Analysis of Aircraft Propulsion System Failure

Dr Arjen Romeyn
Australian Transport Safety Bureau

Author Biography:
Dr Arjen Romeyn (MIEAust, CPEng) has a BSc Hons, MSc, and PhD in Metallurgy from the University of NSW. Since 1984 Dr Romeyn has been employed by the Australian Department of Aviation and the subsequent Australian aviation agencies, Civil Aviation Authority, Civil Aviation Safety Authority, Bureau of Air Safety Investigation, and Australian Transport Safety Bureau. Throughout this period Dr Romeyn has conducted hundreds of investigations in the area of structural and mechanical failures arising from airworthiness deficiencies, safety incidents and accidents. He is currently the Principal Failure Analyst at the Australian Transport Safety Bureau. His area of specialty is the analysis of failures in engineered systems.

ANALYSIS OF AIRCRAFT PROPULSION SYSTEM FAILURE

A. Romeyn
Australian Transport Safety Bureau, PO Box 967, Civic Square, ACT, 2608

ABSTRACT

Engineered structures form the basis of the air transport industry – an industry society expects to be safe. Safe operation of a complex vehicle cannot be assured by simple means. The safety systems that have been developed comprise of a variety of constraints, agreed limitations and multilayered defences. Safety systems are developed in response to expectations, employ the concept of risk and are modified in the light of reality. Complexity is present at many levels in an aircraft and, in particular, an aircraft propulsion system. Complexity plays a major role in the difficulty of matching reality with expectations.

The focus of this paper is the analysis of repeated structural failures of reciprocating engines used to power low-capacity regular public transport aircraft. The analysis draws on the case of a fatal accident involving a double engine failure and a number of serious incidents.

An additional broader focus is a discussion of the methodology employed to determine the factors that initiate failures of technical systems. The process of analysis is not simple. It is a process of learning that involves the elements of seeing, evaluating and communicating.

1 INTRODUCTION[1]

Engineered structures form the basis of the air transport industry — an industry that society expects to be safe.

Airframes, powerplants, propellers, landing gear and other mechanical and electrical systems are essential elements of aircraft. They are designed, manufactured and maintained with the aim of preventing failure during operation.

Since the time of the Wright Flyer, the design of aircraft structures, powerplants and systems has evolved, within the general constraint of society's expectations of safety, to the present day broad range of aircraft (supersonic fighters, jumbo transports, a multitude of medium and small, jet and turboprop, transports and helicopters). Over this period failures of engineered structures and systems have resulted in accidents. The lessons learnt from these failures have been incorporated into design standards, manufacturing and maintenance standard practices, approval and certification of products and personnel and the prescription of operational limitations — a comprehensive, complex, engineering safety system.

A prime goal in the design and operation of transportation systems is the avoidance of threats to safety – safety of operators, passengers and bystanders.

> Design has its first and foremost objective the obviation of failure[1]

However, there are other objectives that must be satisfied if the design is to progress from the drawing board or prototype; purchase price, lifetime cost, running cost, ticket price, operational life, maintainability, performance (speed, payload).

Present day transport aircraft are complex assemblies. Jumbo jets have been described commonly as 6 million parts flying in formation. Aircraft have additional complexity in that they operate as both land and air vehicles.

> The run-up to takeoff is a metamorphosis: here is a pile of metal transforming itself into an airplane by the power of air itself, each takeoff is the birth of an aircraft.[2]

The safe operation of a complex vehicle cannot be assured by simple means. The safety systems that have been developed comprise of multilayered defences covering all aspects of design, construction and operation. Despite our best efforts, and the present day safety systems, failures and accidents still occur. Why? Clearly, safety systems are not ideal and continued learning and adjustment is required.

> To make flight "natural" it had been necessary to formalise it as far as possible, to draw up a complicated grammar of rules and exceptions, a body of procedures and precedents, corrected and emended over the decades in the light of errors and catastrophes, because errors in this grammar were paid in cash, and at top price.[3]

Safety systems are developed in response to **expectations**, employ the concept of **risk** and are modified in the light of **reality**.

