https://ntrs.nasa.gov/search.jsp?R=20110015770 2019-08-30T17:30:03+00:00Z

The Parable of the Boiled System Safety Professional: Drift to Failure

C. Herbert Shivers, NASA Marshall Space Flight Center, Huntsville, Alabama, USA
Keywords: failure, resiliency, vigilance

Abstract

Recall from the "Parable of the Boiled Frog," that tossing a frog into boiling water causes the frog to jump out and hop away while placing a frog in suitable temperature water and slowly bringing the water to a boil results in the frog boiling due to not being aware of the slowly increasing danger, theoretically, of course. System safety professionals must guard against allowing dangers to creep unnoticed into their projects and be ever alert to notice signs of impending problems. People have used various phrases related to the idea, most notably, "latent conditions," James Reason in Managing the Risks of Organizational Accidents (1, pp 10-11), "Drift to Failure," Sydney Dekker (2, pp 82-86) in "Resilience Engineering: Chronicling the Emergence of Confused Consensus in Resilience Engineering: Concepts and Precepts, Hollnagel, Woods and Leveson, and "normalization of deviance," Diane Vaughan in The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA (3)." Reason also said, "If eternal vigilance is the price of liberty, then chronic unease is the price of safety (1, p 37)." Our challenge as system safety proferssionals is to be aware of the emergence of signals that warn us of slowly eroding safety margins. This paper will discuss how system safety professionals might better perform in that regard.

Introduction

Decker calls the "drift to failure" the greatest risk to today's safe socio-technical systems. "'Drifting to failure' is a metaphor for the slow, incremental movement of systems operations toward (and eventually across) the boundaries of their safety envelope (4, p 82)."

People within the system do not recognize the drift because of decisions made with incomplete knowledge in the face of competition, scarcity, etc. All within the system seem to side along with the movement toward the boundaries. "Even if an operational system is 'borrowing more from safety than it was previously or than it is elsewhere by operating with smaller failure margins, this may be considered 'normal,' as the regulator approved it (4, p 82)."

The departure is slow and incremental and everyone goes along with the changing definitions of what is risky or safe. The departures are not considered significant and are seen as adaptive, but eventually what is considered 'normal' might be highly negotiable or subject to various pressures. In my mind as I read these words I think of the parable of the boiled frog, group think, and normalization of deviance.

Background

How do we know that we are drifting toward failure? What data or metrics exist that we can rely on to make sure that we avoid making the decisions or doing the things that take us along that path to failure? Do we rely on doing the best we can and serendipity to get us there? Serendipity has certainly been my friend over the years, as I suspect it has for many people. While we must always be ready to recognize the arrival of serendipity and take advantage of its blessings, serendipity is not good engineering strategy. Carl Metzger, in a book review of Merton and Barber's "The Travels and Adventures of Serendipity," for Professional Safety Magazine (5), points out that the authors say,

"The opportunity for serendipity in loss control presupposes that preventing losses is a scientific enterprise rather than a sociopolitical, legal-regulatory quagmire. Applying what is known from science to preventing losses is where the opportunity rests for making discoveries, by accident and sagacity." We are warned, however, that while "happy accidents and sagacity can expand the field of loss control solutions," we need to "avoid joining the run for this year's injury prevention panacea." So, while serendipity might help us, we certainly should not base a strategy on it.

We need to consider more scientific data including determined or even highly supposed causes and effects if we are to make real progress on having information with which to make sound decisions. If a model for determining that drift has set in or is beginning to occur is useful, then we need to base that model on sound reason.

In trying to determine a model for the drift, Decker indicates that large systems are very complex with dynamic relationships. However, Decker identifies a 'sacrificing decision' as key to understanding the drift. In short, management makes a sacrificing decision to reduce production pressure to reduce risk, for example. "The decision to value production over safety is often implicit, and any larger or broader side effects that echo through an organization go unrecognized (2, p 83)."

The result is riskier organizational and individual behavior, more so than desired in retrospect. A serious failure is sometimes the only thing that brings about awareness of the drift that has already occurred.

Sacrificing decisions are usually set against judgment criteria, schedule and budget pressures, etc., such that the decisions seem to be very sound. Short term incentives tend to drive the decisions within the context of the decision maker's knowledge, goals and focus at the time. Many times in retrospect, the sacrificing decision needs not to have been made because "nothing happened (2, p 83)." That is, the intended result did not come to be. Without good criteria about soundness of decisions as they are being made, we tend to move toward the safety margin boundaries. In essence, all decisions might be seen as sacrificing since they likely involve trade-offs (2, p 84)

"It would seem … that safety and risk in complex organizations are emergent, not resultant, properties: safety and risk cannot be predicted or modeled on the basis of constituent components and their interactions." Given that, a simile such as 'drift' better guides thinking about the change in behavior than would an imperfect model (2, 84). However, even if we cannot model drift, even if safety and risk might not be "resultant," might we not still improve our decision making toward loss control by attempting to determine and monitor manifestations that seem to indicate that drift is occurring? I think that enterprise is worthy.

In the spirit of Reason's Swiss Cheese model (1, pp 9-13), what happens when we make decisions, sacrificing or otherwise, regarding our design and engineering rigor is that we might either make the holes in the cheese larger, shift the position of the holes, or create more holes, or make the holes smaller or fewer. I think we might do all from time to time, making the alignment of the holes in the barriers more likely to line up and result in the failure if we are not smart enough or are unlucky enough. Decker points out that the emergent and nonlinear nature of safety and risk, perhaps we need to add a dimension to the Swiss Cheese and assume that the holes need not align as the "force" may change direction and find its way through an adjacent opening, hence we need to focus on decreasing the total amount of permeability in the barrier rather than the alignment. We shall focus on the "dark side" of Swiss Cheese hole alignment for purposes of this discussion, that is, things that go wrong.

