CONTINUING AIRWORTHINESS - REQUIREMENTS AND SUBSTANTIATION

F. C. Fickeisen
Chief Engineer, Requirements and Compliance, Boeing Commercial Airplane Group
Seattle, Washington

Abstract

Requirements to show that airplane systems continue to operate with levels of safety demonstrated during initial certification processes have been established. These requirements take two forms: 1) Follow approved maintenance procedures and schedules to assure continuation of design reliability levels; 2) Measure reliability levels by use of in-service data and take action when measured values approach levels shown to be necessary by certification analyses. Both processes are used successfully, and each has some inherent limitations. The second process requires in-service data sources, data reduction and analysis, and a method to compare in-service results to predictions. Though the second process is generally more complicated, it has the advantage of providing some insight into corrective actions that may enhance system reliabilities.

I. Background

The airworthiness of a new airplane type, a derivative airplane type or a new system for operation on a new, or derivative or in-production airplane is established prior to type design approval. Both type design approval and operational approval must precede commercial use of an airplane. The type design approval process employs analysis, test and previous relevant experience to show compliance with certification standards. The need to maintain the standards of airworthiness established by the initial approval process is the basis for continuing airworthiness requirements. These requirements have generally been founded on the premise that if airplanes and their systems are properly maintained and operated, then the level of safety intended and originally demonstrated will continue. This reasoning is the basis of the United States Federal Air Regulation 25.1529 and its European counterpart Joint Airworthiness Regulation 25.1529. These regulations and their resulting appendices require the establishment of approved airplane maintenance manuals and instructions. This approach (25.1529) establishes an "open loop" system; "open loop" in the sense that there is no specific requirement to measure and report on the actual levels of achieved reliability. It should, however, be noted that FAR 21.3 requires the reporting of specific individual operational events such as: fires caused by equipment malfunctions, significant primary structural defects, engine failures, complete loss of more than one hydraulic or electric power system, a failure of more than one attitude source and others These individual event reports can be used by certifying authorities to give an overview of system reliability and this has been done in a few cases.

The view and approach to continuing airworthiness discussed above has been expanded in a number of specific areas. The general characteristic of these expansions is that they establish a "closed loop" viewpoint: that is, in-service reliability is reported so that the initial safety analyses can be verified or so that actions to correct low reliability elements can be defined. Examples of expansion of the continuing airworthiness concept are provided below:

I.A. The criteria for "Approval of Category III Landing Minima, Federal Aviation Administration Advisory Circular 120-28C" states,

"OPERATIONAL REPORTING

a. For a period of 1 year after an applicant has been advised that its aircraft system meets Category III requirements, and reduced minima are authorized, the operator is to provide a monthly summary to the FAA of the following information:

(1) The total number of approaches where the equipment constituting the airborne portion of the Category III system was utilized to make satisfactory (actual or simulated) approaches to the applicable Category III minima (by aircraft type).

(2) The total number of unsatisfactory approaches by airport and aircraft registration number with explanations in the following categories - airborne equipment faults, ground facility difficulties, aborts of approaches because of Air Traffic Control (ATC) instructions, or other reasons."

"b. For an Extended Period

(1) For FAA facility review, the operator is encouraged to provide to the certificate-holding office an annual summary of the total number of approaches in weather conditions below Category II minima on which Category IIIa or Category IIIb procedures were used, listed by airport and aircraft type and the number of aborted approaches due to equipment failures or ATC."

I.B. The criteria for "Approval of Airborne Omega Navigation Systems as a Means of Updating Self Contained Navigation Systems, FAA Advisory Circular 120-31A" states,

"ACCURACY AND RELIABILITY. The applicant should show:

a. That an adequate in-flight service reliability rate, stated in terms of in-flight mean time between failures (MTBF), is in existence, with no significant unresolved problems remaining."

I.C. The criteria for approval of "Extended Range Operations with Two-Engine Airplanes (ETOPS), FAA Advisory Circular 120-42A" states,

"11. CONTINUING SURVEILLANCE.
The fleet average IFSD rate for the specified airframe-engine combination will continue to be monitored in accordance with Appendices 1 and 4. As with all other operations, the certificate-holding district office should also monitor all aspects of the extended range operations it has authorized to ensure that the levels of reliability achieved in extended range operations remain at the necessary levels as provided in Appendix 1, and that the operation continues to be conducted safely. In the event that an acceptable level of reliability is not maintained, significant adverse trends exist, or if significant

deficiencies are detected in the type design or the conduct of the ETOPS operation, the certificate-holding district office should initiate a special evaluation, impose operational restriction if necessary, and stipulate corrective action for the operator to adopt to resolve the problems in a timely manner."

