Maintaining a Safety Culture

Dr Stuart Reid

Introduction

According to the automotive safety standard, ISO 26262 [1], organizations that perform activities in the safety lifecycle must create, foster and sustain a safety culture. So, if you are working in the automotive industry on systems that have the potential to cause harm (and it is surprising how many systems can cause harm), then you should be immersed in this safety culture as part of your day-to-day working experience.

This article will consider examples of the safety culture in NASA and Toyota. It will show how even the most well-known and respected organizations can find it difficult to sustain a safety culture when other drivers, such as the desire to grow (in the case of Toyota) or the need to protect the space program (in the case of NASA), come into conflict with the underlying goal of safety.

The concept of a safety culture first originated from the investigation into the world's worst nuclear accident at Chernobyl in 1986 (see Figure 1). Safety culture is a part of an organization's culture, and is a combination of individual and group responsibilities to safety ("the way we ensure safety around here").

The safety culture within an organization is often revisited when a disaster occurs, to try and determine what went wrong – and how to improve the safety culture. In this article, we will look at three separate situations and consider how failures in the safety culture contributed to them. Finally, we will suggest some warning signs to look for that may be early indicators of a breakdown in the safety culture in your workplace.

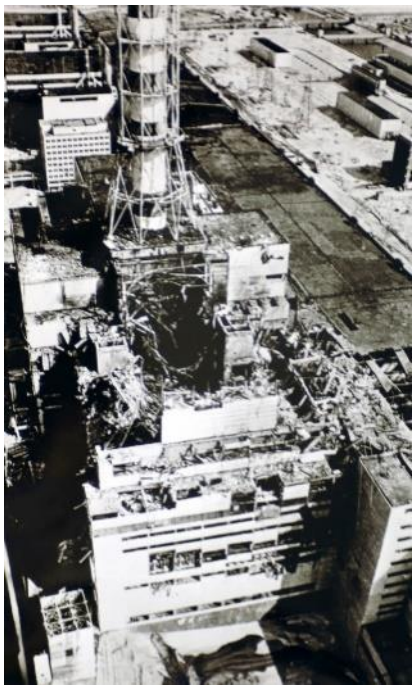

Figure 1: Chernobyl Disaster (Source: Soviet Authorities)

The Shuttle 'Space Transportation System' (STS)

The Space Shuttle program started in 1972, to develop a reusable manned space vehicle to replace the successful, but expensive, Apollo system, which was last used in the mid-1970s. The Space Shuttle system comprised a reusable orbiter (for carrying the crew), two reusable solid rocket boosters (SRBs) to provide extra thrust to get the orbiter into space, and an expendable large external tank (carrying liquid hydrogen and oxygen) that burnt up on each flight.

The first launch (of the Shuttle Columbia) was in April 1981, and with a total of 135 missions, the last shuttle (Atlantis) flew in July 2011. At the end of the 30-year Shuttle program, it had lasted 15 years longer than originally planned, and two missions had ended in failure, with the loss of their crews – a failure rate of 1.5%.

Shuttle Mission STS-51 – Jan 28th, 1986

STS-51 (see Figure 2) was Challenger's 10th mission, and it lasted only 73 seconds due to the failure of the O-rings on one of the SRBs. The accident was witnessed live by more than the usual number of TV viewers since one of the astronauts, Christa McAuliffe, would have been the first school teacher in space.

Figure 2: STS-51 Launch (Source: NASA)

The SRBs are basically long tubes made up of several joined cylinders, and once ignited they provide extra thrust to boost the Shuttle into space until they run out of fuel; they are then detached and fall back to Earth to be recovered and reused. The joints between the cylinders are sealed using O-rings and by the launch of STS-51 it had already been known for about 9 years that the O-rings were known to fail, but no disaster had occurred as on no occasion had both the primary and secondary O-rings failed on the same launch. Once the O-rings failed on STS-51, this allowed hot gases from the SRB to impact the external tank, which resulted in an explosion that engulfed the orbiter, SRBs and external tank. It appears that the astronauts were not all killed in the initial explosion as there is evidence that at least three of them had activated their personal emergency breathing kits (the break up would have been at about 20,000 metres), but the subsequent impact with the sea would have killed any surviving occupants of the orbiter (emergency escape from the orbiter was not possible).