I am particularly interested in this phenomenon as NASA begins to formulate and develop the Nation's next space launch vehicle, along with implementing a different model of commercial sector involvement with development of crew capable launch vehicles. Decisions the Nation makes now will set the foundation for the future success of the Nation's deep space exploration program and decisions we make as the programs and the vehicles mature will subject our program to possible occurrence of this "drift." Ultimately, we as an organization will act within our beliefs relative to where we are in relation to our safety boundaries. When I read Decker's words, I wondered if

proposed changes to models of insight and oversight, for example, might be a drift toward safety boundaries. I suspect that it is, we just don't know how close to the edge or how much of our margin we use in the drift, and therefore need to be conscious of what we decide (sacrificing) to do and its potential system impacts. In the manner of sacrificing decisions, do we know that we actually buy what we intend in the long run by making that decision?

Decker seeks a predictive model for drift to failure or questions whether a model can exist, and postulates that measuring the difference between the operational system designed and the system actually being operated or implemented might be a good start for predicting risk (2, pp 86-90). That is, the system imagined by management is usually different from that implemented on the floor by the technicians, for example, as "better and more efficient methods" are created and employed as the work is performed. I shall not attempt to recreate Decker's work or attempt a model or attempt to identify the panacea, the single best indicator to highlight, but rather seek to find several characteristics to monitor that might provide information upon which to judge risk and determine a drift to failure.

Examples

I've taken somewhat at random several examples of fairly well-known system failure case studies developed by NASA and made available via a public web site. http://pbma.nasa.gov/index.php?fuseaction=pbma.archive (All the following examples are from this NASA web site and hence, are not further cited herein (6).) From those case studies, perhaps we can get some indication on how we might sense drift to failure as it happens. Contributing issues will be provided as a top level summary and not developed in this paper. Interested readers are encouraged to seek out detailed discussions as they wish. Certainly these contributing issues were determined after the fact, but perhaps we might find indicators in them that can be seen before the fact and provide us the tool for sensing a drift to failure.

Chernobyl

On April 26, 1986, two huge explosions blew apart Unit 4 of the Chernobyl Nuclear Power Plant in the Ukrainian SSR. At least 31 workers and emergency personnel were killed immediately or died from radiation sickness soon after the accident. The nearby village of Pripyat, where most Chernobyl plant workers lived, some 200,000 residents, was evacuated and sealed. Radioactive debris was carried by clouds over most of northern Europe. Long term effects still being debated, but increased childhood thyroid cancer in Belarus and Ukraine is tied to the accident.

RBMK reactors ("High Power Channel-type Reactor") possess a number of design features that are considered by Western engineers to be too risky for operation as commercial power plants: Kinetic instability features (can develop local hot spots, and are more difficult to control), old technology instrumentation and control functions inferior to Western equivalents, the RBMK design does not provide for a reactor containment, Aluminum fuel channels were used for cost reasons instead of safer, but more expensive Zirconium alloy (used in US), all U.S. and Western reactors have containment as a critical risk mitigation design feature. But all these design weaknesses did not initiate the Chernobyl accident; they exacerbated its consequences.

Against the advice of the Chief Reactor Operator, the political leader of the plant ordered an unauthorized experiment. The purpose of the experiment was to determine if, in case of a power outage, the kinetic energy of the spinning turbines could maintain the cooling pumps until the emergency diesel generators turned on. Inadequate prior planning and training (for the experiment), combined with poor operational hazard controls resulted in a botched experiment, and an unsafe outcome. The reactor core heated to over 5000 C and parts of the core melted. Molten core metal in contact with water produced hydrogen and the ensuing explosion blew the top off the reactor. A second explosion followed.

The Chernobyl accident was the result of two cause factors: 1) RBMK reactor design weaknesses, and 2) deficient safety culture: the deliberate violation of safety rules, combined with lack of proper planning.

DC-10 Cargo Door System

In 1969 per FAA requirements, Douglas, manufacturer of the DC- 10, asked the Convair Division of General Dynamics, a subcontractor, to perform Failure Modes and Effects Analysis (FMEA) of the DC-10 cargo door system. The FMEA uncovered nine sequences that would potentially threaten life. One of the sequences was failure of the locking pin system causing the door lock not to latch when the door was closed. As a result of this sequence, the door could fly open in flight causing sudden depressurization and possible structural failure of the floor and damage to the tail. The draft FMEA was modified by Douglas to minimize the design deficiency. A ground test failure in May 1970 was blamed on human error, but, in retrospect, poor design was downplayed as a root cause.

During November 1970, internal memos between Convair and Douglas discussed proposed fixes to the cargo door problem but none was implemented. The FAA certified the DC-10 on July 29, 1971 with an unsolved design deficiency.
On June 12, 1972, the cargo door of an American Airlines DC-10 in flight from Los Angeles to New York burst open at 11,500 feet because of a cargo door locking pin failure, resulting in decompression of the aircraft and temporary loss of control of the aircraft. Skillful and heroic acts by the crew resulted in safe landing and no fatalities. Per NTSB investigation results, the FAA drafted an order that would have grounded the DC-10 until the needed design changes were made. In the famous "Midnight Gentlemen's Agreement," the President of Douglas convinced the FAA Administrator not to ground the DC-10.

