Product failure: learning the lessons of Toyota

Published on 6 September 2010

By Malcolm Wheatley

Cars are increasingly complex and software-dependent, yet when lives are at stake what matters is not just building safe software, but how you react when problems start to appear*E&T* asks what other manufacturers can learn from Toyota's recent travails - and how the car giant might have dealt with them more effectively.

It should not have been a surprise that software might be blamed - rightly or wrongly - for the recent high-profile cases of out-of-control Toyotas. After all, faulty software had already been fingered for crashes that were literally out of this world.

It was in late 1999 that two linked missions to Mars finally arrived at the Red Planet after blasting off from Cape Canaveral almost 12 months earlier.

Reaching Mars on 23 September 1999, Mars Climate Orbiter began a 16-minute 'orbit insertion' engine burn, which took it behind the planet, away from direct contact with Earth. It was never heard from again.

The second mission, Mars Polar Lander, reached Mars on 3 December 1999, and duly began its descent. It too was never heard from again, with the last successfully-received telemetry being sent just prior to atmospheric entry.

A subsequent investigation revealed that the most likely cause of the latter mission's failure was a software error that wrongly identified vibrations caused by the deployment of the lander's legs as the vehicle touching-down on the Martian surface. Accordingly, the descent engine would have been switched off 40m above the surface, causing the lander to crash.

In the case of Mars Climate Orbiter, software error was a more certain cause. The computer controlling the directional thrusters on the spacecraft was intended to work in metric, calculating force in Newtons. Instead, organisational failures allowed some software code to be written in pounds force, an Imperial measure differing by a factor of 4.45. The result? The Orbiter descended too steeply into the Martian atmosphere, and was destroyed by atmospheric friction.

The two mission failures are now a decade old, but it seems clear from Toyota's well-publicised travails during late 2009 and early 2010 that their critical lessons had not been absorbed by the company, which is now the world's largest single car manufacturer.

Unintended acceleration

First, let's briefly review the facts. Since 2002, when Toyota introduced an electronic throttle control system, there have been a spate of what are termed 'unintended acceleration' incidents involving Toyota vehicles. Several investigations by the US National Highway Traffic Safety Administration duly followed, and there were a couple of small recalls.

But the problem, it seemed, was mostly ignored by the company, with Toyota - where it did acknowledge a problem - blaming improperly installed floor mats by customers, which then became stuck under the accelerator pedal.

Then, in August 2009, came the harrowing deaths of California Highway Patrol officer Mark Saylor and three members of his family. In a recorded emergency call, the cautious and experienced officer can be heard saying that the accelerator was stuck, and that the brakes weren't working. As he approached an intersection, his last words were: 'Hold on and pray'.

Finally prompted to acknowledge a problem, Toyota subsequently recalled 2.3 million vehicles, blaming an American supplier for faulty workmanship. But the supplier fought back, pointing out that they had only become a supplier in 2005 - three years after reports of unintended acceleration first surfaced. In all, one American firm of safety consultants has identified 2,262 instances of the problem, leading to 819 crashes and 26 deaths.

The world's media - previously fond of extolling Toyota's Just-in-Time productions systems and quality-conscious virtues - now rounded on the company, which quickly found its reputation in tatters. Public apologies soon followed from Toyota president Akio Toyoda, the grandson of the company's founder, as did still further recalls. Yet at the time of writing, no firm cause has conclusively been identified, and Toyota's reputation remains troubled.

Safety 'deafness'

So what could the company have done differently? Talk to some of those close to the issues raised, and it's clear that the outcome could have been very different.

For instance, it seems certain that Toyota could have sidestepped a lot of the flak by being more alert to the charges being levelled against it, and responding more quickly. Instead, in the memorable words of United States Transportation Secretary Ray LaHood, it was steadfastly 'safety deaf'.

Organisational issues seem in large part responsible. Each Toyota model, we now know, is assigned a shusa - or chief engineer - responsible for defining its intended market, creating it, bringing it to market, and hitting targets in terms of metrics such as cost, quality and performance.

Highly respected, and - according to Fortune magazine - granted near-absolute authority, Toyota's 38 shusas all reside at headquarters in Toyota City, where, admits one Toyota executive, they remain isolated from market information.

Yet Toyota could, for example, have instead taken a leaf out of Volvo's book. Earlier this year, the Swedish automaker revealed how it had invested in a 1.7 terabyte data warehouse, specifically to capture the sort of information that Toyota's shusas could have found invaluable: highly detailed warranty information, and diagnostics extracted from the on-board computers built into each Volvo vehicle.

The company already collected warranty data, explains Bertil Angtorp, senior business analyst at Volvo. It was when it began building a larger, separate data warehouse for the diagnostic readout information that it was realised the two datasets were complementary, and should be combined.

'There was clear business value to be gained from the ability to easily match warranty claims against diagnostic data from actual service records,' Angtorp says.

Accordingly, the company began the construction of a data warehouse designed to integrate data from four primary sources: a system for managing vehicle and hardware specifications, a system for managing onboard software specifications, the system that collects vehicle diagnostic data from service centres worldwide, and the warranty administration system.