Figure 3: Challenger after the explosion (Source: NASA)

The accident resulted in a 32 month break in Shuttle launches while the US government-backed Rogers Commission investigated the accident, made recommendations, and NASA acted on them.

The Rogers Commission considered the disaster and made several observations and recommendations. They concluded that the disaster was caused (from a physical perspective) by the failure at one of the joints of both the primary and secondary O-rings, which become brittle in low temperatures. STS-51 launched on a particularly cold morning, far colder than for any previous Shuttle launches.

From a safety culture perspective, they determined that the decision-making that led to the launch was seriously flawed. The night before the launch, engineers had expressed concerns about the O-rings and urged that the launch be delayed. However, there were no members of the NASA 'Safety Council' that makes such decisions at the meeting and there was also no mechanism for the concerns to be easily communicated to those who could have stopped the launch at a high enough level within NASA.

It later became clear that there was a fundamental difference in how NASA management viewed the dangers and the views of the engineers. When questioned, most engineers expressed their belief that the chance of a catastrophic failure of a launch was between 1 in 50 and 1 in 200. The NASA managers expressed their belief that the figure was 1 in 100,000 (Note that it has been pointed out that this extremely optimistic 1 in 100,000 figure would have been the figure used when persuading Christa McAuliffe to join the crew – it corresponds to NASA launching a Shuttle every day for 274 years and suffering only one accident).

A basic flaw in management thinking (and indicative of a poor safety culture) around the O-rings was the idea that because they had found damaged O-rings on several previous launches that had succeeded, then it was safe to continue, because 'nothing bad has happened yet'. This reliance on previous lucky circumstances led to an environment of management overconfidence, which allowed lower level managers to ignore the concerns of engineers and not properly communicate the engineers' (valid) concerns to the higher levels of NASA management, who had the power to delay the launch.

This overconfidence was not just based on the Shuttle launches, but on the previous success of the Apollo program, even though since Apollo, the personnel had significantly changed, and levels of funding had been severely reduced. The threat to funding also encouraged managers to try and maintain the planned launch schedule without any delays, as they believed the Shuttle program would be in danger of being shut down if the launch schedule was not followed (even if risks had been voiced).

In an attempt to restore the safety culture in the Shuttle program, the Rogers Commission recommended, among other things, that NASA create a new Office of Safety, Reliability and Quality Assurance, headed by a NASA Associate Administrator who should report directly to the NASA Administrator.

Shuttle Mission STS-107 – Feb 1st, 2003

STS-107 was Columbia's 28th mission (nearly 22 years after its maiden flight). It lasted 16 days, disintegrating as it re-entered the Earth's atmosphere. All 7 astronauts (see Figure 4) died immediately when the orbiter broke up after heat shield tiles failed to protect the left wing of the orbiter from superheated air at temperatures high enough to melt the aluminium metal struts.

Figure 4: STS-107 Astronauts (source: NASA)

The Columbia accident can be considered as a story about two different thermal protection systems. The orbiter re-enters the atmosphere at a speed of about 10,000 mph and the resulting friction between the orbiter and air molecules raises temperatures to over 1600 C. To protect the orbiter and its crew, thermal tiles are used – these tiles need to be reusable, lightweight and aerodynamic. Different variations of tiles are used in different places on the orbiter dependent on the expected temperatures and air pressures, but their required attributes mean that they are fragile and easily damaged.