In March, 1974, a Turkish Airline DC-10 crashed in France killing all 346 people aboard. The cause of the accident was faulty latches on the cargo door which allowed the differential pressure in the cabin at 11,500 feet altitude to force the door to swing open to the outside of the plane where it was ripped open off its hinges by the air stream. After the accident, the entire DC-10 fleet was finally grounded and the cargo door locking system was redesigned and the problem eliminated.

A safety analysis is no better than the system we have in place to deal with it. A test failure that does not go to root cause is a missed opportunity to prevent future mishaps. A close call should be treated as an opportunity to prevent a mishap.

Bhopal

During the nights of December 2 and 3, 1984, a Union Carbide plant in Bhopal, India, began leaking a deadly gas called *methyl isocyanate (or MIC)*. No safety systems designed to contain such a leak were operational, allowing the gas to spread throughout the city of Bhopal. Half a million people were exposed to the gas. About 8,000 died the first week and 20,000 have died to date (circa 2005). More than 120,000 people still suffer from ailments caused by the accident and subsequent pollution of the plant site.

Six safety systems were designed to control a MIC gas leak hazard. None of the systems functioned when needed. On the night of December 2nd, when an employee was flushing a corroded pipe, water flowed into the largest MIC tank. An uncontrolled reaction ensued, blowing the tank off its concrete sarcophagus and spewing a deadly cloud of chemical which was carried by prevailing winds and settled over much of Bhopal. The proximate cause of the accident was water leak into MIC tank due to pipe failure. Contributing causes were failures of or lack of all 6 safety controls.

Extremely poor maintenance practices and the absence of modern safety procedures and critical configuration management were the next level of causes. The root cause was company management negligence and incompetence. When we operate in a controlled hazard environment, where controls are necessarily limited, we often operate with "accepted risk." We formally accept risk based on reasonable mitigations. We must continuously ensure that controls and risk acceptance rationale remain in place.

BP Texas City Refinery

On March 23, 2005, a BP Texas City Refinery distillation tower experienced an overpressure event that caused a geyser-like release of highly flammable liquids and gases from a blowdown vent stack. Vapor clouds ignited, killing 15 workers and injuring 170 others. The accident also resulted in significant economic losses and was one of the most serious workplace disasters in the past two decades. The total cost of deaths and injuries, damage to refinery equipment, and lost production was estimated to be over $2 billion.

From the Chemical Safety Board (CSB) report, the proximate cause was overfilling the distillation tower resulting in the over pressurization of the blowdown drum.

Underlying Issues include: the design lacked a flare on the vent stack and had an inadequate liquid level detection system; failed operating procedures due to insufficient training and oversight; deferred safety-related maintenance and ignored abnormal behavior from level detectors, control valves, and alarms; and proximity of trailers to hazardous sites.

There was a history of abnormal startups in system including recurrent high liquid levels and pressures. There had been four other serious flammable material releases from the system that lead to ground level vapor clouds between 1995 and March 23, 2005; fortunately none ignited. The system was operated without a flare stack on the vent since its construction in the 1950s. The previous owner replaced the system in kind in 1997, not updating it to include a flare as recommended by corporate refinery safety standards. In 1992 OSHA cited a similar blowdown drum and stack at the Texas City refinery as unsafe because it vented flammable material directly to the atmosphere, but the citation was dropped and the drum was not connected to a flare system.

Other items the CSB noted include: inadequate and nonfunctional instrumentation; serious concerns regarding effectiveness of hazard analyses, change management, and mishap investigation; management of employee fatigue, downsizing of supervision, training and critical staff, and handling of obsolete equipment.

Statement by CSB Chairman Carolyn W. Merritt: "Almost every executive believes he or she is conveying a message that safety is number one. But it is not always so in reality."

The USS THRESHER

In the early years of the nuclear Navy, the most advanced submarine in the world sank during testing and was ultimately crushed by water pressure due to a chain of events that ostensibly started with a small leak of seawater. If so, the sub was destroyed by the simplest of causes—bad brazing in some of its pipes. The disaster killed all aboard the sub and led to the revamping of many of the manufacturing processes for both surface and undersea US naval vessels. The disaster also helped spur the development of deep-sea exploration vehicles. The best theory about what happened, based on the Naval investigation report, is that some pipes had started to leak in the submarine's engine room. These leaks allowed electrically conductive seawater to get into the electronics that controlled the nuclear reactor, which in turn shorted out and shut the reactor down.

The crew presumably attempted to restart the reactor and probably also attempted to get their crippled vessel back to the surface, which would explain the "positive angle" as they attempted to point upward and climb with the propellers. Without the reactor, however, the crew would have been relying on auxiliary power, with far weaker

thrust than the reactor provided. The sub probably also had negative buoyancy, meaning that it would sink if no active measures were taken, and simply didn't have enough thrust to lift its weight to the surface. In order to lighten the vehicle, so that the weakened propellers could get it to the surface, or even allow the sub to float up on its own, the normal procedure would be to blow the water out of the ballast tanks and fill them with air, increasing the submarine's buoyancy. That the sub's crew were attempting to do so is evidenced by the next message from the stricken craft, shortly after the first troubling message—"Attempting to blow." The microphone then picked up sounds of compressed air being blown through the lines to the ballast tanks. At this point, Navy investigators believe, based on tests performed later on another vessel, strainers in the lines upstream of the ballast tank valves iced up because the high volume of air moving past the strainers at such high velocity would have caused them to cool rapidly. Icing of the strainers would have reduced the air flow such that either the tanks could not be cleared at all, or at least not fast enough, because the boat continued to sink. There was only one more ominous voice communication: ."..test depth."

