PERGAMON

Available online at www.sciencedirect.com

ScienceDirect

Acta Astronautica 64 (2009) 195 – 205

ACTA ASTRONAUTICA

www.elsevier.com/locate/actaastro

A study of on-orbit spacecraft failures

Mak Tafazoli

Canadian Space Agency, Canada

Received 5 December 2007; received in revised form 24 April 2008; accepted 16 July 2008
Available online 31 October 2008

Abstract

Even though spacecraft are carefully designed and tested to meet their mission lifetime, many suffer unrecoverable on-orbit failures very early. Other spacecraft, despite severe failures, are able to exceed their expected lifetime when effective failure recovery procedures are applied. In 2005, a study of on-orbit spacecraft failures was undertaken which resulted in identifying 156 failures occurring from 1980 to 2005 on civil and military spacecraft. These failures were analyzed to compare different spacecraft subsystems and estimate their impact on the mission. Although there is no perfect system that could prevent any failure, the lessons learned from the past years show that adequate testing, redundancy and flexibility are the keys to a reliable spacecraft failure recovery system.

1. Introduction

More than 4000 spacecraft have been launched in the past 25 years. Countries around the world are becoming more dependent on space technologies for telecommunication, earth observation and military purposes. Also, the International Space Station and space probes bring new and exciting science discoveries that would not be revealed otherwise. However, the space environment is harsh and each space mission is a great challenge. Many spacecraft have failed before accomplishing their mission although they are using the more recent technologies and are subject to intensive testing. Others have been able to exceed their design lifetime despite severe failures. We identified and studied 156 on-orbit failures that occurred on 129 different spacecraft from 1980 to 2005. The information was gathered from public and private sources such as [1] and [2]. This information was compared to official press releases, failure investigations and reliable science newspapers. These failures were analyzed in order to identify critical spacecraft subsystems and recurrent failure modes. The consequences of the different failure modes on the spacecraft mission are also studied and finally, recommendations on failure recovery are presented. It is important to note that this paper considers only on-orbit spacecraft failures and launch failures are not treated. More information on launch failures can be found in [3]. Moreover, we did not try to estimate the failure cost or failure rates as it is done in other papers [4,5]. Our failure analysis compares the different spacecraft subsystem, identifies the recurrent failure modes and determines the impact of the failures on the mission. The way we classify and identify failures is also novel and different than what has been done in other studies. It is very important to note that our results are only as good as the sources used to generate them and there is some uncertainty in the exact validity of the numbers reported in this paper. This caution having been made however, the results presented will give a general sense of on-orbit failure types and

E-mail address: Mak.Tafazoli@space.gc.ca

0094-5765/$ - see front matter Crown Copyright © 2008 Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.actaastro.2008.07.019

statistics. The next section presents the spacecraft subsystems that were studied and the methodology used in the study.

2. Definitions and methodology

2.1. Spacecraft subsystems

For the present study, we breakdown a spacecraft in the following subsystems: Attitude and Orbit Control System (AOCS), Command and Data Handling (CDH), Telemetry, Tracking and Command (TTC), Structure and Mechanism (MECH) and payload. The AOCS is the combination of two specialized spacecraft subsystems: the Attitude Determination and Control System (ADCS) and the Guidance, Navigation and Control (GNC) subsystems which include the spacecraft propulsion subsystem. The ADCS stabilizes the spacecraft and orients it in desired attitudes during the mission despite the external disturbance torques acting on it. The GNC determines the satellite position and velocity or, equivalently, its orbital elements as a function of time and adjusts the orbit to meet some predetermined conditions. The on-orbit propulsion subsystem provides thrust for attitude control and orbit corrections. Therefore, the AOCS monitors and modifies the spacecraft attitude and trajectory to meet mission objectives despite disturbances during on-orbit operations. The TTC subsystem provides the interface between the spacecraft and ground systems. The subsystem functions include carrier tracking (earth lock), command reception and detection (receive the uplink signal and process it), subsystem operations (point the antennas, detect and recover faults, maintain its own health and status). The CDH subsystem performs two major tasks. The first task is to receive, validate, decode and distribute commands to other spacecraft systems. It also collects and processes spacecraft housekeeping and mission data for downlink or use by an onboard computer. Failures of an onboard computer is also included in this category unless it was explicitly stated that the fault originated from the power subsystem. The power subsystem generates, stores, distributes and controls spacecraft electrical power. It supplies a continuous source of electrical power to spacecraft loads during the mission life. An important function of the power subsystem is to support power requirements for average and peak electrical load. The MECH subsystem mechanically supports all other spacecraft subsystem, attaches the spacecraft to the launch vehicle and provides for ordnance-activated separation. A failure to the payload subsystem refers to a failure isolated to the payload. This failure is not caused by other spacecraft subsystems and does not propagate to other systems than the payload itself.

2.2. Methodology

We consider a spacecraft failure to be an incident that could possibly lead to permanent or temporary mission degradation. A failure to backup systems was also considered, but with a lower priority. Normal depletion of propellant and material integrity were not registered as failure and in order to restrict ourselves to meaningful failure modes, we count only once a group of failures having the same failure mode and affecting the same spacecraft subsystem. For example, the spacecraft BeppoSAX lost all three primary and three spare gyroscopes over the years. We count these failures as a single one because the failure mode and the subsystem were identical for all these failures. However, we do not regroup failures occurring with different failure modes or on different spacecraft. Similarly, a failure source, which triggers failures in different subsystems, will only be counted once and only towards the subsystem containing the failure source. This failure categorization methodology allows us to compare spacecraft that have a lot of data available to others for which there are only limited information. Therefore, this failure database is not too "biased" towards a limited number of spacecraft having plenty of information about them. There are two criteria that describe the magnitude of the damages caused by a failure. The first is *loss of mission* which is when a failure is considered catastrophic, preventing the spacecraft to fulfill its primary mission objectives. The second is *mission degradation* which occurs when a portion of the mission objectives must be abandoned after a failure and includes a permanent or temporary reduction in customer service for commercial spacecraft. A failure leading to insurance claims or a reduction of expected lifetime is also included in the mission degradation criterion.

