Welcome from the Chapter Officers

Serving for 2010:

- Chair: **Shirley Cui Tarantino**
  shirley.tarantino@intertek.com
- Vice-Chair: **Ken Kapur**
  ken.kapur@kla-tencor.com
- Treasurer: **Gary Eldridge**
  geldridge@apple.com
- Secretary: **Roberto Pasos**
  rpasos@elliottlabs.com
- Immediate Past Chair: **Steve Baldwin**
  steve.baldwin@lamrc.com
Sign In & Introductions

Cell phones?

Please sign in

- Please print clearly!
- Add your colleagues to our mailing list!
  - If you think they would benefit (they can always cancel)

Self-Introductions

- Name
- Interest or Affiliation
The PSES Website

Start at:  IEEE dot ORG

Click on “Societies” Tab
Click on “…Product Safety Engineering Society”
Click on “Chapters”, then Santa Clara Valley

Why?

- Copies of Speaker Presentations
- Announcements of Future Meetings / Speakers
Other Chapter Business

Employment Opportunities

- Offering / known openings?
www.belkin.com/careers

- Looking?
www.LinkedIn.com

Other business?
Tonight’s Presentation:

How to Avoid Being the Next Toyota

Ken Kapur (KLA-Tencor)
Mike Silverman (Ops A la Carte LLC)
Eugene Heil (Lewis Bass Intl.)
Mark Montrose (Montrose Compliance Services)
How To Avoid Being the Next Toyota

KEN KAPUR
Audi case set the template for Toyota’s acceleration Troubles  (Mar. 12, 2010)

Cars That Speed Up Mysteriously Spark Bitter Dispute Over Cause (Sep. 3, 1986)

Toyota Complaints Surged After First Recall  (Mar 11, 2010)

CBS Show 60 Minutes made sudden acceleration a household phrase in Nov 1986
Took Audi 15 years to rebuild US sales
<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan Auto Makers Plan Vehicle Recalls</td>
<td>Feb. 26, 2010</td>
</tr>
<tr>
<td>“Toyota Way”, Retain Believers</td>
<td>Feb. 26, 2010</td>
</tr>
<tr>
<td>Congress Targets Safety Rules As Recall Fallout Continues</td>
<td>Feb. 26, 2010</td>
</tr>
<tr>
<td>Subpoenas Hit Toyota On The Eve Of Hearing</td>
<td>Feb. 27, 2010</td>
</tr>
<tr>
<td>Toyota Slams ABC Report On Pedals</td>
<td>Mar. 9, 2010</td>
</tr>
<tr>
<td>Factory Town Stands By Car Maker</td>
<td>Feb 26, 2010</td>
</tr>
</tbody>
</table>
Support Wavers At Auto Maker For Its Embattled President (Feb 23, 2010)

More Clout For Safety Regulators? (Mar. 12, 2010)

U.S. May Push For New Brake Override System (March 3, 2010)
All new US Vehicles should be equipped with technology designed to stop a car when both gas pedal and brakes are activated

Toyota Rouses Japan’s Firms (Mar. 5, 2010)
“This is not just a Toyota issue but a corporate Japan issue”
(Shin Tanaka – President Fleishman Hillard Japan)
New Questions For Toyota  (Feb. 27, 2010)

Car maker mounts china sales push  (Mar. 5, 2010)

Hard Times Engulf Toyota City  (Mar 7, 2010)
“As Tiger Woods has shown us that being on top is a very hard job”
Fumihuki Yumemure

Toyota Rebuts Study  
(Mar. 5, 2010)

Prius Retains Top Spot As Top Seller In Japan  (Mar. 5, 2010)

Toyota Faces $ 16.4 million US fine  (April 6, 2010)
• 2004 – GM $1M Fine for defective windshield wipers in 600,000 vehicles
Toyota Sat On Defects, Feds Say (April 6, 2010)

• “We Now Have Proof That Toyota Failed To Live Up To Its Legal Obligations” - Trans. Secretary Ray LaHood

Toyota’s Tactic In Suits: Evade (Apr 12, 2010)

US Weighs Stricter Car Safety Rules (Mar. 12, 2010)

Toyota Criticizes report by ABC on Acceleration (Mar. 12, 2010)

Are The chickens coming Home To Roost For Lead-Free (Mar. 2010)
Vehicle throttles used to be **directly** controlled with mechanics.

