The Role of Lessons Learned in the Investigate, Communicate, Educate-Cycle for Commercial Aviation

Dr Paul Werner & Richard Perry
Sandia National Laboratories, USA

Author Biographies:
Dr. Werner is a Program Manager in the Airworthiness Assurance Department of the Energy and Transportation Surety Center, Sandia National Laboratories. He holds a BS and MS in physics and a Ph.D. in electrical engineering. Currently, he is leading several teams in support of aviation safety. Much of his work has involved researching and reviewing accidents across many industries, including aviation, for lessons learned. Flight experience includes over 2000 hours in the US Navy's S-3 Viking. Currently a Captain (O-6) in the Naval Reserves, he is serving with Air Test and Evaluation Squadron Three One 0176.

Richard Perry is Manager of the Airworthiness Assurance Department of Sandia National Laboratories. His department promotes validation and industry acceptance for inspection, maintenance, and repair technologies that address aging aircraft issues. A graduate of the Air Force Academy, he holds a MS in aeronautical engineering and is a registered Professional Engineer. He has served as the Director of System Safety and Engineering at the Air Force Safety Center, reviewing approximately 50 accident investigations annually. He holds an Airline Transport Pilot rating with 4600 hours of flight experience in a broad range of aircraft from gliders to heavy jet bombers and transports.

The Role of Lessons Learned in the Investigate, Communicate, Educate-Cycle for Commercial Aviation

Paul Werner and Dick Perry,
Sandia National Laboratories

Aviation safety begins with safe aircraft. The safety of large transport airplanes operating in commercial service throughout the world has steadily improved over the last several decades. Nevertheless, accidents still occasionally occur. When they do occur, it is important to identify the root causes, precursors, and lessons learned of these accidents so that appropriate steps may be taken to reduce the risk of their recurrence. Safety lessons learned from aviation now spans several generations of safety managers and engineers. It is no longer possible for comprehensive knowledge to be exchanged from experienced safety individuals to the next generation of safety personnel through on-the-job training alone. The system is so complex that it is unlikely any one individual can possess truly comprehensive system safety understanding. It is necessary to adopt a more rigorous and systematic approach to lessons learned safety training and management.

When presented with the data, facts, and histories available, it becomes painfully obvious that most, if not all, accidents followed one or more precursors or previous accidents that were not acted on for several reasons. The predominant reason is that those involved were unaware of the significance of what they had observed. This lack of awareness was due to a failure to view the event from the airplane-level rather than the aircraft system, subsystem, or component-level. Another reoccurring reason is that those involved were unaware of the existence of critical relevant information. These reasons are actually common throughout many industries and tolerated or accepted by most. It is unacceptable in commercial aviation.

The aviation industry cannot afford the time and resource costs, and the loss or non-use of important safety information. Work must go on and airplanes must fly. The lessons learned system must allow individuals to do their jobs more effectively and the aviation system to operate safer and more efficiently.

Such a system does not currently exist in the FAA. The need and urgency has been recognized and action taken to move in that direction. The first step is awareness and a transition to a different way of making decisions for regulatory and industry personnel at all levels doing their job.

Safety standards and the methods used to apply them must continually evolve due to advances in technology and demand for higher levels of safety. Each phase of the product life cycle continuum impacts safety as information and experience derived from one phase is systemically applied to the other phases. Success of the entire continuum is dependent on effective safety management in each and every phase, capturing and using lessons learned from all phases of a product's life cycle to continuously improve standards, validate design assumptions, identify precursors, mitigate risk in safety related decision making, and correct underlying sources of problems system wide. Lessons learned from accidents are perhaps the most costly. It is vital to

capture these lessons through investigation, communicate them to the appropriate organizations, and educate people to recognize and use these hard-learned lessons to proactively make commercial aviation safer.

Why lessons learned are important?

Lessons learned are defined as knowledge or understanding gained by experience. The experience may be positive, such as a successful test or mission, or negative, such as a mishap or failure. A lesson must be significant in that it has an impact on safety; valid in that it is factually correct; and applicable in that it identifies a specific design, process, or decision that reduces or eliminates the potential for failures and mishaps, or reinforces a positive result.