All of the above pre-suppose the availability of an adequate source of in-service experience information and a method or methods to determine that required safety or reliability levels have been achieved. These items are discussed in the following sections.

II. In-Service Experience Databases

If assessments of continuing airworthiness, to standards such as those described by I.A., I.B., and I.C. above are to be made, a database indicating in-service experience will generally be required. The world of the 1980s is awash with data and databases. Though these databases are frequently used by scientists and engineers, their sources and structure are not often described in appreciable detail and their limitations may not be well understood. For the purpose of addressing airworthiness issues, a casual approach is not justified. Figures 1a and 1b below show databases that have been employed to assist in addressing the extended range operations continuing airworthiness requirements (see I.C. above).

Figure 1a Database Development Process Using In-Service Information

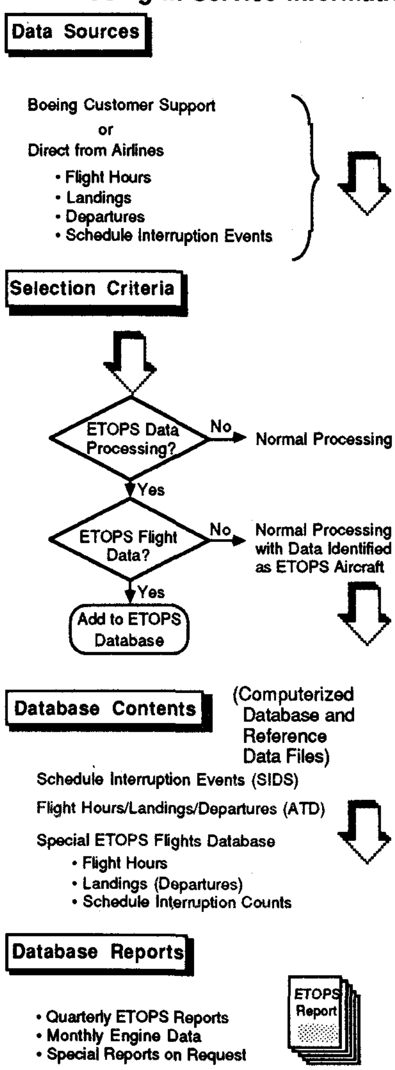
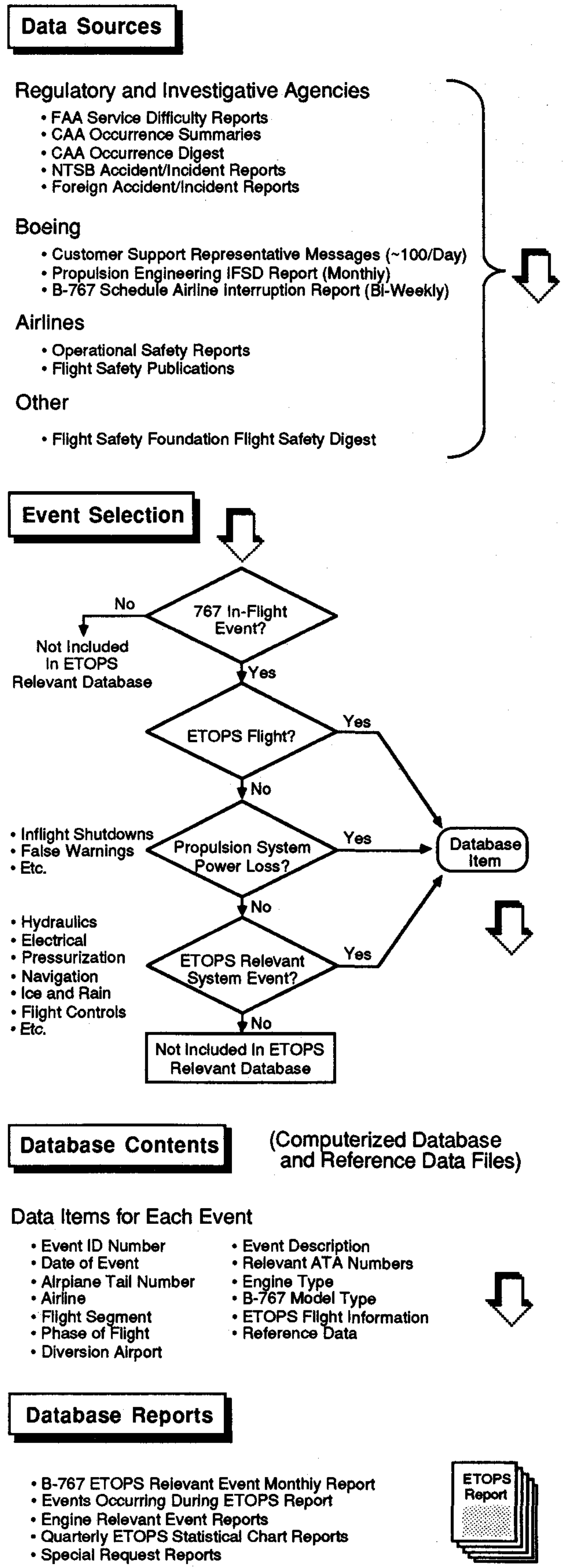


