Proceedings of the ASME 2011 International Mechanical Engineering Congress & Exposition
IMECE2011
November 11-17, 2011, Denver, Colorado, USA

IMECE2011-62037

UNDERSTANDING WHY CODES AND STANDARDS FAIL

Stephen A. Batzer, Ph.D., P.E.
Batzer Engineering, Inc.
P.O. Box 1276
Prairie Grove, AR 72753

John S. Morse, Ph.D., P.E.
John S. Morse, P.E.
P.O. Box 370
Westville, OK 74965

Dong Y. (Don) Lee
The Engineering Institute
P.O. Box 610
Farmington, AR 72730

ABSTRACT

The enduring issues regarding codes and standards for consumer products and corporate behavior are discussed in this paper. It has been frequently asserted that the adherence of a product to a recognized government or private standard ensures that the product has a minimal level of safety, and that said product is therefore presumably non-defective. The agencies which promulgate these codes and standards are ostensibly impartial and informed, and have the public's best interests in mind. This conviction is undoubtedly true in some instances, but is also unquestionably false in others. The issues regarding codes and standards and their impact upon products and the trusting public include, but are not limited to, asymmetric information, cost concerns, ethics, foreseeable misuses, non-alignment of interests, and technological advancements after the standards were adopted. In short, the adherence to the letter, rather than the spirit, of individual codes and standards is a manifestation of the Principal-Agent conflict, in which the agent, acting on behalf of the principal, has a different set of incentives than does the principal. This conflict and the underlying issues listed above are discussed. Case studies of numerous products with possible, known, and unforeseen adverse impacts upon public health and safety will be used as illustrations of products that were within the letter of the code or standard, but manifestly defective.

INTRODUCTION

By what measure does one determine if a product is defective or non-defective? It has been postulated by many, including Ralph Barnett, co-founder of Triodyne Inc., that the line between defective and non-defective is established by whether a product meets the applicable standards [1]. However, even the determination of whether a standard is "applicable" or not can be problematic. Barnett also co-authored a paper in 2002 that condemned the ASME pool drain cover standard, calling it "a license to kill" [2].

The thesis of this manuscript is that while adherence to relevant "standards", be they voluntary standards, codes, laws and/or governmental regulations, often makes products better and safer than they *might* be, it does not necessarily ensure that individual products are reasonably safe. There are many reasons for this, including standards-making processes that lag technological development, lack of sufficient real world testing, ignoring commonplace and reasonably foreseeable misuse, disregarding combinations of failure modes, coziness between a regulating government agency and industry, and failure to consider manufacturing defects. This listing is by no means exhaustive.

If one looks at the broad spectrum of consumer products, the state of standards and regulations varies widely. Prescription drugs require approval by a government agency, the U.S. Food and Drug Administration (FDA). Automobiles have to meet an array of federal standards called the Federal Motor Vehicle Safety Standards (FMVSSs). Housing and building construction is subject to local codes. There are regulations covering passenger-carrying ships. There are voluntary standards for all sorts of things, from ladders to shopping carts to the pay scales for coffee bean growers.

One of the purposes of this paper is to demonstrate that adherence to voluntary and/or involuntary standards does not universally lead to reasonably safe products, even if they are affixed with colorful seals of approval trumpeting said conformance. There are essentially unlimited examples of defective products which met their applicable standard, rule, regulation or were approved by a federal agency, but were either recalled, or perhaps worse, recognized to be unsafe and not recalled, while the issue was subjected to "further study." This paper chronicles an abbreviated sample of these products. These examples show an undeniable fact; meeting a recommendation, standard, rule, or federal regulation does not guarantee a reasonably safe product.

THE PRINCIPAL-AGENT CONFLICT

The most fundamental purpose of corporations isn't to produce products, but rather to produce profits for the owners. This is hard reality. Unprofitable businesses eventually are

sold or closed as the owners tire of losing money. There is a daily pressure placed upon managers to realize a profit, both through increasing revenues and diminishing costs.

In his autobiography, former General Electric CEO Jack Welch repeatedly emphasized that profitability was a moral imperative for every company, for if a company did not make a profit, it would not provide products, nor employment, nor a return on investment [3]. A healthy emphasis on profit is necessary. However, another fundamental ethic is the first rule of the practice of medicine, which is to, "*Do No Harm.*" This can occur when an unhealthy emphasis on profit is made. Greed is one of the seven deadly sins, a common, though not universal, human frailty.

When greed leads to lower costs and better quality for the customers, thereby enhancing revenues, then some view it as a good thing. When greed leads to management instructing the engineers to cut corners and produce products which do not meet reasonable customer expectations, particularly with respect to such qualities as safety, the environment, and long term durability, then this excessive emphasis on making money is commonly viewed as a bad thing.

It is unrealistic to expect the average consumer to produce a roadworthy automobile, healthy unit of insulin, functioning plasma-screen TV, or other product of this nature. The consumer will pay for someone else to design and build these things, as well as test, license, and service them. Because the managers of the companies making these goods work directly for the owners who have a profit expectation, but are working on behalf of consumers with another set of expectations, these companies are subject to the principal-agent conflict.

The true principal in this case is the consumer, who is the end user of the product. Products without a market are not manufactured in the long term. This principal suffers the direct harm when things go wrong. The agent of the consumer is the manufacturer or regulator. The problem is that two sets of interests are not perfectly aligned. Who do the agents (managers) act in the true best interest of? The consumers (principals)? Management? Themselves? Results vary.

F. Ross Johnson, former CEO of RJR Nabisco, had his pet German shepherd, Rocco, flown in a private company jet [4]. It was not reported whether he also provided an air conditioned dog house for Rocco, as did Jim and Tammy Faye Bakker, courtesy of the donations from their televangelism empire [5]. Examples of this type of poor judgment and betrayal of trust are not difficult to find. In no way can these activities be considered within the best interests of the shareholders or the tithing members of the flock.

