System Safety and the Unintended Consequence

Clifford C. Watson, CSP, NASA Marshall Space Flight Center, Huntsville, Alabama, USA

Keywords: unintended, consequence, analysis

Abstract

The analysis and identification of risks often result in design changes or modification of operational steps. This paper identifies the potential of unintended consequences as an over-looked result of these changes. Examples of societal changes such as prohibition, regulatory changes including mandating lifeboats on passenger ships, and engineering proposals or design changes to automobiles and spaceflight hardware are used to demonstrate that the System Safety Engineer must be cognizant of the potential for unintended consequences as a result of an analysis.

Conclusions of the report indicate the need for additional foresight and consideration of the potential effects of analysis-driven design, processing changes, and/or operational modifications.

Introduction

In today's complex world, the System Safety Engineer (SSE) plays an important role when using hazard analyses, failure modes and effects analyses, and other tools that ferret out the myriad of issues that may lead to system failures. It is possible to ask for, or require changes to design, implementation of operational controls, even hardware modifications that may create an unintended consequence. Traditional analysis tends to be rigid; management often tells us "If you bring me a problem, bring me a solution." And so, we sometimes offer 'fixes' that may not be the best solution, in fact, they may lead to serious consequences.

Unintended Consequences In History

Figure 1 SS Eastland capsized at dock

You are boarding the SS Eastland, a passenger ship built in 1903, while it is docked at a Chicago pier on the Chicago River. The date is July 24, 1915. You, and over 2500 other passengers, are embarking on a trip to a company picnic in Indiana. You make your way to the upper deck so you can wave and wish good-byes to your friends on the dock. Suddenly, the boat begins to list; it rolls to port and 844 people die, either from drowning or being crushed by furniture in the cabins that they occupied. Ironically, the 1915 Seaman's Act had been passed earlier that year as a result of the loss of the RMS Titanic. The Act required the addition of lifeboats to the Eastland, which added to

the problem of listing that the ship was known for. Good intentions, exacerbated by poor design and newly imposed regulations were listed as likely contributors to the loss of life.[1]

It's early August in 1919. You are 22 years old and a veteran of the Great War; a war recently ended with the Treaty of Versailles. You are thirsty and go to the ice box; you are looking for a cold bottle of beer, but it is several months after the Eighteenth Amendment to the United States Constitution was passed making the manufacture, transport, or export of liquor illegal.[2] So…what do you do? You walk down the dusty street of your town and visit the Mercantile Store. You nod to the owner and walk past the row of dry goods toward the door marked "Men Only" pushing the door open; then you knock on the right-hand wall and the wall opens to a backroom where you buy a bootleg brew and cool off along with several of your fellow war hero friends. Suddenly there is a commotion outside and the Sheriff, along with several deputies, barges through the door. As the ruckus subsides, the Sheriff has arrested all of the veterans and smashed the keg of beer.

Figure 2 Bootleg Alcohol Raid, Elk Lake Ontario, 1925

So it went. Good intentions led to formerly legal activities being classified as illegal. Gun fights, deaths, broken families, and an underground business that sprung up from the legislation denied the government of taxes while supporting the illegal bootlegging industry.

Fast forward to the 1970's when environmentalists raise the issue of smog and automobile emissions creating an unhealthy environment. One way to reduce the harmful emissions is the reformulation of gasoline by the addition of 'oxygenates'. Two possible candidates emerge – ethanol and methyl tertiary-butyl ether (MTBE). The ethanol requires new production facilities and distribution methods that will take a long time to bring on-line; the MTBE can be produced as a side-stream product of the gasoline production. The Clean Air Act Amendments of 1990 require the use of oxygen-enriched fuels in areas, such as Denver, that have high levels of carbon monoxide.[3] And so, the use of MTBE is expanded. Then, in Santa Monica, California, MTBE is found in drinking water wells; levels much higher than previously measured. This leads to new

Figure 3 Santa Monica Water Treatment/Storage Plant

wells being drilled and storage tanks being abandoned because MTBE has contaminated the tanks and it is difficult to remove. In 1997, the Environmental Protection Agency issued a drinking water advisory that defined the limits of MTBE in drinking water to concentrations below 40 parts per billion (ppb). Air quality improved in the areas where it had been unsatisfactory, but at the cost of drinking water quality in many municipalities, expensive new equipment, and soon, aquifers in outlying areas have become contaminated.