3. Failure analysis

3.1. Overall failure analysis

This section presents the findings obtained on the 156 failure cases studied. Fig. 1 shows the failure breakdown for the different spacecraft subsystems:

The category "other" regroups MECH, payload and miscellaneous subsystem failures. We observe that 59% of all failures affect AOCS and power subsystems. These two subsystems will be studied in more details shortly. Fig. 2 illustrates the occurrence of each failure

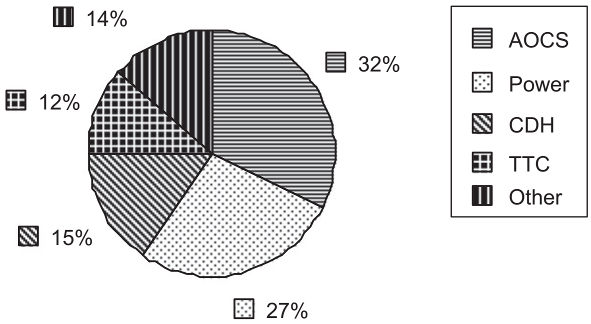

Fig. 1. Spacecraft subsystems affected.

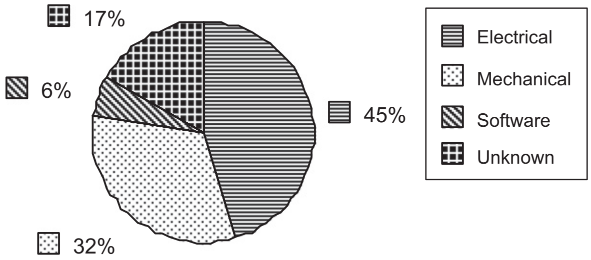

Fig. 2. Spacecraft failure type.

type. The failure types were chosen as follows: mechanical, electrical, software and unknown. A mechanical failure is caused by any mechanical phenomena, such as heat, temperature, external forces, friction and pressure variation. Power overload, short circuit, anomalous battery depletion, etc. are considered electrical failures. Software failures consist mainly of erroneous commands sent to the spacecraft and software flaws.

The spacecraft electrical/electronics are responsible for almost half of the failures with 45%, ahead of the mechanical/thermal failures with 32% which may seem unexpected. One may believe that electronic circuits would deteriorate less over time than mechanical components. While this may be partially true, they are much more electrical components than mechanical devices in modern satellites, which can explain the high percentage of electrical failures. Also, some electrical devices such as solar panels are subject to constant wear out, which makes them vulnerable to failures. Finally, space phenomena such as solar radiation and magnetic storm can heavily affect electronic boards.

We also studied time interval during which the failure occurred, after the spacecraft launch (Fig. 3). It was observe that 41% of all failures happen within 1 year of on-orbit activities, which would suggest insufficient testing and inadequate modeling of the spacecraft and its environment.

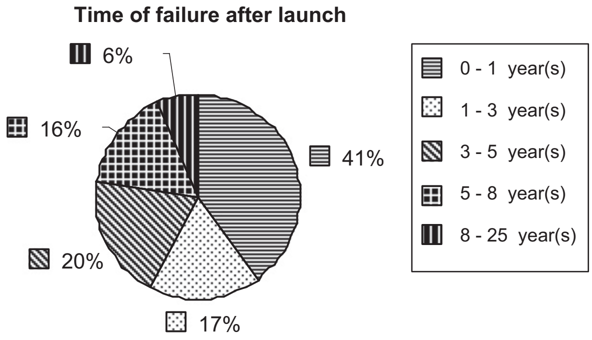

Fig. 3. Time of failure after launch.

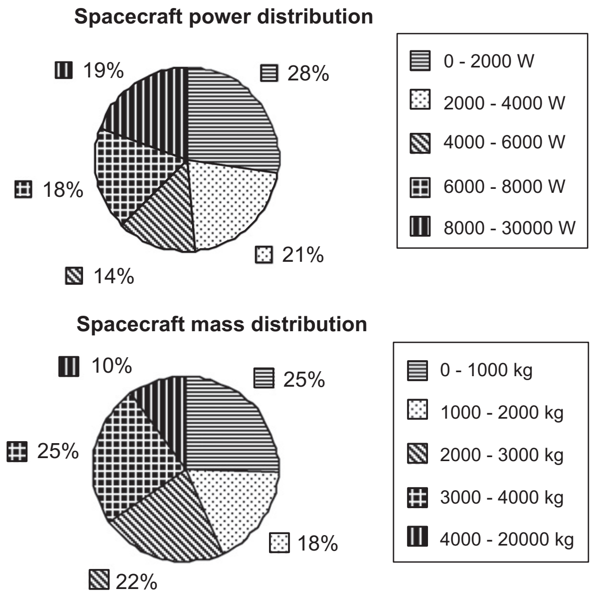

Fig. 4. Spacecraft power and mass distribution.

Other meaningful data that were recorded are the spacecraft mass and spacecraft DC power (Fig. 4). The spacecraft mass refers to the mass at launch and the power corresponds to the total power available at the beginning of spacecraft life. The power and mass generally give a good indication of the overall size and capacity of the spacecraft.

It is noted that the spacecraft mass and power capacities are distributed over a wide range indicating that the spacecraft studied in our analysis go from micro-satellites to larger commercial satellites.

We can evaluate the magnitude of the damage caused by the failures on the spacecraft mission. The loss of mission and mission degradation criteria, described earlier, are presented in Fig. 5.

