

A photograph of an Ariane 501 rocket being launched. The rocket is white with black and blue accents. It has two solid rocket boosters on either side. The boosters have the ESA logo and the text 'ESA' and 'cnes'. The main stage has the 'arianespace' logo and 'SERVICE & SOLUTIONS'. The nose cone has a logo for 'PRODIGE' and '14th Anniversary 1992-2006' and the ESA logo. The rocket is surrounded by a large plume of white smoke and fire. Two tall, thin metal towers are visible on either side of the rocket. The sky is blue with some clouds.

# ROCKETS THAT FAIL SAFELY

*Spacecraft failures are spectacular. These unfortunate events are seared into the public memory. One reason why rockets can fail are software bugs. If a rocket's computer system fails, that infamous blue screen leads to lost work hours, billions of Euro, and lives. Researchers from the Faculty of ICT and Faculty of Engineering (University of Malta) tell **THINK** about their collaboration with the European Space Agency (ESA) to test novel satellite software architecture to prevent rocket failure.*

**J**une 1996, Ariane 5 Flight 501. Twenty years ago, the world braced itself for the very first flight of a giant rocket that was capable of hurling a pair of three-tonne satellites into orbit. Standing proudly at the European spaceport in French Guyana, the rocket represented ten years of progress in launcher technology and was meant to catapult European space science to the forefront.

Less than a minute into the flight, the mighty Ariane 5 suddenly veered off course and broke up. Naturally, when rockets fail, they fail spectacularly. They always do. Ariane 501, the Titanic of European launchers, turned into a massive fireball on its maiden voyage—a sad day for European space science.


The crash inquiry report, published a few months after the incident, revealed that the launcher broke up when it abruptly swerved off course under the command of the flight control system. The culprit was a small bug in its Inertial Reference System (IRS), the system that calculates the altitude of the launcher: a few erroneous lines of code had tried to stuff a 64-bit number into a 16-bit space. This resulted in invalid altitude information being communicated to the flight control computer, which interpreted it as valid altitude input causing three powerful nozzles to swing to an extreme

position. The control system was compensating for a wrong turn that had not taken place, which destroyed the launcher in the process.

A little bug and a big bang: around €6b worth of research and development had fallen victim to a few wrong lines of code. This glitch is infamously considered to be one of the most expensive software bugs in history. Garbage in, garbage out, as fiery bits of debris ended up littering the swamps of French Guiana.

The crash inquiry concluded that the development programme 'did not include adequate analysis and testing of the inertial reference system or of the complete flight control system.' Suitable testing could have detected the potential failure and the appropriate fixes would have contributed to a more robust control system—perhaps robust enough to gracefully deal with unanticipated situations, such as a misleading altitude input.

## **SYSTEM ROBUSTNESS AND THE SPACE SECTOR**

Some bugs do not fly, and this was definitely one of them. Designing robust systems that can deal with such glitches pays off. These software issues are, of course, not just limited to the space sector. The same vulnerabilities may crash your word 



processor. The worst scenario in our everyday lives is hours lost leading to a very bad day. In space, things are a bit different. Considering the number of man-hours of delicate and intricate work involved in design and development, it sometimes means that, kilo for kilo, satellites would cost less were they to be made out of solid gold. Provided the spacecraft has surpassed the critical phase of launch, unrecoverable satellite subsystems may result in the loss of control of the orbiting satellite. Years of work and millions of Euro are turned into a lump of orbiting junk—now that really is a bad day.

Nowadays, spacecraft software design needs an extensive dependability and robustness testing campaign. The stakes in the space sector are too high to get it wrong. But how would you check how robust a piece of software is?

Simply put, the answer is: by making it fail. And by 'causing it to fail', software glitches can be detected before they lead to failure during space flight. Developers may detect and fix bugs they had overlooked during the initial design phase. One way of doing this is to intentionally inject faults within the software being tested and observe how it responds or stops responding.

## SPACE FLIGHT MALTA

To try to make rockets fail safely, Stephen Grixti (supervised by Dr Ing.



**Top: Grixti (second from the left) together with other ISU colleagues at the RF Testing chamber at MDA, Montreal. Below: Grixti with the Artemis Jr lunar rover prototype designed by the Neptec Design Group for NASA and the Canadian Space Agency**

*Considering the number of man-hours of delicate and intricate work involved in design and development, it sometimes means that, kilo for kilo, satellites would cost less were they to be made out of solid gold*

Nicholas Sammut and Prof. Ing. David Zammit Mangion) spent six months at the ESA (European Space Agency) working on the research project. He tested the robustness of ESA's novel satellite software architecture as part

of a collaboration between the Faculty of ICT, the Faculty of Engineering (both at the University of Malta) and the European Space Research and Technology Centre (ESTEC).