The external tank is not reusable and is jettisoned after it is empty to fall back to Earth and break up over the ocean. The thermal protection on the external tank is spray-on foam and it is used to insulate the liquid oxygen and hydrogen in the tank as they both need to be kept at very low temperatures (the foam also provides some structural integrity). From the very first Shuttle launch there was a problem with bits of the foam from the external tank falling off during the demanding environment of the launch and hitting the orbiter (and SRBs). It was normal practice to replace damaged tiles after the orbiter returned to Earth.

On the launch of STS-107 a piece of foam fell from the external tank to the orbiter and hit the leading edge of the left wing at several hundred-mph causing damage about 20 cm in diameter. The problem was noticed by analysing a video of the launch on day 2 of the mission and engineers immediately requested that more information on any potential damage was investigated. However, it appears that the US Department of Defense orbital cameras were busy watching events in the Middle East and it was decided that the crew (who could have gone on an unscheduled spacewalk to look for damage) should

not be told of the potential problem. The lack of urgency in looking for any damage was partly due to the astronauts not having any equipment on board that would have allowed them to make repairs had they found damaged tiles, nor enough fuel for them to reach the International Space Station and await rescue. So, if they had found damage, there was no way to rescue them, anyway. The ethics of telling the crew about the potential damage, or not, is a separate issue, worthy of discussion elsewhere.

The damage to the wing meant that as Columbia re-entered the atmosphere, superheated air entered the wing through the broken tiles, melting struts and eventually (after about 30 seconds) causing the whole left wing to fail. Columbia then disintegrated as it tumbled at 10, 000 mph, killing the crew nearly instantaneously. Figure 5 shows the view from the ground as the orbiter broke up over Texas.

Figure 5: Columbia breaking up on re-entry (Source: AP)

As with the Challenger disaster 17 years earlier, a commission (Columbia Accident Investigation Board - CAIB) was created to investigate the causes of the accident and provide recommendations. The main finding of the CAIB was that NASA had failed to learn the lessons of the Challenger disaster and that the same "flawed decision-making process" that had resulted in the Challenger accident was similarly responsible for the loss of Columbia. Their view was that NASA's organizational culture had as much to do with this accident as the foam – and that this culture had to change.

Despite the recommendation of the earlier Rogers Commission, NASA had not set up a truly independent office for safety oversight. The CAIB recommended that NASA establish an Office of Safety and Mission Assurance, which would be completely independent of the Shuttle program, but would still have direct authority over the entire safety organization. This Office of Safety and Mission Assurance should be an independent Technical Engineering Authority responsible for both the development of technical standards and the granting of waivers to allow these standards to be ignored (when it was considered safe to do so).

For STS-107, the following was part of the current standards at the time of the launch: "…No debris shall emanate from the critical zone of the External Tank on the launch pad or during ascent…". As foam debris had been falling around the orbiter during launches since STS-01, this requirement appears to have been waived from the very start of the program. Managers decided to do nothing (in a similar way to the Challenger disaster) as they had seen the same problems in the past and 'nothing bad has happened yet'.

Toyota Unintended Acceleration

Toyota's problems with unintended acceleration in some of their cars appear to have started with customer complaints starting around 2002, although denial of there being a problem by Toyota meant that the effects of the problem are still being felt now by Toyota, especially in the US market.

In 2005, Toyota set up a ''Customer First' task force, chaired by their then President, however there is little evidence that they took the matter very seriously, choosing to believe that it was more a problem with drivers accidentally hitting the accelerator pedal rather than the brake. By 2009, the task force was shut down "as quality control was now part of Toyota's DNA", however by the end of 2009 there had been two recalls – one for floor mats (the accelerator pedal could get stuck under badly-fitting floor mats) and the other for 'sticky gas pedals' (some accelerator pedals made by a third-party supplier did not immediately return to the 'no gas' position). It was also suggested that if there were any problems with the accelerator, then it could easily be handled by using the brake to control the car's speed. Suggestions that the problem could have an electronic basis were dismissed by Toyota.