[1] The basis of this paper was first presented to the International Conference on Failure Analysis, Melbourne Australia, 20-22 November 2002, proceedings published by Institute of Materials Engineering Australasia Ltd

2 EXPECTATIONS

Everyone has expectations regarding the performance of transportation systems. These expectations are not consistent across all sections of society and may change within a group with time or as the result of personal experience. Expectations are coloured by the perceptions, views, understanding, prejudices and biases of each section of society.

Commercial aviation, nuclear power, petrochemical industries and marine transportation are considered by the general public to be hazardous industries. These industries are expected to operate without mistakes – or at least the sorts of mistakes that have no catastrophic consequences. While other industries develop through trail and error, hazardous industries are expected to develop through trial without error.

The view of a wide section of society is captured by Penelope Layland's article in the Canberra Times 29 July 2000 "Prefer to be bitten if you're shy to fly" following the Concorde accident, 25 July 2000.

> I know the statistics. I am far more likely to die after being bitten by a dog, having the wound turn septic, then having an adverse reaction to an overdose of the wrong antibiotic delivered by a homicidal nurse, than I am to die in an aeroplane crash.
> So what? I'm not scared of dog bites and homicidal nurses. Yet every time I board a plane I am convinced that I am embarking on the final minutes of my life.
> Dogs and homicidal nurses are on my level – ground level. Planes fly. It is unnatural. A few hundred years ago, pilots would have been burned at the stake, and a good thing too.
> To fly one must entirely suspend one's understanding of gravity. Not that my understanding of gravity is particularly sophisticated, I'll grant you, but life experience tells me that if I accidentally drop a particularly cherished vase, there is a very good chance it will break when it hits the floor. The same life experience tells me that several tonnes of metal hurtling through the atmosphere will probably fall too, if something goes wrong with the engines that push them through space.

2.1 Pressures for Learning

The call to learn from incidents, accidents, deaths, disasters and catastrophes in order to save lives has become a catchcry of our time. Articles in professional journals and newspapers all call for increased efforts in learning.

> "More and more it's to learn some lesson from a particular death to save lives;" Mr Dingwall, an ACT magistrate, said. "It's learning from mistakes of the past."[4]

The call for learning from threats to safety come at a time when there are calls for increased learning in organisations to strive for improvements in management, service provision and product quality to achieve efficiencies, increased profits and greater competitiveness.

The expectations of society create the driving force for learning in the air transport industry in two areas:

- Safety, based on the perception of threats to individual and group well being posed by air transport;
- Economic, based on the willingness to pay for tickets, the desire to travel more quickly and the availability of alternate modes of transport.

3 RISK

The concept of risk introduces the sense of a hazard or threat and the likelihood or probability of encountering the hazard.

Traditionally, scientists and engineers have viewed risk as a purely technical issue, one that can be boxed off from the rest of technology and handled separately. It is one more technical issue to be solved. Risk decisions have been made inside the system[5]. However, it is now understood that when risk is involved technical and non-technical issues get tangled to a point that they are impossible to separate[6].

In the past safety issues were addressed by eliminating hazards however, as industries, systems and machines became more complex the way in which people think about safety has changed. It is no longer thought to be possible to engineer for complete safety, to determine the maximum credible accident and then assure that it won't threaten anyone.[7] The best that can be done is to try to make dangerous accidents very unlikely.

The development of risk assessment/management has evolved with experiences in the nuclear power industry. Initially, the threat of a nuclear reactor to public safety was assured by a simple scheme: put the reactor far away from where people lived, the larger the plant the larger the exclusion zone.

An engineered solution that eliminated the need for an exclusion zone was the construction of a "containment" building – a building that would prevent the escape of radioactive materials in the case of an accident. The design of the containment building was based on a determination of the worst possible accident and the impact this would have on structural integrity. The most difficult to resolve issues centred on the so-called loss-of-coolant accident, dubbed the "China syndrome". Safety now was assured by the performance of active safety systems and features such as emergency core cooling systems. Reactor safety design changed from being "deterministic" to "probabilistic". Risk was evaluated by taking into account the probability of safety system failure and the

consequences, in terms of fatalities, of that system breakdown.