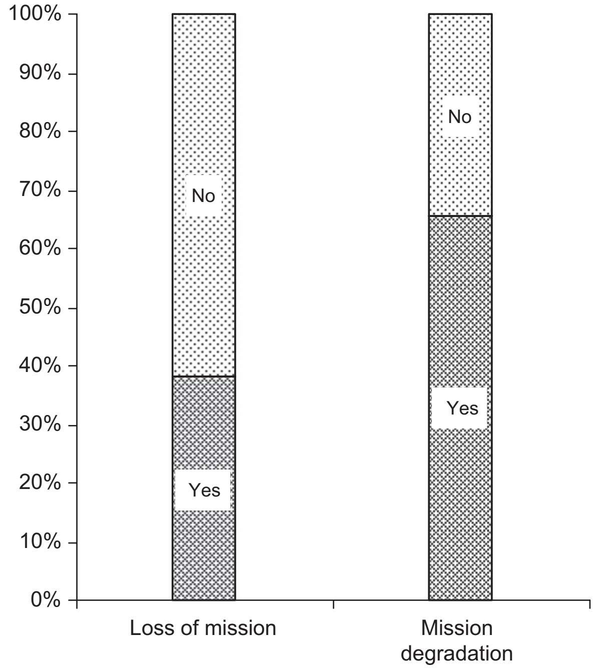

Fig. 5. Spacecraft failure impact on the mission.

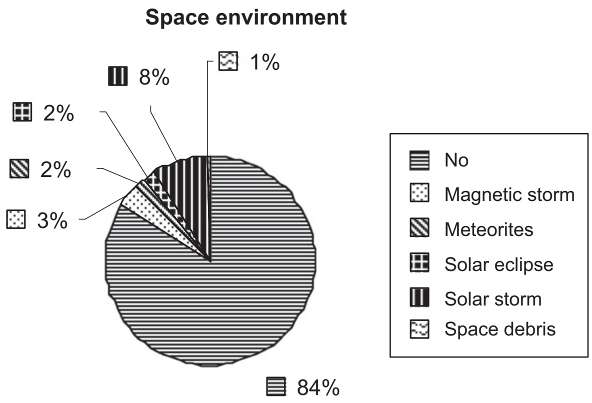

Fig. 6. Proportion of failure due to space environment.

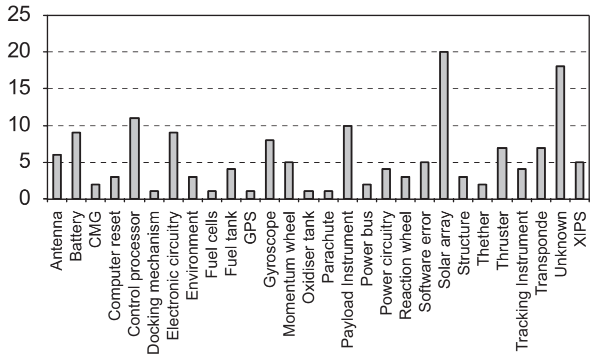

Fig. 7. Spacecraft component failures.

Nearly 40% of the failures studied were catastrophic and the percentage of missions that were degraded (including the mission losses) rises to about 65%. This clearly shows that spacecraft operators and manufacturers are unable to fully deal with a large portion of on-orbit failures and hence the need for efficient recovery systems. We also studied the link between spacecraft failures and external factors such as the effects of space environment and human errors. Solar storms, magnetic storms, meteorites and space debris can have a significant impact on the different spacecraft subsystems. The human error criterion includes operator errors and design flaws. An operator error usually consists of an erroneous command sent to the spacecraft or a misinterpretation of the data collected. A design flaw is an imperfection that has been made in the design stage of the spacecraft. It was found that only 8% of the failures were due to human error. The influence of space environment is shown in Fig. 6.

We observed that space phenomena are directly involved in 17% of all the failures recorded in our database. This ratio was expected despite the considerable funds that are invested to develop computers and electronics equipments that are resistant to solar and magnetic radiations. Human errors are responsible for only 8% of the total number of failures. It is to be understood that we only attributed a human error when it was established that such fault had occurred. Since the spacecraft operators and designers are generally reluctant to disclose such information, this percentage is probably higher in reality. However, as it was pointed out in [4], the level of training of most satellite operators seems adequate. Similarly, the number of design flaws is sufficiently small such that we did not feel the need to further investigate this area.

Finally, we identified the cause of failure (components or otherwise) whenever it was possible. These and their corresponding number of failures are captured in Fig. 7.

We observe that the item that suffered the greater number of failure is the solar array. About 40% of all solar panel failures are mechanical. They are caused by failed deployment and failure to the solar panel structure. The electrical failures are mainly due by short circuit in solar array drive mechanism. The large number of solar array failure is also related to the recurrent problems faced by certain companies. By January 2002, Boeing determined that the use of concentrators on the BSS-702's solar panels to boost the power generation

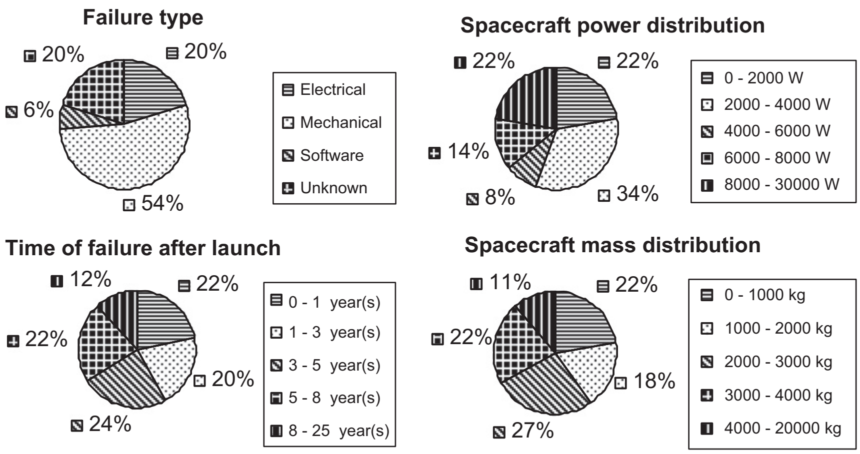

Fig. 8. AOCS failure distributions.

capacity of the solar arrays was responsible for the premature losses of power of at least seven satellites [6]. The solar array failures are also critical due to the fact that 55% occurred within the first year of operation. Therefore, it is important to do sufficient testing and to avoid repeated failures, such as the BSS-702 solar array problems. Enough time and resources should also be allocated to the design of a fault protection system. This system detects, isolates and corrects fault in the power subsystem. Its main purpose is to isolate failed load which draw excessive current leading to an eventual drainage of the energy-storage reserve [7].

