6-2018

Role of Diagnostic Monitoring Software Versus Fault-Tolerant Components in the Development of Spacecraft Avionics Systems

Andrew Attorri

Role of Diagnostic Monitoring Software Versus Fault-Tolerant Components in the Development of Spacecraft Avionics Systems

By

Andrew Attorri

* * * * * * * * *

Submitted in partial fulfillment
of the requirements for
Honors in the Department of Mechanical Engineering

UNION COLLEGE
June, 2018

ABSTRACT

ATTORRI, ANDREW Role of Diagnostic Monitoring Software Versus Fault-Tolerant Components in the Development of Spacecraft Avionics Systems. Department of Mechanical Engineering, June 2018.

ADVISOR: Professor Ann M Anderson

In any spacecraft, there are several systems that must work simultaneously to ensure a safe mission. One critical system is the 'avionics' system, which is comprised of all of the electronic controls on-board the spacecraft, as well as radio links to other craft and ground stations. These systems are present for both manned or unmanned spacecraft.

Throughout the history of spaceflight, there have been several disasters related to avionics failures. To make these systems safer and more reliable, two main strategies have been adopted. The first, more established approach is through use of fault-tolerant components, which can operate under a wide range of conditions in the harsh space environment. The other, newer approach is to use software systems to monitor components in real-time to predict where failures may occur, and if they do occur, reconfigure the system itself to mitigate potential disasters.

Though both approaches are necessary for an effective avionics system in modern spaceflight, monitoring software should be more heavily emphasized moving forward. At this point, the vast majority of avionics failures aren't related to specific component failures, but wider systematic failures. Past history has shown that the ability of crew members and ground controllers to respond to system failures has mitigated potential disaster, and monitoring software is the most effective means of allowing enabling an effective response.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

BACKGROUND

Section 1.1 – Functions of Avionics Systems

During spaceflight, there are many systems and components that must perform reliably in order to prevent disaster. The failure of any component could potentially end in the death of crew members or result in the loss of rockets or equipment costing millions of dollars. One such critical system is the ‘avionics’ system. The term avionics describes the electrical controls on board an air or spacecraft, as well as any ground station. It is often possible for ground station operators to communicate directly with the craft, during either manned or unmanned spaceflight. This communication between ground station and spacecraft is known as telemetry.

Typically when discussing avionics systems for space vehicles, there are four main subsystems: crew interface, flight control, navigation, and communication [1]. These subsystems perform all of the important functions needed for a successful flight. The crew interface is made up of hardware such as switches, heads-up displays, and joysticks that crew members can directly use. Systems that make rocket modules safe for crew members, such as those that keep the cabin pressurized or control air quality, may also be considered part of the crew interface. The flight control subsystem refers to the controls used to adjust the attitude and trajectory of the rocket, while navigation more broadly refers to the path of the rocket during orbit or the coasting flight between two planetary or lunar bodies. The communications subsystems deal with the radio uplink and downlink or telemetry between the spacecraft and ground station. These systems have consistently evolved over the years, and will to continue to change as the functional requirements of avionics systems shift.

Section 1.2 – Risk Factors of Avionics Systems

Figure 1 presents historical causes of mission failure as determined by NASA and shows how the subsystems that comprise the overall avionics system often cause failures.

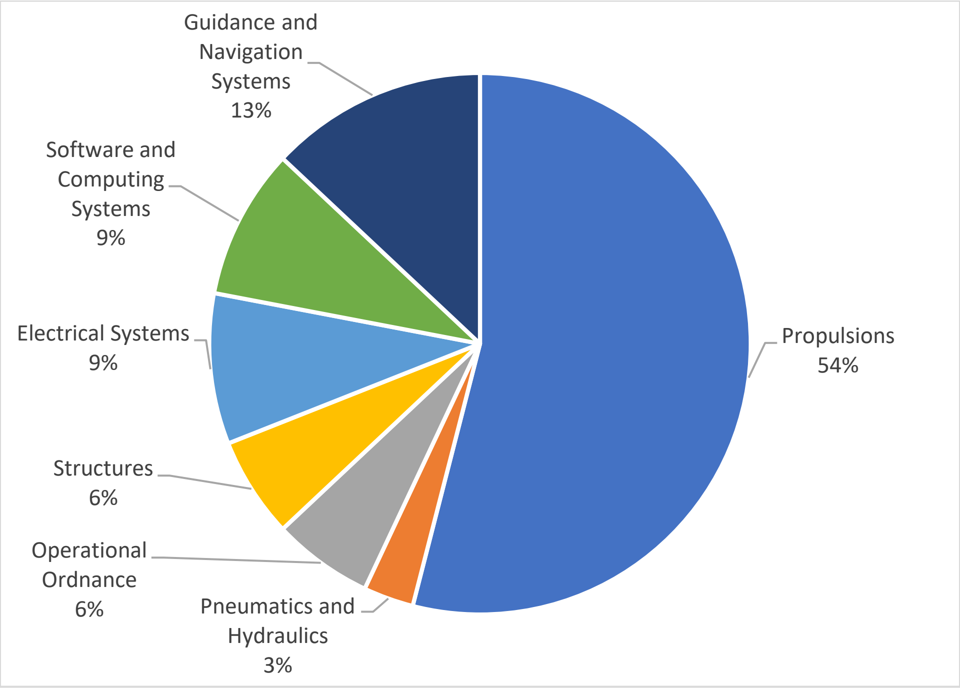


Figure 1- Historical Risk Factors, adapted from [2]

During a normal spaceflight, avionics may be exposed to high acceleration, high temperatures, vibrations, excessive humidity or fluctuations in any of the above conditions as well as changing electrical conditions [3]. Even properly designed and manufactured components may degrade in quality overtime, leading to failures.

While the operating environment inside the spacecraft or directly surrounding the system may cause failure, another factor that must be taken into consideration is the effect of the natural space environment. A perfectly designed and assembled component that operates properly on Earth's surface will still be subject to other harsh conditions while in space.

Among the many effects that can cause an avionics component to malfunction are changes in thermal energy at different points around Earth's orbit, the presence of plasma, and ionizing radiation. According to a NASA study these causes have been the most common cause of failure due to the natural space environment throughout the past few decades [4]. These causes often deal heavily with changes in the chemical makeup of the upper atmosphere, and as a result can be particularly damaging to orbiting satellites.

