

High Expectations: Our Systems are Like (or Could be Like) Airplanes

Mark Nelson, CISSP®, CSSLP®, IBM

David Hayes, United States Government
Accountability Office (Retired)

November 2019

Session **K5**



From Long Ago, but Not so Far Away



Xephon Conference and Exhibition

Principal speakers include:



Myers



Nelson



Wilson

London 6-7 November

E-Security 2000

Securing the enterprise

INCORPORATING

- ▶ RACF 2000
- ▶ E-Business Security

Sponsored by:



High Expectations: Our Systems are Like (or Could be Like) Airplanes

Mark Nelson, CISSP®, CSSLP®, IBM

David Hayes, United States Government
Accountability Office (Retired)

November 2019

Session **K5**

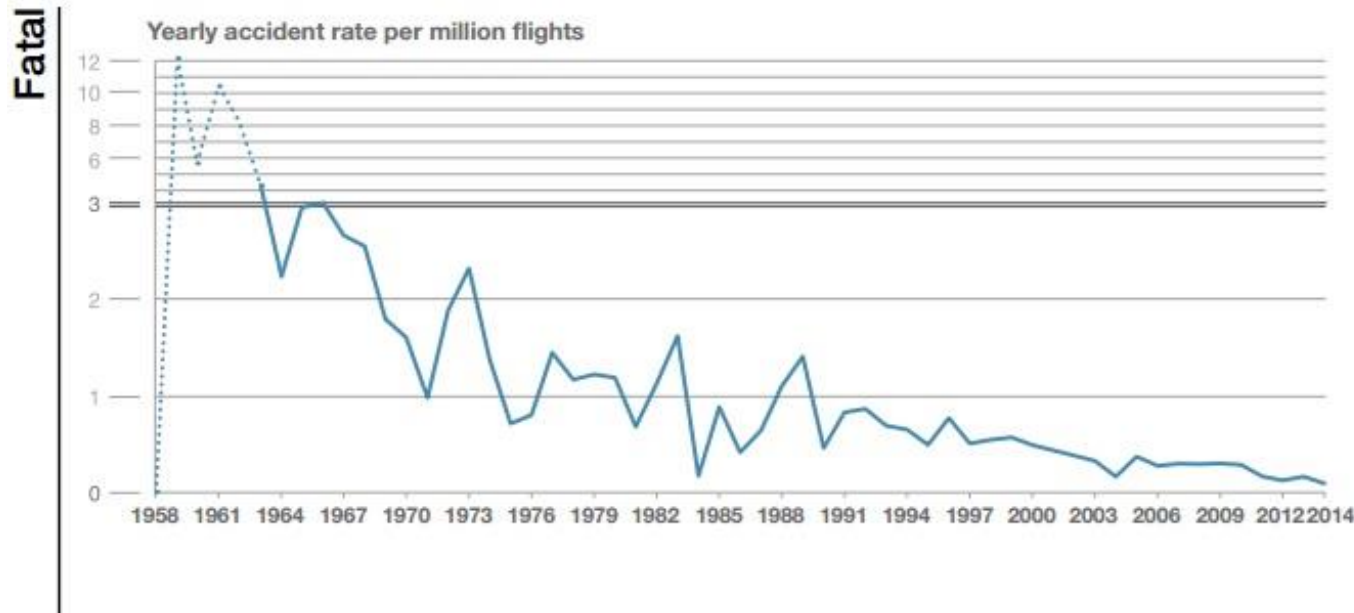


Why am I Interested in Aviation Safety?



Aviation Accident Trends 1958-2014

- The aviation industry has done a commendable job reducing the accident rate

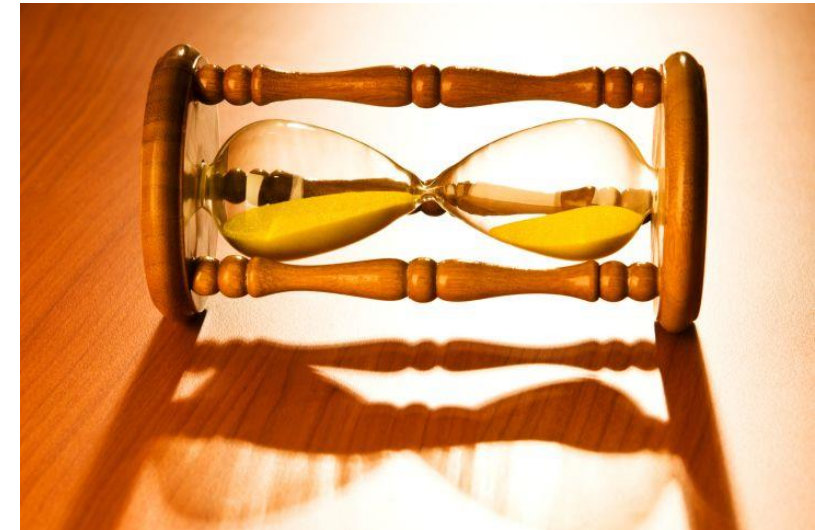


- Can we learn from the success of the aviation industry?