Establishing a culture where we capture and use day-to-day information and experience from certification, maintenance, and operational activities is crucial to improving aviation safety. By doing so, we can expect to gain benefits that include:

- Documented guidance, information and best practices passed on to less experienced people,
- More consistent safety decisions,
- Improved safety by reducing accidents and preventing any repeat accidents, and
- Reduction in safety problems caused by breakdowns in communication between design and maintenance or operation organizations

The best way to learn and improve is to analyze previous experience and draw conclusions for future direction based on them. One way regulators capture lessons learned is through development of regulations, policies, and procedures. The following is a short and incomplete list of major transport airplane accidents that have helped shape US Federal Aviation Regulations (FARs) and policies:

- Ford Tri Motor in U.S.-1930 (engine failure on takeoff)
- TWA L1049/UAL DC-7 near Grand Canyon-1956 (enroute ATC)
- Braniff L-188 near Buffalo, Texas-1959 (propeller whirl mode)
- U.S. operator/Viscount in Maryland-1962 (bird strike to tail)
- Northwest L-188 near Cannelton, Indiana-1960 (propeller whirl mode)
- Eastern L188 at Boston-1960 (bird ingestion to engines)
- Pan Am B707 near Elkton, Maryland-1963 (lightning strike to fuel tanks)
- United B727 at Salt Lake City-1965 (stretchable fuel lines)
- Pan Am B707 at San Francisco-1965 (rotor burst)
- Mohawk BAC1-11 in United States-1967 (APU inlet fire)
- U.S. carrier B727 at Los Angeles Int. Airport-1969 (human factors, cockpit switches)
- Air Canada DC8 near Malton, Ontario-1970 (human factors, spoilers)
- Eastern L-1011 near Miami-1972 (human factors, ATC)
- VARIG B707 near Paris-1973 (smoking/waste bin fire in lavatory)
- Turk Hava Yollari DC-10 near Paris-1974 (pressure relief, human factors)
- Lufthansa B747 near Nairobi-1974 (takeoff warning, human factors)

- TWA B727 near Berryville, Virginia-1974 (human factors, ground prox.)
- Eastern B727 near New York City-1975 (wind shear)
- KLM B747/Pan Am B747 at Tenerife-1977 (human factors, ATC)
- Southern Airways DC-9 near Atlanta, Georgia-1977 (rain ingestion to engines)
- Pacific Southwest Airlines B727 at San Diego, California-1978 (human factors, TCAS)
- United Airlines DC-8 near Portland, Oregon-1978 (human factors, low fuel warning)
- American Airlines DC-10 at Chicago, Illinois-1979 (system isolation, human factors)
- Saudia L-1011 near Ryiadh, Saudi Arabia-1980 (interior fire, human factors)
- Air Florida B737 at Washington D.C.-1982 (human factors, airframe/engine icing)
- British Airtours 737 at Manchester, England-1985 (fuel tank access covers)
- Delta L-1011 at Dallas, Texas-1985 (wind shear)
- Japan Air Lines B747 near Tokyo-1985 (system isolation, pressure venting)
- Mexicana B727 near Maravatio, Mexico-1986 (wheelwell fire)
- Northwest DC-9 at Detriot-1987 (human factors, takeoff warning)
- South African Airways B747 in Indian Ocean-1987 (cargo compartment fire)
- Aloha Airlines B737 in Hawaii-1988 (structural corrosion)
- American Airlines DC-10 at Dallas Ft. Worth-1988 (break wear)
- TACA B737 near New Orleans, Louisiana-1988 (hail ingestion to engines)
- United Airlines 747 in Hawaii-1989 (structural inspection)
- United Airlines DC-10 near Sioux City, Iowa-1989 (system isolation, engine inspections)
- USAir Jetstream 3100 at Beckley, W. Virginia-1991 (tail plane icing)
- Lauda B767 near Bangkok, Thailand-1991 (thrust reverser in-flight deployment)
- American Eagle SF340 near New Roads, Louisiana-1994 (propeller beta in flight)
- Simmons Airlines ATR-72 near Roselawn, Indiana-1994 (freezing rain)
- ValueJet DC-9 near Miami-1996 (haz. mat., cargo fire protection)

What are the attributes of a successful lesson learned process?