Changes in thermal energy have caused issues in several different satellites. In 1993, thermal expansion on the support poles of solar arrays on the Hubble Space Telescope caused vibrations, which negatively impacted pictures from deep space for a short period. Likewise, an antenna on the Galileo probe headed toward Jupiter failed to deploy because the lubricant used on the mechanical joints was outside its temperature range and failed.

The presence of plasma particles in the upper atmosphere can lead to a variety of issues as the imbalance of ions and anions impacts avionic circuitry, especially semi-conductors. According to NASA, over a period from 1971-1993, this effect caused at least 40 different orbiting satellites to experience malfunctions that required maintenance [4]. Many of these issues were due to electrostatic discharge. It is interesting to note how many of these satellites were communications or locating (for example GPS) satellites, which goes to show that avionics failures can have an impact on everyday life, even in unexpected circumstances.

As another major source of avionics failures, radiation has caused numerous incidents throughout the years. It has been speculated that radiation has caused a majority of previously unattributable failures [5]. A good example of this is the 1994 case of the Japanese Engineering Test Satellite (ETS-1). Due to erosion caused by radiation reflected by the Earth, the solar panels that provided power for the satellite dropped from 5.8 kilowatts to 4.7 kilowatts within just one month. The efficiency of the panels further decreased to 2 kilowatts, which was too low to power experiments. The ETS, which had cost $415 million, was only operational for one year [4].

Other potential causes for variations in avionics components are fluctuations in the intensity of solar energy, fluctuations in the Earth's geomagnetic field, and damage caused by space debris.

Based on all of the myriad noted avionics issues, engineers have determined that they must figure operational environment into their designs. To that end, fault-tolerant devices are designed to function properly in a wider range of operating conditions. However, many of the causes of past failures can't be altogether prevented during design or manufacture, though past experiences have instructed the industry on how to improve design. A good example of this is impact that the Apollo 13 accident had on future Apollo missions [6].

While most historical examples of avionics failures have led to changes based on the specific failure mode, a broader approach has been applied to making improvements to the reliability of avionics systems. One tool presented by NASA categorizes failures in terms of mission parameters as way to determine which procedures and protocols had the most positive effect on flight success and crew safety. From a long list of parameters, they determined that focus on design margin, critical system redundancy, emergency systems, and override capability for autonomous systems had the most positive impact [7].

Recent cases of launch failures underscore the inherent effect of human-driven faults, even in cases when the component design is sound. During a 2017 launch, a Russian Fregat rocket that was to ferry a weather satellite into a higher orbit instead fired its engine early and crashed in the Atlantic Ocean. The problem was that the upper rocket stage attached to the satellite was pointed in the wrong direction. It had been launched from the new Vostochny Cosmodrome launch site, and the software engineers hadn't reprogrammed the software [8] to include the new site coordinates, leading to the rocket being pointed in the wrong direction as it fired its engine. Another, non-avionics related case occurred in 2012 when a new model of the Russian Proton-5 rocket was overfilled with liquid oxygen fuel, resulting in an overweight rocket that crashed into the Pacific Ocean along with its payload. The fuel tank had been adequately redesigned, but the procedure for filling the tanks hadn't been updated [8], leading to the error.

The point of these examples, even though one isn't an avionics case, is that even in perfectly designed systems with perfectly reliable components in normal operating conditions, issues can arise when not implemented correctly. In terms of fault-tolerant devices, it illustrates that perfectly designed and manufactured components and subsystems can still perform unreliably outside of expected conditions. This means that a system that can automatically monitor faults is valuable in responding to possible failures.

Section 1.3 – Development of Avionics Through History

Over time, the ability to monitor critical subsystems has evolved. Starting with NASA's Mercury program, most avionics involved the pilot monitoring output on some kind of gauge and comparing it to reasonable minimum or maximum values. Gauge outputs often needed to be cross-referenced with other instruments to confirm the output, as well as verify that the gauge itself was functioning properly [1]. Later, with the Apollo program, avionics increased in power and complexity, and on-board digital computers became more sophisticated as well. As avionics systems have become more complex, on-board computers have been able to process more data, and ground control stations have been able to monitor, give input, and control certain subsystems through telemetry. Fault-tolerant devices began to become more and more commonplace through to the Space Shuttle Program, which saw the first dual tolerant systems [9]. This pattern has continued through the modern era with the incorporation of fault-tolerant systems into the SpaceX Falcon 9 and NASA's Space Launch System (SLS).

Section 1.4 – Approaches to Improving System Reliability

Over the course of the next several decades, the emphasis on reliable avionics will increase. Not only are there dozens and dozens of satellites in orbit around the Earth, but several private companies have made it their mission to push the boundaries of previously explored space. SpaceX founder and CEO Elon Musk wants to put a human on Mars [10], and Blue Origin founder Jeff Bezos wants to establish a human presence in deep space [11]. In the summer of 2018 NASA plans to launch the Parker Solar Probe [12], which will come within 3.8 million miles of the Sun's surface, the closest approach ever made, while NASA's Mars InSight Probe [13], launched on May 5, 2018 to explore the planet surface. These impressive goals and missions are similar in that they are all expected to be very long missions, with the InSight Probe expected to arrive on the Martian surface on November 26, 2018 if all goes well, which would be a nearly seven month-long mission. Given the length of time involved, the likelihood of operating conditions deviating outside the device tolerances are higher than normal. This means that extra consideration to reliability must be made.

In spite of the efforts to learn from past mistakes, one area of continuous development has been subsystem management. This has arisen from the need to continuously monitor the traditional four avionics subsystems [1]. By staying aware of the probability of failure for a given component or subsystem, failures can be actively prevented rather than merely reacted to. In order to meet this end, several different proposals for monitoring systems have been developed. Most of these revolve around some kind of software model to monitor and evaluate system performance in real-time. This approach rests on the principle that incidents can be mitigated in real-time through proper response by operators or by another system. Some examples of these predictive models have been developed by Skormin, et al. [3], Mengshoel, et al. [14], and Xu, et al. [15]. Large organizations such as NASA, the European Space Agency as well as private companies like SpaceX are incorporating some of the principles in their system designs [16].

