1 Design Flaws of the Mars Climate Orbiter

An Analysis of the Design Flaw's Impact, Technical Details, and Connection to Cybersecurity

Megan Erasmus

Department of Computer Science, Western Washington University, Bellingham, WA, USA,
erasmum@wwu.edu

ABSTRACT

The Mars Climate Orbiter, a collaborative mission between NASA and Lockheed Martin, aimed to explore Mars' atmosphere, climate, and surface. However, a critical design flaw in the orbiter's navigation software, where the system used pound-seconds instead of newton-seconds, led to miscalculations. This flaw went undetected, causing the orbiter to deviate from its intended orbit, with the spacecraft disintegrating in Mars' atmosphere. Contributing factors included improper communication and inadequate system engineering.

The impact of the design flaw was profound, leading to the disruption of NASA's Mars Surveyor Program and damaging both NASA and Lockheed Martin's reputations. The failure resulted in direct costs of $125 million. The disaster highlighted the challenges of collaboration in space missions and emphasized the importance of edge case testing, effective communication, robust testing, and proper training.

The technical details revealed a mismatch in unit systems, particularly in propulsion calculations, showcasing the drastic consequences of misinterpretation. Mitigation strategies implemented by NASA included unit standardization, improved communication, rigorous testing, and enhanced training, aiming to prevent similar disasters. The incident underscores the significance of proper coordination, thorough testing, and adherence to cybersecurity principles in space exploration endeavors.

CCS CONCEPTS

Social and professional topics • Mathematics of computing • Security and privacy

2 Introduction

The Mars Climate Orbiter was a collaborative space venture between NASA, the National Aeronautics and Space Administration, and Lockheed Martin, an American corporation specializing in aerospace, arms, defense, information security, and technology corporation [1]. The Mars Climate Orbiter was the second probe in NASA's Mars Surveyor Program, launched in 1998 after the Mars Global Surveyor, which was launched in 1996 [2].

The mission was intended to conduct investigations of Mars' atmosphere, climate, and surface alongside the Mars Polar Lander, which was launched in 1999, shortly after the launch of the Mars Climate Orbiter. The arrival of the Mars Climate Orbiter was dated for September 23rd, 1999, and it was intended to reach its operational intended orbit at 260 miles by December 1st, 1999. On September 23rd, 1999, the Mars Climate Orbiter began the orbit insertion as scheduled, however signal was lost after passing behind Mars. The orbiter missed its intended orbit causing it to fall into the atmosphere of Mars, disintegrating the orbiter due to the atmospheric stress [2]. The orbiter was found to have a single design flaw that led its navigational system to direct its course into the Martian atmosphere.

3 The Design Flaw

The Mars Climate Orbiter was designed specifically to utilize imperial units in its navigation software. The software calculated the thruster force required to maintain on the predetermined course to successfully allow the spacecraft to transition into orbit. The units, pound-seconds, used in the orbiter's software, differed from the units used in the ground-based team's calculations, which happened to be

metric units. The unit calculations done on Earth, in newton-seconds, were sent to the Mars Climate Orbiter. The Orbiter's software did not have a check for units or a unit conversion, and thus the data given to the Orbiter was incorrect when converted to pound-seconds.

The misalignment of units was a simple edge case that was not caught during the design and testing phases of creating the orbiter. This software error was found to have affected the orbiter throughout its entire course, spanning the entire 10 months and 416 million miles that it traveled before the spacecraft was lost. The miscalculations, being minor enough to ignore during the 10 months of travel, set the spacecraft off course from day one. The miscalculations of trajectory were not caught by the JPL (Jet Propulsion Laboratory), and therefore never corrected by the system of checks and balances that were in place to prevent issues such as this [3]. These tiny errors in trajectory compounded over time, eventually leading to the spacecraft's mission failing.

4 Contributing Factors

The failure board compiled a report after the Mars Climate Orbiter was lost detailing eight contributing factors that indirectly and directly contributed to the failure of the mission. The root cause was identified as the incorrect units provided, causing the spacecraft to lead itself into the Martian atmosphere [4]

The board's report lists the first contributing factor as the fact that the calculation errors went undetected throughout the entire interplanetary trip to Mars. The fact that the errors were not noticed throughout the entire process was notable because, as previously mentioned, the JPL was supposed to impose a system of checks and balances to monitor the trajectory.

The board also mentioned that the operational navigation team was not informed of the details on the course of the Mars Climate Orbiter in comparison to the Mars Global Surveyor's mission [4]. With the operational navigation team not having detailed insight on the direction of the orbiter, there was not much that could have been done by the team to prevent the loss of the orbiter.

The systems engineering function within the project was intended to track and check all interconnected aspects of the mission, however the function was not extensive enough. With NASA and Lockheed Martin working together on this orbiter, the system engineering function should have been reevaluated to ensure that throughout the integration of the spacecraft and all other aspects of the system that the overall functionality had been considered robust enough to feel confident that the mission was to succeed.

