware Destruction. Reference IEEE Std. 1100-1999. This in my opinion is the cause of many of the NFFs as well as hard failures of Avionics.

Boeing and the FAA published "Aircraft Electromagnetic Compatibility Final Report" in 1987, (DOT/FAA/CT-86/40). In it page 3 suggests that routing power and power return wire twisted together, not using aircraft structure as a circuit return path will almost eliminate electromagnetic interference modes. This is consistent with National Electrical Code, Article 250 which forbids power current flow over the chassis or ground systems. As a code of practice, NEC is used in litigation to recover damages related to violations.

Does random upset of computers cause flight control problems? Yes, in fact they do. See Dr. Belcastro's papers on the Langley Technical server. http://techreports.larc.nasa.gov/ltrs/abs.html. She has done some fascinating experiments with High Intensity Radiated Field (HIREF) effects on flight control systems. I stipulate here that common-mode coupling issues can cause the same effects Dr. Belcastro noted during her experiments. I have provided her paper; **Closed-Loop HIRF Experiments Performed on a Fault Tolerant Flight Control Computer,** 16th *Digital Avionics Systems Conference* for you with this mailing.

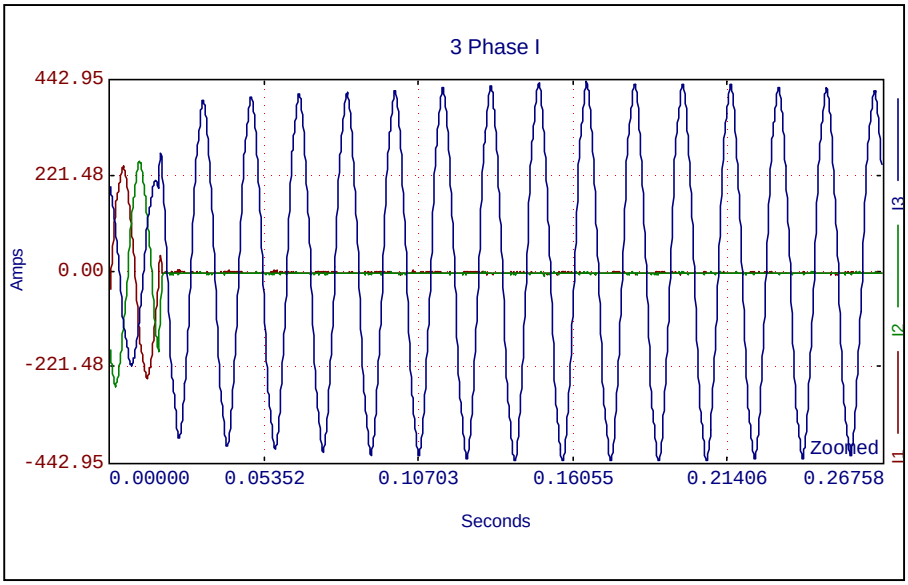
With the fuselage carrying power return currents, and the control circuitry referenced as well to the fuselage, can you not see how power transients can be coupled into control circuits? Even without causative failure, normal load changes can induce large current transients on the airframe, thus inducing –e = L (di/dt) effect transient voltages into Avionics equipment.