And finally, you are on a well-deserved vacation, flying from Okinawa, Japan, to Tokyo, Japan. It is a smooth flight, something you have become accustomed to since it is an All Nippon Airways Boeing 737-700, one of the world's safest airplanes. The date is September 6, 2011.

Figure 4 ANA Boeing 737-700 in Roll and Descent

Suddenly the plane lurches and rolls violently 132 degrees to the left and noses down at a 35 degree down angle, descending 6000 feet! The plane returns to level flight and continues to the Tokyo airport without further incident.[4]

An investigation finds that the captain had taken a toilet break and was returning to the cockpit. This required the first officer to unlock the door (a requirement following the hijacking of U.S. aircraft on 9/11/01). The door lock switch is located just 4 inches away from the rudder trim switch; to operate the switch, it requires a counter-clockwise turn, coincidentally the same motion as unlocking the cabin door; instead of unlocking the door, the first officer operated the rudder trim switch, pitching the plan into a violent roll and descent.

An overlooked human factors consideration, the placement of the door lock switch, could have created a catastrophic accident taking the lives of an airliner crew and over 100 passengers. Having a design flaw, similar-motion switches in close proximity may have been overlooked during the human-factors analysis of the controls.

How The System Safety Engineer Enhances Safety

Early System Safety was first practiced when the first person to create a wheel found that two wheels with an axle between them could be used to transport heavy loads over long distances if pulled by an animal with brute force capability. Of course, the System Safety Engineer (SSE) noticed that the axle had to be restrained to keep it from sliding outboard or inboard, thereby preventing the toppling of the load. An astute SSE also noted that the load needed to be secured to the axle to keep it attached to the wheels. Another improvement has the tongue attached to the carriage, permitting easy control of the load and beast of burden.

System Safety has developed since those early days. Now, the System Safety Engineer may be involved in aerospace design, warfare design, environmental design, and even social design. The above examples provide proof of this fact.

However, as we have seen in the examples, and probably experienced in our own work life, sometimes the fix creates new, unintended consequences that then require further analysis and corrective action. So to limit the number of these consequences, we, as System Safety Engineers, must expand our concern regarding the effects of our suggested actions.

The OSHA Cowboy

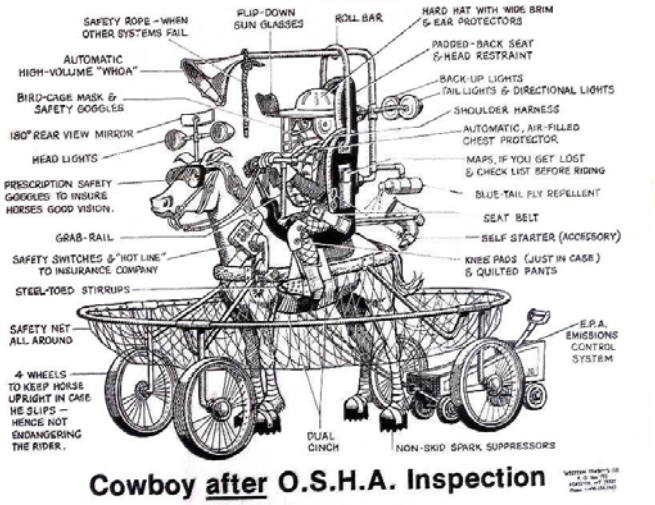


Figure 5 Effects of Over Regulation

This now famous illustration points to the many times that over-regulation creates new problems for the user. The early days of the Occupational Safety and Health Administration were focused on the acceptance and application of 'general consensus standards'; standards that, for the most part, were created for special industries or non-commercial activities, but were now regulatory requirements for many new applications.