Another notable factor mentioned by the board is that communication channels among project engineering groups were noted as being too 'informal' [4]. The informality of communication between engineering groups, particularly on a collaborative mission, allowed for details to be unclear to personnel who were handling and passing critical information to the spacecraft.

Had the software designers for the spacecraft's system included proper edge case checking and testing, it is likely that the bug would have been detected sooner. Clear documentation on the unit conventions used in software could have also allowed for the potential for conversion issue to be noticed sooner.

5 Design Flaw's Impact on the Mission

There were significant repercussions of the design flaw, as the spacecraft in its entirety was lost. This created major issues in NASA's 10-year Mars Surveyor Program. The climate orbiter was launched in a timely manner aiming to reach Mars in the shortest possible route based on the orbits of Earth and Mars. Earth and Mars are only favorably aligned once every 26 months, meaning that the schedule for the Mars Surveyor Program was severely thrown off. NASA would have to wait 26 months from the initial takeoff date before another spacecraft could be launched to potentially replace the Mars Climate Orbiter. This is without considering the time and finances required to rebuild a similar orbiter to perform the functionality required of the Mars Climate Orbiter.

The disaster not only disrupted NASA's Mars Surveyor Program mission, but also did reputational damage to both NASA and Lockheed Martin. The general public and scientific community had expectations for the mission, and when NASA lost a spacecraft, concerns were raised about NASA's ability to execute complex space exploration missions over trivial calculation errors caused by lack of software unit checks. Questions were also raised about the ability for NASA to work and coordinate with different teams and companies. It was said that some communication channels between project engineering groups were too informal, and the process to verify and validate engineering requirements and technical interfaces was lacking between project groups and the prime mission contractor [4].

Lockheed Martin also faced scrutiny, as the company was a primary contractor for the mission. The impact on Lockheed Martin's credibility was notably smaller than NASA's, being less well known, however being a contractor for a spacecraft that failed affected credibility in delivering reliable spacecraft.

6 Stakeholder Impact

The Mars Climate Orbiter disaster implicated multiple stakeholders, including NASA, Lockheed Martin, and the teams responsible for software design and implementation. Communication breakdowns and a lack of tightly designed procedures show the importance of collaboration in space missions, without which large problems can occur. Improper communication impacts all stakeholders, as one error made by team personnel due to a miscommunication can lead to total mission failure.

From a financial perspective, the Mars Climate Orbiter disaster incurred direct costs estimated at $125 million [3]. This number encompasses the investment in the spacecraft's design, development, and launch. However, the indirect costs, such as the loss of scientific data, reputational damage, and the investigations that occurred, significantly inflated the overall damage done by the mission's failure. This idea tightly aligns with the concept that finding bugs in software post-release is much more expensive to mend than if the bugs were found prior to launch. If the issues were detected before the spaceship had launched, the financial impact of the mission would have been less, and there would have been a spacecraft performing its assigned task in space. There would also not be reputation damage for any stakeholders involved.

7 Technical Details of the Flaw

The technical details of the design flaw were rooted in the mismatch of unit systems, particularly in the critical area of thrust propulsion calculations. The spacecraft's software, responsible for trajectory calculations, was programmed with imperial units (pound-seconds) for the thruster force. This information was then sent to the navigation team on Earth, where the data was interpreted using metric units (newton-seconds). The failure to check these units resulted in the generation of incorrect acceleration values during the journey, ultimately leading to the spacecraft's trajectory towards Mars' atmosphere.

To display the discrepancy between units, an example can be used. One pound is equal to approximately 4.44822 newtons. Using a more specific example, in general, the force required for takeoff is 7.2 million pounds of thrust [5]. Converting this to newtons, we find that 7.2 million pounds of force equates to 32 million newtons of force. This extreme example shows how a misinterpretation of data can lead to catastrophic consequences, one that have easily been prevented.

8 Mitigation

To mitigate the risk of such disasters in the future, NASA has and could continue to implement several changes in its processes and procedures. These changes included standardization of units [6], while NASA could continue to improve communication, testing, and training.

NASA implemented a standardization of units across all its projects to avoid any confusion or miscommunication between different teams working on a project. This ensures that all teams are using

the same units of measurement, reducing the risk of errors due to unit conversion. This improved communication between different teams working on a project, since there was no discrepancy on what units to use. Better coordination between the spacecraft's navigation software team and the ground crew would come from this. NASA also could implement better communication protocols to ensure that all teams are aware of any changes or updates to the project. More rigorous testing procedures would ensure that all software and hardware components are working correctly. Clearly defined risk management protocols could also provide a basis for preventing issues that could be caught during testing.

There could have also been better training programs for NASA employees to ensure that they are aware of the risks associated with space missions, and the importance of correctness. Improved training would assist in helping all personnel on a mission to know concepts regarding proper data management and validation [7].