Figure 1b 767 ETOPS Relevant Events Database Process



The first of these specialized databases provides information relative to all aspects of flight (delays, cancellations, air turn backs and diversions). The second provides data only on in-flight events (air turn backs, diversions and flight situations in which the crew has been required to make a turn back/divert/continue-to-destination decision). Because of the nature of these databases and the sources of information there is no substantial concern with irrelevant or incorrect data being entered. There is, however, definitely a concern about completeness. Some events may not be entered or written up by flight or maintenance crews because of time pressures or the judgment that an event may not be particularly significant. Also, operators of small fleets may believe that because they have few events to report their contributions to the whole may be insignificant. Although every effort is made to assure the completeness of these databases, it must be understood that they are not exhaustive.

The second database phase, "selection" is also very important. Some events are the result of more than one cause (two equipment failures-one dormant and one active) or the combination of an equipment failure and a human error, etc. The selection (categorization) process can be partially automated but some level of judgment is always required. This judgment is generally provided by individuals who are knowledgeable concerning airplane operation and/or maintenance.

The final database phase "generation of reports" can generally be handled automatically but the selection of format and the provision of qualifying notes is crucial if the database information is to be "used" but not "misused".

With continuing airworthiness criteria established and with appropriate data sources available, the final step in the continuing airworthiness verification process is to show that the expected level of reliability has been achieved and to define corrective actions that may be appropriate.

III. Verification of the Achievement of Reliability Objectives and Definition of Corrective Actions

Databases of the type described in Section II above can provide information on the frequency of single element or channel failures, multiple element or channel failures, on the nature or type of failures and in some cases the history of failed elements or channels (age or previous failure record). This information can be used periodically to verify that the premises of type design approval are being achieved in airline service. It can also be used to define needed or desirable improvements and to uncover modes of failure which may not have been addressed in the initial approval process. Along with these virtues of the verification process, it should be noted that it can by overused. That is, for a number of systems, an inspection of individual events that have occurred in-service is sufficient to verify the achievement of safety and reliability objectives and to define needed changes: a detailed and structured numerical verification process may serve no practical purpose.

An example of an airplane system that may benefit from a structured review is the electric power system of a current twin jet airplane (Figure 2). The system consists of three main generators (two engine driven and one Auxiliary Power Unit (APU) driven) one hydraulic motor generator system, and a standby battery system. It supplies power to essential flight instruments, navigation systems, and communication devices, so its reliability is essential for safe operation. Certification of the system is based on a combination of test and analysis. A fault tree analysis (Figure 3) is one structured analysis process used to verify that a system can achieve a required level of safety.