Probabilistic assessment relies on calculating the probabilities of chains of events that may lead to an accident. A major weakness is the need to identify all potential failure modes and sequences and assigning probabilities for all events.

An initial estimate of the probability of a reactor core meltdown was once in every million years of reactor operation. A more rigorous assessment documented in the Rasmussen report[8] concluded that the probability of a meltdown could be expected only once in every 17,000 years of reactor operation. Less than five years after the Rasmussen study was completed, on March 28 1979, unit 2 of the Three Mile Island nuclear plant had a major accident. The reactor core melted partially and some radioactive material was released into the atmosphere.

The partial meltdown has reshaped thinking on risk in complex technologies[9].

4 REALITY

4.1 The Need for Prediction in Engineering[10]

An underlying feature of engineering design is the need to predict future behaviour and quantify risk. Will it work safely and will it continue to work safely?

In this less than perfect world our understanding of materials, structures and mechanisms, in the face of complex loading and environmental interactions, is not complete. Engineering design effort still requires human judgement and insight (especially in decisions regarding safety). Structural analysis is done in support of, not in place of, the creative process of design.[11]

If it looks right it will fly right!

Our mathematical models have limitations — they are approximations of reality. The danger is that mathematical models can hide our lack of knowledge. The properties of materials and some loads encountered during operation vary in a random manner, creating uncertainties.

Against a background of uncertainty, design goals are expressed in terms of probability of failure. For critical aircraft structures and systems the probability of failure is required to be 'extremely remote'. In the face of the expectation of an extremely remote probability of failure the challenge is to establish a design basis, to determine the hard values of strength and stress that allow structures and systems to be constructed.

The consequence of uncertainty and variation is the need to apply safety factors to design values. A design is an approximation, hopefully a conservative approximation to an effective structure or system.

While conservative design is necessary for safety it creates a conflict between the other objectives of an engineered structure or system; cost effectiveness, structural efficiency, improved performance. This conflict results in the process of fine-tuning.

The disparate nature of the goals imposed on the creators of aircraft make learning from operational experience a process of fine-tuning safety factors.

People are almost certain to reduce some safety factors after creating a system, and successful experiences make safety factors look more and more wasteful.[12]

People may cut safety factors while designing a socio-technical system. Large safety factors may render projects prohibitively expensive or technically impossible and thus prevent the solving of serious problems or the attaining of important goals. When they extrapolate actual experiences into unexplored domains, safety factors may also inadvertently create hazards by introducing unanticipated risks or by taxing other components to their limits.[13]

The danger of fine-tuning a system that has multiple and conflicting goals is that changes can always be justified and generate a benefit in one area while having an unrecognised effect in another area. The effect of system fine-tuning on safety is usually discovered by analysing accidents and disasters.

4.2 The Learning Process

In reality, there will always be a tension between the desire for decreased threat to life and the willingness to pay. The state of balance between safety and profitability depends on the ability of the creators, operators and regulators of a complex socio-technical transport industry to learn.

The rate at which learning is achieved is dependent on the immediate goals of the various players in the industry, eg. driven by a need to satisfy a market, compete with alternatives or in reaction to a disaster.

Adjustments from learning in one area may result in consequences that are not immediately apparent in another. The connection between cause and effect in different areas may occur over widely different time frames. Learning may also have to wait for developments in the understanding of physical phenomena.

The need to learn, its easy to say. What do we need to learn and how do we learn it? How do we know when we have learnt it?

5 ANALYSIS — HOW WE LEARN

From the perspective of safety it is desirable that air transport systems are examined, tested and analysed to determine when the process of fine-tuning is approaching the boundaries of safe operation, rather than waiting for the boundary to be crossed and analysing the results of accidents.

Traditionally, investigation involved the gathering of facts, what happened, what failed, how did it happen, how did it fail. More recently, there has been a greater emphasis placed on determining why failures occur.