Comparing Aviation and Information Technology – Similarities and Differences

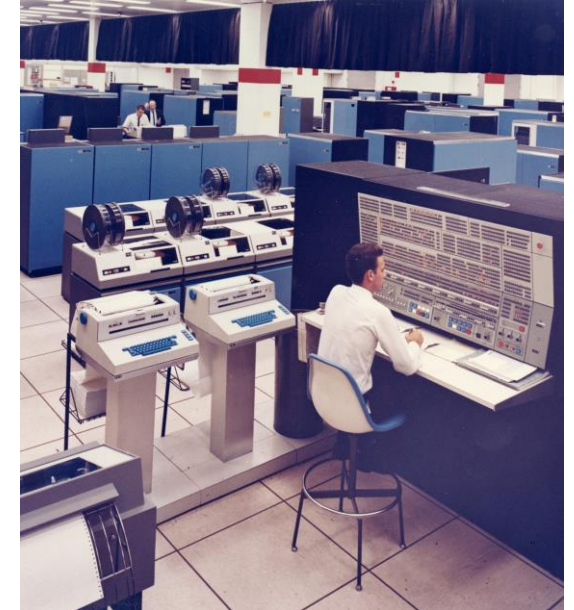
Comparison of Aviation and Info Technology

- **Roots of the modern industry**
 - **1904:** Wright Brothers first heavier-than-air powered flight
 - **1884:** Hollerith files his patent application titled "Art of Compiling Statistics"
- **Coming of age**
 - **1939:** Introduction of the DC3 (the first airliner capable of non-stop long distance flights) and the growth of airlines
 - **1940s:** Stored programmable systems – the move away from mechanical computation of data



Comparison of Aviation and Info Technology

- **Innovation spurs expansion**
 - **1960s:** Boeing 707 and 747
 - **1970s:** Airbus 300
 - **1960s:** System/360



Comparison of Aviation and Info Technology...

- **Both have a mix of uses**
 - **Aviation:** Scheduled air carrier, air charter/taxi, general aviation
 - **Information Technology:** Transactional, communications, process control, AI, analytics, graphics/text processing, publishing...
- **Both are a complex combination of people, processes, and technology**
- **Users/Customers of both have similar expectations of reliability**
- **Both have issues with the intelligence of their end users**



End-User Injected Risk



The Big Difference – Risk Management...

- **Aviation:** Errors and deficiencies result in death, injuries, brand impact and financial loss
 - **Risks are actively identified prior to deployment of any hardware or service** and positively managed in a risk profile
 - **Sources of risk are considered and controlled** through all phases of the life cycle of everything affecting flight operations:
 - Design of hardware and software
 - Manufacture of products used for aviation
 - Qualifications and capability – current and ongoing – of all personnel directly involved in operations
 - Absolute version and change control over all hardware and software
 - Accountability for all actions by operators and maintainers of equipment and critical operations



The Big Difference – Risk Management...

■ Aviation...

- **Losses and incidents that could have created losses are required to be thoroughly researched** and *usually* positive measures are implemented to prevent reoccurrences
- **Aviation product and service vendors can experience severe financial (and possibly legal) consequences** of any lapses in adherence with risk management



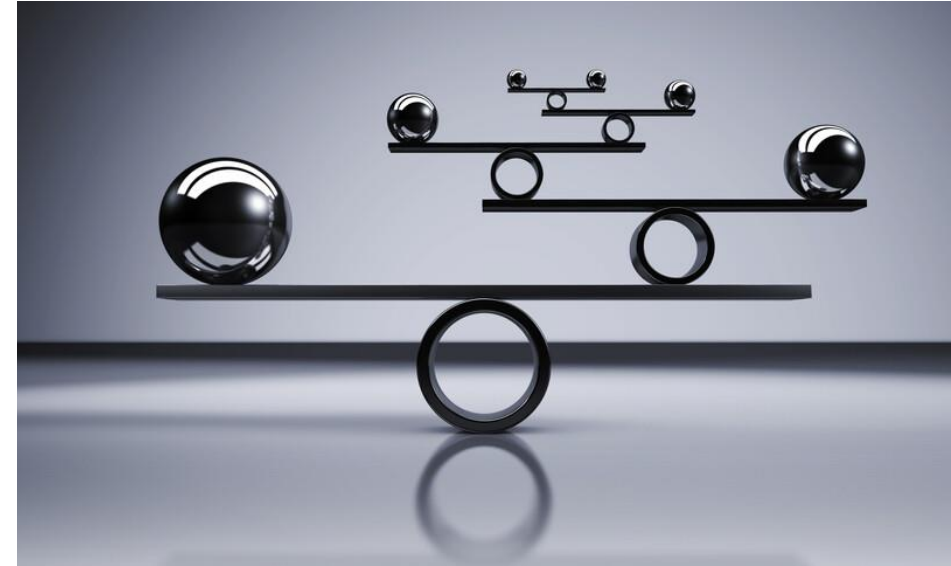
The Big Difference – Risk Management...

- **Information Technology:** Errors and deficiencies **result primarily in:**
 - brand impact and financial loss,
 - although death and injuries are possible



How is the Aviation Risk Profile Managed?