- Metal rod linked directly to driver’s gas pedal
- Spring
But now control is *indirect* via electronics.
Toyota Adds Brake Override System To All Models After Recall  (Jan 12, 2010)

Topics of Concern based on areas of expertise
- Safety
- Reliability
- System Safety
- EMI

Potential Areas that need to be addressed:
- EMI Interference
- Lead-free Electronics
- Software Bugs
- Event Data Recorders?
Toyota Gas Pedal Recall

By

Mike Silverman
IEEE Reliability Chapter Chair and Managing Partner, Ops A La Carte
Introduction

➢ Toyota has been in the news for the gas pedal issue for a number of months.
➢ This month, the Quality Progress magazine had a number of articles about this issue, discussing it to be a Quality Problem.
➢ Tonight the intent is not to figure out what Toyota needs to do differently but rather to see how other companies can avoid falling into the same trap.
Background/History of Issue

Gas Pedal Model CTS
The pedal is designed to have a certain amount of friction or hysteresis built in. This is done so that the fatigue of pressing the pedal continually is not onerous or becomes fatiguing. It also replicates the friction that would normally be present in a conventional throttle cable as it passes through its housing. A throttle assembly without the correct amount of friction or hysteresis would be very difficult to control smoothly.
The affected part is in the lower center of the photo above (A), and in more detail in the one below. It is integral to the part that retains the return spring. The friction area is seen as the small “teeth” or “ears” protruding to the left at the very bottom of the picture. These two teeth ride in the two grooves of the pedal assembly (B), and are held against each other when the spring assembly is locked into position.
The area of friction is seen as the grayish worn area on the teeth just beyond of the (crude) arrow.
There is a certain amount of free play of the spring retainer/friction block unit. Toyota’s graphic shows that unit tilting slightly, perhaps due to too much free play or wear of the plastic components. The steel reinforcement bar (red unit below) is apparently intended to stabilize the angle of the spring retainer/friction block unit, to ensure that the degree of friction is either more consistent or is compensated for the wear that has occurred.
A Few Facts

• 8 Million cars in Recall
• Toyota took no action for months
  – Evidence in factory and field and it was ignored or explained away
• There is evidence that C/A not 100% effective

As a result
• Sales drop 9% in Feb compared to increases by other auto manufacturers.
More recalls – this is not isolated to Toyota

- GM – 1.3M for power steering
- Nissan – 500K for fuel gauge and brake pin
- Ford – 18K for brake s/w
- Honda – 400K for brake issue
Follow-On Actions by Toyota

• President Toyoda blames on quality control lapses in face of rapid growth and long term action is to hire more quality people (including CQO).

  –Is this the right answer. Maybe a good start, but not the only action
What’s Missing?

• Design for Excellence (DfX)
  – DfX addresses all aspect of design including
    • Design for Reliability (DfR)
    • Design for Environment (DfE)
    • Design for Manufacturability (DfM)
    • Design for Testability (DfT)
    • Design for Components (DfC)
    • Design for Safety (DfS)
    • Design for Quality (DfQ)
    • Software Design for Software (SDfR)
    and the list could go on
DfX Process

• Start with a goal statement
• Assess your organization and your vendors to determine if you are capable of meeting this goal.
• Develop a plan to show how you intend to meet this goal
• Execute the plan
Basic safety

- **Common knowledge**
  - Look both ways before you cross the street
  - Trust a man in uniform
  - Don’t touch a hot stove or a live wire
  - Avoid unexpected start-up (LOTO)
  - Documentation (spare parts, maintenance, etc.)
  - Safety devices (test button on smoke detector and GFCI)
  - Housekeeping (turn on, adjustment, electric cords, etc.)
  - Medical effects and first aid

- **Science library**

- **Law**
Basic safety

- Common knowledge

Science library
  - Trade organizations
  - Code books define the “model”
  - Magazines
  - Seminars
  - Text books

- Law
Trade organizations

- A huge number of competing code writing organizations
  - National Fire Protection Association (NFPA)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - National Electrical Manufacturers Association (NEMA)
  - Semiconductor Equipment and Materials International (SEMI)
  - International Code Counsel (ICC)
  - International Association of Plumbing and Mechanical Officials (IAPMO)
  - Underwriters Laboratory (UL)
  - Association of Manufacturing Technology (AMT)
  - American Council for Electrical Safety (ACES)
What is a safe “machine”? 