To determine why a failure occurred, why an error was made, appears to be a logical step and sounds easy, but how do you know if the critical question has been answered? Why do failures still occur? If critical observations and critical questions are not answered then the root causes of system deficiencies and errors will not be determined, the analysis will not be effective and the opportunity to prevent recurrence will be lost. There is a need to examine every level of a system, not just the final outcome, all defences, and not just the final defence.

Analysis is a process of learning. Learning implies the gaining of knowledge. In the case of failure analysis, the gaining of knowledge that allows judgements to be made that result in the right corrections to the engineering safety system in order to fulfil the requirement for future safe operation.

The process of gaining knowledge is a key variable.

Analyses that achieve effective learning involve the processes of, **seeing**, **evaluating** and **communicating**.

All day and every day we are receiving information from our sense organs. The decisions and judgements we make based on the information received and the ways in which we adapt to and deal with new information are the essential features of learning. It is in these processes that variability in learning arises.

Some information sensed is immediately useful and is acted on. Much is not immediately useful: we are aware of receiving it but we do nothing about it. Other information is received without any conscious awareness.

The tools of a scientist, simple lens, electron microscope, thermometer, etc are designed to present to the eye information that is otherwise not available to it.

Every person has a store of information. As a result of seeing, listening, reading, reflecting on our experiences and reasoning we acquire both information and misinformation. Every person also has persistent deep-rooted ways of classifying information, thinking, perceiving and behaving. A person's prior information and behavioural modes determine what we see and how we evaluate information and respond. The process of recognition is the process of matching observations with our prior store of information.

During the investigation of accidents and disasters there is a need to develop an understanding of why the prediction of safe operation was inaccurate. There is a need to analyse issues that were previously unknown.

> Successful detectives differ from less successful ones in their ability to perceive as relevant to the solution of their problem pieces of information which the rest of us ignore, regard as irrelevant, do not see![14]

Important discoveries in science provide clear examples of making use of information that had previously been regarded as unimportant or useless. The ability to address new problems depends on the ability to make new associations between information where, previously, there have been no conventional or traditional relationships.

Successful analysis comes from the conscious consideration of many possibilities rather than jumping to a conclusion without considering the evidence for alternate ones.

5.1 Failure of Analyses

If the success of analyses depends on the mental processes and knowledge of the analyst then, the failure of analyses to prevent recurrence of accidents and disasters is also related to the mental processes, the knowledge of the analyst and the transfer of knowledge to those who are in a position to implement corrective action. There is a need to develop a comprehensive understanding of an industry and its safety system.

The shortcomings of analyses have more to do with mental processes, how information is gathered and used. In the present 'information age', it is not a matter of more information, more training which only involves the transfer of information from teacher to student, but the how information is gathered (seeing), evaluated and communicated.

Classification

Classification provides a link to a greater store of information, experiences and understandings relating to an event. The classification of a fracture links it with a mechanism that has been established by research and allows causal factors to be identified.

> [G. H. Lewes, 1879] And the new object presented to Sense, or a new idea presented to Thought, must also be soluble in old experiences, be re-cognized as like them, otherwise it will be unperceived, uncomprehended.[15]

The process of classification can cause great difficulties. The effect of own assumptions and preconceptions can lead to the incorrect classification of information, incorrect hypotheses and an incorrect prediction of future events.

Communication

Complex technologies are designed, manufactured, operated and regulated by complex organisations employing many people. No one person is responsible for all the actions required to design, monitor and modify safety systems. Effective communication is essential.

Technical descriptors (be it one word or a phrase) serve a vital role in communication about complex phenomena. The common understanding associated with the descriptor allows communication to occur.

The shortcomings of the use of technical descriptors lie in the, sometimes, imperfect connection between descriptor and phenomenon, leading to differing understandings by various people when a descriptor is used. Additionally, especially during investigation processes, the interpretation of the evidence of phenomena may lead to inconsistencies in classification – different technical descriptors may be applied to one phenomenon. For example, the use of the term 'failure' may sometimes be taken to refer to component fracture, loss of function of a component or mechanism, or a change from the normal function of a component, mechanism or process.

It is recognised that no one definition of a technical descriptor is necessarily adequate. It is also recognised that multiple definitions do lead to misunderstandings.