The unknown category of component failure refers to the cases when it was impossible to find the exact source of failure. The number of unknown component failures is high because the commercial companies are reluctant to give the failure details. It is also difficult to retrieve telemetry after a critical failure to investigate the failure.

The second item that suffered an important number of failures is the onboard control processor. These failures are usually less critical than solar array failures since there is usually a backup control processor which becomes active when the primary control processor fails. Nevertheless, the consecutive failures of the primary and backup control processor (or the inability to switch to the backup unit) represent 56% of the catastrophic CDH failure and 8% of all catastrophic failures registered during our study.

3.2. AOCS failure analysis

It is not surprising to see that a large number of failures occur in AOCS. Since this system regroup many critical systems, an AOCS failure can heavily cripple a spacecraft. Fig. 8 regroups the statistics regarding AOCS failures.

We are observing noticeable difference when we isolate AOCS failure from other subsystem failures. We see that more than half of the failures (54%) are mechanical in nature, and a relatively small portion is electrical. It is also interesting to notice that 34% of the failures occur to spacecraft that require high power to maintain their operation. Finally, the time of failure after launch criterion is more evenly distributed for AOCS than for the other subsystems. The time interval 0–1 year contains 22% of the AOCS failures, which is much lower than 41% that was found when combining all the systems together. Fig. 9 display the magnitude of failure damages and the components involved in AOCS failures.

The AOCS failures are less critical and are better recovered than the other subsystems failures. They are approximately 10% less catastrophic failures and 10% less mission degrading failures than what was presented for the overall case. We also see that there is a large portion of unknown component responsible for AOCS failures due to a lack of information. Nevertheless, almost 50% of AOCS failures are attributed to the combination of the following components: gyroscopes, momentum wheels and thrusters (including XIPS).

3.3. Power failure analysis

It was not expected to find as many failures for the power subsystem since as opposed to AOCS, which accomplish a large range of functions, the power subsystem carries out very specific tasks. However, a spacecraft relies heavily on power generation and storage.

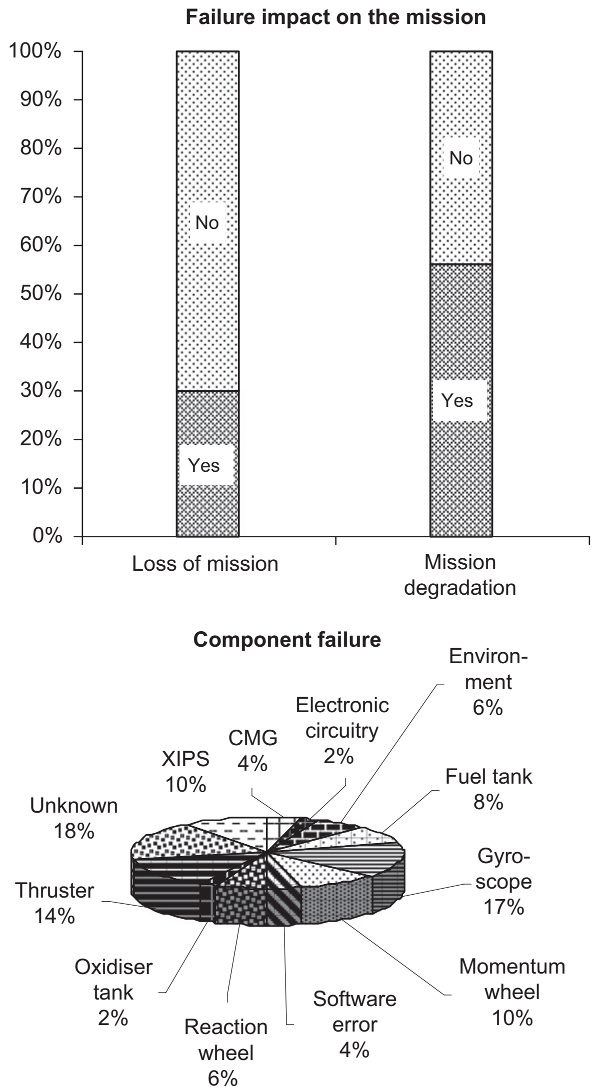

Fig. 9. Failure impact and component failure for AOCS.