Throughout the history of spaceflight, many missions have ended unsuccessfully due to the failure of avionics systems. In some high-profile disasters, these problems have led to deaths. While this is thankfully not always the case, there is still a risk for injury, failure to achieve flight objectives, and the loss of expensive rockets and equipment. In order to mitigate risk to astronauts and protect expensive equipment in future flights, more reliable avionics systems must be developed. To do this, national and international space agencies and private companies are continuing to develop their understanding of what can cause avionics systems to fail. This is in terms of direct mechanical or electrical failures in a specific device, or overarching system failures. It is also important to determine how avionics disasters are most effectively prevented. The two possible approaches are to either prevent incidents before they occur through thoroughly detailed design and testing, or to allow for rapid response to failures, which will inevitably sometimes still occur. Due to the wide variety of potential causes of failure and the numerous situations which may trigger these failures, the best way to prevent future incidents is to emphasize the development of monitoring systems, which allow for maximum adaptability in the event of failure of one component or subsystem. The coming chapters will describe both monitoring systems and fault-tolerant devices in more detail, and will how they can be advantageous when used in avionics systems.

Chapter 2

CASE FOR DIAGNOSTIC MONITORING SOFTWARE

Section 2.1 – Main Advantages of Diagnostic Monitoring Software

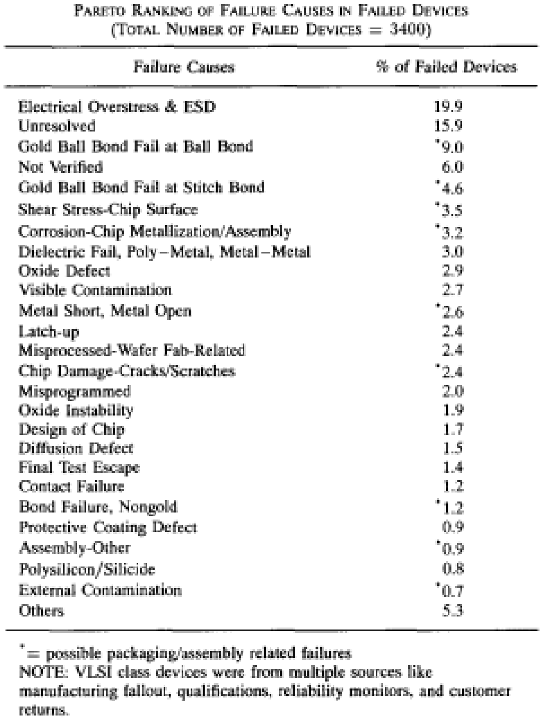
The main benefit of diagnostic and prognostic monitoring software systems is their ability to enable effective responses to component and system level issues. Given the wide range of failure modes that have been demonstrated throughout history, preventing incidents can be difficult due to their unpredictability. Failures can be caused by component failures, system failures, or interconnection issues. As will be discussed below, several historical examples have shown how enabling crew members or ground controllers (for both manned and unmanned spacecraft) to adapt to failures has mitigated potential disasters, and now researchers are attempting to further this trend by developing monitoring software.

While fault-tolerant systems and diagnostic systems are both important to ensure a reliable avionics system and usually work in tandem, emphasizing an effective diagnostic system allows for rapid response by crew members. While systems that automatically diagnose faults through computer software are effective in preventing disasters by immediately addressing time-critical faults, the key advantage is that it allows crew members to manually respond by isolating the fault, switching redundant components on or off, or overriding automatic responses. This is in contrast with fault-tolerant devices, which while effective when used in diagnostic systems, are simply more robust versions of normal devices. While more resilient against failures caused the natural space environment, they are still susceptible to physical flaws caused by mishandling, misassembly, or some other unforeseen accident, in which case, a response would be needed.

Section 2.2 – Causes of Avionics Failures

Avionics failures can be caused by a wide variety of different issues. The most obvious way to determine cause of failure in a system component is to examine any mechanical faults within a device. One summary of these causes outlined by Pecht and Ramappan [17] found that out of a sample of 3400 failed devices from 1971-1991, many different direct causes may result be responsible for failure as shown in Table 1 below.

Table 1- Causes of Failure in Avionics Devices [17]



PARETO RANKING OF FAILURE CAUSES IN FAILED DEVICES
(TOTAL NUMBER OF FAILED DEVICES = 3400)

Failure Causes	% of Failed Devices
Electrical Overstress & ESD	19.9
Unresolved	15.9
Gold Ball Bond Fail at Ball Bond	*9.0
Not Verified	6.0
Gold Ball Bond Fail at Stitch Bond	*4.6
Shear Stress-Chip Surface	*3.5
Corrosion-Chip Metallization/Assembly	*3.2
Dielectric Fail, Poly–Metal, Metal–Metal	3.0
Oxide Defect	2.9
Visible Contamination	2.7
Metal Short, Metal Open	*2.6
Latch-up	2.4
Misprocessed-Wafer Fab-Related	2.4
Chip Damage-Cracks/Scratches	*2.4
Misprogrammed	2.0
Oxide Instability	1.9
Design of Chip	1.7
Diffusion Defect	1.5
Final Test Escape	1.4
Contact Failure	1.2
Bond Failure, Nongold	*1.2
Protective Coating Defect	0.9
Assembly-Other	*0.9
Polysilicon/Silicide	0.8
External Contamination	*0.7
Others	5.3

* = possible packaging/assembly related failures
NOTE: VLSI class devices were from multiple sources like manufacturing fallout, qualifications, reliability monitors, and customer returns.

The most frequent cause of failures seen was electrical overstress due to the operational environment. In addition to other mechanical failures, a significant number of devices were listed as ‘unresolved’ or ‘not verified’. One significant observation made by Pecht and Ramappan is that with the increase in complexity of electrical systems throughout the history of spaceflight, there is a corresponding increase in these nonattributable failures, meaning that typical failure analysis methods are unable to determine the defect. Another area of concern is that even a perfectly designed device may fail if misprogrammed, mishandled, or misassembled before it is even put into use.