Lexus ES 350, San Diego – 28th August 2009

The accident that did the most to raise awareness of the unintended acceleration problem started with an emergency call from a car (see Figure 6) on a highway in California, which was then already travelling at over 160 km/h.

- "We're in a Lexus . . . and we're going north on 125 and our accelerator is stuck . . . there's no brakes . . . we're approaching the intersection . . . Hold on . . . hold on and pray . . . pray."

Figure 6: Lexus after possible Unintended Acceleration (Source: Gomez Law Firm)

The immediacy of being able to hear the last words of one of the passengers (all four occupants were killed in the resultant crash) and the fact that the driver was an off-duty highway patrol officer, who was also a vehicle inspector, suddenly raised the profile of the problem. It was now more difficult for Toyota to suggest that this was driver error – and it also appeared as if the brakes were not capable of providing sufficient control.

US Congressional Investigation – January/February 2010

By early 2010, the US Congress were involved, and in February of that year Akio Toyoda, the President of Toyota, testified in person to the committee. He said he became aware of the unintended acceleration problem towards the end of 2009, which is quite strange as he became an executive vice president and

a representative director, responsible for IT & ITS, quality, product management and purchasing, Japan and overseas sales and overseas operations, in June 2005, becoming overall president in June 2009. While Akio Toyoda stated that he now took personal responsibility for the problem, Toyota still seemed in denial that there was an actual problem, still suggesting that if the mats weren't to blame (many drivers had by now removed the mats), it was probably the drivers, consistently maintaining that the cars' electronic systems were not to blame for the problem. Despite this, in 2010 Toyota recalled more vehicles (8.1 million) than it sold (7.6 million).

An illuminating statement by Akio Toyoda at the hearing was that he believed Toyota had confused its priorities in a rush for growth, and that Toyota had to reassert the values that had been its hallmark.

Toyota Camry, Oklahoma – September 2007

More detailed information on the unintended acceleration problem came out of an October 2013 trial against Toyota regarding a crash in 2007 in which the driver was seriously injured and the passenger killed (see car in Figure 7). This was the first case where the software (rather than the mats or sticky pedal or panicking driver) was the focus of the trial. The result was that the jury awarded $3 million in damages to the driver and passenger's estate. The jury also decided that Toyota acted with "reckless disregard" for the rights of others. The part of trial that would have awarded punitive damages never took place as Toyota settled out of court.

Figure 7: Toyota Camry Crash - Sept 2007 (Source: money.cnn.com/2013/10/25/news/companies/toyota-crash-verdict)

Expert witnesses at the trial blamed the Electronic Throttle Control System (ETCS), citing a defective safety architecture and software defects. This was somewhat surprising as a previous investigation by NASA for the US National Highways Traffic Safety Administration had not found that the electronic systems were to blame, but the new investigation appeared to look at the system in more depth.

Fines and Settlements

In the decade to 2010, the US National Highways Traffic Safety Administration received more than 6,200 complaints on possible unintended acceleration problems with Toyota vehicles, and these included accidents that resulted in 89 deaths.

In 2012 Toyota denied responsibility in response to unintended acceleration claims for models in the years 2002-2010, but started settling unintended acceleration claims in the region of $1.6 Billion, and the brake firmware was updated on 9 models.

In 2014, after a four-year investigation by the US Attorney General, the following statement was made:

- "Toyota misled U.S. consumers by concealing and making deceptive statements about two safety-related issues affecting its vehicles, each of which caused a type of unintended acceleration."

Toyota were fined $1.2 billion for concealing safety defects, and part of the deal was to accept a continuing independent review of safety processes for the next 3 years.