Figure 2 Electrical Power System of a Current Twinjet Configured for ETOPS

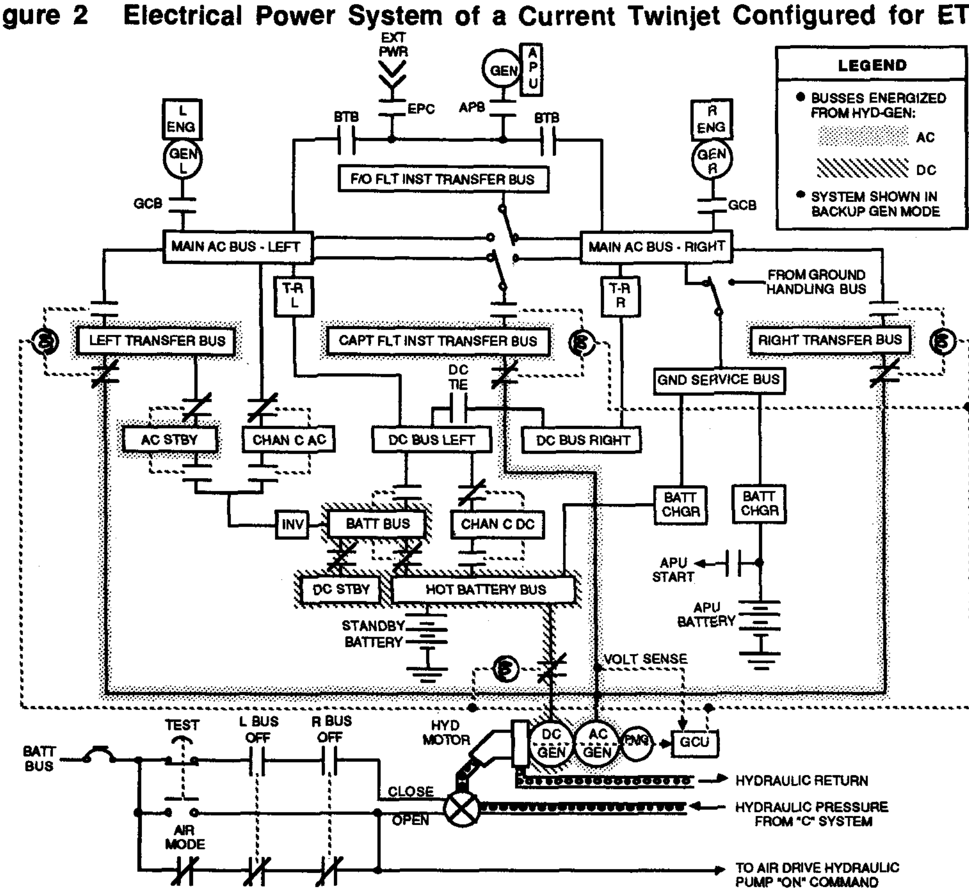
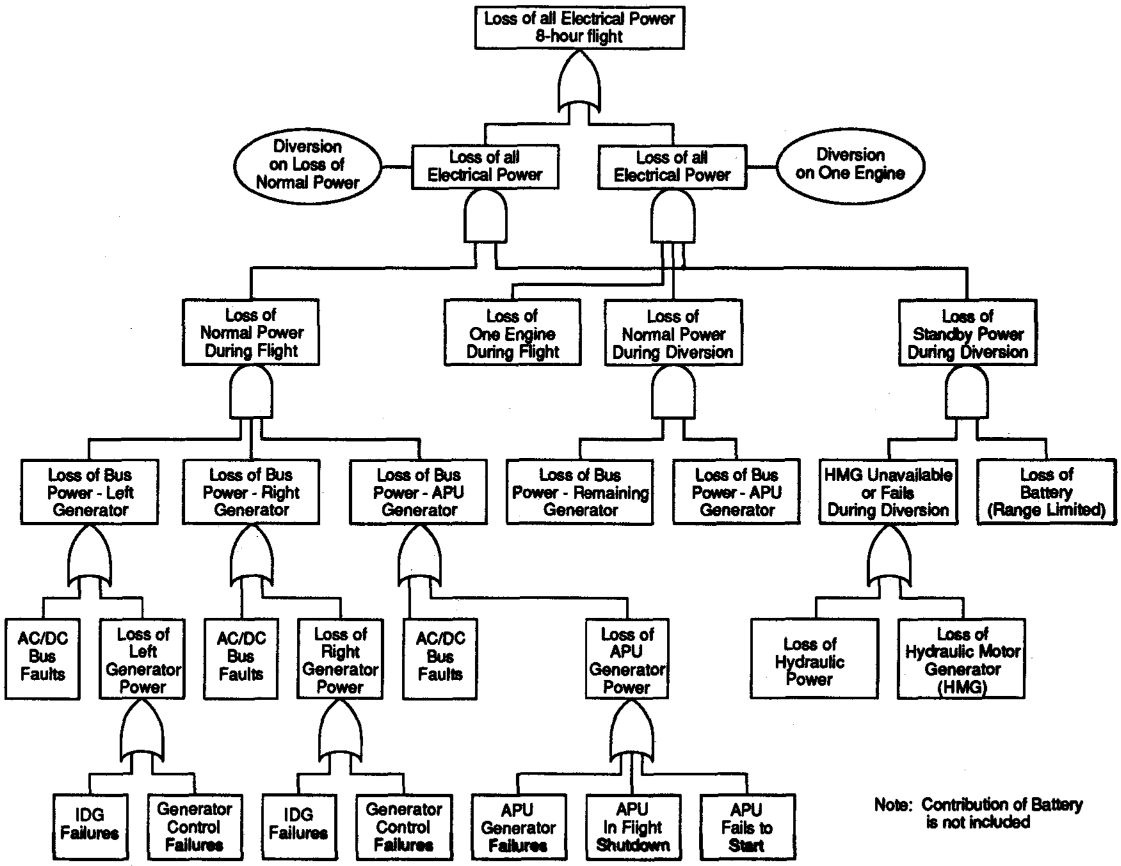