Though these issues may seem simple, easily diagnosed or prevented problems, they can be difficult to detect given the large number devices in a craft, and even simple failures may have a very significant impact. For example, during the Apollo 13 mission that nearly resulted in the deaths of all three crew members, the catalyst was a short circuit that destroyed two oxygen tanks in the command module and caused a small explosion that damaged other components [6].

Another important takeaway from this example is that while individual components may fail within an avionics system, the underlying cause may not be simply a material failure. Stresses caused by the environment in which the component is operating, an assembly failure, or improper connections between components can also cause faults. However, the component itself may not necessarily be the root issue causing avionics failures, as the connection between devices or improper interaction between two subsystems can also cause failures. Some of the general causes leading to these failures were also examined by Pecht and Ramappan as seen in Figure 2.

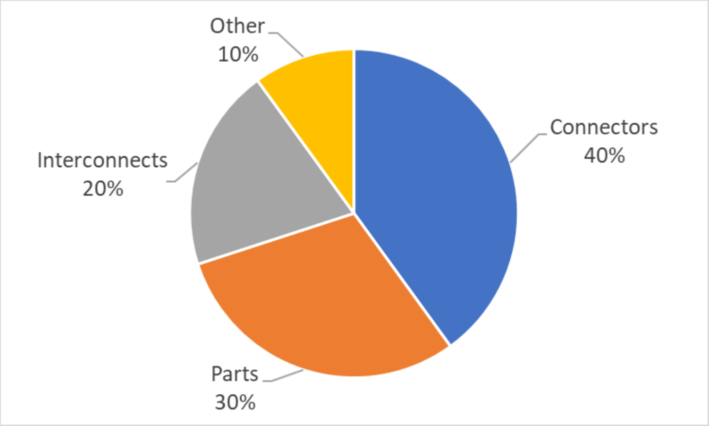


Figure 2- Failures in Avionics Systems, adapted from [17]

Though this figure is now outdated, it illustrates the point that faults in specific parts make up a small fraction of all failures, and that no single category of failures has historically dominated.

Even as avionic devices have improved in quality and reliability throughout the history of spaceflight, the issue of reliability has remained significant. Though no large scope surveys of device failures have been conducted recently, most of the fundamental issues that lead to them still exist. Adding to the challenge of adequately preventing device failures is the wide range of risk factors. This can be seen by expanding on the work of Pecht and Ramappan. Among the many possible mechanical faults are bond failures, oxide defects, corrosion, and electric die defects, among many other faults. In addition to the mere failure modes as listed, these can be caused at different failure sites by different failure mechanisms. An important issue is the difficulty in verifying each of those important failure characteristics. For example, a soldered joint may only become disconnected intermittently. Other causes of inconsistency in otherwise properly functioning devices could be incompatibility between devices or marginal parameter shifts. Devices functioning properly in lab conditions may not operate as expected in its typical environment. Pecht and Ramappan found that 0.6% of failures could be verified as device failures as shown in Figure 3, suggesting that while fault-tolerant devices remain important in any system, there are more significant issues impacting overall reliability.

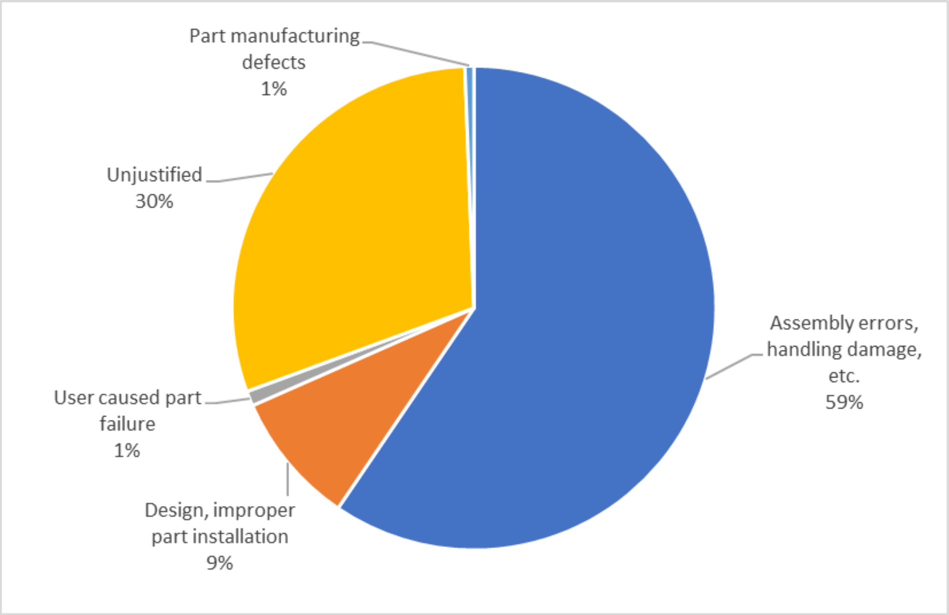


Figure 3 – Failure Modes in Avionics, adapted from [17]

Though the improvements have been made on fault-tolerant devices in the past few decades, many of the same issues regarding system design and assembly remain. Knowing that this is the case, it can be surmised that effective response to these failures is critical.

Section 2.3 – Function of Monitoring Software Systems

A key point in favor of the emphasis of diagnostic systems is that they allow for more effective, proactive subsystem management. As systems become more complex, it is increasingly important that on-board computers monitor devices and subsystems for faults [1]. It is also critical that such systems are capable of isolating faults and reconfiguring systems and devices. This should be able to be done automatically by the software, with the capacity for crew members to override actions. Redundant devices can also be managed through this system. Diagnostic systems function by modelling the operating conditions the devices are operating based on sensor data, and by using real-time artificial intelligence to actively monitor the condition of all components and subsystems. One such example is ADAPT Testbed, described by Mengshoel et al [14]. This method uses a series of Bayesian networks to create a probabilistic model representing each operational mode for each component in a system or subsystem. On the modelling side, each node has a corresponding conditional probability table (CPT) with a large set of continuous and discrete variables. Random variables are sometimes introduced into this model to determine the best way to respond to unexpected faults. Given the finite space and power available in a flight computer, each of the real-time operating systems is prioritized, with the software cycling through each process. This ensures that the most probable failure modes are most frequently reevaluated.