According to the Navy investigation, the proximate cause of the disaster was the leak of seawater into the reactor control electronics. This shut down the reactor, resulting in the inability of the boat to control itself or get back to the surface. According to published reports, there were perhaps several factors that came together to destroy the USS Thresher and its crew. The leak itself probably occurred because of faulty brazing of the piping at the shipyard. Prior to the USS Thresher loss, the installation procedure for pipes less than four inches in diameter was to put a silver ring at the joint between two points and braze the joint with a torch. Subsequent investigation of other ships after the accident showed that, though joints created in this manner appeared solid, when broken apart there was no silver in the joints, indicating much weaker joints than had been previously estimated. In general, the design and standards for the non-nuclear portions of the vessel seemed to have been more lax than those for the nuclear reactor and its associated systems.

The icing of the line strainers, resulting in the failure to empty the ballast tanks of water fast enough, also contributed to events. This latter problem was a failure to meet design specification. Had either of these methods for surfacing been effective, the reactor loss would likely not have been catastrophic, because the crew could have dealt with the leaks and reactor problems on the surface. Finally, had the testing occurred in shallower water (perhaps with the ocean bottom just slightly below test depth), in which the USS Skylark could have potentially come to their aid, the crew might have been saved, if not the USS Thresher.

In summary, the deficiencies leading to the disaster include: Deficient design (ballast tank blow failure); deficient fabrication practices (insufficient brazed joint bonding), deficient quality assurance (inadequate ultrasonic inspections), and deficient operational procedure (difficult access to vital and damage susceptibility of equipment under emergency conditions).

TWA 800 In-Flight Breakup

Trans World Airlines (TWA) flight 800 was only twelve minutes into a July 19, 1996 trip from New York to Paris when an in-flight explosion destroyed the passenger jet, plunging it into the Atlantic with 230 people on board. Flight 800 was destined for Paris, France, and because the distance from New York to Paris did not require additional fuel, the center wing fuel tank (CWT) only contained a relatively small amount of fuel that remained from the inbound flight. After the 230 passengers and crewmembers boarded, they waited through an hour-long delay when a disabled ground service vehicle blocked the airplane at the gate. At 8:19 pm, TWA 800 departed JFK. The aircraft reached its assigned altitude of 13,000 feet without incident, but at 8:29 pm, the cockpit voice recorder (CVR) recorded the captain saying, "look at that crazy fuel flow indicator there on number four…see that?" Immediately following this comment, the pilots received air traffic control instructions to climb to 15,000 feet. At 8:30, the CVR recorded the captain ordering, "Climb thrust." The flight engineer replied, "Power's set." Then at 8:31, as the 747 approached 14,000 feet, the CVR recorded interruptions in the background electrical noise, a "very loud sound," and an unintelligible word. The CVR and flight data recordings then terminated abruptly.

After an exhaustive investigation, the NTSB determined that "the probable cause of the TWA flight 800 accident was an explosion of the center wing fuel tank, resulting from ignition of the flammable fuel/air mixture in the tank." The source of ignition energy for the explosion could not be determined with certainty, but, of the sources evaluated

by the investigation, the most likely was a short circuit outside of the CWT that allowed excessive voltage to enter it through electrical wiring associated with the fuel quantity indication system. Contributing to the accident was a design and certification concept that fuel tank explosions could be prevented solely by precluding all ignition sources. The design and certification of the Boeing 747 with heat sources located beneath the CWT without means to reduce the heat transferred into the CWT or to render the fuel vapor in the tank nonflammable also contributed to the accident.

B-747 uses Jet-A fuel from seven fuel tanks. Each wing contains three tanks, and the lower fuselage holds a seventh tank known as the center wing fuel tank (CWT). Whenever the six wing tanks hold sufficient fuel for a flight, the CWT only contains residual fuel from the last flight. Inches below the CWT, three air-conditioning packs rest in an un-insulated, unvented area. The CWT absorbs the heat generated by the air-conditioning packs. Testing found that a near-empty tank heats quickly, speeding fuel evaporation and increasing flammability of the ullage (the unfilled portion of the tank above the surface of the fuel).

The Fuel Quantity Indication System (FQIS) includes probes and compensators connected in series inside each fuel tank. The minimum ignition energy for hydrocarbon fuels is 0.25 millijoules (mJ). To keep vapor in the fuel tanks from igniting, power supplied to FQIS wiring was intended to have a limit of 0.02 mJ. FQIS wiring runs from the fuel tanks to the flight decks along raceways shared with other circuits carrying much higher voltages and energies than those allowed in the FQIS.

NTSB determined the probable cause of the accident was an explosion in the center wing fuel tank resulting from the flammable fuel/air mixture inside the tank. NTSB could not determine the ignition source with certainty, but it concluded the most likely was a short circuit outside the CWT that allowed excessive voltage to enter it through the FQIS. Because FQIS wires are the only wires to enter the CWT and because they are co-routed within wire bundles containing circuitry from higher-voltage systems, investigators theorized that a high-voltage circuit contacted FQIS wires due to chafed, frayed, or otherwise damaged conditions. Then, a latent fault on the probes inside the CWT may have caused an electrical arc and subsequent tank explosion.