If a manager manufacturers his goods to the minimum required to meet the letter of the law, that can free up money for additional profits. For decades, the U.S. has seen a large influx of cheap goods manufactured in low cost countries which are modeled after premium goods from first-world countries. They might not quite have the fit, finish, performance, and durability of the goods for which they serve as Doppelgängers, but when new, they are attractive in their own low cost way. Costs that would have been devoted to design, analysis, testing, and high quality raw materials can be redirected towards the bottom line and advertising.

This brings about the reasonable question in this conflict. *Whose interest is paramount*? Again, opinions vary. Fortunately, there is a coherent statement of this available to engineers. The NSPE Code of Ethics [6] clearly states as the first Fundamental Canon**, "**Engineers, in the fulfillment of their professional duties, shall hold paramount the safety, health, and welfare of the public." This is a clear light unto the path of the engineers who are responsible for the design and manufacture of products destined for a trusting public.

CASE STUDY 1 – THE TITANIC

One of the most famous tragedies of the 20th century is the sinking of the Titanic on April 15, 1912, during its maiden voyage. Hundreds lost their lives needlessly due to a lack of lifeboats, and stunningly, because the lifeboats were not used to capacity. It is a one-ship seminar on appalling judgment.

Shortly after the sinking, official inquiries were conducted both in the United States and in Britain. The British board of inquiry was held in June and July of 1912, headed by Lord Mersey. His report revealed that the Titanic carried 20 lifeboats that could hold a total of 1,178, or just under 54 percent of the combined crew and passengers, but actually exceeded government requirements [7].

The British inquiry found that 711 passengers and crew were saved out of a total of 2,201 (32 percent) [8]. A disproportionate number of women (74 percent) and children (52 percent) were saved, due to the proverbial "women and children first" loading of lifeboats. Nevertheless, the lifeboats were grossly underutilized. The inquiry found a number of reasons for this, including a reluctance of passengers to leave the ship, fear of being lowered about 65 feet to the water in a lifeboat and the fact that no ship-wide lifeboat drill had ever been held by the passengers or the crew.

The British inquiry examined the reasons for insufficient lifeboat capacity. The extant lifeboat rules were promulgated by the British Board of Trade and had not been updated since 1894. The rules required a specified volume capacity of lifeboats based on the tonnage of the vessel, not on the number of passengers. The tables topped out at 10,000 tons [9]. The inquiry board noted the largest emigrant ship in 1894 was the Lucania at 12,952 tons. For a ship the size of the Titanic, the required lifeboat capacity was 962 passengers, as calculated by the board of inquiry. However, its gross capacity was 46,328 tons, far above anything anticipated by the 1894 rules.

Sir Alfred Chalmers, the retired Nautical Advisor to the Board of Trade, explained why the lifeboat rules were not updated from 1894 until after the sinking of the Titanic.

> "I considered the matter very closely from time to time. I first of all considered the record of the trade - that is to say, the record of the casualties - and to see what immunity from loss there was. I found it was the safest mode of travel in the world, and I thought it was neither right nor the duty of a State Department to impose regulations upon that mode of travel as long as the record was a clean one. Secondly, I found that, as ships grew bigger, there were such improvements made in their construction that they were stronger and better ships, both from the point of view of watertight compartments and also absolute strength, and I considered that that was the road along which the shipowners were going to travel, and that they should not be interfered with. I then went to the maximum that is down in the Table - 16 boats and upward, together with the supplementary boats, and I considered from my

experience that that was the maximum number that could be rapidly dealt with at sea and that could be safely housed without encumbering the vessel's decks unduly. In the next place, I considered that the traffic was very safe on account of the routes - the definite routes being agreed upon by the different companies, which tended to lessen the risk of collision, and to avoid ice and fog. Then, again, there was the question of wireless telegraphy, which had already come into force on board of these passenger ships. I was seized of the fact that in July, 1901, the 'Lucania' had been fitted with wireless telegraphy, and the Cunard Line, generally, fitted it during that year to all their ships. The Allan line fitted it in 1902, and I am not sure that in 1904 it had not become quite general on the trans-Atlantic ships. That, of course, entered into my consideration as well. Then another point was the manning. It was quite evident to me that if you went on crowding the ships with boats you would require a crew which were not required otherwise for the safe navigation of the ship, or for the proper upkeep of the ship, but you are providing a crew which would be carried uselessly across the ocean, that never would be required to man the boats. Then the last point, and not the least, was this, that the voluntary action of the owners was carrying them beyond the requirements of our scale, and when voluntary action on the part of shipowners is doing that, I think that any State Department should hold its hand before it steps in to make a hard-and-fast scale for that particular type of shipping. I considered that that scale fitted all sizes of ships that were then afloat, and I did not consider it necessary to increase it, and that was my advice to Sir Walter Howell." [9]

Notice the reasons for not requiring more lifeboat capacity as ships got bigger: the ship owners were voluntarily installing more lifeboats than were required, the ships were better, stronger and had more watertight compartments, there was not enough room for all of those lifeboats, passenger ships were the safest mode of transportation, there was little risk of collision with other ships or ice, the ships all had radios, and there were just not enough crew members to man all those lifeboats. Sir Chalmers did not want to interfere with the waterway that the shipowners were navigating, even if it included a waterfall.

Those explanations sounded like flimsy rationalizations to the public in 1912. Exceeding government regulations had not ensured that the Titanic was reasonably safe.

CASE STUDY 2 - PHARMACEUTICALS

Numerous drugs approved by the FDA have later been withdrawn from the market due to health concerns. According to David Willman of the Los Angeles Times, seven FDA-approved drugs were withdrawn between September, 1997 and November, 2000. These drugs were marketed under the trade names Lotronex, Redux, Raxar, Posicor, Duract, Rezulin and Propulsid [10].

Rezulin, also known as troglitazone, is a classic example of a recalled drug. It was approved in January, 1997 as a treatment for type 2 diabetes. Within a few months of its introduction on the market, reports of liver failure were coming in to the FDA. By March 21, 2000, when the drug was withdrawn by its manufacturer, the FDA had confirmed 63 deaths from liver failure [11]. In the interim, the product warnings were reworked four times to instruct patients and doctors to follow a regimen of liver function monitoring. The admonitions grew to encompass more frequent monitoring over longer periods of time. FDA senior scientist Dr. David J. Graham warned in March, 1999 that no reliable way existed to protect Rezulin patients from liver failure [11]. Graham concluded that there was no scientific basis to assert that liver monitoring would prevent liver failures in patients taking Rezulin.