Another approach proposed by Skormin et al. involves the use of ‘knowledge discovery from data’ (KDD). This tool using data mining software is used to determine the probability of failure in flight-critical components. This includes any failures due to a single effect, failures due to a collection of effects, and predicting failures based on known operational conditions. The KDD method uses Bayesian networks similar to those implemented by the ADAPT method. The history of abuse based on known operating conditions and given time into the future are variables input into a decision tree, with each node representing input arguments. Data is ranked based on how likely it is to predict a fault, and is subsequently separated into subsets. This allows environmental factors that lead to general or particular failures to be ranked according to likelihood and severity of risk. The software can then assess combinations of factors that may lead to failures. This model can provide justification for development of more highly tolerant devices that can prevent specific failures. In an attempt to decrease the amount of computational power required, the system iteratively determines ‘informativity’ of data, which is then used to reduce the specifications used in experimental data. This can both prevent emergencies and guide maintenance scheduling for at-risk components.

Another important feature of a good monitoring system is the ability to predict the likelihood of failure for different devices and systems. This means that software is able to prognosticate potential faults and either reconfigure automatically or alert crew members or ground station controllers of unmanned spacecraft. This means that a good system will not just have the ability to rapidly and effectively react to failures, but also to proactively take action against likely sources of failure. This is significant not only in that potentially devastating failures may be mitigated before they occur, but also potentially unforeseeable operating conditions can be taken into account on device or system performance. A key aspect of good systems is to ensure that crew members are able to manually override computer commands.

Section 2.4 – Historical Examples of Effective Responses to Failures

The main strength of monitoring software is that rapid responses to faults are possible. While this is important theoretically, there are numerous past examples of times when an appropriately timed response by crew members and ground stations allowed for safe missions.

One of the most famous cases of an averted disaster during spaceflight is the Apollo 13 mission. During this mission, an oxygen tank exploded after a short circuit created a spark. This not only severely eroded the crew’s oxygen supply, but damaged other systems. With the primary electrical power source out of order, the crew was forced to move into the lunar landing module. Though the consequences could have been severe, the crew was able to adapt to the situation. To do this, they transferred from the command module into the lunar lander, which still had systems in place that allowed them to survive. Though the lunar module was designed to support two crew members and wasn’t nominally equipped with enough consumables for three crew members over the final leg of the flight they were able to survive by complementing with command module’s remaining resources with those in the lunar module.

Several specific actions taken during the aborted mission showcase how an adaptive response can be so effective. Because they could communicate with ground control, the crew was able to receive assistance and instruction at different points. Upon reentry, the command module was needed, as the lunar module wasn’t designed for the descent through Earth’s atmosphere. To provide the power necessary to reboot the critical systems, batteries on board the command module were powered by the lunar module. Another necessary modification that was implemented for future flights was the redesign of the oxygen tank and fuel cell valves [6].

Another case exhibiting the necessity of override capability was NASA’s Gemini 8 mission. During this mission, which sought to complete the first successful docking of two orbiting spacecraft, the craft went into an uncontrolled spin. With the ability to switch out of the main attitude control system and into the reentry control system, mission commander Neil Armstrong was able to switch into the thruster mode and correct the attitude of the craft before reentering into the atmosphere [18].

Another example is the Mir EP-3, during which Russian cosmonaut Vladimir Lyakhov and Afghan cosmonaut Abdul Ahad Mohmand experienced an issue during reentry after their nine day stay on the space station. Due to a sensor failure combined with a software problem, the engines didn’t burn for a long enough time, so the capsule wasn’t able to reach the intended orbit before reentry. Lyakhov figured that the sensors had received incorrect readings due to solar glare, and after another two Earth orbits, reentry was attempted again, with the same premature engine cutoff. Finally, ground control in Russia determined that the flight computer had on the second attempt tried to execute the same burn pattern used to dock the capsule to the Mir station earlier in the flight. After reconfiguring the computer, the capsule was finally able to successfully reenter Earth’s atmosphere [8].

The overarching theme of these examples, especially the Apollo 13 example, is that by enabling the crew and engineers on the ground to be able to adapt to the situation, creative solutions could be implemented. Due to the unfortunate certainty that there will be more avionic failures in the future, it is imperative that such measures are taken that will allow such responses to be made. It also shows that backup systems and the skill of crew members is important in mitigating negative effects from failures. In the official Apollo 13 mission report, it was written that “The effectiveness of preflight crew training, especially in conjunction with ground personnel, was reflected in the skill and precision with which the crew responded to the emergency” [6].

In spite of these examples that support the development of monitoring software, there are disadvantages to emphasizing it during the development of avionic system architecture.

Chapter 3

CASE AGAINST DIAGNOSTIC MONITORING SOFTWARE

Section 3.1 – Main Disadvantages of Diagnostic Monitoring Software

Though diagnostic monitoring systems have certain advantages in increasing the reliability of avionics systems, there is an argument in favor of emphasizing fault-tolerant devices in future designs. The technology is more developed, they have exhibited economic viability, and can prevent failures caused by specific sources. On the other hand, diagnostic software adds complexity to the overall design, can sometimes make it more difficult to attribute failure modes, and perhaps most importantly, are not nearly as widespread or developed as fault-tolerant devices. This chapter will discuss how these disadvantages would seem to discourage the emphasis of monitoring software in avionics systems.

Though most experts would argue that diagnostic systems and fault-tolerant devices are both important to a safe and reliable avionics system, the argument could be made that robust components are the critical piece of the puzzle. This argument centers around the idea that developing fault-tolerant devices is a more proactive strategy than diagnostic systems, which is mainly a reaction to faults. Fault-tolerant devices have been shown to be more robust in harsh environments while remaining economically viable, with less of a risk of systematic faults occurring the way they could in a diagnostic driven system.