Development and implementation of an effective lessons learned process is critical for improving aviation safety. Ideally, it would be an integrated, common infrastructure that captures and provides access to lessons learned safety information throughout a product's life cycle. As such, a successful lessons learned process would have the following characteristics:

- A structured process for incorporating lessons learned into rules, policies, and procedures for certification, maintenance, and operations. The process should ensure that in service lessons learned are incorporated in design or certification methods of compliance, and results of project-specific decisions are easily accessible by other certification projects.
- Use of a disciplined, data driven approach to find root causes and determine the best actions to break the chain of events that lead to accidents.
- A process that includes periodic reviews and feedback. This should be a unique task from daily business for a 'look back," and should ensure reviews are conducted at regular intervals.
- A process that ensures corrective actions are implemented for all root causes assessed, so that underlying sources of problems are corrected system-wide.

What are the barriers to capturing and using lessons learned?

Several observations have been noted across diverse industries regarding effective capture and use of lessons learned. First, most organizations strive to reuse all kinds of documented experience but that it is not easy to do so in an effective manner. The reuse is rather ad hoc and unplanned and it is often hard to know what to search for or how to find useful documents. Another observation is that the "right" knowledge for solving a problem often exists somewhere within the organization, but the challenge is to take the time to search for it, identify it, get access to it, and then learn from it. Due to the fact that experience is represented internally by experts, the major problem is often finding and getting access to the "expert" in order to solve a problem.

In today's complex and fast moving aviation system, engineers and inspectors often don't have the time to do extensive research and analysis of aircraft accidents and incidents. Instead, they must rely on their experience and training, and possibly the insight of others. So, why are lessons not learned?

- Cultural barriers such as the lack of time to capture or submit lessons and a perception of intolerance for mistakes,
- Organizational barriers such as communication across companies or lines of business is often difficult or non-existent,
- Lessons are not routinely identified, collected, or shared across organizations and industry due to a lack of communication or other factors, and
- Unorganized lessons are hard to use with too much material to search; it may be formatted differently for different accident reports; the information needed is not available; it's not quickly available; or work pressures don't allow the time or resources.

Critical Concepts

The concepts discussed in this section are critical to the identification of design and certification lessons learned from accidents. First, let's look at aircraft-level awareness.

Aircraft-level Awareness

When presented with the data, facts, and histories available, it becomes painfully obvious that most, if not all, accidents followed previous events that were not acted upon because someone was unaware of the significance of what they observed. Often this was because they failed to view the significance of the event at the airplane level rather than the system, subsystem, or component level. In most cases, those involved were unaware of the existence of critical relevant information, i.e., lessons learned.

A conclusion from many of the accidents reviewed during the Commercial Airplane Certification Process Study (March 2002) was that adequate processes do not exist within the FAA or in most segments of the commercial aviation industry to ensure that the lessons learned from specific experiences in airplane design, manufacturing, maintenance, and flight operations are captured permanently and made readily available to the aviation industry. Consequently, the failure to capture and disseminate lessons learned has allowed airplane accidents to occur for causes

similar to those of past accidents. In response to this concern, Change Area 1.C, Precursor Awareness, was tasked to specifically:

> *"Develop AVR airplane-level awareness for improved identification and risk assessment of accident precursors. Define methods to capture, share, and use lessons learned information throughout industry and the life cycle."*

Precursors

The role and importance of accident precursor recognition cannot be over emphasized. Precursor data can be a valuable source of information for decision-making, either directly or as a supplement to risk analysis. Moreover, precursor data inherently incorporates the effects of factors such as human errors and inter-system dependencies.

Accident precursor identification should identify latent and potential design, certification, and operational safety issues and correct them before they become accidents through:

- Comprehensive monitoring, sharing, and use of design and operational safety information and a consequent growth in the understanding of current and emerging accident precursors and direct causes;
- Immediate certification and operational interventions at the regional, national, and international levels.