- **Speed of adoption of technology**
 - New technologies are introduced slowly, only after substantial design and implementation reviews
 - Contrast this with the information technology philosophy of “ship it now, fix it later”
- **Regulatory environment**
 - All participants (pilots, controllers, mechanics, manufacturers, instructors, medical providers, passengers) are subject to active controls
 - Contrast this with the primarily voluntary compliance with industry-defined standards and unevenly enforced government standards in information technology



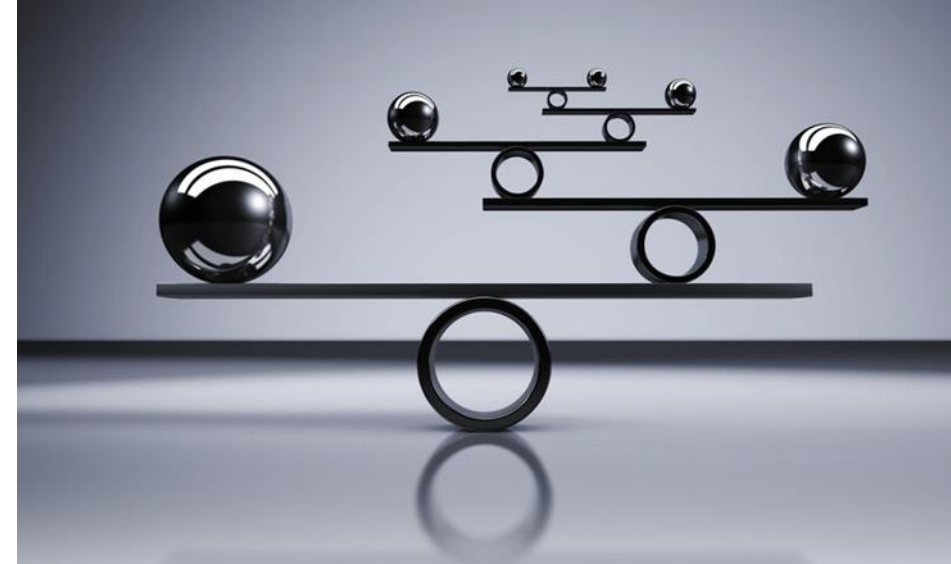
How is the Aviation Risk Profile Managed? ...

■ Training Standards

- All participants are required to undergo periodic education and almost all must periodically demonstrate proficiency

■ Operational Standards

- Deviations during execution that compromise safety are noted and investigated



What Can we Learn from the Aviation Industry?

- Can we slow down the speed of adoption of new technology? *No way!*
- Can we create a more regulated environment?
Probably not, but the management of compliance with the regulations already in place could be improved.
- Can we upgrade our training? *Yes!*
- Can we better manage our risk acceptance? *You bet!*
- Can we improve our operational activities?
Absolutely!



Risk Management

Managing Risk in Aviation

- Aviation risk is managed in accordance with the “Safety Risk Management Policy” (SRM), as documented in US Department of Transportation Federal Aviation Administration, National Policy Order 8040.4A, effective 30 April 2012
- Impact is categorized into five categories:
 - **Catastrophic:** Multiple fatalities
 - **Hazardous:** Multiple serious injuries, fatal injury to a relatively small number of persons (one or two), or a hull loss without fatalities
 - **Major:** Physical distress or injuries to persons, substantial damage to aircraft
 - **Minor:** Physical discomfort to persons, slight damage to aircraft
 - **Minimal:** Negligible safety Impact



Managing Risk in Aviation...

- **Likelihood is categorized into five categories:**
 - **Frequent:** Expected to occur routinely
 - **Probable:** Expected to occur often
 - **Remote:** Expected to occur infrequently
 - **Extremely Remote:** Expected to occur rarely
 - **Extremely improbable:** So unlikely that it is not expected to occur, but it is not impossible

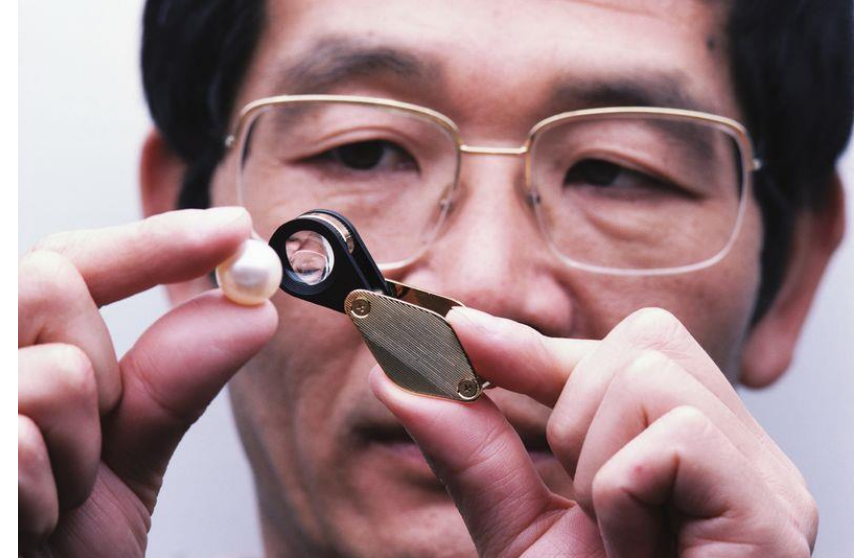


Aviation Risk Matrix

	Minimal Impact	Minor Impact	Major Impact	Hazardous Impact	Catastrophic Impact
Frequent	Acceptable	Acceptable with risk mitigation	Acceptable with risk mitigation	Unacceptable	Unacceptable
Probable	Acceptable	Acceptable with risk mitigation	Acceptable with risk mitigation	Unacceptable	Unacceptable
Remote	Acceptable	Acceptable	Acceptable with risk mitigation	Unacceptable	Unacceptable
Extreme Remote	Acceptable	Acceptable	Acceptable	Acceptable with risk mitigation	Unacceptable
Extremely Improbably	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable with single point of failure