The FDA had performed another review of Rezulin in 1999 and concluded that no recall was necessary. According to the FDA press release dated March 21, 2000 [12], “In March 1999, FDA's Endocrine and Metabolic Drugs Advisory Committee reviewed the status of Rezulin and its risk of liver toxicity and recommended continued availability of this drug in a select group of patients -- patients not well-controlled on other diabetes drugs.” Nevertheless, a year later the drug was pulled from the market, after the death toll had hit 63. FDA approval had not ensured that Rezulin was reasonably safe.

Vioxx (a drug prescribed to one author) is another prescription medicine approved by the FDA and then later withdrawn from sale. Also known as rofecoxib, Vioxx is a non-steroidal anti-inflammatory drug (NSAID). It was approved by the FDA in 1999 to treat osteoarthritis pain and inflammation, and for treatment of acute pain. Later, Vioxx was approved by the FDA to treat rheumatoid arthritis [13]. Vioxx was withdrawn from the market by its manufacturer on September 30, 2004. The company found a doubled heart attack risk for long term users of the drug, along with an increase in stroke risk. The FDA characterized the risk for an individual patient of a heart attack or stroke as “very small” [13].

Cylert is another prescription drug approved by the FDA and later withdrawn from the market. The FDA pulled the plug on Cylert and its generic form, pemoline, in October, 2005 after concluding the risk of liver toxicity outweighed the benefits of the drug [14]. Cylert’s manufacturer stopped selling and marketing the drug in the U.S. in May, 2005. Cylert was used to treat Attention Deficit Hyperactivity Disorder (ADHD) by stimulating the central nervous system. In both cases, Cylert and Vioxx, FDA approval was the last step in allowing a dangerous product into the stream of commerce.

CASE STUDY 3 - LADDERS

The ANSI portable ladder standards have several major shortcomings that have allowed thousands of defective ladders to be produced and later recalled (or worse, not recalled). Some ladders had design defects, others had manufacturing defects. All of the recalled ladders met the standards (according to the manufacturers) and many thousands bore Underwriters Laboratories (UL) stickers attesting to the fact that they passed the standards. Not all of these ladder models had been tested by an independent agency, such as UL. All Krause ladders the authors have examined violated the rung spacing requirements in the A14.2 standard.

Six months’ worth of Krause articulated ladder production from 1997 and 1998 was recognized by Krause as defective. Over 70,000 ladders were recalled because the joints could fold up and collapse the ladder while in use [15].

The recalled ladders passed the tests for the ANSI A14.2 portable metal ladder standard and bore UL stickers. However, they could collapse while a user was just standing on them. The ladders were either 12 or 16 feet in total length and com-

posed of four sections fastened together using three pairs of hinges that each went into three different positions. A small percentage of the recalled ladders were made of two six-foot sections connected with one pair of hinges. Each hinge used a locking bolt to hold it in the desired position.

Krause switched to a locking bolt made of sintered steel in December, 1997. It was coated with Xylan 5250, as several years' worth of Krause locking bolts had been coated. The coating was red, to increase the visibility of the locking bolts.

Edward Hansen, former Krause controller, testified that ladder collapse claims began to rise after the ladders with the new locking bolts were put into the stream of commerce [16]. Hansen said claims went up in January, 1998 and continued to rise in February and March. In May, Hansen received a phone call from a ladder user who was also an engineer. The engineer witnessed the failure of a locking bolt. Hansen said the engineer then repeated the scenario, with the same result [16].

Hansen said he and company engineer Jerry Antosch developed a vibration or shake test to check what the ladder user told him. He said in the first shake test, he placed 150 pounds on a Krause Multimatic while it was in the scaffold position, and began to vibrate the ladder with his hands. Hansen said Antosch watched the center hinges, and saw the locking bolts began to disengage. The locking bolts moved backwards in the slots that held the ladder joint in a locked position, duplicating the caller's observations.

Krause determined the problem was a combination of the Xylan coating and the sintered steel. This diminished the friction and allowed the bolts to slide backward from the locked position, even though spring pressure was pushing the bolt into the locked position. This was a design defect, not a manufacturing defect. A lot of 50 recall ladders was tested by Krause and all 50 were found to fail the shake test [17].

This defect eventually led to the bankruptcy of the company, even though Krause stopped production immediately after it was discovered and went back to using a previous style of locking bolt. For all the testing Krause and UL had conducted, this defect was not detected by Krause until after a phone call from a user. The ANSI portable metal ladder standard in effect at the time (A14.2 -1990) had many load tests, but none revealed this ladder defect. The Krause ladder passed all the A14.2 load tests. The standard failed to prevent the design and sale of the defective ladders.

Krause filed for Chapter 11 bankruptcy reorganization in July, 2000, due to tort liability from recalled ladders. Krause eventually filed Chapter 7 dissolution bankruptcy and sold its assets to another firm. The defective design not only injured unsuspecting customers, it put the company out of business.

Defective ladders can also be produced due to loopholes in the standards. The A14 portable ladder standards only require load testing to be performed on the "climbing" side of extension ladders. Unfortunately, ladders are not always set up with the user on the "climbing" side. If a ladder happens to not be sturdy enough for this reverse orientation, a failure will occur, even though the ladder passed the standard.

One prominent ladder expert, retained by a ladder manufacturer, testified that it was foreseeable for an extension ladder to be set up in the backwards orientation [18]. It is a reasonably foreseeable orientation. At least two different sets of defective ladders have turned up that fail in the reverse orientation. One set was a series of fiberglass extension ladders from a now bankrupt manufacturer, Keller. The ladders were not strong enough to hold approximately the rated load while in the reverse orientation. To compound the problem, Keller placed a setup sticker on each ladder showing it set up both as a front fly and rear fly ladder. The sticker made it appear that either orientation was correct.