The Passenger Airbag Regulation for Vehicles

Seat belts became required equipment in all new passenger vehicles beginning in 1968. The regulation was based on tests that showed serious injury and death could be prevented by the use of restraint systems. The law required seat belts to be installed for all occupants. Use of the seat belts, was left to the occupant until state laws began requiring their use. New York became the first state to enact a seat belt use law in 1984. After years of philosophical, judicial, social, and political wrangling, the U.S. government passed federal regulations that required all cars built after 1996 to have airbags. Although automotive safety experts and design engineers disagreed on the effectivity of airbags, case studies of vehicle accidents that deployed driver's airbags (the only airbags available in early years of deployment) indicated that lives could be saved. And so, passenger airbags were added as an additional safety improvement.
Airbags, or so it seemed, had become one of the leading contributors to the reduction in auto fatalities. Still, there were problems looming:

Case 1. In October 1995, in Utah, a 5-year-old child sitting in the front passenger seat of a 1994-model automobile was killed when the passenger-side air bag deployed during a collision. Preliminary information indicates the child was not restrained by the lap/shoulder belt. The child sustained a skull fracture as a result of head contact with the air bag and subsequent head contact with the roof of the vehicle.

Case 2. In July 1995, in Pennsylvania, a 20-day-old infant seated in a rear-facing convertible child safety seat in the front passenger seat of a 1995-model automobile was killed when the passenger-side air bag deployed. The infant sustained multiple skull fractures and crushing injuries to the brain as a result of the impact of the air-bag compartment cover flap with the back of the child safety seat at the location of the child's head. At the time of collision, the vehicle was traveling at approximately 23 miles per hour. The vehicle had a label on the right front sun visor warning against using a rear-facing child safety seat in the front passenger seat. The child safety seat also had a warning label that read, "when used in a rear facing mode, do not place in the front seat of a vehicle that has a passenger air bag."

Case 3. In April 1993, in Ohio, a 6-year-old child who was sitting unrestrained in the front passenger seat of a 1993-model automobile was killed when the passenger-side air bag deployed during a collision with a stopped vehicle. The child died from a brain injury caused by blunt force trauma. [5]

As a result of an investigation of air-bag related fatalities and serious injuries to child passengers, the National Transportation Safety Board (NTSB) recently released safety recommendations regarding children and air bags (2).

NTSB recommends collaboration between automobile and safety-seat manufacturers, the news media, health and medical organizations, and the National Highway Traffic Safety Administration (NHTSA) to inform motorists and parents of the correct procedures for transporting children in vehicles equipped with air bags. NHTSA has enacted several regulatory measures addressing the air bag/child passenger problem, including labeling requirements for vehicles and child safety seats and specifications for air-bag cutoff switches.[6]

Figure 6 Passenger Airbag Switch

Automatic vs. Manual Operated Fire Protection Systems

The use of probabilities in the determination of the safety of a system has grown and is now a prominent method of evaluating the operability of complex systems.

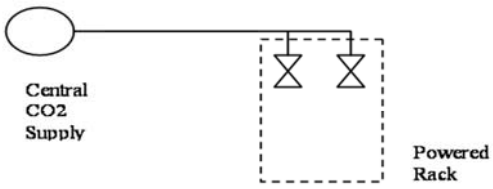


Figure 7 Early Design for ISS CO2 Fire Suppression

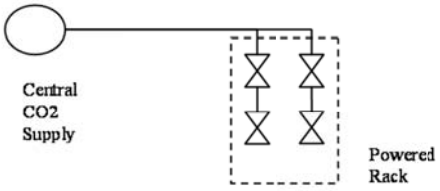


Figure 6 "Improved" ISS CO2 Fire Suppression System

The early design of Space Station provided a central CO2 Fire Suppression capability.
System Safety required a single fault tolerant system, thus, a single valve would be unacceptable. The solution could be two valves in parallel, thus if one failed to operate, the second might be expected to operate and extinguish a fire. However, this system has a flaw; if one of the valves leaks, the second valve can do nothing to stop the flow; the results are an empty fire extinguisher system and possible asphyxiation. The new solution is to install a parallel-series set of valves. In the event of one valve not operating, the parallel leg could be activated; if one leg leaks, the series valve (if it is downstream!) can cut off the flow of CO2 and the system is safed.

However, this system also presents a new dilemma. Up-mass is important to launch programs since each pound of material costs thousands of dollars to lift to orbit. And the reliability drops from 0.9975 for the parallel system to 0.9905 for the series/parallel system. The solution? Use portable fire extinguishers. At least that was the conclusion by the Reliability Engineers.