Section 3.2 – Developments in Fault-Tolerant Components

The point made earlier by Pecht and Ramappan that increased software complexity could be a contributing factor in many nonattributable device failures suggests that increasing the complexity of diagnostic software may not necessarily be the best idea. Rather, it could be that increasingly robust and durable components will negate a significant proportion of failures. Some of the improvements that have come with fault-tolerant devices have not only improved the durability of individual components, but also shown that products and avionics architectures developed by new private companies can be commercially bought off the shelf. One such company, Curtiss-Wright, reports that increasing the tolerance to radiation still allows the cost to be lowered [19]. This is done through use of their "Smart backplane", which would be used for their flight computers. This allows them to increase tolerance at a board level rather than component level. Without spending for more robust components, it still aims to improve individual component life cycle.

The Air Force Research Lab has also made strides in trying to develop a useful avionics interface that can allow systems to be used on different craft, similar to the way in which USB technology has been standardized for use in almost any laptop or desktop computer [20]. Standard software interfaces can reduce cost, and significantly reduce scheduling time. The AFRL TacSat-3 mission was the first test of Plug-and-Play avionics. Its main advantage is that it is both modular and reconfigurable. It included lots of different sensors, mainly for guidance navigation and control, with a built in performance self-testing platform. Different interfaces were used for different types of sensors and different systems. Interface issues found during installation were able to be reconfigured rather than requiring reassembly of the computer.

Though some standard interfaces already existed, the AFRL PnP interface standardizes more criteria such as application conventions, data conventions, connectors and pin-outs. Experimentally, all PnP hardware/electronics performed nominally over a year in orbit. Scheduling benefits were demonstrated during integration with the TacSat-3. Though still not entirely developed, especially from an economic standpoint, this effort is representative of an industry that is currently moving in that direction. The concept of modularity is seen as likely inevitable, and a majority of industry insiders interviewed in 2013 considered themselves to be among potential early adopters of PnP avionics as shown in Figure 4 [21]. They also generally agreed that this system would improve mission scheduling and reduce the labor needed. Another perceived strength of this system was the flexibility provided by the PnP system. However, as shown in Figure 4, the cost is the major concern to be addressed. If/when this becomes more economically viable and the technology becomes more mature, PnP becomes more feasible within the industry.

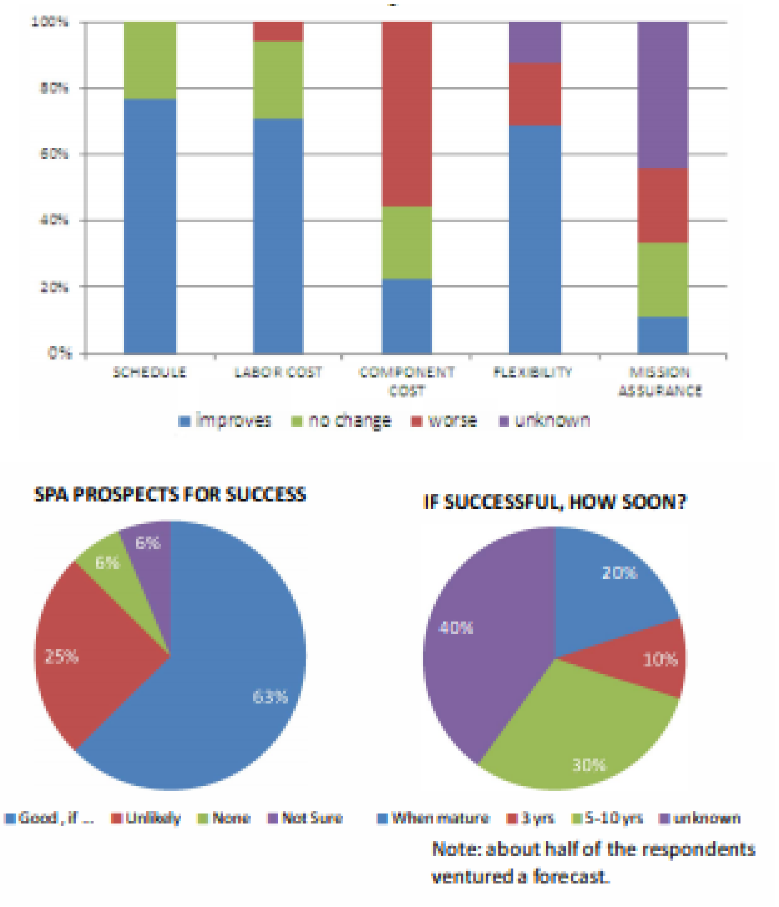


Figure 4 - Industry Review of Air Force Research Laboratory's Plug and Play Avionics [21]

Section 3.3 – Advantages of Fault-Tolerant Components

Another key point in favor of fault-tolerant devices is the sheer complexity of diagnostic and prognostic systems. As described by Skormin, Mengshoel, and others, these diagnostic/prognostic systems can require a large amount of computing power, which can also lead to an increase in weight. This dovetails with the larger point that increasing system complexity adds to the challenge of determining system failures.

One of the main issues with avionics devices is the harsh, often unpredictable nature of the operating environment, both inside the craft and outside. Fault-tolerant devices provide a defense against such common faults such as those caused by radiation which is seen as a major factor in causing a number of device failures [5]. Fault-tolerant devices can also lengthen the useful life of devices. This is similar to the maritime industry in which designs are rated to withstand the maximum size wave the vessel is probable to experience over a given length of time. For example, a 100-year event is an event with a 1% chance of occurring during any given year, and large craft may be designed to withstand a 25-50 year event, while smaller craft are generally designed with smaller-scale events in mind. This is because while this is great in theory to plan for the worst possible environmental exposure, it isn't practical economically to always plan for the maximum stress. Likewise, even though redundant systems are important in reliable avionics, they add weight, cost, and complexity that may not always be feasible.

One interesting concept that could possibly mitigate the added weight and cost of certain components within an avionics system could be to move towards wireless communications. This has been proposed and tested with NASA's Ames Research Center [22]. They have done this using the ZigBee avionics architecture, which is already in wide use. The main challenge with this is that currently there is no existing framework governing the standards for such a system. For example, the IEEE standards for WiFi aren't viable in spaceflight due their excessive power consumption and incompatible architecture. The main benefit for wireless communication is that the weight of wires is removed from the system, which could theoretically enable more complex or redundant components to be implemented.