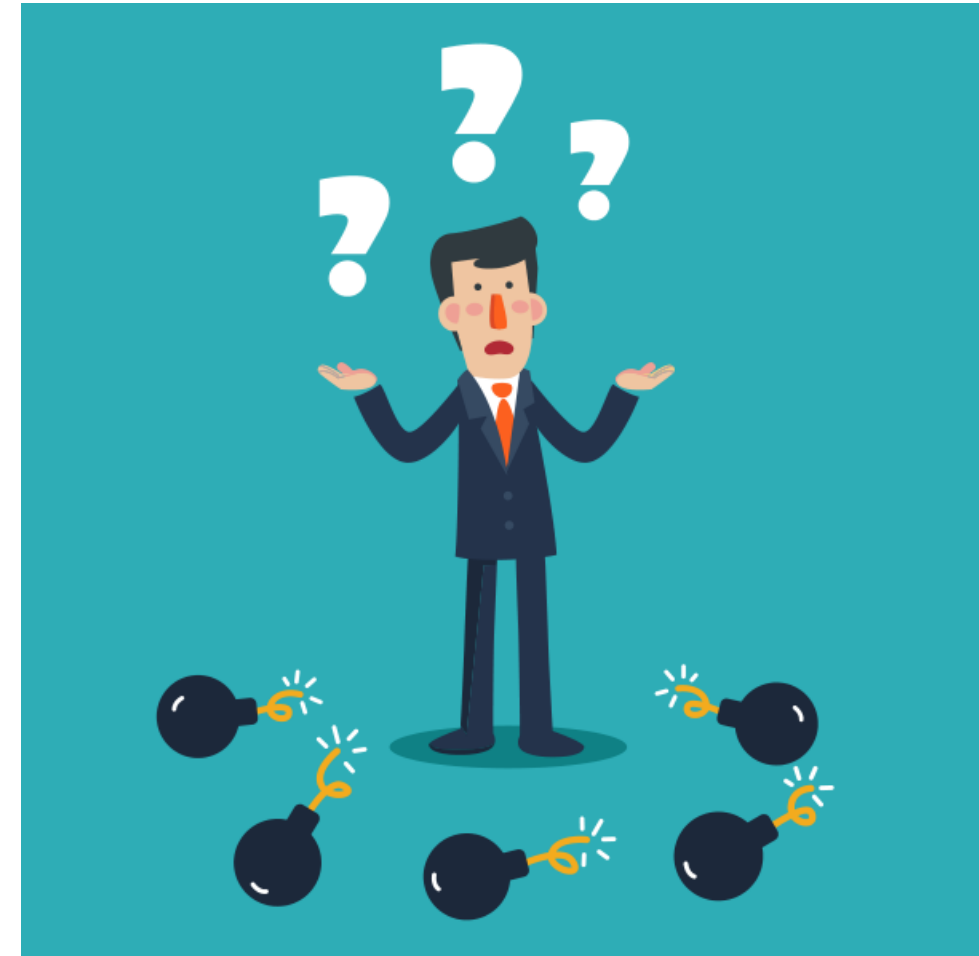
Things to Notice on the Aviation Risk Matrix

- The impacts and likelihoods are *pre-defined* and not subject to negotiation
 - Interpretation, perhaps, but not negotiation
- Risk acceptance is a defined part of the process, guided by the pre-defined impacts and likelihoods
- “Catastrophic” and “Hazardous” impacts have very little “wiggle room” on risk acceptance
 - Even “*extremely remote*” needs to be addressed!
- How can we adapt this approach to information technology?



How Would we Characterize Impacts from an IT Perspective?

- **Catastrophic:**
 - Unrecoverable loss of a mission-critical IT system
 - **Hazardous:**
 - Recoverable loss of a single mission-critical application with minimal recovery time
 - **Major:**
 - Impaired service delivery to organizations/customers that prevent achieving required outcomes
 - **Minor:**
 - Impaired service delivery to organizations that limits the expected outcomes
 - **Minimal**
 - All impacts which don't fit into a category above
- **Let's just focus on *catastrophic***



What are Examples of Catastrophic Impacts?

- **Physical or logical destruction of a mission-critical IT asset, without possibility of recovery**
 - By a trusted actor (rogue systems programmer?)
 - By a non-trusted actor (malicious actor who has found a misconfiguration or vulnerability?)

... and since these are catastrophic events, the risk matrix approach dictates that any non-**extremely improbably risk**" must be addressed!



What are the counter measures that are needed to eliminate these risks?

- **Effective physical security**
- **Demonstrable disaster recovery and real-time redundancy**
- **Proper system configuration**
- **Proper logical security**
- **... and many more...**



What Logical Security Lapses Could Allow a Catastrophic Event?