A machine is presumed to be safe if the machine is:

1. Build according to a “model” code, and
2. Certified by a competent “third party”

California Code of Regulations (CCR) title 8, section 3206 specifically states:

“When the term “approved” is used in these orders, it shall refer to products, devices, systems, or installations that have been approved, listed, labeled, or certified as conforming to applicable governmental or other nationally recognized standards, or applicable scientific principles. The approval, listing, labeling, or certification of conformity, shall be based upon an evaluation performed by a person, firm, or entity with appropriate registered engineering competence or by a person, firm, or entity, independent of the manufacturer or supplier of the product, with demonstrated competence in the field of such evaluation.”
Basic safety

- Common knowledge
- Science library
- Law
  - Fed OSHA and Cal OSHA (protect workers)
  - Building department (includes machinery)
  - Fire department (includes hazmat)
  - Product liability (tort) case law
  - How does this product compare to others?
Reliability and safety hierarchy

- **Prevention** – training, design, process capability
- **Appraisal** – testing, customer feedback
- **Scrap and rework** – fix it in the factory
- **Warranty** – fix it in the field
- **Insurance** – protect your investment
- **Law suit** – compensate for negligent defects
Product liability definitions

- **Dangerous** is the result of scientific method (example: automobiles, knives, ladders, vaccines)
- **Defective** is a legal conclusion
- **Foreseeability** is about anticipated danger, risk, usage ("woulda" – "coulda" – "shoulda")
- **Negligence** is about irresponsible conduct (example: failure to anticipate, design, test, or warn)
- **Tort** is compensation to make someone “whole” again
- **Warranty** is a financial reserve for anticipated returns
Three tests for a defective product

- **Imputation of knowledge**
  Do you know your customer usage, competition, state of the art?
  Example: would you sell a cup of scalding hot coffee?

- **Risk utility test**
  Does the customer utility significantly outweigh the risk?
  Hazard analysis: probability, severity, detection, avoidance, plus lack of a substitute, and a high enough price to absorb loss.
  Example: would you sell a rabies vaccine knowing that it kills 1% ?

- **Consumer expectation test**
  Did the product behave as a reasonable customer would expect?
  Example: a plywood sanding machine that ejects thin sheets.
Principles of high reliability

1. **Train the engineers** in the discipline of quality, reliability, and safety.
2. **Carefully specify** the entire system and all of the interacting components.
3. **Determine the weakness** of the system and its components.
4. **Exacerbate the weakness** through accelerated stress testing using factors such as temperature, humidity, altitude, start/stop, vibration, clock timing, etc.
5. **Design (and redesign) reliability** into a system by using robust parts, fault tolerance, cooling, maintenance, etc.
6. **Minimize the number of suppliers** and treat them like family so problems are not covered up.
7. **Instrument every system** with a “crash log” for forensic analysis.
8. **Operate a large rotating population** of systems to predict what will happen in the field.
9. **Promote excellent customer relationships** so that the rare critical failures can be preserved for investigation.
10. **Treat customer complaints as epiphany.**
Lewis Bass International, headquartered in the Silicon Valley, is a small group of affiliated experts in business over 30 years.

We help companies produce machinery that can meet complicated safety regulations of both the US and the European marketplace.

We have expertise in mitigating machinery hazards including: electric shock, energy, mechanical, fire, toxic, and corrosive. Benefit to the manufacturer is: 1) much faster installation and permit approval, 2) a more common, lower cost design that works in all the various markets, 3) reduced risk of accidents and negligence, and 4) consultations under the cover of attorney client privilege.
Eugene Heil

Eugene is the principal engineer at Lewis Bass International for electrical field labeling of industrial machinery, CE Mark, SEMI S2, robotic work cells, and hazard analysis.