These changes have helped NASA to avoid similar disasters in the future. The Mars Climate Orbiter disaster highlights the importance of proper communication and coordination between different teams working on a project. It also emphasizes the need for proper testing and validation of software and hardware components to ensure that they work correctly.

9 Future Disaster Prevention

To prevent incidents like the Mars Climate Orbiter disaster in the future, where software design flaws resulted in mission failure, several key practices and protocols can be implemented. An idea that would prevent conversion-specific issues would be to standardize units across all components of a mission to ensure consistency and eliminate the risk of errors caused by unit mismatches.

Other factors that would aid in preventing incidents like the Mars Climate Orbiter disaster include implementing automated checks within the software for verifying correct unit usage during the development and testing phases. Increased facilitation of verification of calculations and parameters by different teams, particularly those responsible for software development and mission planning, can provide multiple perspectives to catch any bugs or potential issues. Additionally, rigorous testing procedures that include testing under various conditions and all edge cases, ongoing training programs for mission teams, and highly organized risk management protocols can be beneficial in preventing software-related risks.

10 Connection to Cybersecurity

The Mars Climate Orbiter incident and its preventive measures are connected to cybersecurity principles through the context of information security, risk management, and system integrity. In the context of cybersecurity, ensuring the integrity and accuracy of data is fundamental. User input validation (UIV) can help ensure the accuracy of data and can prevent incorrect data from being given to a system. The Mars Climate Orbiter incident underscores the critical importance of accurate data in space missions. In cybersecurity, accurate data is crucial for making informed decisions and preventing security breaches.

Both space missions and cybersecurity have inherent risks. Implementing strong risk management protocols, as suggested for preventing future space mission failures, is also applicable to cybersecurity. Identifying, assessing, and mitigating risks are crucial aspects in terms of maintaining the security of information systems.

The concept of implementing edge case testing, potentially automated checks, within software to verify the correctness of unit usage is closely related to edge case testing and security checks in cybersecurity. Checking for vulnerabilities in all scenarios works towards ensuring the security of systems.

11 Conclusion

The Mars Climate Orbiter disaster serves as a reminder of the critical importance of edge case testing, rigorous software testing, attention to technical details, effective collaboration, and continuous

improvement in processes within the aerospace industry. The catastrophic failure of the Mars Climate Orbiter, stemming from a seemingly simple design flaw in the spacecraft's systems, resulted in profound consequences for NASA's Mars Surveyor Program, producing high financial costs for stakeholders, and damaged the reputations of both NASA and Lockheed Martin.

The incident outlined the challenges of collaboration in space missions, showcasing how improper communication and insufficient system engineering can affect a mission. The impact on stakeholders, including financial costs and reputational damage, shows the importance between effective communication and mission success.

The technical intricacies of the design flaw demonstrated the potentially catastrophic consequences of misinterpretation, emphasizing the need for precision in calculations, especially in crucial areas such as thrust propulsion.

NASA's mitigation efforts, including unit standardization, are a step towards preventing disasters such as this in the future. More changes can be made, such as focusing on improving communication, training, and testing. These changes aim to prevent similar disasters and ensure the success and safety of future space missions.

Ultimately, the Mars Climate Orbiter serves as a valuable lesson, emphasizing testing systems, communication, collaboration, and the importance of technical accuracy. The incident is a reminder of the need for change to mitigate the risk of failures and create more successful missions in the future.

REFERENCES

[1] Leading Aerospace and Defense (no date) Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/index.html (Accessed: 16 November 2023).
[2] Mars Climate Orbiter (2017) NASA Science. Available at: https://science.nasa.gov/mission/mars-climate-orbiter/ (Accessed: 16 November 2023).
[3] MARS CLIMATE ORBITER FAILURE BOARD RELEASES REPORT, NUMEROUS NASA ACTIONS UNDERWAY IN RESPONSE (1999) Mars Climate Orbiter Failure Board releases report. Available at: http://sunnyday.mit.edu/accidents/mco991110.html (Accessed: 16 November 2023).
[4] Sawyer, K. (1999) Mystery of Orbiter Crash Solved, The Washington Post. Available at: https://www.washingtonpost.com/wp-srv/national/longterm/space/stories/orbiter100199.htm (Accessed: 16 November 2023).
[5] Welcome to how things fly (2014) | How Things Fly. Available at: https://howthingsfly.si.edu/ask-an-explainer/how-much-force-rocket-launch (Accessed: 16 November 2023).
[6] Anon. Units of measure - NASA science. Retrieved November 16, 2023 from https://science.nasa.gov/learn/basics-of-space-flight/units/
[7] Hoffman, E. Deficiencies in Mission Critical Software Development for Mars Climate Orbiter (1999). Retrieved November 16, 2023 from https://llis.nasa.gov/lesson/740