Precursor events can be any service information or experience, or test or inspection data that could be interpreted as a predictor that the event consequence could occur if the event conditions were present. Accident precursor data can be from any discipline (e.g., risk analysis, statistics, engineering, ergonomics, psychology, sociology, organizational behavior).

Daniel Cheney of the Federal Aviation Administration suggested the following definitions of Precursor Types:

> Type 1: Precursors with no protection or mitigation elements associated with the prevention of the event initiation, progression, or consequences. Types 1 are the most potentially serious of all precursor events.
>
> Type 2: Precursors with no consistent or dependable protection or mitigation elements associated with the prevention of the event initiation, progression, or consequences. Nearly as potentially serious as Type 1, but may have an opportunity for intervention by flight crew, ground crew, or others.
>
> Type 3: All other precursor events; those that have at least one consistent or dependable protection or mitigation element associated with the prevention of the event initiation, progression, or consequences. Type 3 precursors require at least one other condition in addition to the event condition to occur. These represent the vast majority of service information (i.e., data) used in the safety oversight process.

An example of a Type 1 precursor for the 1979 American Airlines DC-10 crash would be the 1978 pylon flange failure on a Continental Airline DC-10 during maintenance. This incident was

essentially masked in trivia in a report circulated to other airlines and did not specifically identify that the failure was related to the method used to remove the pylon.

Precursors are not just technical in nature. The DC-10 example also shows how precursors can be related to procedural/human factors, political events, and decisions. Accident precursor recognition is a vital part of a proactive intervention strategy and needs to be an important part of any safety management program.

Root causes

A driving reason for investigating accidents is to prevent future accidents. By identifying root causes (a cause is a set of sufficient conditions, each is necessary but only together are they sufficient), we can potentially avoid a whole "class" of accidents. Unfortunately, there is significant variation in people's perceptions of accidents. For example:

- Viewing accidents as a single event. This often includes regulatory compliance/violation thinking;
- Linear chain-of-events thinking, like knocking over a row of dominos;
- Statistical analysis methods;
- Viewing an accident as a process involving concurrent actions by various actors to produce an unintended outcome.

At the heart of root cause analysis is the knowledge that things do not just happen. Events are caused to happen and by understanding the causes we can decide which ones are within our control and manipulate them to meet our goals and objectives. Root causes can be defined as the first factor in a chain of events that can be controlled through a regulation, policy, or standard. It is a point in the chain of events at which internal control can be exercised. Simply put, they can be found by stating the end-result and keep asking "why?" until you have found a factor that can be corrected by the application of a regulation/policy/standard at the governing/management, implementing, or individual level, or you have reached a non-correctable situation. There may also be insufficient data to proceed further.

There is a strong link between root causes, decision-making, and lessons learned, especially in:

- establishment and communication of a regulation or policy;
- application of a regulation or policy;
- establishment and communication of monitoring and oversight; and
- enforcement of that regulation or policy, based on monitoring and oversight.

System Safety

In commercial aviation, a single accident is often disastrous. One obvious lesson from the short history of aviation is that most accidents are not the result of unknown scientific principles but are more likely result from the failure to apply well known engineering practices. A valuable lesson is that technology alone will not provide a solution; another lesson from history is that the non-technical issues cannot be ignored. Safety requires control of all aspects of the development and operation of a system. System safety covers the entire spectrum of risk management, from design of hardware to the culture and attitudes of the people involved.

Safety is a property of a system. For example, determining whether an aircraft is acceptably safe by examining the landing gear, or any other component, is not possible. Talking about the "safety of the landing gear" out of context of the aircraft and how it operates is really meaningless. Safety can only be determined by the relationship between the landing gear and other aircraft components, that is, in the context of the whole aircraft and its environment.

A systems approach provides a logical structure for problem solving. It views the entire system as an integrated whole. To make the system safe, we must manage safety (risk) and we must assess safety. Management is what is done to assure safety (limit risk) and assessment (surveillance, in this case) is what is done to determine whether the results are satisfactory. One cannot be practiced without the other to have a positive impact on safety.

System safety is characterized by the systematic identification and control of hazards throughout the lifecycle of a system. It calls for the timely identification of system hazards before the fact and emphasizes the designing an acceptable level of safety into the system.