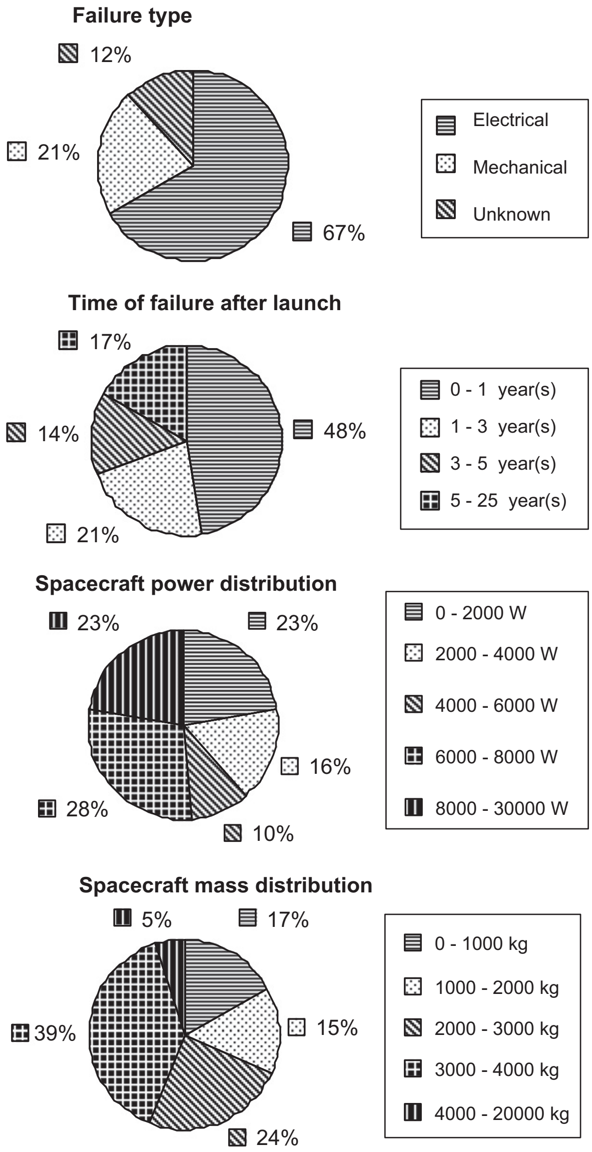

Fig. 10. Power failure distributions

Any fault or reduction of power may easily disable a mission if some important payload or spacecraft core function are disabled. Fig. 10 shows the relevant statistics for power subsystem:

We see that 67% of the failures are electrical, which is expected for power systems. The failures seem distributed among the different power ranges. However, the most interesting fact is the time of failure after launch. Almost half of the failures (48%) occur during the first year of operation, which again could be attributed the inadequate ground testing. Fig. 11 display the magnitude of failure damages and the components involved in power failures:

As it was expected, the power failures are critical to spacecraft. Forty-five percent (45%) of the failures result in a loss of mission and about 80% significantly affects the spacecraft missions. Moreover, almost half of the power failures involved the solar arrays. This component is responsible for more failures than any other spacecraft components. It is also directly responsible for the impressive percentage of power failures in the first year. Many solar array problems are due to panel deployment mechanism failures (and could be arguably tallied up under the MECH subsystem failures) and insufficient power generation. This usually happens early when the spacecraft is in orbit. More ground testing could reduce considerably the number of defects that

