Ariane V Disaster

From: https://softwareengineering.stackexchange.com/questions/149888/what-was-the-historical-impact-of-ariane-5s-flight-501

The flight control software was recycled from the earlier Ariane 4 rocket, a sensible move given how expensive it is to develop software, especially when it's mission critical software which must be tested and verified to far more rigorous standards than most commercial software needs to be.

Unfortunately, nobody bothered testing what effect the change in operating environment would have, or if they did they didn't do said testing to a sufficiently thorough standard.

The software was built to expect certain parameters to never exceed certain values (thrust, acceleration, fuel consumption rates, vibration levels, etc). In normal flight on an Ariane 4 this wasn't a problem because those parameters would never reach invalid values without something already being spectacularly wrong. The Ariane 5, however, is much more powerful and ranges that would seem to be silly on the 4 could quite easily happen on the 5.

[When the Ariane Vflight trajectory exceeded the profile expected for an Ariane 4 flight,] the software was unable to cope and suffered an arithmetic overflow for which there had been insufficient error checking and recovery code implemented. The guidance computer started sending garbage to the engine nozzle gimbals, which in turn started pointing the engine nozzle pretty much randomly. The rocket started to tumble and break up, and the automatic self-destruct system detected the rocket was now in an unsafe irrecoverable attitude and finished the job.

This particular case was especially glaring because a shortcut taken to save money ended up costing a huge amount, both in terms of money and lost reputation. If the software had been tested just as robustly in an Ariane 5 simulated environment as it had been when it was originally developed for Ariane 4, the error surely would have come to light long before the software was installed in launch hardware and put in command of an actual flight. Additionally, if a software developer had deliberately thrown some nonsense input into the software then the error might have even been caught in the Ariane 4 era, as it would have highlighted the fact that the error recovery that was in place was inadequate.

From the "Full Report" at: http://www-users.math.umn.edu/~arnold/disasters/ariane5rep.html

It would have been technically feasible to include almost the entire inertial reference system in the overall system simulations which were performed. For a number of reasons it was decided to use the simulated output of the inertial reference system, not the system itself or its detailed simulation. Had the system been included, the failure could have been detected.