- **Too many to list! Some examples include:**
 - Improper controls on resources which allow extraordinary access, such as System libraries (APF, System REXX, critical CLISTs, production batch jobs, etc.)
 - Not pervasively encrypting
 - Not using multifactor authentication
 - Not continuously monitoring
 - Having improper network controls
- **Think of all the ways that these lapses could be exploited.**
- **Since these are needed to eliminate the risk for a catastrophic event, they must be addressed.**



Control Techniques

Control Techniques Used in Aviation

- Aircraft have only two states: Airworthy or un-Airworthy
- An Airworthy aircraft is the result of:
 - **100% compliance 100% of the time with all standards** – Type Certificates and Airworthiness Directives
 - **Positive (required) multi-level inspections** of all critical system components by trained and licensed personnel – annually, daily, before every flight and as dictated by maintenance inspection schedules for each specific model of equipment



Control Techniques Used in Aviation...

- **An Airworthy aircraft is the result of...**
 - **Absolute version and change control** – all critical components are inspected, updated, maintained and/or replaced in compliance with either time in service, calendar time or operational cycles. *There is no such thing as deferred maintenance or unsupported “versions.”*
 - **Hardware redundancy** when any single point of failure can be practically eliminated.
 - **100% accountability for all activity involving the equipment** – accurate, complete and timely record keeping of all operations and maintenance must be in place before an aircraft is available for operations
- **Where could our systems be more like an Airworthy Aircraft?**



Qui facit iudicium? (Who Makes the Decision?)

- **14 CFR 91.3 - Responsibility and Authority of the Pilot in Command**
- (a) The pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft.
- (b) In an in-flight emergency requiring immediate action, the pilot in command may deviate from any rule of this part to the extent required to meet that emergency.
- (c) Each pilot in command who deviates from a rule under paragraph (b) of this section shall, upon the request of the Administrator, send a written report of that deviation to the Administrator.



Information Systems Control Techniques

- **Some areas where our systems could be more like an airworthy**
 - **Positive control of data access**
 - Pervasively encrypting, PROTECTALL(FAIL), ERASE(ALL), BATCHALLRACF, multifactor authentication, activating the JESSPOOL class, backstop profiles on general resource classes
 - **Redundancy**
 - Effective use of Sysplex features and application features (such as a properly maintained, duplexed, and backed up RACF DB)
 - **Integrity of the Operating Environment**
 - Operating system implementation that puts a loss of integrity of the operating system in the “Catastrophic” category
 - Effective matching of implementation and security policy
 - *“The price of security is eternal vigilance”*
 - **Expectation of compliance**
 - Adherence to controls and risk management is monitored and enforced at the executive level