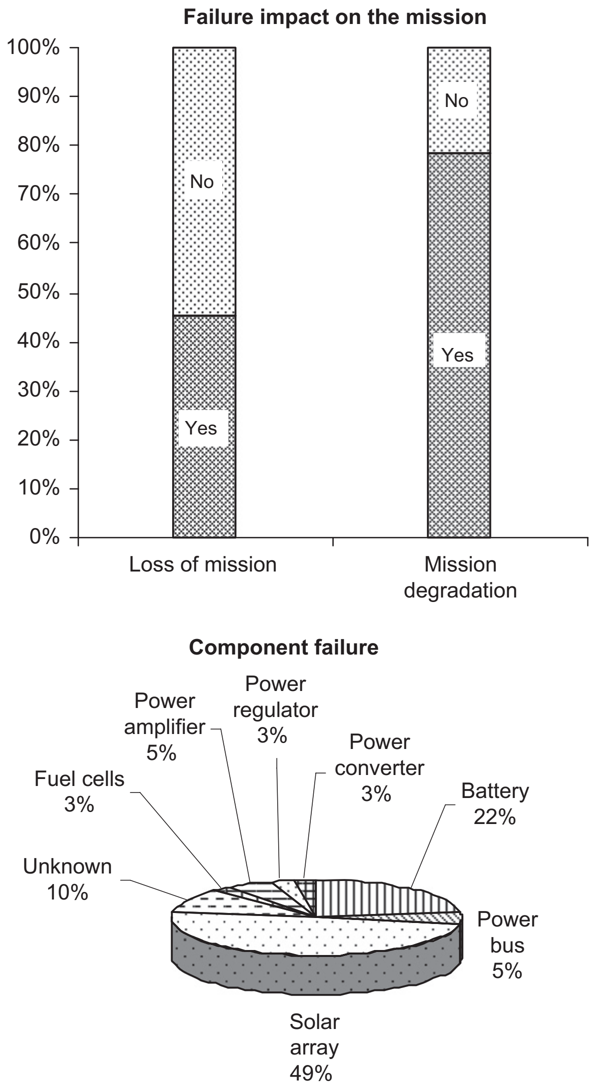

Fig. 11. Failure impact and component failure for power subsystem

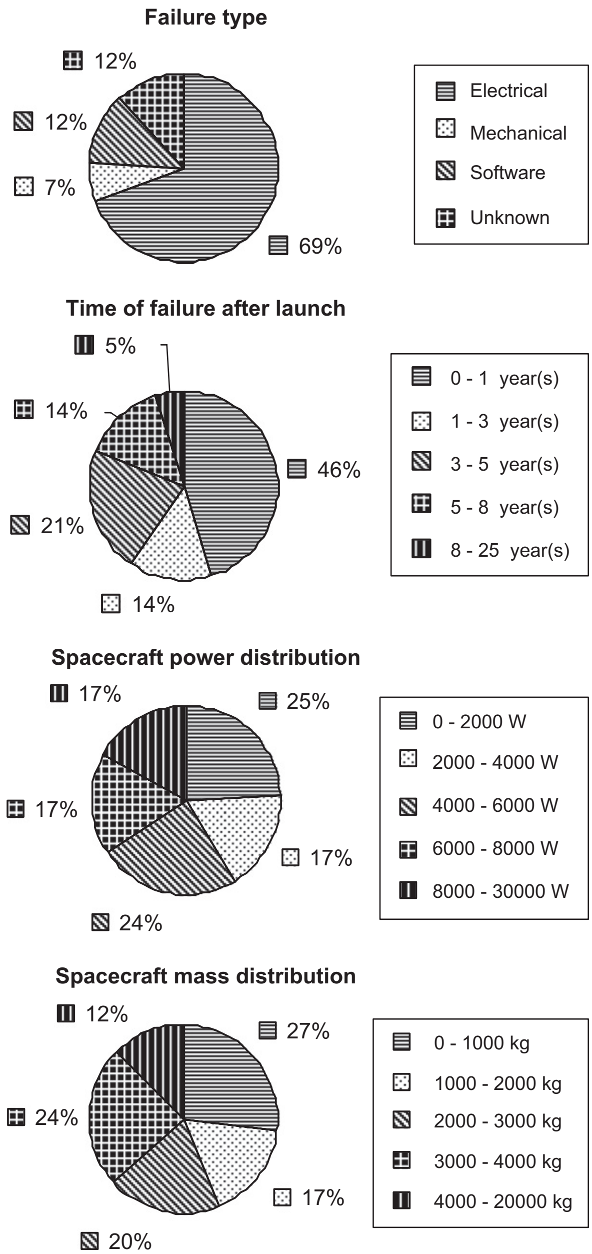

Fig. 12. CDH and TTC failure distributions

were uncovered during onboard operations. However, more ground testing costs more money and takes more time and hence must be traded off with the risks of reducing ground tests.

3.4. CDH and TTC failure analysis

The CDH and TTC subsystem failures were grouped together because a smaller number of failures were found and the results of their analysis are similar in many respects. Fig. 12 displays relevant data describing CDH and TTC subsystems:

We observe that the largest portion of the failures is electrical, which is expected again for the two subsystems under consideration. This category also contains the largest number of software failures. The software failures mainly consist in erroneous command sent to the spacecraft and software bugs. The most famous of software failure certainly occurred during the Mars Climate Orbiter (MCO) mission. The MCO mission has brought controversy within NASA organization when the spacecraft was lost during the Mars orbit insertion maneuver. The root cause was found to be a failure to use SI units in the coding of a ground software file used in a trajectory model. This underestimated the effect on the spacecraft trajectory by a factor of 4.45, which is the required conversion factor from force in pounds to Newtons. An erroneous trajectory was computed using this incorrect data. The MCO trajectory was too close to Mars, which destroyed the spacecraft [8]. Another similarity with the power subsystem failure analysis is the time of failure after launch. We see that 46% of failures occurred within one year of operation. The TTC subsystem is largely responsible for this high failure rate. More than 70% of the TTC failures occurred during the first year versus 24% for the CDH subsystem. There are several occurrences of antenna anomalies, ranging from failed deployment to unexplained loss of signal, and many transponder malfunctions. Fig. 13 displays the magnitude of failure damages and the components involved in CDH and TTC failures.

Similar to AOCS failures, the CDH and TTC failures are less critical and are better recovered than most of the failures. The loss of mission and mission degradation criteria are about 10% less than what was found in the overall case. This is expected since spacecraft components such as control processor (i.e., onboard computer), transponder and traveling-wave tube amplifier often have backup units. The relatively low number of failures from TTC (12% of all failures) and CDH (16% of all failures) subsystems is also a good indication of their reliability.

The space environment is an important criterion for this category. It is responsible for 21% of the failures that occurred to the CDH and TTC group. Solar storm and magnetic storm are causing single event effects and computer reset, which can be critical if they are not handled appropriately by a fault detection, isolation and recovery (FDIR) system. The effect of the space environment on the CDH and TTC subsystems is shown in Fig. 14.

3.5. MECH, payload and miscellaneous subsystems failure analysis

This category regroups the subsystems having less failures (based on our methodology in failure assignments) and also uncommon failure modes. Although, it would be relatively easy to find many more failures relating to spacecraft payloads, it was decided not to include any payload failure at the beginning of the present study. This was mainly due to the fact that spacecraft payload (i.e., instruments) have very specific applications and their technology cannot be easily compared

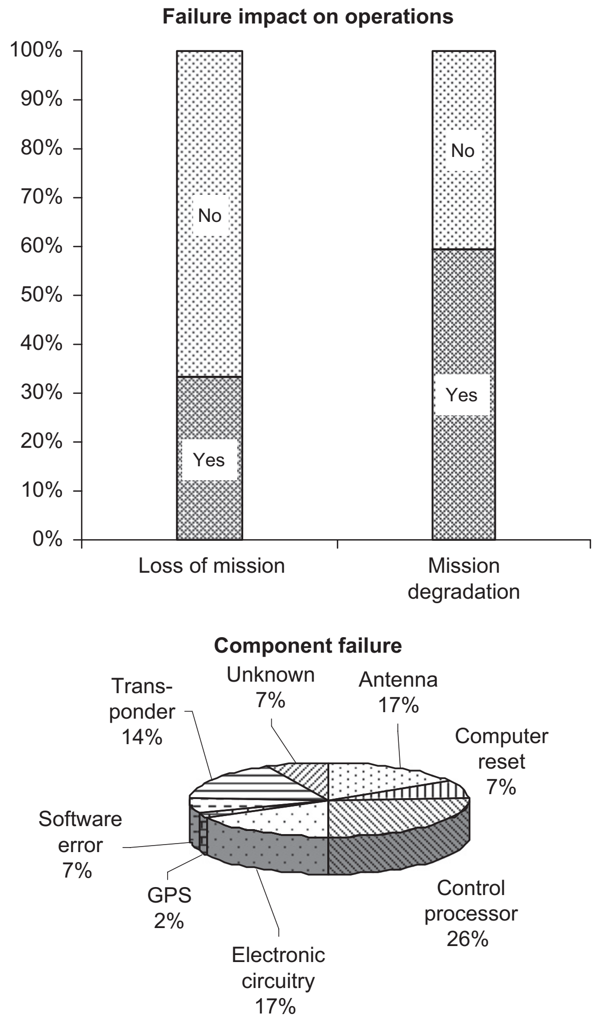

Fig. 13. Failure impact and component failure for CDH and TTC subsystems.