Some basic concepts of system safety are:

- Safety should be built into the system, not added on to a completed design.
- Safety is a property of the system, not a component.
- Accidents are not always caused by failures and all failures do not cause accidents.
- Analysis to prevent the accident is emphasized instead of reacting to the accident.
- Emphasis is on identifying hazards as early as possible and then designing to eliminate or control those hazards (more qualitative than quantitative).
- Recognize tradeoffs and compromises in system design.
- System safety is more than just systems engineering.

Design Safety Concepts

Aviation safety begins with safe aircraft. The safety of large transport airplanes operating in commercial service throughout the world has steadily improved over the last several decades. Many techniques are used to achieve a safe design and include:

- Design Integrity (will not fail or has very high margins, e.g., propellers, landing gears, turbine rotor discs) and Quality
- Redundancy
- Isolation
- Reliability
- Failure Indication
- Flight Crew Procedures
- Checkable/Inspectable
- Damage Tolerance
- Failure Containment
- Designed Failure Path
- Margins/Factors Of Safety
- Error-Tolerance

The Four Basic Elements of Design Safety (US Transport Category Aircraft)

ELEMENT NO. 1. Basic Design Philosophy and Methodology
The design philosophy governs the overall design approach, establishes design criteria and dictates failure assumption. The fail-safe philosophy is the chosen basic design philosophy and from this has emerged the fail-safe design concept; i.e., "no single failure or probable combination of failures during any one flight shall jeopardize the continued safe flight and landing of the airplane."

Design safety precedence:

- Design to minimum hazard - Design the hazard out. If it cannot be eliminated, minimize the residual risk.
- Use safety devices - Do this by incorporating a fail-safe mode, safety devices, or fault-tolerant features.
- Use warning devices - Done through measuring devices, software, or other means. The warning should be unambiguous and attract the operator's attention.
- Use special procedures - Used when the above means are unable to control the hazard.

ELEMENT NO. 2. The Official Code of Airworthiness Design Standards for Transport Category Aircraft, Engines, Propellers, and APUs.
This is the legal codification of Element No. 1 and is usually referred to as the Type Certification Code. The legal design safety code specifies how the design safety methodology is to be applied; what general or specific design safety methods are to be incorporated; what, if any, specific exceptions are to be allowed; and, any specific additions.
FAR Parts 25, 33, and 35 are the legal codifications of the basic "fail safe design concept" that was developed by the U.S. aircraft transport industry over a period from the days of the Ford tri-motor of the 1920s until the present day.

ELEMENT NO. 3. The Type Design Check.
The purpose of the "design safety check" is to verify or validate that the design does in fact meet the required minimum safety standards embodied in Elements 1 and 2. The "Type Design Safety Check" is formally completed with the issuance of an FAA type certificate. The design safety check also includes the manufacturer's in-house safety assessments, flight and laboratory test programs, qualification test programs and the FAA Type Design Certification Program.

ELEMENT NO. 4. The Official Accident Investigation and the Finding of Probable Cause.
This includes an official public report of the accident findings. The knowledge contained in the findings, especially the lessons learned, is used to improve and strengthen the design philosophy, code and checks of Elements 1, 2 and 3.

Safety and Reliability
System safety and reliability are often confused. Although similar, it is important to first understand the difference between the two. Fundamentally, the two disciplines ask and seek to answer two different questions about two different concepts. Reliability asks, " How often does something fail?" System safety asks, "What happens (to the system) when something fails or behaves unexpectedly?" Although it is obviously concerned with system failure, reliability is

usually concerned with individual parts. Remember, a reliable system is not necessarily a safe system.

As applied to civil aircraft designed to FAR 25, safety is not reliability. As standards, they are related but distinctly different concepts with different objectives. Both are concerned with the causes of failure. The difference is, briefly, reliability is concerned with the frequency of failure and safety is concerned with the impact of failure. An aircraft design can be safe but unreliable; it can be reliable but unsafe; and it can be safe and at the same time reliable. Safety and reliability are essentially related, independent design parameters that tend to complement or oppose each other but one cannot be substituted for the other. The type certification process finds an aircraft design to be in compliance only with safety standards; it does not and cannot establish the reliability level of the design.