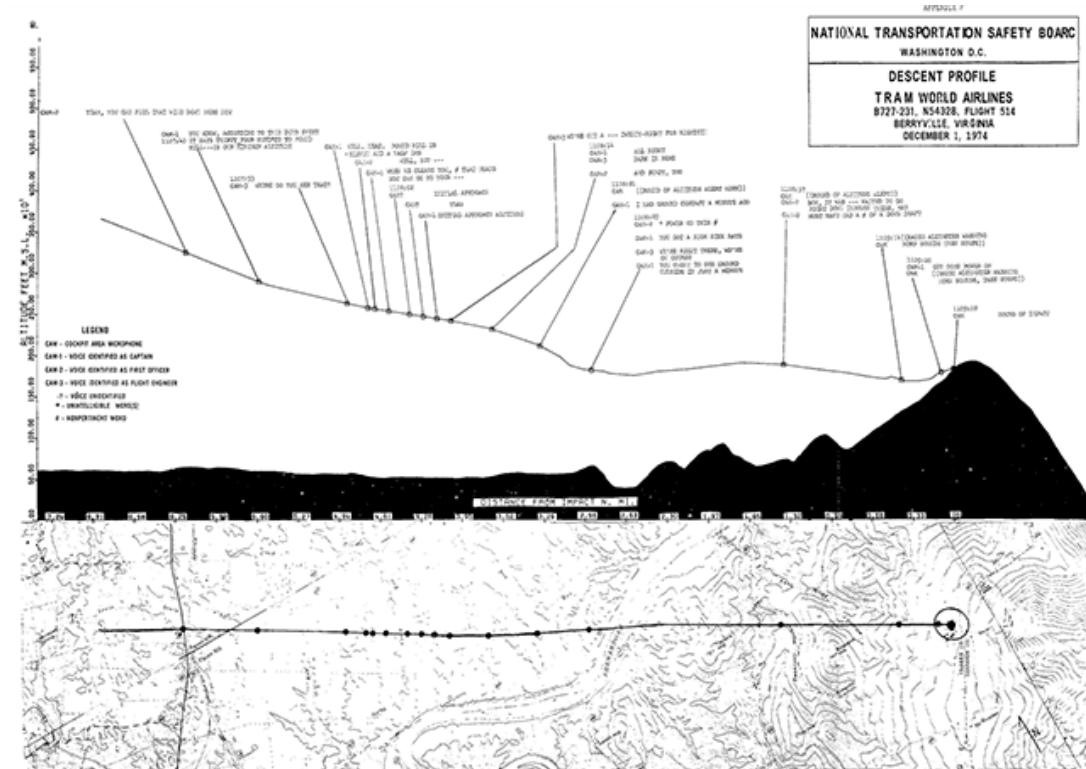


Reducing Risk by Learning from the Past

Learning from Mistakes Before they have a Big Impact

■ TWA Flight 514

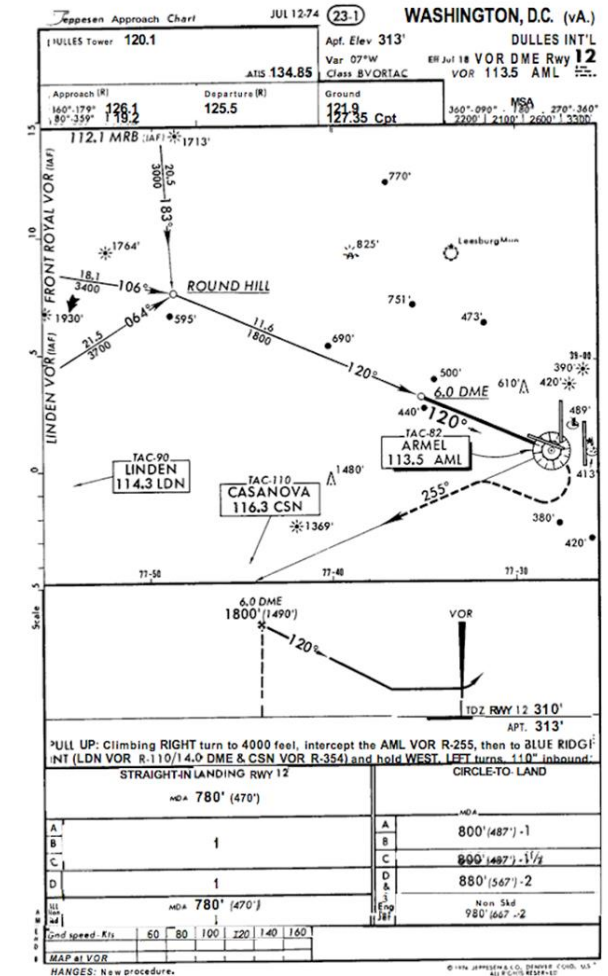
- B727 (N54328) inbound to Washington National Airport from Columbus Ohio on 1 December, 1974
- Diverted to Dulles airport due to high winds and vectored to a non-precision approach to runway 12 at Dulles
- While cruising at 7,000 feet the pilots were "cleared for the approach" into Dulles
- The pilots began a descent down to 1,800 feet
- Intense downdrafts caused minor (100'-200') altitude deviations
- The aircraft impacted Mount Weather (summit 1,754 feet) at 1,670 feet, with first impact being 70' tall trees
- Eighty-five (85) passengers and seven (7) crew perish in the crash



Learning from Mistakes Before they have a Big Impact...

■ Investigation

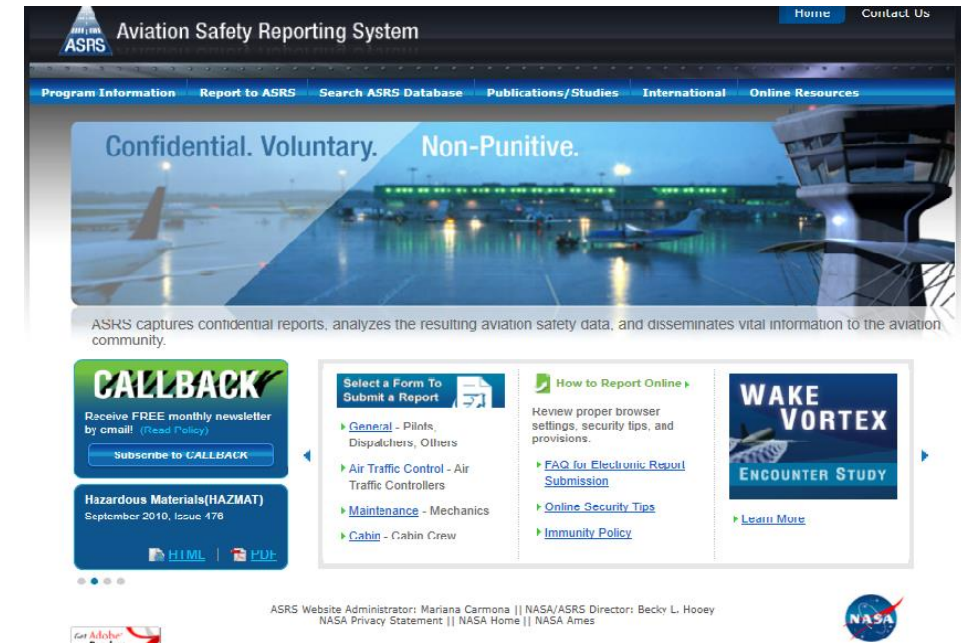
- The National Transportation Safety Board (NTSB) report determines that the primary cause is “Misunderstanding of orders or instructions”.
- During the investigation, the NTSB discovers that a **United Airlines flight had made the exact same error six weeks earlier, but had recognized the error and recovered in time.**
- The investigation reveals that the **misunderstanding of “cleared for the approach” was widespread and that pilots were reluctant to report the confusion.**
- The result of the investigation is the creation of the Aviation Safety Reporting System (ASRS).



Learning from Mistakes Before they have a Big Impact...