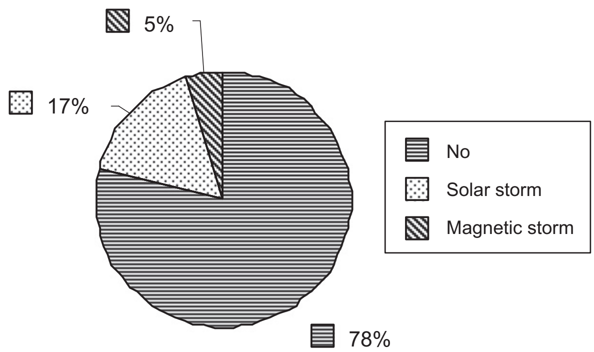

Fig. 14. Proportion of failure due to space environment.

from one spacecraft to another. Such comparisons can be done much more easily for bus components (e.g., momentum wheel or solar array). Consequently, we

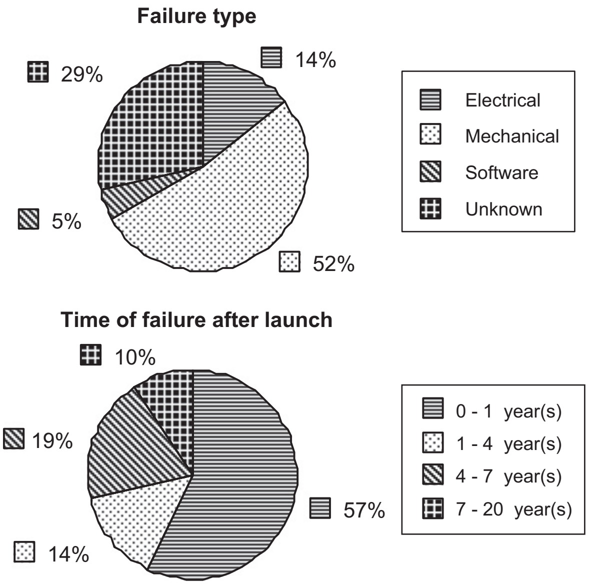

Fig. 15. MECH, payload and miscellaneous failures.

decided to include only payload failures causing significant mission degradation if they were not handled properly. We also regrouped all the different payload failures occurring on one satellite into a single failure entry. For example, numerous instruments failed over the years on NOAA-11 satellite: Advanced Very High Resolution Radiometer, High Resolution Infrared Radiation (Temperature) Sounder, Microwave Sounder Unit, Solar Backscatter Ultraviolet (radiometer). Regrouping the failures help us to keep an unbiased failure distribution. Most of the payload failures occurred on earth observation and scientific satellites. The miscellaneous category refers to failures that could not be linked to the main stream subsystems, such as tether and spacecraft docking mechanism failures.

Fig. 15 shows relevant data describing MECH, payload and miscellaneous subsystems.

We observed that half of the failures included in this category are mechanical and that most of them (57%) occurred in the first year of operation. From the mass and power distribution graphs, we see that the spacecraft are relatively small and require low power.

Fig. 16 reflects the magnitude of failure damages and the components involved in MECH, payload and miscellaneous subsystems.

We see that both criteria have a very high percentage. This is mainly due to MECH and miscellaneous failures. Although they occur rarely, at least 75% of the failures classified in both categories resulted in a loss of mission. The impact of payload failure is similar to what was

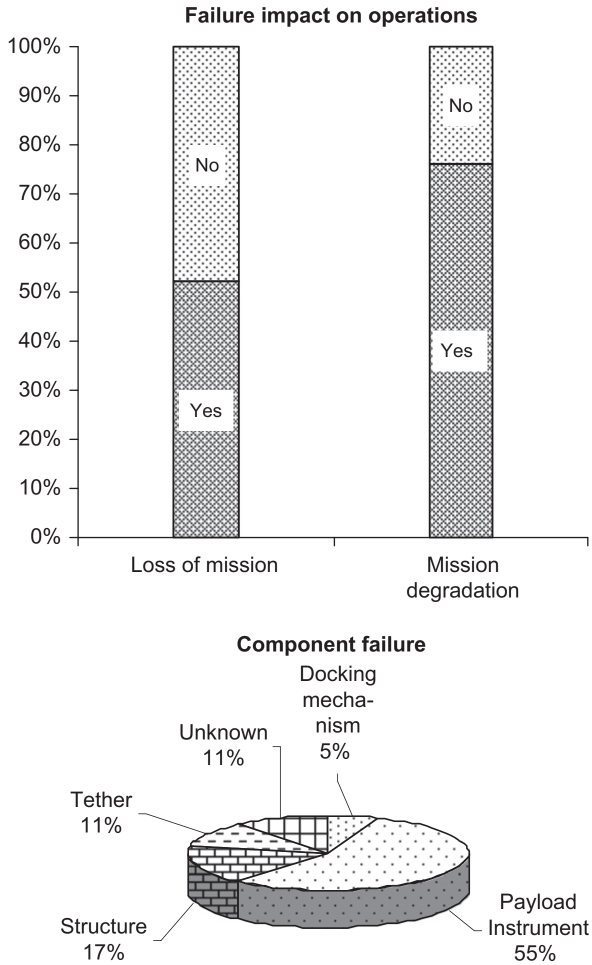

Fig. 16. Failure impact and component failure for SAM, payload and miscellaneous subsystems.

observed for the previous subsystems. Many payload failures were recovered due to recovery systems and redundancy.