When FQIS probes went through qualification testing in the 1960's, examiners found the probes to be free of arcing up to 2,000 volts. The FAA thus deemed the probes "explosion-proof." When NTSB investigators tested FQIS components from aircraft that had been operating for more than 30 years (the length of time TWA 800 had been operating), they discovered silver sulfide deposits had accumulated on the probes. The semi-conductive nature of the probes was probably enough to induce an electrical arc in the CWT at minimal voltage. Although the FQIS system displayed explosion-proof capability at the time of aircraft certification, designers did not account for the effects of age upon the system, and once certified as explosion-proof, the probes were never retested.

When the B-747 was in development, it was generally believed that design practices were capable of completely eliminating in-tank ignition sources. Such a conclusion depended on an explosion-proof FQIS system, appropriate wire configuration, and sufficiently sensitive circuit breakers. In addition to discovering latent faults on FQIS components, investigators examined wire configuration on old and new aircraft and discovered that wire layout imposed mechanical wear on insulation that placed the system at risk for failure. The thermally activated circuit breakers with which the aircraft was equipped also proved insufficient. Post-accident testing showed currents of 2 to 4 joules could transfer between wires for as long as 25 minutes without heating a wire to the level required to trip such a circuit breaker.

Soyuz-11 Depressurization

On April 19, 1971, the Soviets launched the world's first space station, *Salyut*. Ground controllers soon discovered that *Salyut*'s OST-I telescope cover failed to jettison properly, limiting achievement of critical scientific objectives. With new non-astronomy objectives hastily assigned, three cosmonauts blasted off aboard *Soyuz*-10 on April 23 to dock with and spend a month on the station. Unfortunately, the *Soyuz*-10 docking apparatus suffered damage during

unsuccessful docking maneuvers, and ground control aborted the mission. To compensate, program leaders planned two more June 1971 flights to *Salyut*.

On June 29, the three cosmonauts transferred mission materials from *Salyut* to *Soyuz* in preparation for the return to Earth. After the crew closed the hatch between the descent vehicle and the orbital compartment, the "hatch open" caution and warning panel light did not turn off. Once the descent module separated from the rest of the spacecraft, that hatch would be exposed to open space. A cosmonaut capsule communicator instructed the crew to open the hatch, and move the wheel (to engage the hatch latches) to the left to open. Close the hatch, and then move the wheel to the right 6 turns with full force. Finally after several attempts and exceeding 6 wheel turns, the light went out. The crew then lowered the pressure on the other side of the hatch in the orbital module to verify the hatch was sealed.

Pressure inside the descent module leaked into the vacuum of space when a pyrotechnic ventilation/equalization valve designed to open when the vehicle reached an altitude of 2.5 miles (4 km) instead opened at a height of 105 miles (170 km). In an effort to determine what caused the valve to open early, engineers simulated varying loads on the valve, and deduced that the pyrotechnic fasteners that should have fired sequentially during capsule separation from the orbital module and descent module fired simultaneously instead. The resultant force jarred a ball joint in the pyrotechnic valve mechanism loose. This forced the valve open and depressurized *Soyuz*-11. Other pyrotechnics blew a valve seal clear at about 4 km altitude per design intent to equalize cabin pressure with the atmosphere—but the prematurely open valve had already done so in vacuum. Analysis of automatic attitude control system thruster firings made to counter the force of escaping cabin pressure, along with the pyrotechnic powder traces found in the throat of the valve determined when the valve had malfunctioned, causing the depressurization.

Once the equalization valve opened, the cosmonauts lacked a backup procedure or control mechanism to close it. They were aware of a pressure leak seconds after it began, but surrounding distractors would have slowed their search for its cause. Noise from the transmitters obscured the leak's telltale sound, and the earlier "hatch open" warning light could have misled them into thinking the frontal hatch seal was involved. The designers included a warning light to notify crewmembers when the hatch seal was insecure. The two ventilation valves (one for air in and one for air out), also paths to vacuum, lacked both a warning system and a closure mechanism. Designers may not have conceived of a failure mode forcing either valve to open and prematurely rupture the seal. Verification testing did not include the higher shock of simultaneous pyrotechnic fastener firing.

Ventilation valve design did not meet the worst-case scenario of structural shock resulting from simultaneous firing of the orbital/descent module separation pyrotechnic system. Ventilation valves design was sensitive to the unanticipated higher shock loads from the explosive bolts firing simultaneously. Ventilation valves did not have associated alarms in the event that the seals somehow opened prematurely, so the crew spent precious seconds searching for the leak's source. Ventilation valves were placed behind the control panel –a location inaccessible to the crew. Ventilation valves lacked a backup closure procedure or mechanism, so once the crew members realized where the leak was coming from, they were powerless to correct the situation.

Based on examination of the hatch and valves, officials determined that air leaked from one of the two ventilation/equalization valves, located behind the control panel. Although the crew would have been immediately aware of the leak, they had to determine its source, so they switched off radio transmitters to isolate the leak's noise. Crew commander Dobrovolskiy's body was found apparently attempting to cover the control panel with a checklist. The crew could not close the valve because it lacked a manual closure mechanism and was inaccessible. Within 40 seconds of depressurization during descent, the crew suffocated.

Minneapolis Bridge Collapse

On Wednesday, August 1, 2007, the Interstate 35West (I35W) bridge in Minneapolis, Minnesota collapsed into the Mississippi River. Four weak gusset plates fractured under the combined burden of rush hour traffic, concentrated construction equipment and previous, heavy renovations on the bridge. Of the 190 people on or near the bridge, thirteen died and 145 were injured.