But, what happens if the crew is asleep and a fire breaks out in the experiment racks…there is no one to extinguish the fire and the automatic system has been disabled. And so, the installed system was ultimately rejected in favor of

a portable fire extinguisher discharge through a port in the rack face;[7] a system with one inline valve and a reliability of 0.95, lower than either of the more complex systems.

How the System Safety Engineer Can Avoid (Hopefully) Unintended Consequences

Research Similar Issues

Very few of the designs we are asked to analyze have no history in operation or construction. We, as engineers, learn from previous designs and apply the "knowledge of the known" to the "new" and look for the "unknown unknowns". How good we become is relative to our ability to look at the "whole" not only in design but also in functionality and use. Common databases of lessons learned are available, but are under-utilized in the investigation of the new designs. Since the laws of physics are rarely found to be flawed, and chemistry is a generally well-known constant, base your conclusions on these non-variable factors.

Identify and Talk to Stakeholders

Usually, the person (or group/client/agency) that has asked for the system, has projected the level of safety, with which, they expect the system to perform. Asking the 'buyer' how they expect the system to perform, and the response to adverse conditions have usually been thought out by them. The safety analyst then identifies what can go wrong, how it can be detected, and how it can be mitigated. Often, however, as shown in the leading examples, we fail to 'think outside the box' and look to the controls that are recommended to identify issues with the 'fix'.

Simulate the Revision

Placing the new system in use without conducting simulations should be regarded as malfeasance in the design and delivery of the system. How the system reacts in the environment-of-use is desirable for several reasons. The lessons of the passenger airbag illustrate how new hazards can creep into designs if they are not simulated (versus testing with real infants).

Test New Designs

When physical testing can be performed, it validates designs in the environment-of-use and provides proof of functionality. However, it should also be tested in environments that it *could* be exposed to; test the system using the controls that have been prescribed; evaluate the design in environments that could be detrimental; test it for environments that are 'outside of the box'.

Conclusions

When performing System Safety Analyses, the System Safety Engineer must look beyond the anticipated use and evaluate the potential uses and pitfalls of the design in non-traditional use, including the controls that have been developed. Limiting the evaluation of hardware design to the intended use may overlook some less-than-obvious responses to the hardware use.

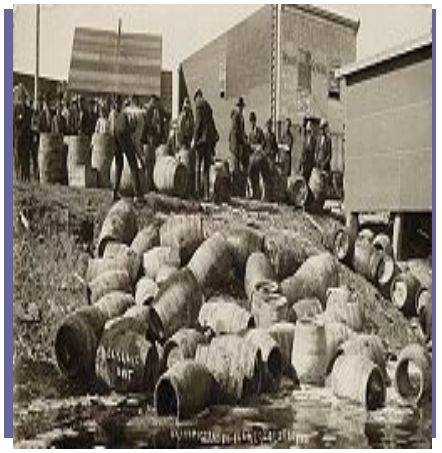
References

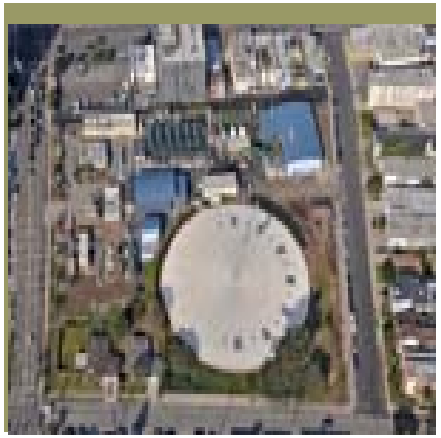
1. http://www.damninteresting.com/the-fall-of-the-eastland/
2. http://en.wikipedia.org/wiki/Eighteenth_Amendment_to_the_United_States_Constitution
3. http://www.epa.gov/mtbe/faq.htm#pagetop
4. Http://avherald.com "Incidents and News in Aviation"
5. Traffic Safety Programs, National Highway Traffic Safety Administration. Div of Unintentional Injury Prevention, National Center for Injury Prevention and Control, CDC.
6. National Transportation Safety Board. Safety recommendation, H-95-17. Washington, DC: National Transportation Safety Board, 1995.
7. Factors which Limit the Value of Additional Redundancy in Human Rated Launch Vehicle Systems Joel Anderson, et al Marshall Space Flight Center, Safety and Mission Assurance, Spaceops 2008