Culture

Cultural issues have a significant effect on the communications between the originators of new ideas (analysts) and those who are in a position to implement corrective actions or changes (managers). Additional communication difficulties are created when investigations are fragmented across a broad range of engineering disciplines. Each group has its own culture, preconceptions and, possibly biases.

Culture may also provide a resistance to change and a barrier to new thoughts.

> In periods of stability or of slow change the broad outlines of the pattern of culture are accepted by the majority almost unthinkingly and without challenge, and the principles that should govern behaviour are so thoroughly inculcated that they hardly need verbal reinforcement or even expression.[16]

Occasionally, the time must be right for learning to spread to those who are in a position to implement change.

> [On Young (Young's modulus)] a man of great learning but unfortunately he never even began to realise the limitations of comprehension of ordinary minds.[17]

The Effect of Complexity

Complexity is not merely a matter of the number of parts of the system. If system parts interact in a simple linear fashion, that is there is a simple linear dependency between the parts, a system with many parts is not complex.

The defining feature of a complex system is how its parts interact. If the behaviour of any part of the system depends or is influenced by the behaviour of other parts the system is considered to be complex - the more interaction and the increased multiplicity of interaction, the more complex the system.

The greatest effect of complexity is on the prediction of system behaviour and the less likely control will be reliable.

Complex industries operating complex machines have developed, over time, a multiplicity of overlapping and mutually supporting defences that make these industries largely proof against a single failure of a defence. However these "defences in depth" are a mixed blessing. They make the overall safety system more complex, more opaque and make a buildup of minor failures go unnoticed, weakening the entire system, making a catastrophic accident more likely[18].

The analysis of the Three Mile Island accident revealed that beyond individual errors and component failures and shortcomings in probabilistic risk assessment the complexity of the system created a situation where a number of seemingly minor events could interact to produce a major accident[19].

> People have also come to appreciate how complexity changes the risk equation, how it makes risk harder to calculate by making it difficult to understand all the ways that things can go awry. But equally important, complexity can amplify risk. The more complex a technology, the more ways something can go wrong, and in a tightly coupled system the number of ways that something can go wrong increases exponentially with the number of components in the system. The complexity makes a system more vulnerable to error. Even a tiny mistake may push the system to behave in strange ways, making it difficult for operators to understand what is happening and making it more likely they'll make further mistakes[20].

6 AIRCRAFT PROPULSION SYSTEMS, A COMPLEX SYSTEM

Complexity is present at many levels in any industry, from wide organisational arrangements to seemingly simple components whose apparent simplicity belie an underlying complexity in factors that determine their successful operation and effect on other closely coupled components.
An essential element of an aircraft is the propulsion system. That system provides the forward thrust necessary for flight. While gas turbine engines are the basis for propulsion systems for many aircraft, especially large civil transport aircraft, reciprocating engines coupled to propellers are used to provide the propulsive force for many smaller aircraft types. The high power variants of horizontally opposed, six-cylinder, air-cooled reciprocating engines coupled to constant speed propellers are used to power many aircraft employed in low capacity public transport operations.

It is important to recognise that, in reciprocating engine installations, the engine and propeller form an interdependent system. Constant speed propellers are coupled with high power reciprocating engines in installations that allow the propeller speed and engine power to be set separately to obtain the best combination of performance and fuel economy for all phases of flight.

Just as the engine and propeller form an interdependent system, the engine and fuel consumed in the engine form an interdependent system. Engine performance and fuel properties are closely linked. The history of engine development has been a process of mechanical refinement to extract the available energy contained in a fuel (aviation gasoline) under controlled combustion conditions and a concurrent refinement of gasoline formulation to allow advantage to be taken of mechanical refinements.

Finally, it is important to realise that the pilot and maintenance engineer, through their actions and knowledge, also form an interdependent system with the engine and propeller.

6.1 Expectations of Reciprocating Engines

The safe operation of aircraft relies on the correct operation of all the systems that combine to allow aircraft to function. The propulsion system is one of these systems.

Propulsion systems must have a high power to weight ratio, they must be economical, but above all they must be reliable.