Another key consideration is price. Given that the aerospace industry is becoming increasingly privatized, it is important any new components or subsystem within an avionics system are economically viable. While it is important to note that detailed information regarding the avionics systems of private companies is hard to come by, it should be noted that many companies have been working on fault-tolerant devices for many years, which helps drive down the price. Furthermore, it has already been shown that such devices can be effective.

Given some of the disadvantages with diagnostic monitoring software systems, such as their complexity and their immaturity as a technology, the argument can be made that fault-tolerant devices should be emphasized in the development of future avionics systems. From an industry perspective, they represent a known commodity that is improving and are increasingly viable to buy off-the-shelf.

Chapter 4

DISCUSSION

In an effective and reliable avionics system, it is critical that the system has the ability to monitor the operating environment in real-time to predict future failures. It is also very important that the hardware involved in the system is able to stand up to the harsh conditions of the space environment, in addition to the operating environment of the spacecraft itself. As previously discussed, these two factors are critical to the performance of avionics systems. In all systems, there must be active monitoring of component health and operational environment.

The ability to diagnose avionics faults is very important in that it allows for quick and effective response, either by an automatic response from the flight computer, from the crew members, or from ground control stations. There are several examples in the history of manned flight in which humans have been able to respond to electronic or component failures. Even with improving tolerance at the component level, there are still errors due to process or simple human-caused errors. While it may seem ironic that the solution to potential human caused failures is to enable humans to effectively react, it has been shown that the ability to adapt to unexpected scenarios in creative ways can mitigate avionics failures. Historical examples such as Apollo 13 underline this point.

There are several other advantages to diagnostic systems. These systems allow for real-time monitoring as well as predictive modelling that can allow preventive actions to be taken. An effective system allows for automatic or manual reconfiguration of components and subsystems when issues are likely to arise. When a device or system failure triggers an automatic response from the flight computer, and also allows for a manual override to that response, it allows the software to immediately handle issues that may be time-critical while allowing crew members or ground-control to respond as they see fit.

On the other hand, diagnostic/prognostic systems can be very complex. This creates more chances for something to go wrong, and historically the increase in ‘unattributable’ failures has coincided with the increase in software complexity. This makes it even more difficult to study modes of failure. Another potential issue is that systems focusing too heavily on diagnostics may be too reactive in their approach to reliability.

Fault-tolerant devices meanwhile are more proactive in the sense that their entire design concept aims to prevent failures by maximizing the range of operating environments under which a component can operate. This can be either operating conditions within the spacecraft itself (vibrations, etc.) or the natural space environment (radiation, etc.). The additional stresses on the devices from these causes can both directly cause failure, lead to operation of devices at non-nominal states, or indirectly lead to failures by reducing the lifespan of the device. The ability of fault-tolerant devices to mitigate these effects is important in that over the course of long missions with unpredictable changes in operating conditions, and the increased probability of conditions exceeding the nominal tolerance of the device.

For all of the benefits of using increasingly fault-tolerant devices, there are some downsides. There are still many failure modes related to the application of the device, including mishandling, improper assembly, or poor interconnections between devices. Even perfectly designed and manufactured devices will still operate differently in real operating conditions than in a lab or factory setting. Even when properly implemented into an effective avionic architecture, there is still no emphasis on an appropriate response without the presence of a diagnostic/prognostic system as well.

It is most important to note that both fault-tolerant electronics and diagnostic systems are not only important, but necessary for an effective avionics system. However, given the volatile nature of spaceflight as has been shown during its history, a heavy emphasis must be placed on diagnostic/prognostic software monitoring systems. Given the wide range of possible causes of device failures, and the infeasibility of preventing each of them through increased tolerancing, both due to cost as well as the likelihood of increased weight, means that mechanical failures are still possible. Additionally, increasing the fault-tolerance of devices doesn’t guarantee that failures won’t occur. As we have shown, human-related errors do occur relatively commonly, and will always be an inherent risk during spaceflight. The overriding conclusion from this is that failures of avionic devices and subsystems is inevitable, especially as humankind aims to expand its presence in space and embarking on lengthier missions than ever before.

While diagnostic and prognostic monitoring software isn’t a perfect solution for avionic failure modes, either those inherent in avionics systems or in terms of covering the weaknesses of fault-tolerant devices, it has the most potential for effectively responding to the failures that will inevitably occur. These systems, even with the increase in complexity and potential for unattributed failures, still allows crew members and ground control to reconfigure systems, manually correct automatic responses for time-critical failures, and alert crew of the need to preemptively replace or give maintenance to specific devices.

Though monitoring software should be emphasized in the future design of avionics systems, it needs to be fully understood that they cannot function effectively without some sort of fault-tolerant devices. The software can't perform its given functions if the devices can't handle their operating conditions. Responses triggered by an effective monitoring system won't be effective if the devices being reconfigured aren't functional, which would make the capability to adapt futile. By the same token, extremely reliable devices on their own can't be adequately reliable due to the incapability of the system to adjust when necessary.

One important factor in spaceflight in general that hasn't been covered in great detail in this paper is the cost effectiveness of avionics systems and how that might impact the development of the field. Fault-tolerant devices have been used on spacecraft for decades, and on a certain level are more economically viable than diagnostic monitoring systems, which remain less developed in terms of their actual applications by space agencies and private companies. However, given the increasing need for modularity, reconfigurability, ability to interface between different systems, and the fact that there is still no set of industry-wide standards, the business case for fault-tolerant electronics isn't optimal.

In spite of this, it is clear that as the need for reliable avionics increases, the benefit of protecting billion-dollar investments means that it is worth putting the time, effort, and resources into avionics systems that will play a large part in protecting large-scale projects. Over the long-term, these systems will pay off, assuming that they function as intended. Just as with other technologies and industries, as engineers develop more efficient designs, manufacturing methods, installation procedures, and industry-wide standards, these devices and systems will become cheaper, with more options on the market as the technology becomes accessible to more manufacturers and contractors.

While the focus of this paper has been safety and reliability, there are many other significant functions of avionics systems that make them of interest for future spaceflight. The on-board electronics that are included in avionics systems can be used for any number of experiments within the spacecraft or in the natural space environment. These types of experiments aren't safety critical, but are often used to help guide the goals of future missions or to broadcast mission events. Some examples of this throughout history have included early on the Mercury and Vostok missions which sought to explore the effects of space, television feeds of the Apollo moon landings, pictures taken by the Hubble Space Telescope, and data from probes visiting other planets. A few current examples of this are the Parker Solar Probe and the InSight Mars lander.