The second set was a series of Krause ladders. When Krause ladders with zinc locking bolts were set up as straight ladders, in the reverse orientation, with only one locking bolt engaged in the middle set of hinges, a heavy user (but weighing less than 300 pounds), and a setup angle that was shallower than the recommended 75 degrees, the single locking bolt could fracture, dropping the user.

All these conditions were foreseeable. The ladder was typically tested to three-and-a-third to four times the rated load, due in part to the fact that a user may set the ladder up at a shallower angle than the recommended 75 degrees. The reverse orientation will be used. There is nothing visible on the Krause ladder to warn the user that it is backwards. Only four small words on one label indicate that the ladder has a front and a back. The middle hinge issue was well documented, even by the Consumer Product Safety Commission [19]. On occasion, only one locking bolt in the middle hinge set would engage, and no amount of shaking the ladder would cause it to engage.

In this scenario, several things must go wrong at one time to cause an incident. However, all but one of these conditions is accounted for in the A14.2 ladder tests, and the combination is reasonably foreseeable. There is a load test that requires one middle hinge to be unlocked in the straight ladder position while three-and-one-third to four times the rated load is applied. However, the test is only conducted in the climbing orientation. If Krause had been forced to test the ladder in the reverse orientation, it would have failed. Because of this loophole, a number of ladder accidents happened with ladders that passed the standard.

Sometimes a recall is due to a problem that a standard ignores. Keller recalled 29,600 extension ladders due to a false lock problem [20]. Keller determined that a brace on the base section could interfere with the rung locks, creating a condition known in the industry as false lock. The false locked ladders could collapse in use, causing injury. When a ladder is false locked, the rung locks are not fully locked, even though the user believes that they are. Each of those ladders met the A14 standard, yet they were defective and unreasonably dangerous. Keller recalled each ladder that used that particular design. The only test in the ANSI A14 portable ladder standards that detects false lock is a flylock endurance test. If a false lock occurs from a broken part, the test will catch it. Otherwise, false lock is not looked for.

Other recalls are driven by manufacturing defects that are not caught by the ladder standards. Louisville Ladder recalled 3,000 ladders because the rungs could break near the side rail [21]. Bauer recalled thousands of ladders because the ladder rivets could break while the ladder was in use [22]. Both of these ladder designs met the A14 standard, yet they were not reasonably safe and were recalled.

CASE STUDY 4 – PASSENGER VEHICLE TIRES

Tires are considered consumer products that require nominal maintenance rather than professional care. Removing

nails, repairing small holes, ensuring the balance weight remains in place and maintaining adequate air pressure is, near enough, comprehensive. Tires do not require filling with dry nitrogen. This is a recent strategy to separate safety-conscious consumers from their money, and is another manifestation of the principal-agent conflict.

Manufacturers must consider all foreseeable use conditions by consumers when they design and manufacture their products. Tires should provide endurance to the vehicle load and speed, durability to wear, traction under dry, wet and snow conditions, and handling (maneuverability).

The relatively recent (2000) recalls of Firestone tires associated with Ford Explorer vehicles were not the company's first foray into this territory. Firestone realized that they were having problems with their 500-series steel belted radials in 1973. However, instead of withdrawing this model until a satisfactory fix could be determined and implemented, they continued to sell them and made running changes to the manufacturing line. In 1976, Firestone continued to have such disproportionate problems that the federal government became interested. NHTSA initiated a safety standard compliance investigation of the 500 steel belted radials after dropping an investigation of the 500 steel belted bias ply tires. In November, 1978, Firestone recalled 4.5 million of these tires [23].

In August, 2000 and in June, 2001, Firestone and Ford Motor Company conducted even more massive tire recalls, covering over 20 million Firestone P235/75R15 ATX and 15, 16 and 17-inch Wilderness AT tires [24, 25]. These recalls triggered Congress to pass the *Transportation Recall Enhancement, Accountability, and Documentation Act* (TREAD) that directed NHTSA to adopt a new regulation improving the safety performance of passenger vehicle tires in several critical areas. An investigative report by NHTSA [26] identified several root causes. They included shoulder pocket design, inflation pressure issues, and belt adhesion problems associated with Firestone's Decatur plant. These tires were particularly dangerous because they would delaminate, and did so at a rate much higher than other tires.

Firestone had tested its various tires to the then-current standards for durability, FMVSS-109, *New Pneumatic Tires*, and FMVSS-119, *New Pneumatic Tires for Vehicles Other Than Passenger Cars*. These standards were introduced in 1967 before radial tires became dominant and eventually nearly universal. These two standards remained virtually unchanged until they were superseded as a result of the second Firestone recall.

FMVSS-109 specified the requirements for all tires manufactured for use on passenger cars built after 1948. This standard, issued in 1967, specified tire dimensions and required them to meet specified strength, resistance to bead unseating, endurance, high speed performance, and labeling information requirements. It applied to passenger car (P-metric) tires produced for use on sedans, light trucks, and multipurpose passenger vehicles (MPVs), including sport utility vehicles.

FMVSS-119 specified performance and labeling requirements for new pneumatic tires designed for highway use on MPVs, trucks, buses, trailers and motorcycles made after 1948. These tires had to meet requirements that were qualitatively similar to those in FMVSS-109 for passenger car tires.

Largely in response to the needless deaths and injuries that led up to and post-dated the recalls, NHTSA established FMVSS-139, *New Pneumatic Tires for Light Vehicles*, replacing FMVSS-109 and 119 in November, 2002. It became fully in force in September, 2007.

The new FMVSS-139 standard has more stringent test requirements compared to the previous standards. Compliance to this standard does not ensure that tires will not fail, because the tire's contact patch is consumed in use, much like a pencil eraser. Any tire used for too long will fail. It is the goal of tire and wheel designers to ensure that they fail in a manner that is safe to the user:

1. Under extreme loads or when filled with air at too high of a pressure, the tire should debead, rather than the wheel explode.
2. The tire should "blow out" prior to delaminating.

When a tire is placed upon the wheel, it may be inadvertently overloaded with air. This should cause a rapid depressurization that is not injurious to those nearby. When a tire delaminates, it is much more likely to precipitate loss of control by the driver than is a blowout (carcass breach). Despite the enhanced test conditions that were elicited by unexpected failures, the new standard, FMVSS-139, still does not ensure the safe manners of failure described above. Neither does the new standard define "failure mode" in its test protocols.

