The Ariane 5 Launcher Failure

June 4th 1996

Total failure of the Ariane 5 launcher on its maiden flight

Ariane 5

- A European rocket designed to launch commercial payloads (e.g.communications satellites, etc.) into Earth orbit
- Successor to the successful Ariane 4 launchers
- Ariane 5 can carry a heavier payload than Ariane 4

Launcher failure

- Approximately 37 seconds after a successful lift-off, the Ariane 5 launcher lost control.
- Incorrect control signals were sent to the engines and these swivelled so that unsustainable stresses were imposed on the rocket.
- It started to break up and was destroyed by ground controllers.
- The system failure was a direct result of a software failure. However, it was symptomatic of a more general systems validation failure.

The problem

- The attitude and trajectory of the rocket are measured by a computer-based inertial reference system. This transmits commands to the engines to maintain attitude and direction.
- The software failed and this system and the backup system shut down.
- Diagnostic commands were transmitted to the engines which interpreted them as real data and which swivelled to an extreme position resulting in unforeseen stresses on the rocket.

Software failure

- Software failure occurred when an attempt to convert a 64-bit floating point number to a signed 16-bit integer caused the number to overflow.
- There was no exception handler associated with the conversion so the system exception management facilities were invoked. These shut down the software.
- The backup software was a copy and behaved in exactly the same way.

Avoidable failure?

- The software that failed was reused from the Ariane 4 launch vehicle. The computation that resulted in overflow was not used by Ariane 5.
- Decisions were made
  - Not to remove the facility as this could introduce new faults;
  - Not to test for overflow exceptions because the processor was heavily loaded. For dependability reasons, it was thought desirable to have some spare processor capacity.

Why not Ariane 4?

- The physical characteristics of Ariane 4 (A smaller vehicle) are such that it has a lower initial acceleration and build up of horizontal velocity than Ariane 5.
- The value of the variable on Ariane 4 could never reach a level that caused overflow during the launch period.

Validation failure

- As the facility that failed was not required for Ariane 5, there was no requirement associated with it.
- As there was no associated requirement, there were no tests of that part of the software and hence no possibility of discovering the problem.
- During system testing, simulators of the inertial reference system computers were used. These did not generate the error as there was no requirement!

Review failure

- The design and code of all software should be reviewed for problems during the development process
- Either
    - The inertial reference system software was not reviewed because it had been used in a previous version;
    - The review failed to expose the problem or that the test coverage would not reveal the problem;
    - The review failed to appreciate the consequences of system shutdown during a launch.

Lessons learned

✧ Don’t run software in critical systems unless it is actually needed.

✧ As well as testing for what the system should do, you may also have to test for what the system should not do.

✧ Do not have a default exception handling response which is system shut-down in systems that have no fail-safe state.

Lessons learned

- In critical computations, always return best effort values even if the absolutely correct values cannot be computed.
- Wherever possible, use real equipment and not simulations.
- Improve the review process to include external participants and review all assumptions made in the code.

Avoidable failure

- ✧ The designer’s of Ariane 5 made a critical and elementary error.
- ✧ They designed a system where a single component failure could cause the entire system to fail.
- ✧ As a general rule, critical systems should always be designed to avoid a single point of failure.