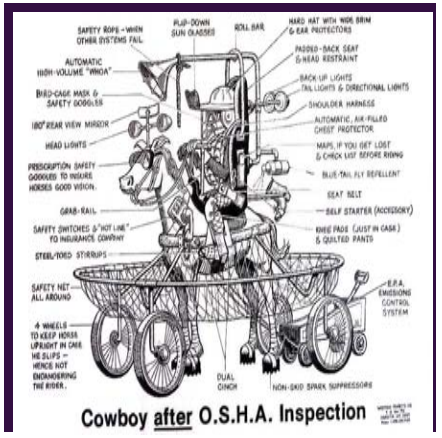
Biography

Clifford C. Watson, CSP, NASA Marshall Space Flight Center, Huntsville, Alabama, USA Telephone (256) 544-7067, email – Clifford.c.watson@nasa.gov

Mr. Watson is a Certified Safety Professional by examination, and has over 37 years of Health and Safety experience. He is currently the System Safety discipline representative to the Safety and Mission Assurance (S&MA) Assessment Team responsible for technical reviews of Integrated Hazard Reports for NASA's Space Launch System. Clifford has been recognized as a System Safety Expert by MSFC S&MA; he is a graduate of Indiana University of Pennsylvania with a B.S. in Safety Management.







System Safety and the Unintended Consequence

Presented by: Clifford Watson, CSP
NASA Marshall Space Flight Center

System Safety and the Unintended Consequence

- The analysis and identification of risks often result in design changes or modification of operational steps. This paper identifies the potential of unintended consequences as an over-looked result of these changes. Examples of societal changes such as prohibition, regulatory changes including mandating lifeboats on passenger ships, and engineering proposals or design changes to automobiles and spaceflight hardware are used to demonstrate that the System Safety Engineer must be cognizant of the potential for unintended consequences as a result of an analysis.

- Conclusions of the report indicate the need for additional foresight and consideration of the potential effects of analysis-driven design, processing changes, and/or operational modifications.

System Safety and the Unintended Consequence

- In today's complex world, the System Safety Engineer (SSE) plays an important role when using hazard analyses, failure modes and effects analyses, and other tools that ferret out the myriad of issues that may lead to system failures. It is possible to ask for, or require changes to design, implementation of operational controls, even hardware modifications that may create an unintended consequence. Traditional analysis tends to be rigid; management often tells us "If you bring me a problem, bring me a solution." And so, we sometimes offer 'fixes' that may not be the best solution, in fact, they may lead to serious consequences.

System Safety and the Unintended Consequence

- SS Eastland July 24, 1915
- Docked at pier in Chicago River
- 2500 passengers on board to attend a company picnic
- Suddenly, she lists, rolls to port – 844 people die
- Cause – top heavy design (lifeboats added to upper deck following RMS Titanic sinking)
- Good intentions – poor

System Safety and the Unintended Consequence

- U.S. Prohibition 1919
- Eighteenth Amendment to U.S. Constitution makes manufacture, transport, export of liquor illegal.
- "Bootlegging" fills the need for liquor, resulting in feuds, arrests, killing and loss of taxes.
- Cause – temperance movement led to government intervention
- Good intentions – poor execution

System Safety and the Unintended Consequence

- Santa Monica, CA 1970s
- Smog caused by auto emissions create unhealthy environment
- Clean Air Act Amendment of 1990 require use of 'oxygen-rich' fuels in areas of high smog.
- Ethanol is a candidate but requires much infrastructure – Methyl Tertiary-butyl Ether (MTBE) is chosen
- MTBE found in drinking water
- Cause - cost and schedule chosen over environmental concerns
- Good intentions – poor due diligence

System Safety and the Unintended Consequence

- All Nippon Airways flight Sept. 6, 2011
- Boeing 737 suddenly lurches and rolls violently 132 degrees left and 35 degrees down descending 6000 feet
- Investigation finds the Captain had taken a toilet break and upon return to cabin, First Officer reaches for door switch but twists rudder trim switch only four inches away sending plane into downward spiral.
- Cause – Lock required following 9/11/01 attack / Human error and Bio-engineering failure
- Good intentions – poor ergonomic design

