Online Ethics Center
FOR ENGINEERING AND SCIENCE

Cars That Won't Stop: Are Computers the Problem?

Author(s)

Stephen H. Unger

Year

2010

Description

This article by Stephen Unger examines the causes behind the Toyota vehicle recalls of 2009 and 2010. It also discusses the role of computers in controling vital components of automobiles and some useful lessons from the incident.

Abstract

Jamming your foot on the brakes and having your car speed up instead of slow down happens in nightmares--or in Toyotas. Fortunately, the probability of such a nightmare actually occurring is extremely low. But just how low is low enough, given that brakes are applied so often and that the consequences of such a failure can be catastrophic? Let's consider the causes of this problem, what can be done about them, and just how serious the whole matter is. What useful lessons can be learned?

Body

Causes

The first suspect in any auto accident is the driver [Stephan]. In the case of an SUA (sudden unintended acceleration) incident, the most obvious explanation is that the driver's foot was on the wrong pedal. This could be due to confusion caused by unfamiliarity with the auto (rented cars were disproportionately involved), emotional upset, general incompetence, or a combination of these effects. There may also be cases where SUA reports are fraudulent, motivated by the prospect of a lucrative law suit.

Toyota has conceded that some incidents resulted from floor mats jamming the accelerator pedal, and others from worn gas pedal mechanisms that increase friction under certain conditions, causing the pedal to stick [Borenstein]. Nothing new here. Automobiles have always been vulnerable to such problems.

Another possible cause of SUA is more interesting. In the not distant past, driver-activated controls such as brake pedals were mechanically linked to the brakes, engines, etc. by steel cables or rods. But many new cars employ "drive-by-wire" [Charrette1], where driver controls serve as inputs to computer-based electronic systems that also receive other inputs, e.g., from speed sensors, and then generate outputs that activate the brakes, control fuel flow, etc. There are reports that some SUA problems may have been caused by computer failures such as program bugs [Emison]. However, perhaps, because of the complexity of these systems and the rarity of problem incidence, specific bugs have not, to my knowledge, been identified, {and it seems unlikely that a program bug was a factor [Gold]}. The search for an explanation is not helped by the incredible fact that, despite the massive use of computers in automobiles, the National Highway Traffic Safety Administration (NHTSA), the federal agency tasked with monitoring the safety of autos sold in the US, does not have any computer engineers on its staff [Charette2].

How Worried Should We Be?

There are about 200 million American drivers (and even more cars). Over 40,000 Americans are killed annually in auto-related accidents. If frequency of accidents

were the sole concern, an average of fewer than 6 SUA-caused deaths per year would not warrant a big response [Bensinger]. Doubtless, the reason the Toyota problems have received so much attention is the spectacular nature of the accidents. A story about a car racing down a highway at 110 MPH with the driver desperately, but unsuccessfully, trying to slow down gets a lot more attention than a story about a pharmaceutical product that causes tens of thousands of people over a period of several years to die under dreary circumstances [Deer]. This is not to say that faults causing even a small number of accidents should not be remedied.

Looking Ahead

We may, however, be seeing a development that could lead to more numerous and serious problems if not properly monitored. Given the frequency with which our personal computer systems fail in small ways, and occasionally big time, it is not comforting to contemplate computers playing critical roles in the control of such dangerous devices as automobiles. While there is no hard evidence at present that computer errors were responsible for SUA accidents, it seems to me that the question is not *whether* this will occur in the not-distant future, but rather whether the harm done by such accidents will increase to a point where they will become a serious matter.

This will depend on the extent to which engineers are involved in the formulation of standards for computer use in automobiles, and the extent to which they are allowed to abide by them. All too often we see companies set high standards on paper, ignore them in standard operating practice, and even punish engineers who insist on adhering to them when violations would be profitable in the short-term [Unger]. It would be highly beneficial if regulatory agencies such as the NHTSA had, and actually used, the power to back up engineers trying to maintain high safety standards, and if engineering societies gave real support to ethical engineers. The former will never happen until voters demand it, and the latter will never happen until society members insist on it. It would be helpful in achieving this goal if consumer organizations and public interest groups joined with professional societies to support measures to back up conscientious engineers and to apply pressure to corporations to make safety a top priority.

A fundamental engineering ethics principle is that the public, health, safety and welfare be held paramount. This means that it is not acceptable to trade away safety for cost. It does not follow that unlimited cost should be incurred to reduce the likelihood of some hazard by an infinitesimal amount. There are generally discrete decisions to be made involving significant safety improvements for reasonable incremental cost.

A bad decision of this type was knowingly made by Ford management to omit a baffle proposed by its engineers, costing under $20, that would have prevented rear-end collisions from igniting gas tanks in the 1970 Ford Pinto [Dowie]. In real world engineering situations, such a sacrifice of safety in order to lower cost is easy to recognize as improper once the facts are revealed.

An example of a Toyota failure to maximize safety is the omission of a mechanism for automatically cutting fuel flow to the engine when the brake pedal is depressed. Such a feature, utilized by some other manufacturers, would, by itself, prevent most SUA incidents. But it is important that it be implemented by a simple mechanical interlock rather than by a computer routine, which might be disabled by a computer software or hardware failure

Common Sense and Computer Technology

Computer technology serves some very worthwhile functions in automobiles. Examples include air bag activation, controlling air and fuel flow to the engine, implementing anti-lock brakes, regenerative braking, and electric power assisted steering. When properly designed, these are very beneficial, reducing fuel consumption, reducing harmful emissions, improving driver control thereby reducing the likelihood of accidents, or, in the case of airbags reducing the harmful effects of accidents. But, the introduction of computers in the control of braking and steering, and engine control in particular, could result in accidents due to computer failures due to various causes.