Yet, as always, merely gathering data together adds little value without an ability to intelligently analyse that data, transforming it into insights and information.

'A car contains thousands of parts, both mechanical and electrical, and finding evidence of a model-wide issue rather than an isolated fault can be like finding a needle in a haystack,' says Niall O'Doherty, European director of business development at Teradata. 'We spent 12 months working with Volvo to develop the advanced analytical models required to detect worrying changes in reliability without either overwhelming the organisation with false alarms, or stating the obvious once it was too late.'

Nor should the computer horsepower required be underestimated, if the job is to be done properly. Compared to its previous - and much smaller - data warehouse, Teradata's 'massively parallel' processing architecture made short work of the complex analyses required.

A daily fleet mileage calculation that previously took two hours, for instance, now ran in five minutes. And a comprehensive report of diagnostic failure codes by model, by year of manufacture, now took 15 minutes - down from two weeks.

Better still, whereas performance constraints had previously restricted the number of people who could have access to the system, the new platform provided ready access to over 300 employees, spread across product design, manufacturing, quality assurance and warranty administration.

In other words, were repeated failures to occur, it's likely that product design and other engineering functions would see the critical data far more quickly than seems to have been the case at Toyota.

'Our decision-making has become more fact-based,' sums up Volvo's Angtorp. Now, whenever a questions arises, people invariably ask: 'What is the data telling us?' And once we've verified the existence of a problem, we use the data to determine the scope and scale of our response. It helps us to make sure that we're focusing on the things that are most likely to affect the customer experience.'

Social networking

Large databases aren't the only way of keeping close to what's going on in the marketplace. Through the use of online social media, it transpires that computer manufacturer Dell is also getting early warning of any problems.

'Dell is doing a great job - it's doing everything right,' enthuses Connie Bensen, the director of community strategy at brand market specialists Alterian. Simply put, she explains, Dell has a team of 36 people trawling the Internet, joining in on-line 'conversations' when issues with Dell equipment are raised, and offering solutions, discount coupons and suggestions.

As more and more people interact through media such as Twitter, Facebook, LinkedIn and other online virtual communities, the ability to respond quickly not only identifies problems more quickly, but is seen by consumers as very positive and proactive.

'Dell has been able to identify over $1bn in sales from this initiative,' explains Bensen. 'Plus, it's really got its finger on the pulse in terms of reliability.'

Consequently, she's in no doubt that a similar initiative by Toyota would have led to a different outcome. 'Quite simply, the company would have heard of the problems sooner, and would have been better positioned to respond,' she asserts.

Of course, response isn't the only course open to manufacturers. Prevention is better than cure. What could Toyota have done to identify and fix the cause of the unintended acceleration incidents - before the vehicles were being driven by consumers?

Whether or not software is implicated, the eventual analysis of what went wrong at Toyota, there are lessons to be learned from the IT industry, it seems.

Increasingly, points out Dr Bill Curtis, chief scientist at software quality specialist Cast Software, director of the Consortium of IT Software Quality and the creator of the well-known Capability Maturity Model (CMM) methodology, vehicles are complex systems that are akin to very large IT systems.

'You can have a hundred million lines of software code in a modern automobile, spread across a wide variety of sub-systems - brake servo, fuel injection, cruise control and so on - and it's difficult to understand all the interactions between them, and then write test scenarios for those interactions,' he points out.

Consequently, he adds, 'It can be difficult to think of all the possible conditions in which something can fail, and then deliberately stress it so that it operates in those conditions - and especially difficult to do that when all those components are built by different companies.' Nevertheless, if vehicles are to be safe, the industry needs to do just that, he says.

And if software error is implicated in the Toyota problem, a mandatory testing standard could help prevent such bugs in future, says Robert Dewar, professor of Computer Science at the Courant Institute of New York University, and co founder and CEO of avionics software firm AdaCore, which has developed code for the Boeing 787 'Dreamliner' and Airbus' latest 380 and 350 models.

Pointing to the existence of 'safety critical' standards for applications such as avionics (the DO-178B standard), railway systems (RIA-23) and industrial automation (IEC 61508), Dewar argues that there has never been a death on a commercial aircraft as a result of a software problem - despite modern aircraft containing many more lines of code than the latest generation of cars.

'We still don't know what went wrong at Toyota, although there's a significant suspicion that software has at least played a part,' he says. 'In other industries - such as avionics, for example - there's a mandatory requirement for a Federal Aviation Administration-certified software auditor to go through the software from a safety and quality perspective before it can be certified as fit for use.'

The answer? 'Software for cars should be subject to the same rigorous testing procedures as software in other industries,' he insists. 'Hardware for vehicles is subject to exacting tests - so why not software?'

In short, a reasonable conclusion. But will it happen? Don't hold your breath. In an industry that has yet to agree a standard barcode format, software standards may be a bridge too far.

Further information

- Adacore
- Avionics Systems Standardisation Committee and DO-178B standard
- CAST Software
- Mars Climate Orbiter
- Toyota's recalls and the electronification of the car
- Evolution of the Toyota Production System
- Toyota's ecologically friendly car plant

Comments

All comments