System Safety and the Unintended Consequence

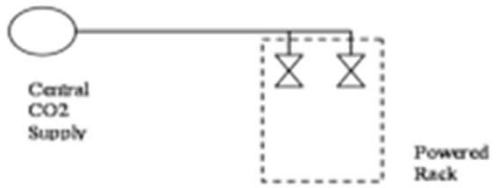
- http://www.youtube.com/watchv=PSGBAs412Lw&feature=related

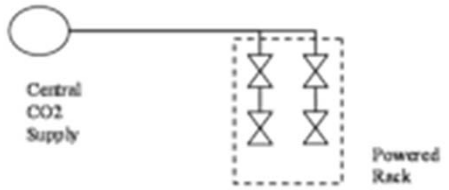
System Safety and the Unintended Consequence

- Auto passenger airbag regulations and airbag switch installation
- National Transportation Safety Board (NTSB) recommends airbags for all front seat personnel >1996 vehicles
- October 1995, five-year-old killed when airbag deploys in crash
- July 1995, 20-day-old infant killed in rear-facing child safety seat in passenger front seat in crash
- April 1993, six-year-old child, unrestrained by seatbelt killed by airbag in crash
- Cause – higher than expected mortality/lobbying
- Good intentions – ignored available data

System Safety and the Unintended Consequence

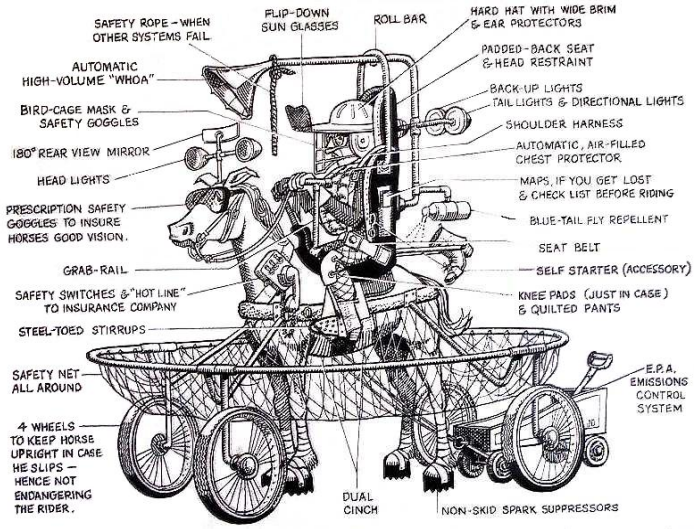
- International Space Station – current
- CO2 system installed onboard for fire suppression – top diagram
- System Safety required single-fault tolerant system
- Proposed solution shown in bottom diagram
- Added weight; increased complexity reduced reliability; costly revision
- Solution – portable fire extinguishers
- Cause – rigid requirements
- Good intentions – lack of foresight





System Safety and the Unintended Consequence

- The OSHA Cowboy – 1970 to ?
- Use of 'general consensus standards' in inappropriate circumstances
- Use of Personal Protective Equipment
- Design for maximum safety
- Lobbying
- Cause – over-zealous regulation
- Good intentions – costly/irrelevant requirements



Cowboy after O.S.H.A. Inspection

System Safety and the Unintended Consequence

- **How the System Safety Engineer Can Avoid (Hopefully) Unintended Consequences**
  - **Research Similar Issues**
    - Previous designs
    - Study the 'whole' not the 'individual' effects
    - Use non-variable constants such as physics and chemistry
  - **Identify and Talk to Stakeholders**
    - Ask the 'buyer'
      - How will the system will be used
      - What is expected
      - What might the adverse conditions of use be
  - **Simulate the Revision**
  - **Test New Designs**

System Safety and the Unintended Consequence

- **Conclusions**
  - System Safety Engineers must look beyond the anticipated use
  - Evaluate potential uses and pitfalls of the design
  - Consider the controls – are they adequate
  - Look for the 'unknown unknowns'
  - Evaluate the system 'Outside the Box'