Toyota's Safety Culture

Toyota are rightly famous for their Toyota Production System (TPS), a framework for manufacturing based on lean principles that aims to improve both productivity and quality. One of its major practices is Jidoka, encouraging a culture of stopping to fix problems, with the aim of getting quality right first time. However, in the late 1990s Toyota embarked on a new regime aimed at increasing production to new levels that required the building of new factories and taking on new suppliers. Up until then a core group of engineers had maintained the 'Toyota Way' and ensured that it was practiced throughout the organization. With rapid expansion, it appears as if the Toyota Way was not always fully implemented across the organization, and the price was a reduction in quality.

Figure 8: Akio Toyoda, Tokyo 2011 (Source: Bertel Schmitt)

Akio Toyoda (shown in Figure 8), giving evidence to the 2010 Congressional Hearing, stated that he believed that after 2003 a misguided strategic focus at Toyota warped the order of Toyota's traditional priorities and that quality was no longer Toyota's number one priority. Although refreshing in its honesty, this was a bit late – Toyota appeared to understand there was a problem long before 2010.

Early investigation of the unintended acceleration problem by Toyota engineers appears to have resulted in conflicting outcomes, suggesting that there were already problems with the application of the Toyota Way long before 2010. In 2005, a Toyota engineer claimed that:

- "In the Toyota system we have a failsafe, so a software abnormality would not be involved with any kind of unintended acceleration (UA) claim"

Whereas a 2007 Toyota email states:

- "In truth technology such as failsafe is not part of the Toyota engineering division's DNA"

In 2008, Toyota's Technical and Regulatory Affairs Vice President warned that "some of the quality issues we are experiencing… we now have a less defensible product that's not typical of the Toyota I know."

2010 saw the US government taking the matter seriously enough to hold a Congressional Hearing and start a four-year investigation. Toyota responded by creating a Special Committee for Global Quality and a Swift Market Analysis Response Team (SMART). By 2011, Toyota had changed its development processes and created a new quality group of 1,000 engineers.

In 2014, Toyota stopped denying that there was a problem with unintended acceleration and admitted to misleading consumers and the NHTSA about safety issues related to unintended acceleration in its cars. Alongside this, Toyota also said it had made fundamental changes in its corporate structure and internal safety controls.

Conclusions - Toyota Unintended Acceleration

Toyota started from a position of strength as far as safety is concerned, with the Toyota Production System and the Toyota Way. However, in the past 15 years, it appears as if they became complacent about the need to improve their quality systems as they expanded production, while also assuming that their systems were infallible, leading to them continuing to deny that there could be any major problems with their cars.

Their president, Akio Toyoda, has admitted that the rapid expansion of the company led to quality taking a back seat. The unintended acceleration problem has highlighted several safety failings, with denial of the problem being one of the most obvious (it is difficult to know how much Toyota really believed that the major problem was that drivers were accidentally pressing the wrong pedal when they wanted to stop). Since 2010, Toyota have made several steps towards addressing their problems, by changing their processes, appointing 1,000 quality engineers and making fundamental changes to their safety controls. In 2014, they even admitted to misleading consumers and the NHTSA about safety issues related to unintended acceleration in its cars – so, perhaps their years of denying there was ever a problem are over.

Their software development practices, many of which were made public in the 2013 trial, tell us something about Toyota's attitude to safety and software development practices in this period. It seems that reliance on old in-house Toyota standards took precedence over newer industry standards (e.g. the MISRA coding standards). Toyota also seemed to be using outdated software development practices (e.g. Toyota software engineers appeared to be ignorant of some parts of the V-lifecycle model, used no formal reviews, did not use formal configuration management and had no systematic defect management system).

How is your Safety Culture?

Overconfidence

In many organizations, good initial safety practices can be progressively eroded over time. Good practices are set-up and then engineers and managers forget why the practices were initially implemented. This statement is from a NASA official - one year before the Challenger Disaster:

- "The Shuttle has become a mature and reliable system … about as safe as today's technology will provide."

By 1985, many NASA managers believed they were working with an operational system, whereas it should really still have been considered as an experimental system, given the limited number of launches and the major changes that were made to the system on a frequent basis.