Two last points are also worth making. First, all tires have a "shelf life" and become stale and less safe. This life is approximately seven years, but nothing on the tire indicates to the uneducated consumer when he or she should discard the tire. Many of the deaths due to the defective Firestone tires that were on Explorers were being used as spares. Spare tires (out of sight, out of mind) are often subject to exhaust heat cycling which can also be deleterious. Second, when two new tires are placed on the vehicle, they should be placed upon the rear axle, as the rear tires are the "feathers of the arrow." Counter-intuitively, a failure of a rear tire is more likely to lead to a directional loss of control than is a front tire. No law that the authors are aware of mandates the placement of new tires on the rear axle. In fact, a common preference is to place new tires on the front axles of front wheel drive cars as this is thought to be the more stringent condition.

CASE STUDY 5 – COMMERCIAL VEHICLE ROLLOVER CRASHWORTHINESS

The rollover injury and death problem of passenger vehicles is well recognized, and extensively covered in the peer reviewed literature. NHTSA recently upgraded FMVSS-216, *Roof Crush Resistance*, to substantially increase the required roof strength of passenger vehicles, and implemented a new standard for most, but not all, side windows, FMVSS-226, *Ejection Mitigation* [27, 28]. These two standards should ensure that the vast majority of U.S. automotive travel will be inside of vehicles that have roofs strong enough to resist the force of rollover impacts, and window portals that remain substantially blocked during collisions to prevent partial and full ejection injuries.

Both requirements can be addressed using low-technology fixes (i.e., stronger steel, laminated side glass) that have been available for over 40 years. The implications are obvious; NHTSA's previous standards on roof strength and glazing performance [29, 30] are inadequate. Thus a vehicle design that

was legal (and presumed safe) to produce and sell one day will become illegal (and presumably unsafe) the next.

Neither of these safety upgrades apply to the majority of commercial vehicles, which are generally classified based according to their weight. For example, the crew cab pickup shown below is sufficiently heavy that it was not required to be compliant with the FMVSS-216 standard under which it was manufactured. This truck was in use as a family vehicle at the time it rolled 2.5 revolutions.

Fig. 1: 2002 Ford Super Duty crew cab pickup after fatal roll-over and righting [31].

Such roof performance of heavy vehicles is in no way exceptional [32]. Roof performance in rollover of Class VIII semi-tractors is unregulated by federal law. The private U.S. standard that is applicable to semi-tractors, SAE J2422, is a two-part destructive test [33]. The first dynamic load approximately simulates impact forces to the roof as if the tractor were not attached to a trailer and simply tipped over onto its side from a halt. The second quasi-static load on the damaged roof equals the rating of the front axle. Actual accident loads typically substantially exceed these force levels.

U.S. motorcoaches and buses, which are multi-passenger commercial vehicles, do not even enjoy an *inadequate* non-government standard for roof strength. Their side window glass is also unregulated for occupant containment, even with the new FMVSS-226. Further, though NHTSA has proposed requiring seatbelts for occupants, this rule has not yet gone into effect [34].

Figure 2 shows a commercial limousine bus that was equipped with tempered side glass in its large, picture windows. This type of glass will not retain occupants when shattered. It was outfitted with a single seat belt for the driver. It underwent a very minor, ~4 mph, lateral change in velocity when the inattentive driver drifted across the highway and impacted the Jersey barriers (shown on left of bottom photo). A pole-mounted traffic sign immediately broke the majority of the side picture windows. Due to the impact pulse, two occupants were fully ejected to their left through open window portals and were killed when they impacted the oncoming light poles. Another occupant was only partially ejected, but suffered severe brain damage due to pole impact. This limousine was fully compliant with all federal regulations. While this was not a rollover accident, the inclusion of passenger seatbelts in this vehicle, along with the addition of windows designed to mitigate ejection, would have saved lives in an accident that would otherwise have been minor.

Fig. 2: 2007 Limousine bus post-crash (top) and at point of rest after accident (bottom) [35].

CASE STUDY 6 – FIREARMS

The vast majority of gun laws regard their acquisition, ownership, transportation, use and misuse. Very few laws actually govern the design principles behind firearms. It is self-evident that the discharge of a firearm without depression of the trigger is evidence of a defect. Catastrophic firearm failures, in which the pressure developed by the burning gunpowder overwhelms the strength of the barrel and/or locking mechanism, are rare. They usually occur due to an obstruction of the bore, but also arise due to overly hot hand-loaded cartridges and a myriad of other causes. Perhaps surprisingly, failures of this type are rarely fatal, and the prudent wearing of

purpose-designed eye protection eliminates most serious ocular injuries [36]. Other firearm failures/defects include firing out of battery, inertial discharge, and safety actuation.

Firing out of battery occurs when the firearm discharges in an unlocked or partially-locked state. For high pressure cartridges, this failure can blow the bolt backwards and kill the user. Canadian soldiers during WWI could assemble their Ross rifle bolts incorrectly, allowing a .303 round to be chambered and fired with none of the seven locking lugs engaged.

A bolt that has failed to fully engage or seat is usually a sign of inadequate lubrication and/or burned powder and debris fouling. Blowback firearms are particularly prone to this occurrence. In general, these firearms fire low-pressure cartridges and do not lock, but rather use the weight of the breech block to ensure that the casing remains in the bore and the pressure has sufficiently dropped prior to extraction. Virtually all .22LR semi-automatics are blowback operated. In a dirty firearm or one with a tight "match" chamber, the straight-walled .22LR cartridge may only partially seat, leaving the base of the brass cartridge unsupported. If the design of the mechanism allows the firing pin to strike the .22LR rim when the base of the cartridge is significantly outside of the chamber, then the casing will split, spraying molten brass and hot burning gases out of the ejection port. Users of current Smith and Wesson M&P 15-22 rifles and SIG Sauer MOS-22-B pistols have complained of this defect.