At ESTEC, the research heart of

the ESA in the Netherlands, and later at UoM, ESA's satellite software was tested by scientists trying to make it fail—and unfortunately (or fortunately) it actually did fail! Grixti found a number of critical design flaws that led ESA contractors to re-evaluate their systems to avoid the same kind of fault that had led to the destruction of the Ariane 501.

Through this study, a black-box robustness testing methodology was tailored to inject faults within the separation kernel of a Time and Space Partitioned (TSP) spacecraft on-board software. The devised testing architecture was then used to investigate the robustness of ESA's own EagleEye spacecraft. EagleEye is an ESA testbed representative of typical Earth observation satellites—that is, the satellites that snap those beautiful Earth photos from around 800 km. The case study detected a number of issues with robustness at the satellite's software core. It picked up on a glitch that led to the system's catastrophic failure.

## A PASSION FOR SPACE TECHNOLOGY

Grixti looks back at his research experience and recollects many fulfilling memories. Every time an ESA satellite was launched, a large crowd would gather and the event was streamed live from the launch site. Those present could sense a mixture of tension, passion, and excitement ➔



## WEIGHTLESS AT LAST

Space science and technology research projects open unique opportunities. Sammut reminisces about a unique experience when a collaborator from the Centre National D'Etudes Spatiales (CNES) invited him to a free parabolic flight. These flights are performed by aircraft such as the Airbus A300 aircraft that briefly leads to near-weightlessness as they shoot up to very high altitudes simply to hurtle back down to earth. They are used to conduct microgravity experiments for scientists to understand the behaviour of matter in the absence of gravity. Apart from research, such flights usually serve as training for astronauts.

'During the microgravity flight, you first feel twice your weight, and you can hardly lift your own hand. Then all of a sudden you are completely weightless, floating around freely and upside down. If you just hit the wall a little, you are sent hurtling towards the other side of the cabin,' comments Sammut as he reminisces about his wonderful experience.

Microgravity Parabolic Flights on the CNES Airbus A300 Zero-G plane last approximately 2.5 hours with 15 parabolas totalling five minutes of weightlessness. Parabolic arcs are performed to create a weightless environment, allowing passengers to float, flip, and soar as if they were in space.

'It has been a lifelong dream to be an astronaut,' states Sammut. 'Now I know what it feels to be an astronaut for a day, or rather, for five minutes.'



Dr Ing. Nicholas Sammut during the parabolic flight on the CNES Airbus A300 Zero-G plane

among the onlookers. These researchers felt responsible for that spacecraft; it was their baby.

But perhaps the best cocktail of passion, pride, and champagne came in November 2014 with the Rosetta mission making the news all over the world. Philae, a lander the size of a washing machine, was released from the Rosetta satellite and made the first ever comet landing. Rosetta and Philae had been travelling for 10 years in space and Gixti was fortunate enough to be stationed at ESA when this landing happened. The Rosetta control room was streamed live in the auditorium and once the landing was announced the tense, never-ending silence broke into cheers, claps, and the winning sound of popping champagne bottles. Again, there was an infectious sense of achievement and belonging. This was one small step for the Rosetta

mission, but one giant leap for science.

There was more to come. Half-way through his project, Gixti was sponsored to attend a two-month space studies course in Montreal, Canada. This was organised by the International Space University (ISU), a community of space professionals from all over the world that harbours a healthy network of influential space experts, which includes political figures and numerous astronauts.

## THE RESEARCH EXPERIENCE

The whole research project was a memorable journey. The value gained does not only come from the technical experience and the excellent results achieved, but from meeting people from different cultures in an international setting. By venturing outside of their comfort zone up and

coming scientists can learn and be inspired by world renowned specialists and astronauts within an environment of collaboration.

Reading about satellites and space technology is exciting, but actually living it through such collaborations takes the experience to an entirely different level. That is what successful rocket launches do all the time, and once they lift off they are difficult to access. Robust systems are critical for space travel. Finding critical flaws through testing like those found by UoM researchers could have saved the Ariane 5 Flight 501 in 1996. **T**

**The University of Malta research team would like to thank Prof. Edward Gatt from the Faculty of ICT, and the Flight Software Systems section in ESTEC for their support throughout the research project.**