Chapter 5

CONCLUSIONS

Few subsystems on any spacecraft are unimpacted by the avionics system. Aside from the subsystems that directly fall under the umbrella of avionics, any actions depending on electronic triggers, sensors, or actuation are still impacted by the performance of the avionics system. This can be everything from an actuator adjusting the position of a flap or panel, to controlling the flow of a liquid fueled engine, to triggering the deployment of a parachute. Each of these systems is intertwined with the avionics, meaning that the reliability of the avionics system is important even beyond the scope of the system itself. A good example of this is a launch in Brazil in 2003 [8]. During the takeoff sequence, the solid fuel booster exploded, killing 21 people and nearly destroying the launch site. The cause of this horrific accident was electrostatic discharge from the avionics bay. This caused a spark which ignited the fuel when the rocket was still on the launch pad. Even though there was nothing fundamentally wrong with the propulsion system itself, it still caused a disaster because the on-board avionics didn’t function properly. Just as diagnostic/prognostic monitoring software on the flight computer and fault-tolerant electronics don’t operate in a vacuum, each major system of a spacecraft must compatibly work in tandem. Recent cases of launch failures underscore the inherent effect of human-driven faults, even in cases when the component design is sound. Space travel is can be very risky, and it is the responsibility of engineers to protect the safety of everyone involved.

REFERENCES

[1] Kayton, M., “Avionics for Manned Spacecraft,” IEEE Transactions on Aerospace and Electronic Systems, vol. 25, 1989, pp 782-827.

[2] May, T., 2013, “Space Launch System (SLS) Safety, Mission Assurance, and Risk Mitigation,” from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20130011203.pdf

[3] Skormin, V.A, Gorodetski, V.I., Popyack, L.J., “Data Mining Technology for Failure Prognostic of Avionics,” IEEE Transactions on Aerospace and Electronic Systems, vol. 38, 2002, pp.388-403.

[4] Bedingfield, K.L., Leach, R.D., Alexander, M.B., 1996, “Spacecraft System Failures and Anomalies Attributed to the Natural Space Environment,” NASA Reference Publication 1390, National Aeronautics and Space Administration, Marshall Space Flight Center, Alabama.

[5] Perez, R., 2008, "Methods for Spacecraft Avionics Protection Against Space Radiation in the Form of Single-Event Transients," IEEE Transactions on Electromagnetic Compatibility, vol. 50, no. 3, pp. 455-465.

[6] McDivitt, J., 1970, “Apollo 13 Mission Report,” MSC-02680, National Aeronautics and Space Adminstration, Houston, Texas.

[7] Packham, N., Pate, D., Opaskar, J., Ali, F., Stockton, B., 2013, “Significant Incidents and Close Calls in Human Spaceflight,” from https://spaceflight.nasa.gov/outreach/SignificantIncidents/index.html

[8] Pappalardo, J., 2018, “10 Rocket Launch Failures That Changed History,” from https://www.popularmechanics.com/space/rockets/g18751736/rocket-launch-failures/

[9] Chapline, G., Sollock, P., O’Neill, P., Hill, A., Fiorucci, T., Kiriazes, J., “Avionics, Navigation, and Instrumentation,” from National Aeronautics and Space Administration, https://www.nasa.gov/centers/johnson/pdf/584731main_Wings-ch4e-pgs242-255.pdf

[10] 2018, “Making Life Multiplanetary,” from http://www.spacex.com/mars

[11] Fishman, C., 2016, “Is Jeff Bezos’ Blue Origin the Future of Space Exploration?,” from https://www.smithsonianmag.com/innovation/rocketeer-jeff-bezos-winner-smithsonians-technology-ingenuity-award-180961119/

[12] Garner, R., 2018, “Parker Solar Probe: Humanity’s First Visit to a Star,” from https://www.nasa.gov/content/goddard/parker-solar-probe-humanity-s-first-visit-to-a-star

[13] 2018, “Key Facts About NASA's InSight Lander,” from https://mars.nasa.gov/insight/mission/overview/

[14] Mengshoel, O.J., Darwiche, A, Cascio, K, Chavira, M, Poll, S, Uckun, S, “Diagnosing Faults in Electrical Power Systems of Spacecraft and Aircraft,” 20th

National Conference on Innovative Applications of Artificial Intelligence, vol. 3, 2008, pp. 1699-1705.

[15] Xu, J., Meng, Z., Xu, L., 2015, "ISHM-Oriented Hierarchical Effectiveness Evaluation Approach for Spacecraft Avionics," IEEE Systems Journal, 9(2), DOI 10.1109 / JSYST.2013.2279734

[16] SpaceX News, 2013, "Avionics Tower," from http://www.spacex.com/news/2013/05/16/avionics-tower

[17] Pecht, M., Ramappan V., "Are Components Still the Major Problem: A Review of Electronic System and Device Field Failure Returns," IEEE Transactions on Components, Hybrids, and Manufacturing Technology, vol. 15, 1992, pp. 1160-1164.

[18] Mathews, C., 1966, "Gemini VIII," MSC-G-R-66-4, NASA Manned Space Center, Houston, TX.

[19] Lowney, D., 2017, "Lowering the Cost of Spacecraft Avionics by Improving the Radiation Tolerance of COTS Electronic Systems," Space Tech Expo Europe.

[20] Martin, M., Summers, J., Lyke, J., 2012, "AFRL plug-and-play Spacecraft Avionics Experiment (SAE)," *IEEE Aerospace Conference*, Big Sky, MT, 2012, pp. 1-6.

[21] Franck, R., Graven, P., and Lynda Liptak. 2013 "Industry perspectives on Plug-&-Play Spacecraft Avionics," IEEE Aerospace Conference, DOI 10.1109/AERO.2013.6497323.

[22] Stone, T., Alena, R., Baldwin, J., Wilson, P., 2012, "A Viable COTS Based Wireless Architecture for Spacecraft Avionics," IEEE Aerospace Conference, Big Sky, MT, 2012, pp. 1-11.