As surely as a vehicle will catch fire and explode as it pitches nose first over a steep hillside, a pistol or rifle will discharge if dropped; at least according to the movie industry. In reality, most modern firearms are carefully designed and tested to ensure that they do not discharge when dropped. Note that dropping pistols and rifles is not a minor problem. All objects which are handled are dropped by their imperfect owners, which is one reason that inexpensive shock-absorbing sleeves are manufactured for cell phones. The German Schützpolizei issued SIG P6 pistols with a notch cut into the base of the round "burr" hammer. Dropping the pistol onto the hammer forces notch closure and alerts the armorer that this particular *Pistole* has been dropped.

Inertial discharge is a characteristic of the original single action army (SAA) revolvers. That is, the firing pin is attached directly to the hammer and rests on the primer when the hammer is in the down or "at rest" position. If the revolver is dropped onto the hammer spur, the weapon's inertia drives the cartridge and primer into the pin. The primer ignites and the weapon fires. Two-shot "Derringer" pistols also manifested this problem. Colt stopped production of SAA pistols, also known as .45s and "Peacemakers" during World War II, and did not restart production until much later. Interest in these pistols found resurgence as a result of the popular cowboy television series of the 1950s. The firm Sturm, Ruger, and Company introduced the "Single Six" .22LR revolver, and later the Blackhawk revolver to fill market demand. Ruger's pistols were redesigned copies of Colt's SAA with frame mounted firing pins, but would also discharge when dropped. After various accidents, injuries, and lawsuits, the problem was solved by the use of a redesigned hammer and firing pin combination that did not ever directly touch. As the new trigger was pulled, a "transfer bar" interposed itself between the hammer and pin to transmit hammer energy. This simple and elegant design has been used via license by many other manufacturers. Addressing inertial discharge is rather straightforward in theory, but can be somewhat difficult in practice; see, for example, the 2008 Ruger SR9 recall.

Other firearms can, via shock loading, disengage the sear from the cocked hammer, and unintentionally discharge. Colt's model of 1911, which was used by the U.S. Army until its replacement beginning in 1986, was not originally designed with a "drop safe" mechanism. Impact shock could disengage the sear from the hammer and fire the pistol.

The Remington Model 700 has been described as a target rifle that was sold as a hunting rifle. While it has undergone various modifications since its debut in 1962, the original rifles were equipped with the Walker trigger [37] using a connector between the trigger and the sear to, "provide a sear and control…which operate on barely perceptible movement of the trigger, yet releases the firing pin instantly and completely." In general, the shorter the travel and lighter the required release force, the more susceptible a particular trigger design is to an unintended discharge. Two defects are present in the Walker design, though their existence is hotly disputed by Remington. First, while the striker (the spring-loaded firing pin) is blocked from forward movement when the safety lever is engaged, the original lever would not mechanically reset the linkages. Thus, when the safety is disengaged, the sear actually might not be in contact with the striker, allowing unexpected release, causing the rifle to discharge. Second, the connector, which is a more or less free floating stamping that separates the trigger from the sear, diminishes the fire control systems reliability. The Walker connector is a feature found in no other bolt-action rifle trigger, and acts as a force decoupler. It is not constrained to move with the other parts, but is free to move within the trigger housing subject only to spring force. Material such as manufacturing debris, contamination, and hardened lubricants can interfere with the motion of the components and lead to an unintended discharge. An internal document from Remington estimated that on the order of one percent of these rifles could be "tricked" into unintended discharge. This trigger design did not violate any federal firearms standards, and rifles so equipped were never recalled.

CASE STUDY 7 – TOYOTA SUDDEN ACCELERATION

The U.S. auto industry's historic attitude toward safety has been checkered. In 1974, Lee Iacocca (then working at Ford) was secretly recorded by President Richard Nixon saying, "Shoulder harnesses and head rests are complete wastes of money. Safety has really killed off our business." [38] Of course, Mr. Iacocca was thoroughly mistaken, and later went on to "The New" Chrysler to tout his company's airbags as a definite safety advantage. Today, automobiles are heavily regulated consumer products, with federal standards governing bumpers, fuel systems, roofs, glass, seatbacks, and other characteristics including airbags which are now standard on virtually every vehicle sold. It is unrealistic, other than with deliberately vaguely worded language, for the government to make all-encompassing rules that prohibit manufacturers from making vehicles which are dangerous beyond the public's general expectations. The majority of FMVSSs give numeric targets which manufacturers can ensure they meet *a priori* to new model debut. It has been found that some vehicles which com-

fortably pass numeric standards are still defective and do not behave as the public expects.

In 2009 and 2010, the Toyota Corporation, long a paragon of the automotive industry, was stung in general by the unsafe performance of some of their cars, and in particular by the undeniably disingenuous behavior of their management. Toyota produced defective cars that have demonstrated "Sudden Unintended Acceleration" (SUA), and recalled in 2010 far more vehicles than it sold. This SUA defect has been responsible for numerous deaths, including one in which a 9-1-1 phone call documented the uncontrollability of the vehicle prior to the crash [39]. In this sobering, well-documented example, an off-duty California patrolman crashed a 2009 Lexus ES350 at highway speed, killing himself, his wife, their daughter, and his brother-in-law. Toyota's explanation was that a stuck floor mat was responsible [40].

Other issues associated with this vehicle's design include brakes that do not reliably overcome the engine's power, and an ignition switch that will not turn the vehicle off when a panicked operator rapidly and repeatedly presses it, rather than performing a single prolonged engagement as a calm operator parking the vehicle would. It is simply unreasonable for Toyota to produce vehicles that will not respond to driver inputs.

The corporate response was viewed to be egregious by the federal government, precipitating testimony by the company's president Akio Toyoda (the founder's grandson) before hostile federal legislators and a historic fine of over $16 million dollars. Toyota in essence pled "no contest" to the accusations, paying the fine without admitting guilt.

Fig. 3: Left front brake disc from the Lexus crash showing clear evidence of prolonged emergency braking.