Ongoing advances in integrated circuit technology can be exploited to reduce delays, power consumption, physical size, or some combination of these benefits. Microprocessors intended for use in automobiles should be robust and as simple as

possible, so as to minimize hardware design bugs or component failures. This is not the place to exploit advances in chip technology to maximize performance. Nor would it be appropriate to employ highly complex architectural features such as superscalar and dynamic pipelines, which enhance performance, but which often have design bugs and which may entail low probability risks of subtle timing failures. They should be programmed in the most straightforward manner, particularly for safety related routines. This is also *not* the place to cut costs, particularly by economizing on chip testing. The prime goal should be simple, fail-safe designs. Consideration might be given to setting up a cooperative body that would facilitate the exchange of information among competing manufacturers about methods for maximizing safety. Professional engineering societies, such as the ACM and the IEEE, could play an important role in establishing and operating such an organization.

Throw out the Computers?

The fact that computers in control of automobile brakes, steering, or engines could malfunction to cause serious, life threatening accidents could be used to argue that they shouldn't be used for such purposes. But we must also consider the *positive* value of computer use. Anti-lock brakes, for example, almost always function properly. It is reasonable to assume, even in the absence of hard data, that they prevent a great many accidents--far more than the very small number of accidents that can, at present, be attributed to their malfunctioning [Newman]. Carefully implemented computer technology can, on balance, promote safety. Similar considerations hold wherever computers are involved in critical processes, e.g., in hospital intensive-care units, or in the control of trains. Rather than reject computers in such cases, we need to set and adhere to very high standards for their use where failures could cause great harm.

A Disclaimer

This essay is mainly about computers controlling vital components of automobiles. It is *not* about the role of automobiles in our society, and it should not be inferred that I am in any way an automobile enthusiast. In my opinion, the widespread use of cars in the US, and in many other countries, as the principal means of transportation of

people is an ongoing disaster of the first magnitude. The annual death toll of 40,000 mentioned above and an order of magnitude more injuries (just in the US) is only the most obvious harm. To this, we must add major environmental damage, waste of energy and other resources, and wasteful use of good land.

References

1. Bensinger, Ken and Ralph Vartabedian, "Toyota faces new reports of sudden-acceleration deaths", Los Angeles Times, http://articles.latimes.com/2010/feb/15/business/la-fi-toyota-deaths16-2010feb16, February 15, 2010.
2. Borenstein, Seth and Ken Thomas, "Why are Toyota gas pedals sticking? It's complicated", The Japan Times, http://search.japantimes.co.jp/cgi-bin/nb20100130a2.html, Jan. 30, 2010.
3. Charette (1), Robert N., "This Car Runs on Code", Discovery News, http://news.discovery.com/tech/toyota-recall-software-code.html, Feb 5, 2010.
4. Charette (2), Robert, "US National Highway Traffic Safety Administration Has No EEs or SW Engineers Working For It ", IEEE Spectrum blog, http://spectrum.ieee.org/riskfactor/computing/it/us-national-highway-traffic-safety-administration-has-no-ees-or-sw-engineers-working-for-it?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+IeeeSpectrum+ , February 23, 2010.
5. Deer, Brian, "Vioxx death toll may hit 2,000 in UK", The Sunday Times, http://www.timesonline.co.uk/tol/news/uk/article557471.ece, August 21, 2005.
6. Dowie, Mark, "Pinto Madness", Mother Jones, http://motherjones.com/politics/1977/09/pinto-madness, September/October 1977.
7. Emison, Brett A., "Opinion: Toyota's Acceleration Problem and Carwashes", Modern Car Care, http://www.moderncarcare.com/articles/toyota-acceleration-problem-and-carwashes.html, March 5, 2010.
8. Gold, Aaron, "NHTSA report: Most Toyota 'unintended acceleration' cases due to driver error", Aaron's Cars Blog, http://cars.about.com/b/2010/08/11/nhtsa-report-most-toyota-unintended-acceleration-cases-due-to-driver-error.htm, August 11, 2010.
9. Newman, Rick, "What Toyota Probes Are Likely to Find", Seeking Alpha, http://seekingalpha.com/article/196755-what-toyota-probes-are-likely-to-find,

April 2, 2010.
10. Stephan, Karl, "Toyota Revisited: Unintended Acceleration of Judgment?", Engineering Ethics Blog, http://engineeringethicsblog.blogspot.com/2010/04/toyota-revisited-unintended.html, April 12, 2010.
11. Unger, Stephen H., "Man Rescues Coast Guard", Ends and Means blog, http://www1.cs.columbia.edu/~unger/articles/deKort.html, July 8, 2007.

Notes

Author: Stephen H. Unger, Professor Emeritus, Computer Science and Electrical Engineering, Columbia University.

(Modified version of the blog article accessible from http://www1.cs.columbia.edu/~unger/myBlog/endsandmeansblog.html).

Rights

Resource Type

Published Work