The capability of an engine to produce the power specified by the engine manufacturer reliably throughout flight is a fundamental requirement of safe operation. Conversely, the failure of engines to produce specified power levels or the complete failure of an engine during flight is a threat to safe operation. That expectation is expressed simply in the design standard for aircraft engines, eg Federal Aviation Regulations Part 33 Airworthiness Standards: Aircraft Engines:

> Engine design and construction must minimise the development of an unsafe condition of the engine between overhaul periods.

And the International Standards for Airworthiness of Aircraft contained in Annex 8 to the Convention on International Civil Aviation (the Chicago Convention). Annex 8:

> The engine complete with accessories shall be designed and constructed so as to function reliably within its operating limitations under the anticipated operating conditions when properly installed in the aeroplane.

6.2 Reciprocating Engine Risk Management

The confidence that an aircraft engine will perform reliably, that risks are managed, is achieved by regulatory authority certification that the engine has passed an extensive testing program combined with approved instructions for operating limits, lubrication, inspection, component replacement, testing and adjustment. These design requirements form the basis of a comprehensive safety system.

The impact of the need for structural efficiency

Structural efficiency in design is necessary to achieve high power to weight ratios. The requirement that an engine design is reliable, within defined operating limitations, is demonstrated by performing the test program contained within the engine design standard (FAR 33). Instructions for maintenance are designed to ensure continued airworthiness under operational conditions. Operating limitations are determined for horsepower, RPM and manifold pressure at rated maximum continuous power. Items such as fuel grade, oil grade, cylinder head temperatures, oil temperatures, turbine inlet temperatures and component life are specified.

The strength and robustness of engine components and mechanisms, within the defined engine operating limits, is achieved by using materials that comply with standard specifications (to guarantee that the properties of the materials used match those assumed in design), and by a comprehensive test program.

> The engine must be designed and constructed to function throughout its normal operating range of crankshaft rotational speeds and engine powers without inducing excessive stress in any of the engine parts because of vibration and

> without imparting excessive vibrational forces to the aircraft structure[21].

Further demonstration of the adequacy and robustness of the engine is provided by an endurance test (FAR 33, subpart D, section 33.49). Engines are subjected to blocks of engine operation under a variety of operating conditions to a total of 150 hours of operation. At the conclusion of the endurance test the condition of components and mechanisms is assessed during a teardown inspection. Each component must retain the functioning characteristics that were established at the beginning of the test.

The structural requirements of propellers are addressed by other sections of the aviation regulations (FAR part 35).

The impact of combustion abnormalities

Combustion in spark ignition engines is designed so that a flame front moves across the premixed fuel-air charge in the combustion chamber resulting in a controlled increase in gas pressure. Under certain conditions, rapid oxidation reactions occur at many locations within the unburned charge, leading to very rapid combustion throughout the volume. This essentially volumetric heat release in an engine is called autoignition, and the very rapid pressure rise leads to the characteristic sound of engine knock[22]. Within the aviation industry this process of autoignition or knock is referred to as 'detonation'. Detonation can cause mechanical damage through the creation of abnormal loads. It can also cause component overheating and melting by its effect on heat transfer mechanisms.

Detonation of the fuel-air charge in a reciprocating engine is the principal factor limiting the maximum power that can be produced by an engine. Its importance is recognised in engine design standards, eg FAR 33, subpart D, section 33.47 requires that:

> Each aircraft engine type must be tested to establish that the engine can function without detonation throughout its range of intended conditions of operation.

Avoidance of detonation is achieved primarily by the use of fuel with a known resistance to detonation (octane or performance number rating scales) and limitations on engine operating parameters.

6.3 Reciprocating Engine Reality

In reality components of propulsion systems do fail and flight safety may be threatened by the total loss of thrust, partial loss of thrust, damage to other structures and systems by the effects of fire or impact. Because of the complexity of the systems the consequences of a component failure may be benign or it may be catastrophic.

Operational experience is a test of safety system design – does reality match expectations, has the management of risk matched expectations.