The newly constructed bridge opened to traffic in 1967. Ten years later the State added two inches to the deck thickness, increasing the dead weight load by 13.4%. In 1991, inspectors labeled bridge "structurally deficient." (Not uncommon for this bridge design; 31% of this bridge type was labeled this way.) In 1994, inspectors reported gusset plate rust, corrosion, and section loss, but no corrective action was indicated as needed. Four years later, the State installed a median barrier to the bridge decking that increased dead loading by another 6.1%. Photographs taken in 1999 show bowed gusset plates that inspectors dismissed as an artifact unchanged since original construction. In June 2007, contractors begin resurfacing the bridge.

At 2:30 p.m. on the day of collapse, contractors placed equipment and materials for the concrete pour on the bridge deck. At 6:05 p.m. during evening rush hour traffic, the gusset plates fracture, causing the bridge to collapse.

The gusset plates were half as thick as the design loading required. A design calculation error escaped contractor quality checks. State design review did not provide a full verification of design work (not unusual). Inspectors assumed gusset plates to be stronger than the attached beams. Inspectors failed to report the bowing of gusset plates for at least eight years prior to collapse assuming this to be an artifact present since construction. Inspectors reported corrosion but did not record dimensional changes (reduction of section thickness due to corrosion) to gusset plates over time.

Renovations in 1977 and 1998 increased the dead weight load by 19.5% over the original design rated load. Contractors placed heavy equipment and material load in a concentrated area on the bridge deck. Rush hour traffic loads further stressed the bridge structure.

The Valero Refinery Fire

On February 16, 2007, propane gas leaked from the McKee Refinery's Propane Deasphalting Unit in Sunray, Texas. As winds carried the vapor cloud, a spark ignited the propane and the entire cloud burst into flames. The fire spread quickly, forcing evacuation of the refinery as firefighters battled the blaze. Three workers suffered serious burns and the refinery was shut down for two months.

In 1992, a control station in the PDA unit was shut down. Rather than remove or positively isolate the idle subsection, operators simply closed the six-inch valves around this section, intentionally creating a "dead-leg" of pipes that were supposed to have nothing flowing through them. Unfortunately, a foreign object blocked one of the valve seats, preventing the valve from sealing completely. Sometime during the isolation period of fifteen years, water passed through the jammed valve and settled. Although the operating sections had freeze protection, the "dead-leg" did not.

In February 2007, a four-day cold front froze the trapped water in the dead-leg, causing the water to expand and crack the pipe. When the ice thawed, propane escaped through jammed valve and out the crack at 4,500 pounds per minute. Wind carried the propane vapor cloud toward a boiler house, where it likely found an ignition source. A high-pressure propane jet fire launched into a steel column supporting a pipe bridge filled with petroleum products, further fueling the fire. The fast propagation of the fire prevented operators from closing the manual valve shutoffs to cut off the fuel for the fire. The fire was finally extinguished approximately 24 hours later.

There was no record that the refinery conducted a formal management of change review when the control station was taken out of service. Valero did not have a formal written program to identify, review or freeze-protect dead-legs and other infrequently used piping. A Process Hazard Analysis (PHA) performed by the previous refinery owner in 1996 identified the need for remotely operated shut off valves (ROSOV's). None were installed; yet the

action item was checked complete. Valero's 2006 PHA did not revisit findings from the 1996 PHA and violated its own requirements by not installing the ROSOV's.

Fire-proofing standards required fire protection for piping within 50 feet of a potential source. Steel columns within 30 feet of the PDA unit had been fireproofed, but unprotected pipe 77 feet away was not fireproofed and collapsed in the fire. The unprotected pipe was listed in a loss-prevention report as a fireproofing "top-priority" but had not been fireproofed by February 2007.

X-31 Mishap

On the morning of January 19, 1995, a final series of flight tests was conducted for the first of two aircraft built for the X-31 Enhanced Fighter Mobility Demonstrator program. While executing a sequence of maneuvers for the third and final flight of the day, the pilot noticed a discrepancy in his air speed indication. About two minutes later, the aircraft began to oscillate out of control, pitched up violently, departed into a spin, and crashed. The pilot ejected safely and was recovered less than one mile from the crash site. An investigation of the X-31 crash examined the mechanical, procedural, and human systems that supported X-31 and continue to support projects throughout the aerospace community.

The X-31 program began in the early 1980's to explore the tactical utility of a thrust-vectored aircraft with advanced flight control systems. The X-31 aircraft was designed specifically for this task, with large paddles to redirect exhaust flow as well as an advanced "fly-by-wire" flight control system. Thrust vectoring refers to an aircraft's ability to redirect the thrust from its main engine in a direction other than straight backward.

On January 19, 1995, during a routine flight test, the X-31's flight control computers (FCC) began registering errors in flight data about 20 minutes after take-off. No one knew that ice was accumulating and blocking air flow around the 'Pitot tube' (used for measuring air speed). Later in the flight, the pilot noticed further errors in airspeed indication, prompting him to notify the control room and turn on the Pitot heat. The control room notified the pilot that the Pitot heat might not be hooked up. Shortly after this message, the aircraft began to oscillate out of control and then violently pitched upward. The pilot ejected before the aircraft departed into a spin and impacted the ground.

Pitot tube icing caused incorrect total air pressure data to be sent to the FCCs by the Pitot-static system. Pitot tubes are susceptible to accumulation of ice which causes them to malfunction. Accurate airspeed measurements were especially critical to the X-31's FCCs which were responsible for vectoring thrust to keep the aircraft stable and on course.