Figure 3 Fault Tree - Loss of All Electrical Power



With a fault tree and with a set of operational constraints defined (as examples: number of elements that may be unserviceable at dispatch, maintenance requirements that limit unserviceability time periods, crew actions resulting from inflight element failures, etc.), a numerical analysis is performed to show that the reliability objective (loss of all electrical power) is met. This is illustrated by Figure 4. It should be noted that structured safety or reliability analysis approaches other than the fault tree method described here may be effectively employed in some cases (e.g., a Weibull analysis: the analysis technique may dictate the database requirements.

Figure 4 Analysis Matrix for Loss of All Electrical Power

Dispatch Configuration	Engine Driven Generator Channel Failure Rates (×, * exposure)	Engine Driven Generator Channel Failure Rate (×, * exposure)	APU Channel Failure Rate (×, * exposure) + APU Failure to Start Rate	HMG Failure to Start/Run Rate	
Normal	(2 x 2.00E-04 x 6.30)	(2.00E-04 x 0.85)	((6.10E-04 x 3.15) + 0.03)#	(2.16E-03)	= 2.95E-11
IDG Inop	(2 x 2.00E-04 x 6.30)#		((6.10E-04 x 0.85) + 0)	(2.16E-03)	= 2.82E-09
APU Inop	(2 x 2.00E-04 x 6.30)#	(2.00E-04 x 0.85)		(2.16E-03)	= 9.25E-10
HMG Inop	(2 x 2.00E-04 x 6.30)	(2.00E-04 x 0.85)	((6.10E-04 x 3.15) + 0.03)#		= 1.36E-08

Dispatch Configuration	Engine Failure Rates				
Normal	(2 x 6.80E-05 x 3.15)#	(2.00E-04 x 1.00)	((6.10E-04 x 1.00) + 0.03)	(2.16E-03)	= 5.66E-12
IDG Inop	(2 x 6.80E-05 x 3.15)#		((6.10E-04 x 1.00) + 0)	(2.16E-03)	= 5.64E-10
APU Inop	(2 x 6.80E-05 x 3.15)#	(2.00E-04 x 1.00)		(2.16E-03)	= 1.85E-10
HMG Inop	(2 x 6.80E-05 x 3.15)#	(2.00E-04 x 1.00)	((6.10E-04 x 1.00) + 0.03)	(2.16E-03)	= 1.62E-09