Feedback on actual engine performance/behaviour is an essential element in determining the adequacy of the safety system and, if necessary, making adjustments to the safety system. Component failure, unless considered to be the consequence of normal operation, indicates a weakness or deficiency in the safety system.

Effective feedback depends on effective analysis. Effective analysis requires the consideration the effects of complexity and knowledge of the safety system.

A dilemma has been created by the need to quantify risk. The act of quantifying risk results in the acknowledgment of a finite probability of failure. If failure occurs, is this the failure predicted by statistics? If a predicted, extremely rare, event occurs can it be argued that analysis to prevent recurrence is unnecessary because of the small probability of recurrence?

The view taken from a safety standpoint, in contrast to a reliability standpoint, is that the system should be analysed on the basis of potential consequences, not on the basis of likelihood of occurrence[23].

In reality, in the light of recurrent component failure do expectations change?

Recurrent failure may change views of normality. Those within the safety system may come to view certain failures as normal; their expectation may change from one of reliability to one failure. If a fracture control plan isn't working is it because of some statistical variation created by some unknown microstructural variation? This subtle change in expectation may lead to the establishment of latent failures in the safety system. Those outside the safety system may not share the subtle change in expectation and may judge things differently in the light of accidents.

Numbers of failures do not provide a good measure of the health of the safety system. In the case of components the probability of failure when subjected to a tensile stress is given by the overlap of the distributions of the tensile strength of the component and magnitude of the applied tensile stress[24]. The numbers of failures don't give complete information regarding the nature of the distributions, just the margin between the weaker components and the higher stresses. It doesn't give any information regarding the shape of the distributions and whether the current distributions are the same as those assumed during design. In a similar manner numbers of failures of a safety system may be considered to represent the overlap of distributions of system strength and system stress.

The robustness of a safety system relies on all levels of the system functioning as planned, the prevention of latent system failures and an effective analysis and feedback process to correct deficiencies strengthen weakness.

6.4 Reciprocating Engine Failure Analysis

A recent study by the ATSB[25] of the structural failure of high power reciprocating engines (greater than 300HP) has revealed that failures are not restricted to one component.

The study found that the factors initiating a series of events that result in the failure of a powertrain component can be grouped according to several fundamental physical, chemical and thermal processes. For example, mechanical loads created by the pressures developed in the combustion chamber are a result of the combustion process. Component temperatures are a result of the heat balance between the component and its environment which, in turn, depends on resistances to heat transfer. Bearing damage is a function of the process of lubrication and frictional heating. Bolted joint behaviour depends on the nature of deformation (elastic or plastic) between abutting components.

Component fracture or failure to perform its function occurs when the controls or limits on these fundamental processes have been exceeded or been ineffective. For example, component stresses arising from the pressures developed in the combustion chamber will be affected adversely by combustion abnormalities. The boundary between normal and abnormal combustion depends on factors that may be controlled by the pilot (power, mixture, temperature and rpm setting), specified operational procedures (power, mixture rpm, and temperature), maintenance personnel (the actions and procedures involved in adjustment, calibration, repair, and overhaul), and fuel supply (octane rating).

Gaining an understanding of why the controls and limits had been exceeded or ineffective forms the basis for prevention of further failures

7 CONCLUDING REMARKS

The major effect of complexity is its impact on our ability to predict the future behaviour of socio-technical industries. Complexity affects all levels of these industries, from human interaction and operation to the design and behaviour of mechanical systems and structures.

Complexity increases the demands on failure analysis. There is a need to move from one-dimensional analyses or compartmentalised analyses to analyses based on a multi-dimensional understanding of safety systems and identify weaknesses and deficiencies in the safety systems.

The process of analysis is not simple. It is a process of learning that involves the elements of seeing, evaluating and communicating. The effectiveness of analysis is built upon the process of increasing individual information stores, developing mental processes that allow new problems to be addressed, gaining an awareness of factors that limit learning and developing strategies for communicating.

On the issue of communication it is important to be aware that mere logical reasoning will not be enough to achieve acceptance of the findings of an analysis by everyone. People may have non-logical reasons for believing the things they do. Compassion, honesty and tact are as important as logic in gaining the acceptance of findings[26].