Toyota's story as to the root cause evolved orthogonally with time. Toyota's original solution was to blame the floor mats, and to initiate a voluntary minimalist recall to affix the mats to the floor, preventing entanglement with the accelerator pedal. The analysis then pointed to the accelerator, an electronic gas pedal without a direct mechanical linkage to the throttle. Toyota's "game plan" [41] was to delay and diminish their recall activities, saving the company a hundred million dollars, undoubtedly at the cost of human life and suffering. Toyota's attorneys hired Exponent to research and publish their analysis of the issue. As of May 20, 2010, after 1,100 hours of work, Exponent said that their engineers and technicians were unable to replicate the SUA problem.

Fig. 4: Post-crash remnants of Lexus.

The unsafe technology and egregious actions of Toyota confirm that safety standards are minimal, incomplete indicators of safety. Conformance to a standard is a form of negative evidence, in that it suggests that a component or system is not defective with respect to the characteristics tested, rather than a positive affirmation of a defect-free condition. It is simply unreasonable to expect the FMVSSs to be comprehensive, particularly with evolving technology. Lawmakers recognized this and noted that, "Compliance with any Federal motor vehicle safety standard issued under this title does not exempt any person from any liability under common law." [42]

WHY CODES AND STANDARDS FAIL

There are numerous reasons that adherence to a standard does not guarantee reasonably safe products. Several of these reasons were listed earlier, though that listing was not exhaustive. Sometimes a standard fails to produce reasonably safe products because the issue is apparently so obvious that no one could imagine it would be a problem. Who would design a car with an electronic ignition switch that would not turn the car off in an emergency when the button was pushed, over and over and over? Toyota would.

Who would build a single-shot machine gun? Maremont would. The gas piston on the U.S. Army's Vietnam-era M60 general purpose machine gun could be reinstalled backwards into its sleeve after cleaning, turning the weapon into a single shot rifle. This defect was found almost immediately by troops, but took decades for the U.S. Army to address. In the interim, they relied upon the "Be Careful" strategy [43] to minimize improper assembly.

Who could imagine that a ladder would collapse while a person was just standing on it? Why would testing it with three-and-a-third to four times the rated load fail to reveal this problem? The static nature of virtually all the A14 load tests did not create dynamic conditions that would reveal the Krause defect. The standard simply didn't incorporate appropriate dynamic testing, to simulate actual use.

However, dynamic testing was not even required to reveal the Krause defect. On May 25, 1998, four days after the first shake test, Krause personnel discovered the ladder could collapse under a 150-pound static load if it was applied for a "long period of time" [15]. This example points out the need for real world testing. The load tests from ANSI A14.2-1990

were typically limited to one-minute loading periods. There were no load tests with extended loading times, more indicative of how users actually load ladders.

The reverse orientation ladder failures were allowed to pass the standard due to a failure to address commonplace and reasonably foreseeable misuse. Yes, the ladders were facing the wrong direction. As noted previously, only four small words on one sticker identify the Krause ladder has a front and back orientation. The appearance of the ladder is completely ambidextrous. The rungs are square tubing set parallel to the rails, so it feels and looks the same whether the ladder is set up forwards or backwards. It is completely unsurprising when a ladder, particularly a Krause, is set up backwards. In fact, the only people who are surprised are the users who get hurt when their ladder fails because it was set up backwards.

These failures of the standards ultimately lead to defective products and injured users when manufacturers rely solely on the standards to guarantee reasonably safe products.

The Rezulin recall illustrated the dangers of too cozy of a relationship between an industry and its regulators. Willman [11] described a culture within FDA that favored (or forced) quick review of new drugs, but supplied insufficient manpower to thoroughly examine and evaluate the manufacturer's studies. He also described a culture that was deferential to the pharmaceutical industry and hostile to those who would question its drug safety and efficacy studies. After all, the drug manufacturer had spent millions developing the drug and testing it, and possibly millions of patients could be helped by it. Who would want to interfere with that? These influences, whether subtle or overt, could blind a government agency to the dangers of a given product.

From the description given by Willman, some senior FDA officials were too close to the manufacturer of Rezulin or gave them too much deference when evaluating their studies.

According to Willman [11], Dr. John L. Gueriguian was initially tasked with evaluating Rezulin. He said that it was not significantly better than other drugs on the market and that it could cause heart and liver damage. He recommended not approving the drug. Willman said that Rezulin's manufacturer complained to senior FDA official Murray "Mac" Lumpkin, who pulled Gueriguian off the Rezulin project and purged his medical reviews from the FDA files. Willman said the message inside FDA was "challenging Rezulin was not without risk to one's career."

The drive to recall Rezulin did not originate within the ranks of FDA management. That effort was led by a small group of people within FDA called, "The Termites." The Termites were a group of about a dozen physicians, spearheaded by Graham, who compiled studies and data on the dangers of Rezulin [11]. They ultimately convinced FDA senior management to pull the plug on the drug, but not before 63 patients had died from liver failure.

CONCLUSION

Codes and standards fail because they are written and enforced by people. And people are fallible. They suffer from many shortcomings, including shortsightedness, hubris (particularly with regard to technology), refusal to consider multiple simultaneous failures and refusal to grapple with commonplace and reasonably foreseeable misuse. Further, people are successful in pushing technology, and may easily outstrip the ability of standards-making bodies to keep up.

There can be a financial reason to maintain standards in line with previous generations of products. It is common for victims of products that do not conform to state-of-the-art safety practices to seek redress. It can be difficult for a manufacturer to explain to a jury why a product lacked a certain safety device that was technologically and economically feasible, but was not used because it was not required by a standard, if the current standard requires that device.

In contravention to Barnett's blanket assertion that reasonably safe is defined by adherence to the standards, adherence to the plain meaning of the first fundamental canon of the NSPE Code of Ethics is the appropriate measure. When engineers design and build products, they will be judged by their performance measured against the state of the art, including technologically and economically feasible safety solutions, as outlined by the National Safety Council hazard evaluation and design priority procedures [44].

REFERENCES

[1] Barnett, R. L., "On Safety Codes and Standards", Triodyne Safety Briefs, 1983.

[2] Barnett, R. L., and P. Poczynok, "Critique: Drain Cover Standard ASME/ANSI - A112.19.8M-1987 (1996) Case Study: Steering Wheel," Safety Brief, Triodyne, Inc., Vol. 19, 4, February, 2002.