Prior to Lewis Bass, Eugene worked 25 years managing the development, quality, and reliability of computer mass storage products for Hewlett-Packard, Unisys/Convergent, Shugart, and a couple start-ups.

B.S. in Electrical Engineering and an M.S. in Engineering Management.

California licensed as a Professional Electrical Engineer, Electrical and General Contractor, and Real Estate Broker.

Member of the ASSE, IAEI, and IEEE.

408-726-1863 cell
Product liability references

- “Managing for Products Liability Avoidance”, by Lewis Bass (editor) et al., 2004, CCH, ~320 pages
- “Is there anything optional about safety” by Kenneth Ross, IN Compliance magazine, 2010 annual guide, 3 pages. www.productliabilityprevention.com
Sudden Acceleration - it’s the Electronics!

TOYOTA TRUTH MEDIA BRIEFING

Dr Antony Anderson CEng FIET MIEEE  (Electrical failure expert)
antony.anderson@onyxnet.co.uk  www.antony-anderson.com

Dr Brian Kirk CEng, MBCS  (Safety software expert)
system.software.safety@gmail.com  www.robinsons.co.uk

EurIng Keith Armstrong  CEng FIET SMIEEE ACGI  (Electronics and EMI expert)
keith.armstrong@cherryclough.com  www.cherryclough.com

National Press Centre  |  Washington DC  |  March 23  |  2010
Why is sudden acceleration unresolved?

- Automakers *claim* absence of a detectable fault *proves* absence of design defect.
- But, had Newton looked for gravity inside the apple that inspired him — *he’d still be looking!*
- Like gravity, we should deduce electronic failures from their effects on vehicle performance:
  - *eliminating mechanical and human failures leaves only electronics as the cause*
- 30 years empirical evidence *overwhelmingly* points to SA being caused by electronic system faults *undetectable by inspection or testing*
Vehicle throttles used to be *directly* controlled with mechanics.
But now control is *indirect* via electronics.
Electronics have weaknesses and can go wrong in many ways

- mostly it recovers, leaving no trace
- e.g. when you reboot your computer

- Many electronic throttles are not safe enough
  - it is easier to blame drivers, floormats, sticky pedals
  - *whatever diverts attention away from the electronics*
We will now examine Automakers’ *claims* about electronics

- **De-mystify them**
  - and *show why they are wrong*!

- We will compare their *claims*...
  - with good safety engineering principles...
  - well-established in *all* other safety-aware industries
  - since *before 2000*
We back up our arguments…

- with public standards, peer-reviewed papers, textbooks, and other world-class experts...

- Electronics in automobiles behaves just like electronics *in all other industries*
  - *fundamental principles apply in all cases*
  - *the auto industry has no pixie dust!*
• Automakers *claim* that because they can find no defect after a sudden acceleration (SA) incident...
  • the SA could not have been caused by a design fault
    • so it must have been the driver!

• **BUT IN FACT:**
  • this argument uses false logic
  • and most electronic faults don’t leave any evidence
    • especially after the ignition has been switched off (i.e rebooted)!
Automakers **claim** that with their so-called “redundant systems”, no dangerous malfunctions can occur.

**BUT IN FACT:**

- the systems are only partially redundant, because they use identical technologies...
  - so have no protection **when** they fail the same way at the same time.

The so-called “dual-redundant sensor” in Toyota gas pedal.
Automakers claim they do comprehensive EMI testing

**BUT IN FACT:**

- their tests don’t cover most real-life EMI (EMI means electrical disturbances in the circuits)
- they don’t simulate typical faults, to verify their back-up or fail-safe measures work
- and no practical amount of testing can ever be sufficient anyway...
  - given the huge number of possible test combinations required
Automakers *claim* their electronics are “totally shielded against EMI”

**BUT IN FACT:**

- this is not achievable
- they use *unshielded* wires to carry electronic signals
- some manufacturers (e.g. Toyota) use *unshielded* plastic connectors for their engine control modules
- Toyota gas pedal and throttle sensors use *only partially shielded* plastic housings (leaky umbrella!)
Automakers *claim* their software is “bug-free”

**BUT IN FACT:**

Carnegie Mellon University says the highest-quality code (e.g. Space Shuttle) has about 1 *latent* bug per ten thousand lines of code