In 2009, Toyota disbanded a high-level task force set up in 2005 to deal with quality issues. A Toyota manager explained that management believed that quality control was part of the company's DNA and so they didn't need a special quality committee. Just one year later Toyota recalled 8.1 million vehicles and their President was called to give evidence before a US Congressional Hearing.

Toyota and NASA were very successful, but they were both being driven to meet ever more difficult targets with limited resources. In each case, they were confident in their abilities (based on their past results) but when they came under pressure they didn't take the time to question whether they were still able to guarantee the level of quality and safety they had before.

NASA especially suffered from the mentality of falsely believing you are safer than you are that comes from surviving a near miss (or several near misses). Near misses need to be reviewed to ensure that the previous near miss does not escalate into a disaster the next time.

If you start hearing the following statement by your colleagues, start worrying:

- "We always do it like that"
- "We are a 'can do' organization"
- "We got away with it last time - so why not this time?"
- "That standard is only there for show – we don't need to worry about it."
- "Our standards give us more room for innovation than the industry standards"

Safety Leadership starts at the Top

A safety culture needs to be endorsed and supported from the very top of organizations.

The following statement from Daniel Goldin, NASA Administrator from 1992 to 2001, is not an ideal example of leadership reinforcing a safety culture:

- "When I ask for the budget to be cut, I'm told it's going to impact safety on the Space Shuttle…I think that's a bunch of crap."

Many of the statements quoted from Akio Toyoda reflect well on his attitude to quality and safety in Toyota, although it could be argued that many of his statements were made with hindsight and in response to the investigations by the US regulators. His following statement does not seem to reflect the reality of the handling of the unintended acceleration problem:

- "It is in Toyota's DNA that mistakes made once will not be repeated."

Safety Engineers and Managers

Many organizations treat safety as a secondary issue – and this can sometimes lead to poor resourcing of the safety positions within the organization. Ask yourself the following questions:

- "Are your safety engineers fully qualified?"
- "Are all the safety positions (engineers and managers) filled?"
- "Are safety engineers the most or least experienced engineers in the organization?

Safety Communication

Both NASA and Toyota exhibited examples of poor communication. Several NASA engineers fundamentally disagreed with the decision to launch Challenger, given what they knew about the O-rings, but there appeared to be no mechanism for getting that message to the people in NASA who made the launch decision. In Toyota, different engineers had completely different views on failsafe as can be seen from these views from Toyota engineers:

- "In the Toyota system we have a failsafe, so a software abnormality would not be involved with any kind of unintended acceleration (UA) claim"
- "In truth technology such as failsafe is not part of the Toyota engineering division's DNA"

In a true safety culture, staff must be confident that they can state any concerns they have about safety without worrying about these statements affecting their careers. You should worry if the people who ask safety questions are:

- considered to not be 'team players'
- endangering their careers
- considered to be negative

Care needs to be taken that concerns about safety are not filtered and that they reach the right audience. Ensure that messages about safety are:

- not getting 'toned down' as they move from engineers to managers
- being shared with other groups in the organization
- not being restricted to a limited audience
- not being queried by management (for instance, are you required to provide proof of everything before a concern can be raised)

Production ahead of Safety

In a true safety culture, safety takes precedence over everything else. In both NASA and Toyota, we can see that meeting deadlines and increased production targets meant that, at times, safety took on a secondary role. For NASA engineers working on Shuttle launches at the time of the Columbia disaster,

they needed to make sufficient launches to meet targets for building the International Space Station. For Toyota, the focus on expansion and increased production meant that, as stated by Akio Toyoda, “priorities became confused in a quest for growth at the expense of safety concerns”.

It is when situations such as these start to occur that it is really important that there is an independent safety body within the organization that has the power to make itself heard and bring the organization back onto the course of a true safety culture.

References

[1] ISO, Road vehicles - Functional safety, ISO 26262 Parts 1-10, ISO, 2011.