[3] "Jack: Straight From The Gut", Jack Welch and John Byrne, Warner Books, Inc., New York, 2001.

[4] "Barbarians At The Gate: The Fall Of RJR Nabisco", Bryan Burrough and John Helyar, Harper Business Essentials, 1990.

[5] Tammy Faye Bakker, 65, "Emotive Evangelist, Dies", Anita Gates, New York Times, July 22, 2007.

[6] National Society of Professional Engineers Code of Ethics, www.nspe.org/Ethics/CodeofEthics/index.html, 2011.

[7] British Wreck Commissioner's Inquiry Report, Report on the Loss of the "Titanic." (s.s.), www.titanicinquiry.org/BOTInq/BOTReport/BOTRepLSApp.php, 1912.

[8] Ibid, www.titanicinquiry.org/BOT-Inq/BOTReport/BOTRepSaved.php, 1912.

[9] Ibid, www.titanicinquiry.org/BOT-Inq/BOTReport/BOTRepBOT.php, 1912.

[10] Willman, D., Los Angeles Times, "New FDA: How a New Policy Led to Seven Deadly Drugs," December 20, 2000.

[11] Willman, D., "The Rise and Fall of the Killer Drug Rezulin," Los Angeles Times, June 4, 2000.

[12] Food and Drug Administration, P00-8, "Rezulin To Be Withdrawn From The Market", March 21, 2000.

[13] Food and Drug Administration, P04-95, September 30, 2004, "FDA Issues Public Health Advisory on Vioxx as its Manufacturer Voluntarily Withdraws the Product".

[14] Food and Drug Administration, FDA ALERT, "Liver Injury Risk and Market Withdrawal", "Alert for Healthcare Professionals Pemoline Tablets and Chewable Tablets (marketed as CYLERT)", October, 2005.

[15] Hansen, E., Full Report of Krause Inc. (to CPSC), June 8, 1998.

[16] Hansen, E., deposition in Travers v. Home Depot and Krause, Hillsborough County, FL, case 03-4178, p. 179, January 22, 2004.

[17] Hackett, P. L., CPSC Product Safety Assessment Report, PSA No. 0814.98, p. 1, August 18, 1998.

[18] Ver Halen, J. B., deposition in Weller v. Keller Industries, Hancock County Circuit Court, Hancock, IN, 30C01-9107-CT-541, p. 19, February 4, 1994.

[19] Hackett, P.L., CPSC Product Safety Assessment Report, PSA No. 0645.98, p. 4, June 23, 1998.

[20] CPSC, Release 96-095, Keller Announces Recall of Certain Model Fiberglass Extension Ladders, April 10, 1996.

[21] CPSC, Release 06-038, Louisville Ladder Announce Recall of Industrial Ladders, November 23, 2005.

[22] Bauer Corp., Ladder Safety Recall, October 8, 2003.

[23] NHTSA, Recall Campaign 78T031000, 1978.

[24] NHTSA, Recall Campaign 00T005000, 2000.

[25] Jackson, Michael P., Deputy Secretary of Transportation, Statement before the Subcommittees on Telecommunications, Trade and Consumer Protection and Oversight and Investigation of the Committee on Energy and Commerce, U.S. House of Representatives, June 19, 2001.

[26] Department of Transportation, "Engineering Analysis Report and Initial Decision Regarding EA00-023: Firestone Wilderness AT Tires," October, 2001.

[27] Department of Transportation, NHTSA, Federal Motor Vehicle Safety Standards, Federal Register, Vol. 74, pp. 63180 – 63233, December 2, 2009.

[28] NHTSA, Federal Motor Vehicle Safety Standards, Ejection Mitigation; Phase-In Reporting Requirements; Incorporation by Reference, January 19, 2011.

[29] Federal Motor Vehicle Safety Standard No. 216, *Roof Crush Resistance*, January 4, 2004.

[30] Federal Motor Vehicle Safety Standard No. 205, *Glazing Materials*, October 1, 2002.

[31] Montana Crash Investigator's Report 0700014490703, July 7, 2007.

[32] Batzer, S. A., B. E. Enz, G. G. Herndon, C. K. Thorbole, R. Hooker, T. K. Parnell, and M. Ziejewski, "Heavy Truck Roll Cage Effectiveness," *ASME International Mechanical Engineering Congress & Exposition*, Lake Buena Vista, FL, IMECE2009-12423, 2009.

[33] SAE J2422, "Cab Roof Strength Evaluation – Quasi-Static Loading Heavy Trucks," December, 2003.

[34] Department of Transportation, "U.S. Department of Transportation Motorcoach Safety Action Plan," DOT HS 811 177, November, 2009.

[35] Georgia Uniform Motor Vehicle Accident Report, 07-1811729, June 30, 2007.

[36] Hatcher, Julian S., "Hatcher's Notebook," Stackpole Books, 1962.

[37] Walker, M. H., and P. R. Haskell, "Firing Mechanism for Firearms," US Patent 2,514,981, July 11, 1950.

[38] CBS News Online, "Mustang: A Classic Danger?", http://www.cbsnews.com/stories/1999/05/17/60II/main47539.shtml, February 11, 2009.

[39] Wall Street Journal Online (Uncredited), "Toyota Sued over Fatal Lexus Crash," http://online.wsj-.com/article/SB10001424052748703862704575099861335382140.html, March 5, 2010.

[40] Jensen, C., "Toyota Acceleration Problem is Still Unresolved," New York Times Online, November 3, 2009.

[41] Whoriskey, P., "Toyota used its 'game plan' to escape a major early recall," Washington Post online, March 19, 2010.

[42] 15 U.S.C. 1398.

[43] Morse, J. and S. Batzer, "Prevention Through Design – An Idea Whose Time Has Come," *ASME International Mechanical Engineering Congress & Exposition*, Lake Buena Vista, FL, IMECE2009-12148, 2009.

[44] National Safety Council, "Accident Prevention Manual for Business and Industry," Engineering and Technology, 11th edition, Itasca, IL, 1997.