The safety of complex, risky technology lies in human hands, however the complexity of the technology guarantees that there will always be surprises. And in the case of surprises, the best defence is human competence, expertise and imagination[27].

…Therefore, go forth, companion: when you find
No highway more, no track, all being blind,
The way to go shall glimmer in the mind.

Though you have conquered Earth and charted Sea
And planned the courses of all Stars that be,
Adventure on, for the littlest clue
Has come whatever worth man ever knew;
The next to lighten all men may be you…..
John Masefield[28]

REFERENCES

[1] H. Petroski ,*To Engineer is Human*, Vintage Books, NY, 1992, p2
[2] D. del Giudice, *Takeoff*, Harcourt Brace and Co, NY, 1996, p5
[3] ibid, p39
[4] Honey Webb, *Coroners playing the more preventative role: magistrate*, Canberra Times, 13 October 1999
[5] R Pool, *Beyond Engineering, How Society Shapes Technology*, Oxford University Press, NY, 1997, p 186
[6] ibid p 186
[7] ibid, p 203
[8] *Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Plants* [Rasmussen Report], WASH-1400, NUREG 75/014. Nuclear Regulatory Commission, Washington, D.C., 1975
[9] R. Pool, op. cit, p 199
[10] Sections 4.1 to 4.4 are drawn from a paper titled "*Analyses of Failures and Failures of Analyses – Experiences in the Air Transport industry*" presented to

an Institution of Engineers Australia seminar titled "*The Worst Failure The Failure to Learn*" by the present author, 2 November 1999
[11] H. D. Curtis, *Fundamentals of Aircraft Structural Analysis*, Irwin, 1997, p 34
[12] W. H. Starbuck and F. J. Milliken, *Challenger: Fine-Tuning the Odds Until Something Breaks*, J of Management Studies, 25(4), July 1988, p 333
[13] ibid
[14] M. L. Johnson Abercrombie, *The Anatomy of Judgement*, Penguin Books, Harmondsworth England, 1969, p.60
[15] ibid, p. 59
[16] ibid p. 68
[17] J. E. Gordon, *New Science of Strong Materials*, Penguin Books, Harmondsworth England, 1968, p. 38
[18] J Reason, *Managing the Risks of Organisational Accidents*, Asgate Vermont, Aldershot England, 1997, pp 7,8
[19] R. Pool, op.cit, p202
[20] R. Pool, op cit, p204
[21] Federal Aviation Regulations Par 33, Airworthiness Standards: Aircraft engines, Subpart C, Design and Construction; Reciprocating Aircraft Engines, Section 33.33 Vibration
[22] An Introduction to Combustion, Concepts and Applications, S R Turns, McGraw-Hill, 1996, p 6
[23] A Weir, *The Tombstone Imperative, The Truth About Air Safety*, Pocket Books, London, 2000, p 235
[24] ASM Handbook Vol 8, ASM International 1992 USA, p 627
[25] Aircraft Reciprocating Engine Structural Failure, ATSB Technical Analysis Safety Study, in preparation
[26] Stephen's Guide to the Logical Fallacies, http://www.datanation.com/fallacies/howto.htm , p2
[27] R Pool, op. cit, p 204
[28] N Shute, *No Highway*, Mandarin Paperbacks, London, 1990, preface

SELECT BIBLIOGRAPHY

M. L. Johnson Abercrombie, *The Anatomy of Judgement*, Penguin Books, London, 1969
J. Passmore, *The Philosophy of Teaching*, Duckworth, London, 1980
Hidden Histories of Science, ed R. B. Silvers, Granta Books, London, 1998
M. J. Moroney, *Facts from Figures*, Penguin Books, London, 1954
W. H. Starbuck and F. J. Milliken, *Challenger: Fine-Tuning the Odds Until Something Breaks*, J of Management Studies 25(4) July 1988
J. E. Gordon, *The New Science of Strong Materials*, Penguin Books, Harmonsworth, England, 1968
R Pool, *Beyond Engineering How Society Shapes Technology*, Oxford University Press, NY, 1997