- **Aviation Safety and Reporting System (ASRS)**

- A voluntary program which allows anyone involved in the aviation industry to report issues that will be investigated by an independent agency, the National Aeronautics and Space Administration (NASA)
- Reports are anonymized when brought into the ASRS system to preserve the confidentiality of the reporter



Learning from Mistakes Before they have a Big Impact...

- **Aviation Safety and Reporting System (ASRS)...**

- Reporters have an incentive to report issues:

- If the FAA independently detects an issue and takes an action, if the person under investigation is found “guilty”, and if the person had reported the issue to the ASRS, the penalty will be waived. Key provisions:

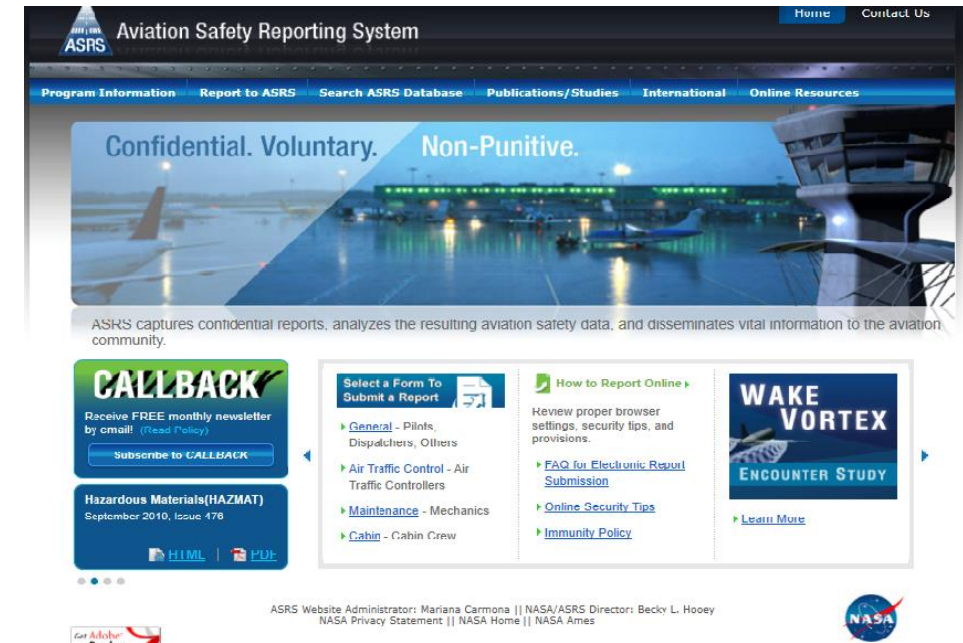
- No limit on the number of reports
 - Can be used to waive a penalty once per five years, and
 - Cannot be claimed if the action was illegal or willful (loses anonymity as well)

- **NASA analyzes trends and makes recommendations. Many of these have been adopted by the FAA**

- Publishes monthly two-page report called “*Callback*”

- Similar process in the UK is called CHIRP (Confidential Human (factors) Incident Reporting Process)

- However, there is no “incentive” to file a report.h



Learning from Mistakes Before they have a Big Impact...

- ASRS Celebrated its 40th Anniversary on 16 April, 2016



40th The ASRS Celebrates Anniversary 1976 - 2016

Safety Depends on Lessons Learned

On April 16, 2016, the NASA Aviation Safety Reporting System (ASRS) celebrated its 40th year of continuous operation in service to aviation safety. The longevity and success of the ASRS program are remarkable examples of how aviation system users can contribute their "lessons learned" to a safety program that collects and analyzes this information to resolve issues associated with our modern aviation system.

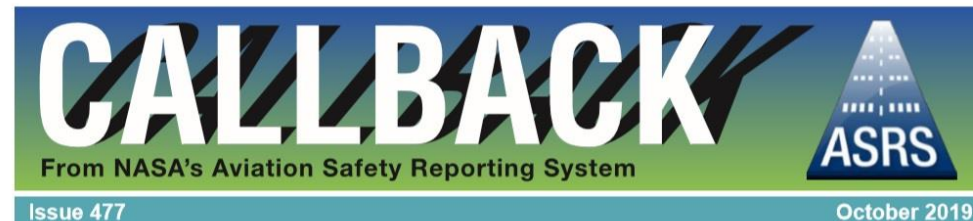
The Origin of ASRS

On December 1, 1974, TWA Flight 514 was inbound through cloudy and turbulent skies to Dulles Airport in Virginia. The flight crew misunderstood an ATC clearance and descended to 1,800 feet before reaching the approach segment to which that minimum altitude applied. The aircraft collided with a mountaintop, killing all aboard.

The FAA and NASA Collaborate

The first step in establishing a national aviation incident reporting program was to design a system in which the aviation community could place a high degree of trust.

The FAA Administrator recognized that the regulatory and enforcement roles of the FAA would discourage the aviation community from using a new safety program that



Interactions in Sync – or Not?



In the 1700's, David Hume observed that, "He is happy whom circumstances suit his temper; but he is more excellent who suits his temper to any circumstance." A century and a half later, Dale Carnegie admonished, "When dealing with people, remember you are not dealing with creatures of logic, but creatures of emotion." These precepts, ever present in aviation, can be constructive when examining human interactions that occur during aviation incidents.

