

With PolySpace ADA Verifier, Increased dependability for EADS-LV Space Vehicles

JOB DESCRIPTION: SPACE TRANSPORT

EADS-Launch Vehicle¹ is a prime architect for space vehicles. Its mission: integrate the components required for putting satellites into orbit.

The equipment and software on board the vehicle accompany the payload into orbit or when it comes back down to earth. These are also present during space missions or for military applications.

To ensure that these precious passengers are not lost in transit, EADS-LV must imperatively guarantee the reliability of its vehicles into space. However, the incorporation of many different pieces of software is not always easy, and their integration may be complex. Thus, validating the reliability and coherence of on-board systems is a major milestone, because the stakes for EADS-LV are enormous.

The loss of a space vehicle would have a catastrophic effect on customer orders.

TEST AND CORRECT EVERY ERROR

To guarantee the mission's safety, countless verifications and tests must be performed, simulating software's execution environment.

All these tests take place on the ground, because in-flight intervention would be impossible.

Thus, it is with great care that 100,000 lines of code are minutely scrutinized.

Because, at EADS-LV «we are most careful with errors leading to a software halt. These cannot be tolerated». Indeed, they may lead to the destruction of the space vehicle.



«We are most careful with errors leading to a software halt. These cannot be tolerated»

The principal difficulty is to integrate external software, subcontracted to third parties, which must function together in an embedded environment. Errors may arise simply from the context in which the software is used.

This is the priority for EADS-LV: to ensure that software errors can in no way endanger a launch.

¹ Previously AEROSPATIALE MATRA LANCEURS
[http : //www.lanceurs.aeromatra.com](http://www.lanceurs.aeromatra.com)

« POLYSpace ADA VERIFIER INTERVENES TO FIND RUN-TIME ERRORS »



Traditional test cases are not exhaustive. They do not allow to conclude with certainty that all errors have been identified. «This is where PolySpace Ada Verifier's solution is unique - it detects run-time errors without execution and also has the advantage of being exhaustive». It detects all run-time errors (overflow, non-initialized variables, access conflicts, etc.) without requiring a single test case. It then detects two types of errors: certain errors and potential errors. «Even the detection of potential errors is appreciated» underscores EADS-LV. An error costs approximately one hour when identified during software development, ten hours when during integration, one hundred hours when during final validation, and more than a thousand hours after deployment ! PolySpace Ada Verifier allows developers to no longer miss any of these errors. What is more, it saves precious time by localizing precisely the sections of code to be verified.

«This is where PolySpace Ada Verifier's solution is unique - it detects run-time errors without execution, and also has the advantage of being exhaustive».

POLYSpace ADA VERIFIER USE POLYSpace ADA VERIFIER TO GUARANTEE QUALITY AND SECURITY

EADS-LV uses PolySpace Ada Verifier as a «final quality control» tool. All software written in Ada, whether subcontracted or developed in-house, is systematically verified by PolySpace Technologies' tool.

This applies to application software for equipment, as well as for central software integrating the applications on the operating platform. The results of these tests (certain or potential errors) then provide pertinent questions for the software designers.

In using PolySpace Ada Verifier at the start of the verification process, EADS-LV will be able to speed the detection of errors that have slipped into software, and thus reduce costs and time to market.

Another use of the technology is under consideration: using PolySpace Ada Verifier to identify test cases for software designed by EADS-LV. This would allow even greater market reactivity, thus saving time... and money.