In the original X-31 design, the Pitot tube was mounted on a "Rosemount probe" which had a heater to prevent Pitot tube icing. To improve performance, the Rosemount probe was replaced with a Keil probe which did not have a heater.

The risk of iced Pitot probe was identified in the hazard analysis, but because of the low likelihood of occurrence, not all failure modes were addressed. When the Kiel probe was installed, the probe was not equipped with Pitot heat as the Rosemount probe had been. Yet, only a limited number of flight personnel were aware of this change. Configuration change documentation was not routed to the test team and no placard was placed in the cockpit near the Pitot heat switch. Operating procedures for the Kiel probe were not reviewed and distributed. Pitot icing risk was not included in pre-flight brief to the pilot because the hazard analysis didn't label Pitot icing a "critical hazard." An available reversionary flight mode was not put into effect because the flight team had not tested/trained with it properly. The test flight also incorporated a chase plane that followed along to assist in observing the flight. In typical test flights, chase pilots are included in "hot mike" conversations and serve as an extra set of eyes to help maintain flight safety during tests and maneuvers. There was lack of communication between the X-31 and the chase plane because of faulty "hot mike" technology. The "hot mikes" had been disabled due to excessive static.

Issues and Solutions

The system failures discussed share some common issues and exhibit some unique issue. Various solutions exist for the many system failures described. Here are some issues and solutions in no particular order, but loosely grouped by commonality, that apply to one or more of the failures:

Design

Consider environmental effects on a process, especially when environmental changes are intermittent or cyclic rather than constant.

Calculate actual energy releases possible within a system to be realistic when estimating safety margins.

Include ‘damage control’ capability into the system where mass and other considerations allow.

Complex systems can defeat attempts to ensure comprehensive human understanding of designs.

Eliminate common cause failures through proper design for failure tolerance and appropriate analysis of accident scenarios.

Provide sufficient resources (funding, education, expertise) for a proper design review.

Develop controls that detect and correct latent conditions in unused equipment or facilities.

Isolate sources where high energy release potential exists, to contain component or assembly failures from initiating a chain reaction leading to system failure.

Design intent can be inadequately communicated or misinterpreted as the design progresses through its life cycle.

Products in the concept phase of the project life cycle should account for the effects of age and include a means to later analyze the system’s integrity.

Test

Design engineers must test critical components versus worst case off-nominal events to uncover single-point failures.

Aggressively test critical hardware/software systems in nominal and off-nominal operational regimes to flush out latent design defects and test assumptions.

Analysis

Prove a system is safe. Actual system performance is indifferent to human assumptions.

Use a systematic approach and technical expertise appropriate to the task.

Rigorously apply analyses and properly interpret the results.
Conduct and verify hazard analyses to determine where and how hazards might arise.

Encourage and reward hazard identification beyond any checklist used for inspection.
Hazard analysts may be more challenged to deduce or discover failure modes overlooked during design than by quantifying risk inherent to known scenarios.

Configuration Management

Exercise quality control in the design process and over the design products.

Assess and evaluate adverse impact to systems when replacing components or removing portions of the system from design. Ensure the changes do not compromise safety, system efficiency, and system life cycle.
Assess all the impacts to the original design when modifying, especially when use has changed and the design is well into its expected life.

Ensure effective communication and rigorous configuration management, even with operationally mature programs and projects.

Risk Management

Consider both the likelihood and consequence of risk – even a very unlikely event could jeopardize mission success and crew safety.
Plan for contingencies, understand systems well enough that teams can react to and handle unplanned contingencies as well.

Review decisions to 'mothball' a system and, if sections must remain, render them inert (incapable of energy release).

Continue questioning initial assumptions about operations, equipment, and facilities.

Sustaining rigorous maintenance and quality checks underscores recognition that failure modes cannot always be identified at the time of a product's inception.

Maintain the level of rigor required to effectively understand and manage program risks.

Project Management
Schedule is an important element of any program, but when it becomes the big driver, leaders must ensure they understand the risks to performance and safety, and mitigate appropriately.

We must not let schedule define our test program, but rather, let it be defined by risk and technical performance … allow for the chance that we may need another test before we "go operational."

All project team members must fully understand and implement program processes and procedures.

Conclusion

Common and unique issues contribute to system failures. This paper has merely touched on the concept of drift to failure as a cautionary message. What, then, is the point?

The point is that, in the words of James Reason, "If eternal vigilance is the price of liberty, then chronic unease is the price of safety (1, p 37)."So what should be the focus of our chronic unease? I submit that the following suggestions, gleaned from the foregoing discussions, are but a start. Managers and leaders, design team members, fabricators and assemblers, analysis and assurance personnel, and others associated with operating and maintaining systems, need to pay attention to identify the manifestation of individual and collective behaviors that might indicate slips in rigor or focus or decisions that might eat away at safety margins as our system drifts to failure.

During the design phase the design team must consider whether necessary imagination is imparted to identifying all the various extreme environments the system might encounter. If vigorous discussion doesn't routinely take place regarding whether a particular environment is likely possible or not, or on a number of other design issues, someone must ask why. If people resolutely accept design decisions and alternative selections without questioning why or asking what if, someone must ask why. Someone needs to ask about common cause failures and find out how common cause failures are identified and eliminated in the design.