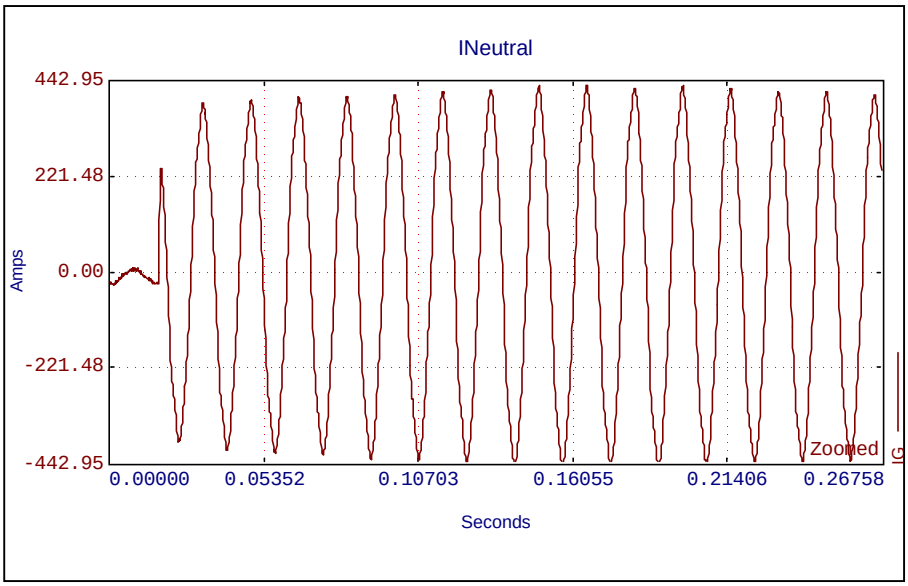
The above is a normal current transient caused by an SH-60 Helicopter auxiliary hydraulic pump start. The Avionic boxes are bonded to the aircraft and the bond serves as a connection to a voltage reference – the fuselage. Any degradation of the bond, *as in aircraft aging, for instance,* and –e = L (di/dt) voltage transients are developed. These transients may cause a Type I, II, or III upset of the Avionics as per the IEEE-1100 standard.

Current and voltage transients caused by component failures are very similar. When a power-switching component is degraded, an induced transient can form. The below shows a fault with a ship's shore power circuit breaker or line contactor. During the shift from shore to ship power, one of the three phases failed to disconnect for approximately one second. This resulted in a severe current transient being induced through the hull of the ship.

The current plot showing phase C failing to open.



The resulting Neutral current surge.



Interestingly, during faults in which a phase opens and causes current to flow over structure, the structural current path mirrors the routing of the power conductors. This is known to cause arcing at conduit joints. This is one of the reasons why the NEC considers an AC distribution system with a multiple grounded neutral to be a fire hazard.

So, in summation, I see that in my opinion, only one of the three apparent primary issues is valid. That of improving procedural rules to illuminate trends. Is more comprehensive testing necessary, or new, parallel processing test methodology needed?

Improved digital testing may help detect latent failures such as the IEEE Std 1100-1999, Type II failures. But perhaps much more improvement would be needed to make a real difference. For instance, if the ATE systems used allowed a history file of test results for each serial numbered LRU, than perhaps trends, including incipient failures (marginal pass) could be identified before they became an in-flight issue. But first things first.

Get the basics right. Eliminate the common-mode entry paths that upset the control system. By not taking all necessary steps, including applying known recommended practice, the aircraft industry has failed to provide the public with an *Intrinsically Safe* system.

I will be happy to continue this discussion at your convenience.

Very truly yours,

Michael E. McClelland

Senior Principal Systems Engineer
Anteon Corporation
(559) 583-7491

PS:
Dr. Celeste M. Belcastro's papers on Langley technical server:

Paper no. 351. Celeste M. Belcastro, Robert Fischl and Moshe Kam, **A Monitor for the Laboratory Evaluation of Control Integrity in Digital Control Systems Operating in Harsh Electromagnetic Environments,** NASA TM-4402, October 1992, pp. 21.

Paper no. 1586. Celeste M Belcastro, **Closed-Loop HIRF Experiments Performed on a Fault Tolerant Flight Control Computer**, *16th Digital Avionics Systems Conference*, Irvine, California, October 26-30, 1997, (2MB).

Paper no. 2464. Celeste M. Belcastro, **Detecting Controller Malfunctions in Electromagnetic Environments: Part II---Design and Analysis of the Detector**, *1999 IEEE International Conference on Control Applications*, Kohala Coast, Hawaii, August 22-27, 1999, (783KB).