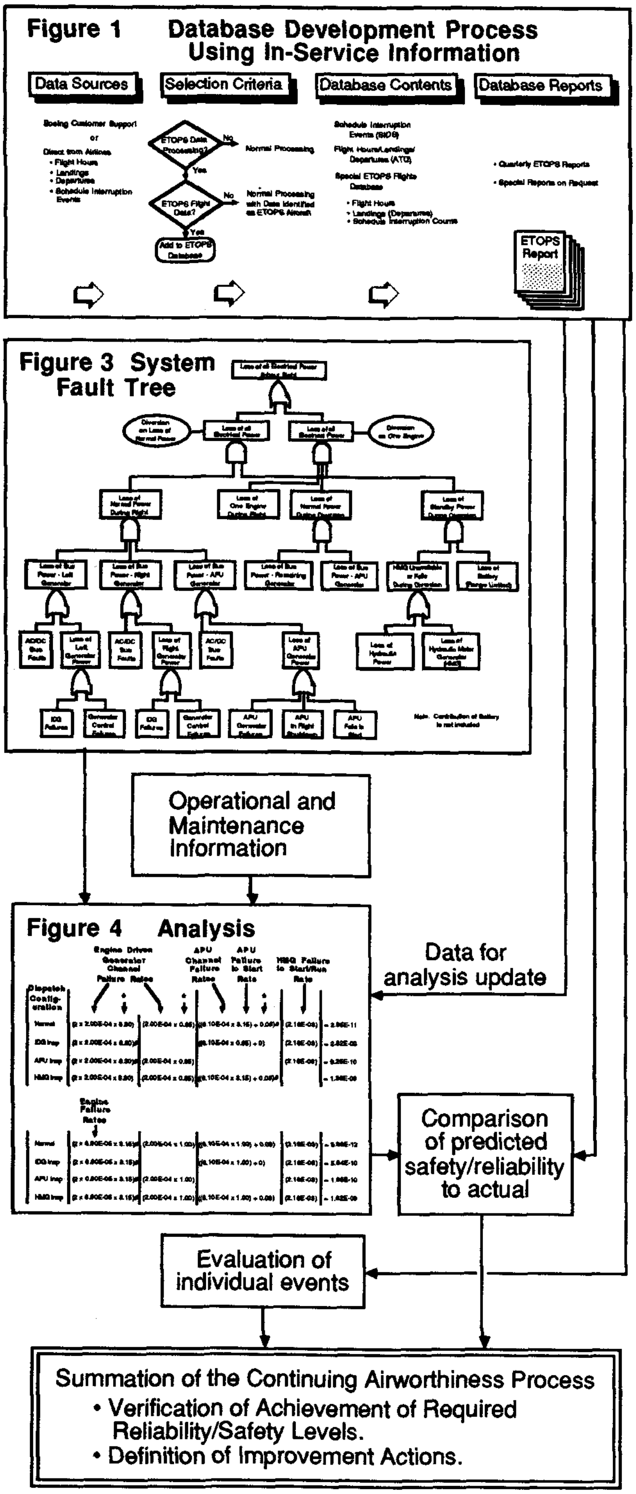
* Exposure Times (A function of the most extensive operation - length and distance from alternate airports.)

Resulting Likelihoods of Loss of All Power (Per Flight Values)

The resulting likelihoods of loss of all power must be combined based on dispatch and maintenance considerations if an average likelihood of loss of all power is to be established.

The likelihood of loss of all power per hour of flight values may be established by dividing the per flight values by flight duration.

Figure 5 A Continuing Airworthiness Process
An Example



The analysis illustrated above is part of the basic certification process and for such a system, periodic re-evaluation contributes to the continuing airworthiness review process.

Using the figures provided above, a total continuing airworthiness review process can now be seen (Figure 5).

The process involves the structured use of all of the elements discussed in this paper (requirements definition, data accumulation and categorization, review of individual events and comparison of achieved, predicted, and required safety or reliability levels). The use of such a process does raise a number of questions. When achieved reliability falls below predicted reliability what action thresholds should exist? To what degree, and how, should individual operator reliability records be compared to fleet averages? What reliability rates should be used (cumulative, running averages, etc.)? These questions and others related to the process must be carefully considered. Answers are a function of the system being assessed, its criticality and the margin of safety it provides over and above the required level. There are, of course, variations to this process as a function of the systems complexity and criticality. However, the process goals remain constant

- verification that needed reliability levels are achieved
- definition of needed or desirable improvement action.

IV. Conclusion

The requirements for a continuing airworthiness process have been outlined. They are based on the obvious need to have reasonable assurance that safety requirements are being met in airline operation. Data sources are required for the conduct of continuing airworthiness review processes. Such sources are available and their use is appropriate assuming that their limitations are recognized. Techniques for conducting continuing airworthiness reviews include: the comparison of predicted reliability levels to actual levels, and the review of the individual events. The results of the process are: verification that required reliability levels have been achieved, and definition of needed or desired system improvements. The continuing airworthiness process if employed judiciously can be a significant contributor to the continuing improvements in commercial aviation reliability and safety.