Someone must ask what happens to the components of the system over time and if maintainability has been designed into the system. If a complex design is not rigorously discussed so that all understand its nuances, someone must ask why. If all energy sources and proper robust controls are not included in a design analysis, someone must ask why. If design reviews are hurried and review teams are minimally staffed, if certain design elements are not included or are ground rules out, someone must ask why. If as the design matures, someone does not go back to the beginning and make sure the design is meeting original intent, someone should ask why. If laid by or inactive facilities or systems are not vigorously analyzed for hazards, someone must ask why.

If little insight and oversight are planned in the project plans, someone should ask why. If insight and oversight activities seldom find any issues, someone should ask why. If insight and oversight activities are reduced and related risk discussions do not include the impacts, someone should ask why.

If test protocols do not include expected off nominal conditions, someone must ask why. If test preparations and plans do not have adequate scrutiny in pre-test reviews, someone must ask why. If test results aren't brought back for discussion before the larger project team, someone must ask why.

If the project team is directed to prove the system is not safe in order to make their arguments, someone should ask why. If analysis teams are not staffed with appropriate expertise, if hazard analyses are not given due credit and consideration rather than being after thoughts, if hazard analyses do not affect design, then someone should ask why. If analyses are not rigorous and systematic, if analysts are not challenged to support their results, if interpretations are not questioned for clarity, someone should ask why. If hazard analyses don't go beyond the normally expected scenarios and routine failure modes, someone should ask why.

If Configuration Management is not a rigorous activity, someone should ask why. If change requests flow through a change review board with little or no discussions or difficulty, or simply are approved outside the board, someone should ask why. IF changes are not evaluated for impacts to safety, to efficiency and effectiveness and to design life, someone should ask why. If project team members do not get full awareness of changes, if change orders are not quickly added to project documentation and if there is not an efficient closed loop verification system that ensures change orders are reflected in documents and implemented in hardware, someone should ask why.

If there is no routinely held discussion of project risks, someone should ask why. If risk management discussions do not include lively debate and questioning, someone should ask why. If risk management documentation does not reflect changes as the project matures, someone should ask why. If risk mitigation plans do not encompass all reasonably foreseen contingencies, someone should ask why. If mitigation plans are not robust enough to encompass contingencies beyond the experience base, someone should ask why. If discussions generally result in likelihood or severity being reduced, someone should ask why. If no one asks about assumptions, if assumptions are not clearly described and justified, someone should ask why. If risks to inactive facilities or systems are only

slightly addressed, someone should ask why. If innovations and creative method are not vigorously analyzed and discussed relative to risk, someone should ask why.

When schedule is the dominant discussion in team meetings, someone should ask why. When risks are evaluated primarily to their impact on schedule, someone should ask why. If needed tests are dropped from the schedule, someone should ask why. If schedule slack to add additional tests is eliminated, someone should ask why. If everyone is not trained in and does not demonstrate understanding of project processes and procedures, someone should ask why.

If everyone is always in agreement and things always run smoothly, someone should ask why.

Decker (1, p 92) says that we must constantly check our ideas about reality versus what is reality if we are to predict (I say prevent) the *next* accident. If the "ask why" statements in this paper help us to consider whether our project environment is different from what we think it should be, then a useful tool or idea is presented her for you. If we learn to pay attention to what we should expect and compare that to what we get, maybe, unlike the boiled frog, we can ask why the temperature around us seems to be rising and instead of just adjusting to the temperature or ordering a cool drink, we find a way to make the environment correct.

In short," someone" must be paying attention to the potential signs of drift to failure and must speak up. Who is "someone?" All of us.

References

1. James Reason, Managing the Risks of Organizational Accidents, Ashgate, Burlington, VT, 1997.
2. "Drift to Failure," Sydney Dekker (pp 82-92) in "Resilience Engineering: Chronicling the Emergence of Confused Consensus in Resilience Engineering: Concepts and Precepts," Hollnagel, Woods and Leveson, Ashgate, Burlington, VT, 2006.
3. Diane Vaughan, "The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA," the University of Chicago Press, Chicago, 1996.
4. Hollnagel, Woods and Leveson, Resilience Engineering: Chronicling the Emergence of Confused Consensus in Resilience Engineering: Concepts and Precepts," Ashgate, Burlington, VT, 2006.
5. Carl Metzger, book Review for Merton and Barber, "The Travels and Adventures of Serendipity," in Professional Safety Magazine, April 2011, pp 14-15.
6. NASA Systems Failures Archive, http://pbma.nasa.gov/index.php?fuseaction=pbma.archive

Biography

Dr. Charles H. "Herb" Shivers, acting director of the Safety and Mission Assurance Directorate at NASA's Marshall Space Flight Center in Huntsville, Ala., is responsible for safety, reliability and quality assurance of the full range of Marshall Center programs, projects and institutional services in support of NASA mission goals, including space shuttle, space station, space exploration and Marshall facility safety and quality activities. He also provides technical and managerial guidance associated with related engineering, scientific and program management activities. Dr. Shivers was appointed by the NASA Chief Engineer as the NASA System Safety Engineering Technical Warrant Holder from March 2005 to July 2006, ensuring certain safety requirements on the space shuttle were met for Shuttle Return to Flight. In October 2006, Dr. Shivers was appointed to the Senior Executive Service, the personnel system covering top managerial positions in approximately 75 federal agencies. Dr. Shivers earned a bachelor's

degree in industrial engineering from Auburn University, a master's degree in industrial and safety engineering from Texas A&M University, and a doctorate in industrial and systems engineering and engineering management from the University of Alabama in Huntsville. Dr. Shivers also graduated from the US Army's Graduate Safety Engineering Intern Program.