4. Recommendations

4.1. Testing

One of the most important facts that were revealed in this study is the impressive number of failures occurring during the first year of operation. Contrary to expectations, the AOCS is the subsystem that obtained the lowest ratio of failures during the first year. Power and TTC have a very high ratio of failures during the first year. These subsystems are mostly made of electronic components and they should be reliable at least during 3–5 years of operation (depending of the part selection). Also, it was observed that many failures occurred right after launch. The following cases illustrate some of these failures: The Abrixas satellite, launched on 28 April 1999, had its main battery overheating after only 2 days. The batteries of the satellite Asusat 1 never received any charge from its solar array. After the Simplesat satellite deployment on 20 August 2001, no contact could be established. The most likely cause seems to be spacecraft transmitter arcing. Although many spacecraft are built under severe budget and time restrictions, it is important to conduct basic testing, especially when these tests represent a tiny fraction of the launch cost.

4.2. Redundancy

Having enough redundancy (both hardware and functional redundancy) is a key solution to improve spacecraft reliability. It is one of the main reasons that explained the reliability of AOCS actuators, AOCS sensors and spacecraft onboard processors over a 5-year period. The BeppoSAX spacecraft and ERS 2 both lost their three primary and three spare gyroscopes over a period of 5 years. Radarsat-1 and Echostar V lost one of their primary momentum wheels, which were substituted by a spare wheel allowing a standard attitude control during 7 years for Radarsat-1 and 4 years for Echostar V. Moreover, DirecTV 1, DirecTV 3, Galaxy VII, NOAA 14, and PAS-4 suffered a failure to their primary control processor. In each case, a backup processor was switched-on and the satellites had a lifetime exceeding 7 years. The lack of redundancy also leads to the retirement of one of the most important science satellites, the Compton Gamma Ray Observatory. After the failure of one of Compton's three gyroscopes, NASA decided to bring the satellite back via a controlled reentry. NASA determined that it was much safer to bring the satellite back now to safe guard against further system failures in the spacecraft that might hinder a controlled reentry. Spare gyroscopes could have further extended the life of this spacecraft, which cost $0.8 billions and took 9 years to develop. These facts demonstrate the importance of redundancy in failure recovery.

4.3. Flexibility

The flexibility provided by the system design in the spacecraft software and hardware could allow the ground engineers/operators to reprogram the different spacecraft systems. This is also a valuable asset in failure recovery. The spacecraft BeppoSAX and ERS 2 did not only use spare gyroscopes to recover from AOCS failure, but the flexibility provided by the AOCS software allowed the ground operators to upload a new gyroless attitude control mode. BeppoSAX's new gyroless control mode replaced the gyroscope measurement by a combination of star trackers and magnetometers. The star tracker handling was completely redesigned because the same star tracker needed to track 2 stars, up from 1 star. Amazingly, the quality of the images gathered in this mode was unchanged [9]. The flexibility of Radarsat-1 and Echostar V AOCS systems further extended their lifetime. Both spacecraft suffered a second failure to a momentum wheel. Echostar AOCS was modified to use thrusters to compensate for the missing wheel and this operating mode is not expected to reduce the estimated design life of the satellite to less than 12 years. Radarsat-1 used magnetic torque rods to de-saturate the Roll and Yaw reaction wheels and to provide pitch stabilization while keeping the failed pitch wheels completely disabled. This new configuration did not introduce any significant performance degradation [10]. This satellite is still providing useful science data 5 years after the last pitch wheel failure.

5. Conclusions

This paper presented a study of 156 on-orbit spacecraft failures conducted on more than 130 different spacecraft. The failures were carefully analyzed to characterize the different spacecraft subsystems and identify recurrent failure modes. The results showed the inability to deal with many on-orbit failures and the important number of failure occurring during the first year of operation. It also shows how spacecraft are vulnerable to failures occurring on key components such as solar arrays. An overall picture of the failures affecting the different spacecraft subsystems was also given. The last section contains pertinent recommendations based on this study and relevant failure cases. Besides conventional recovery systems, the emergence of Fault Detection, Isolation and Recovery (FDIR) systems may considerably increase the ability to autonomously detect and recover on-orbit failures occurring. These systems, which are currently developed for spacecraft, UAV and rovers, could significantly increase spacecraft reliability in recovering failures that may not be seen or "treated" on time by ground operators.

References

[1] Satellite news digest, URL: ⟨http://www.sat-index.com/failures/⟩ (accessed 29.04.05).

[2] The satellite encyclopedia, URL: ⟨http://www.TBS-satellite.com/tse/online/REG/main_index.html⟩ (accessed 29.04.05).

[3] C. Gunn, Failures are not an option, Launchspace (1098-6405), vol. 4, no. 1, February 1999, pp. 24, 26–29.

[4] N. Sultan, P.H. Groepper, Analyzing real cost of past orbital failures for satellite test effectiveness and insurance, in: AIAA International Communications Satellite Systems Conference and Exhibit, 18th, Oakland, CA, USA, 10–14 April 2000.

[5] M.L. Shooman, P.M. Sforza, A reliability driven mission for Space Station, in: Annual Reliability and Maintainability Symposium Proceedings, 2002.

[6] M. Caceres, Satellites and launches trend down, Aerospace America (0740-722X), vol. 42, no. 1, February 2004, pp. 18–20.

[7] J.R. Wertz, W.J. Larson, Space Mission Analysis and Design, third ed., Microcosm Press, Torrance, CA, USA, 1999.

[8] National aeronautics and space administration, Mars climate orbiter mishap investigation board phase I report ⟨ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/MCO_report.pdf⟩ (accessed 18.04.05).

[9] P. Martella, A. Tramutola, M. Montagna, Fine gyroless attitude control—the SAX experience, Space Technology 21 (4) (2001) 133–144.

[10] Y.V. Kim, G. Deraspe, Resolving RADARSAT1 momentum wheels failure problem, in: 54th International Astronautical Congress of the International Astronautical Federation (IAF), Bremen, Germany, 29 September–3 October, 2003.