Design Integrity

The probability of failure of an aircraft component is controlled by its design specification, including its qualification testing, and is a measure of its design integrity. The concept of design integrity is concerned with the quality of the design and its ability to perform its intended functions as required by the design specification and FAR 25.1309(a). Design integrity is generally established through the qualification testing of individual aircraft components to their design specification requirements. Design integrity is an integral part of the basic aircraft safety concept. The achieved reliability of a component in service is a measure of its design integrity. The operator's approved maintenance program and the operator/manufacturers product improvement program control the reliability of an approved aircraft design.

Aircraft-Centered System

As discussed earlier, accidents, and consequently the lessons learned, are products of system interactions. Therefore, it is critical to have at least a minimal understanding of all the subordinate elements and how they behave as a system in order to identify, understand, and apply lessons learned.

The hierarchical breakdown used here is consistent with and adds to the Air Transport Association (ATA) index. This breakdown provides a familiar structure and is consistent with normal systems engineering practice. It is convenient for lessons learned because it groups subsystems together technologically. The aircraft is broken down as:

Airframe – This element includes wing, fuselage, and empennage.
Mechanical – This element includes landing gear, hydraulics, flight controls, and cargo loading equipment.
Electrical – This element includes electrical power and lighting.
Propulsion – This element includes the engine pod and pylon and their components, fuel components, and thrust management components.
Avionics – This element includes communication, navigation, and aircraft monitoring equipment.
Environmental – This element includes cabin pressure, air conditioning, and oxygen equipment.
Interior – This element includes crew and passenger accommodations.
Auxiliary, other – This element includes auxiliary electrical and pneumatic power supplies.

Other Factors in aircraft accidents

Aging Aircraft - The average age of the U.S. commercial aircraft fleet today already exceeds 75 percent of the typical nominal 20-year design life of a passenger aircraft. Significant attention must accordingly be given to better understanding and quantifying the mechanisms of aircraft aging. If these failure mechanisms are left unchecked, the significantly longer times in service that can be anticipated could lead to a significant increase in the accident rate.

Human Factors - Basic automated flight control systems and electromechanical displays are giving way to new generations of jet transport aircraft equipped with highly automated flight management systems and flat panel or liquid crystal displays. The new technology has significantly changed the work of airline pilots and has implications for all elements of the aviation system, especially design and safety regulation. Air safety investigators and researchers worldwide have witnessed the emergence of new human factors problems related to the interaction of pilots and advanced cockpit systems.

Environment – This is the environment external to the aircraft. Weather is the probably the most prominent factor.

Maintenance, Operations – Maintenance and operational events are the primary source of information for accident precursors and lessons learned.

Regulations, policies, standards – Past lessons learned are often captured in regulations, policies, and standards. Most accidents have factors related to the absence of or misapplication of such guidance and direction. Accident precursor information and lessons learned are a valuable source to aid in interpretation, implementation, and certifications decisions.

Software – All commercial transport aircraft designed and built within the last 15 years have some computer technology, mostly in the cockpit. The computers are intended to make flying easier and safer, and in general they do. But when things don't happen as expected, it can be hard to figure out quickly what's going on, and how to deal with it. The safety of an aircraft depends on designing and building it to the highest standards of safety we know and the same goes for its computer systems. Careful attention must be paid to how well we design and build those computer systems.

Most accidents will have lessons learned in more than one of the elements mentioned above and involve one or more of the concepts and factors discussed.

Conclusion

Lessons learned are defined as knowledge or understanding gained by experience. The lessons learned system must allow individuals to do their jobs more effectively and the aviation system to operate safer and more efficiently. Safety standards and the methods used to apply them must continually evolve due to advances in technology and demand for higher levels of safety. The

first step is awareness and a transition to a different way of making decisions for regulatory and industry personnel at all levels doing their job.

The role of lessons learned in the *Investigate, Communicate, Educate-Cycle* for Commercial Aviation can not be overstated. It is a necessary part of the organizational safety strategy involving continuously improving standards, validating design assumptions, identifying precursors, mitigating risk in safety related decision making, and correcting underlying sources of problems system wide.