While aviation, in general, aspires to excellence, many aviation decisions and actions involve interaction between at least two persons. During an interaction, individual nuance, emotion, and uniqueness are frequently at play. Egos

Checklist, which we confirmed and began. I handed aircraft control to my First Officer (FO) along with the radios. We had about 7.5 on the fuel, so we decided quickly that we were going to our alternate. ... I ran the checklist and programmed up the runway and communicated with Dispatch through ACARS, notifying them of our decision and need for landing data.

We [got priority handling] out of an abundance of caution. The [cabin] crew and ...passengers were notified of our new destination. ... The FO did an exceptional job of staying between the flaps 25 overspeed and the gear warning horn [speed], and also landed the plane.

Learning from Mistakes Before they have a Big Impact...

- **Aviation Safety and Reporting System Intake in August, 2019**

- Air Carrier/Air Taxi Pilots: 5,833
- General Aviation Pilots: 1,500
- Flight Attendants: 973
- Controllers 536
- Military/Other 343
- Mechanics 283
- Dispatchers 198
- TOTAL 9,666



Lockheed C-140 Jet Star

Question: *Why can't we have an ASRS-like process in our environments?*

Learning from Mistakes After they have a Big Impact

■ United Airlines 232

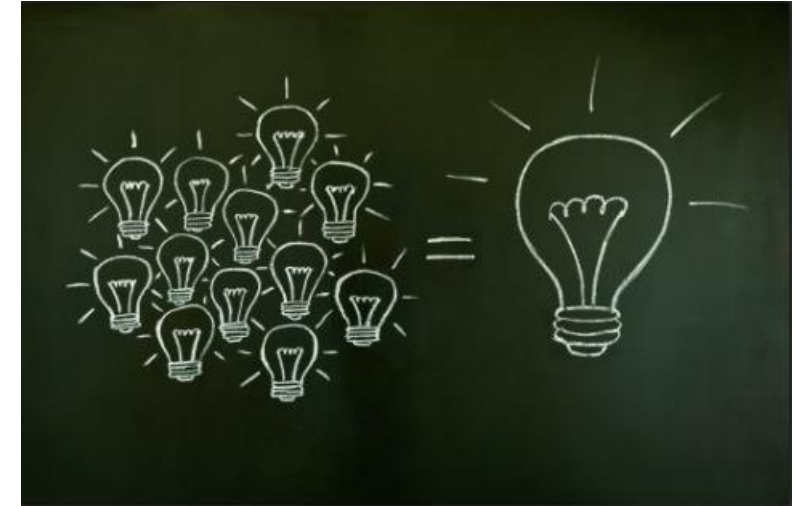
- DC10 (N1819U) inbound to Chicago O'Hare from Denver Stapleton on 19 July 1989 with 296 onboard
- 57 minutes into the flight, the fan disk of its tail-mounted GE CF6-6 engine disintegrated. The shrapnel from the disintegration punctured all three hydraulic lines, rendering the ailerons, elevator, and rudder inoperative.
- The crippled airliner landed at Sioux City, Iowa
 - ... with 185 surviving the ensuing crash



Learning from Mistakes After they have a Big Impact...

■ Why Were there So Many Survivors?

- UAL 232 pilot-in-command Captain Al Haynes attributes the high survival rate to:
 - **Cooperation and communication**
 - The crew was trained on Crew Resource Management (CRM) techniques encouraged all members of the flight crew to share information and expertise
 - **Preparation**
 - Just the day earlier, Sioux City had performed a drill that was very similar to the actual crash
 - **Luck**
 - The flight was during daylight and the weather was good
 - The accident occurred at a shift change
 - Simulations of the accident with over 50 equivalently-trained crews resulted in far worse outcome



Learning from Mistakes After they have a Big Impact...

- **What was learned?**
 - CRM works!
 - Aviation instrumentation was upgraded to allow flight management systems to successfully complete a landing under similar conditions.



Parting Thoughts

- Are the concepts and many of the tools and techniques that have been developed in over a century of aviation applicable to strengthen information technology?
- How many positive controls that are available now in information technology that reduce risk are not being implemented for reasons that would not be possible in aviation?



Parting Thoughts...

- What is really preventing the implementation of some of the available controls we all know would reduce risk (think of the areas in the aviation risk matrix that MUST be addressed)?
- Would the adoption of an aviation-type risk management approach for information technology generate positive outcomes, such as being more competitive in the marketplace, for you and/or your organization?
- How can we work together to increase the awareness of how risk management can be improved for information technology?



Parting Thoughts...

Please do not attempt to fly your systems, but please do strive to make your systems more like an airplane!



Please submit your session feedback!

- Do it online at <http://conferences.gse.org.uk/2019/feedback/nn>
- This session is **K5**



1. What is your conference registration number?

💡 This is the three digit number on the bottom of your delegate badge

2. Was the length of this presentation correct?

💡 1 to 4 = "Too Short" 5 = "OK" 6-9 = "Too Long"

1 2 3 4 5 6 7 8 9

3. Did this presentation meet your requirements?

💡 1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1 2 3 4 5 6 7 8 9

4. Was the session content what you expected?

💡 1 to 4 = "No" 5 = "OK" 6-9 = "Yes"

1 2 3 4 5 6 7 8 9

High Expectations: Our Systems are Like (or Could be Like) Airplanes

Mark Nelson, CISSP®, CSSLP®, IBM

David Hayes, United States Government
Accountability Office (Retired)

November 2019

Session **K5**