- a typical modern car has 20+ *million lines*, of lower quality code than the Space Shuttle
- so we should expect at least two *thousand* latent bugs in every car !!!
- many auto recalls today are for software reprogramming
• **AND IN FACT:**

  • Aviation and rail vehicle software must comply with tough public, regulated safety standards
    • *and be* independently audited for compliance

  • Cars *have at least as much* software
    • and expose many more people to risks of injury and death...
    • yet automakers’ software is unregulated
Automakers *claim* these prove their electronics are working correctly throughout a SA

**BUT IN FACT:**

- fault codes and black box recorders in cars rely on the very electronics *they are monitoring*
- therefore *cannot* be relied upon
- a “no fault” record after an SA can also be caused by the fault not being detected in the first place
- due to inadequate software system specification
Intermittent Faults (come and go apparently at random)

- Automakers don’t mention these at all

**BUT IN FACT:**
- intermittents have plagued electrics and electronics for as long as they have been used in cars
- and could easily be a cause of sudden acceleration undetectable afterwards
- particularly if the investigator has a “mechanical mindset”
Many automakers now use lead-free soldering

Unfortunately, long thin “tin whiskers” may grow on printed circuit boards when lead-free solder is used

– these can cause intermittent short-circuits

– and because they are so thin (about ¼ the thickness of a human hair) they are difficult to see, and easily brushed off, or moved by a draught of air

– so an investigator may not discover them, unless he/she was aware and took appropriate
Why Can No-one Prove SA by Testing?

- NHTSA has had up to 3,000 SA complaints in one year (1989-90)

- Assuming 30 million vehicles on the road, that’s a rate of 1 in 10,000 per vehicle per year
  - assuming an average drive of 1 hr/day, 6 days/week, gives us one SA per 3,120,000 hours of driving

- To detect one SA in just one model would require testing 36 vehicles, 24/7, for 10 years !!!!
  - or driving a single vehicle about 200 million miles
What about Toyota’s so-called “brake over-ride” Solution for SA

• It is merely a software change that relies upon the same electronics *that already causes the SA!*

• So it does not address the real problem

• A true safety over-ride must be a *totally independent system*
  
  • *e.g. to protect against elevator safety failure, there is an independently-wired emergency-stop button*
If we don’t control auto electronics, the future is scary.

- Worsening electromagnetic environment
- Rapidly increasing use of electronics in safety-related applications
- More complex circuits, systems, systems-of-systems
- Increasing susceptibility of electronic devices

But there are NO Regulations or standards that adequately control electronic system-safety issues.

- Manufacturers under increasing pressure to reduce costs and timescales
- Manufacturers comply with the minimum set of safety standards required by law

Rapidly increasing safety risks for users and third parties

Rapidly increasing financial risks for manufacturers
Vehicles with radar and infrared obstacle-avoidance systems, wirelessly networked to improve safety.
How to Make Electronics Safe Enough

• There are well-established design techniques used to achieve safety in other industries
  – automakers could also use them, at a reasonable cost

▪ Congress should mandate that NHTSA require automakers to comply with standards for the safe design of the drive-train electronic systems
  • in consultation with the IEEE, etc., following the best practices already used in aviation and other transport industries
Automakers claim absence of a detectable fault proves absence of design defect.

- **Not true!**

Remember Newton’s apple?

30 years of empirical evidence *overwhelmingly* points to SA being caused by electronic system faults that are undetectable by inspection or testing.

Like Newton and gravity, we should deduce electronic failures from actual vehicle performance.
For the key Toyota models exhibiting SA, NHTSA must obtain:

- for all drivetrain electronic systems and components
  - their safety specifications
  - software source codes, hardware design schematics
  - material, production and quality specifications
  - test specifications and results
- then co-ordinate expert teams working in parallel, to:
  - systematically classify the fault potential mechanisms and their context of occurrence
  - evaluate the data and use it to monitor and improve safety across the industry
Sudden Acceleration - it’s the Electronics!

Thank you for your interest

Dr Antony Anderson – Electrical failure expert

Dr Brian Kirk – Safety software expert

EurIng Keith Armstrong – Electronics and EMI expert

National Press Centre | Washington DC | March 23 | 2010