NINETEENTH EUROPEAN ROTORCRAFT FORUM

Paper No A5

SAFETY ASSESSMENT OF HELICOPTER ROTOR AND TRANSMISSION SYSTEMS

by

D. ASTRIDGE*, P. MONTANO, V. VACCARO
AGUSTA, ITALY

*Derek Astridge & Associates, UK

September 14-16, 1993
CERNOBBIO (Como)
ITALY

ASSOCIAZIONE INDUSTRIE AEROSPAZIALI
ASSOCIAZIONE ITALIANA DI AERONAUTICA ED ASTRONAUTICA

SAFETY ASSESSMENT OF HELICOPTER ROTOR AND TRANSMISSION SYSTEMS

D. ASTRIDGE*, P. MONTANO, V. VACCARO,
AGUSTA, ITALY

* Derek Astridge & Associates, UK

Abstract

Design safety assessment procedures offer significant safety benefits to rotor and transmission systems. Safety assessment methods developed for parallel path systems require tailoring for this challenging application. Revised procedures are described which produce failure probability predictions in both quantitative and qualitative terms, aimed at satisfying current and emerging airworthiness requirements. Principal features include a strictly independent approach to the Hazard Assessment, a systematic approach to the identification of potential failure causes, use of incident data rather than reliability data as a basis for occurrence probabilities, and the application of engineering judgement to the selection of appropriate data and to the evaluation of technology improvements. Unrelated to any particular project application, the paper reviews design/technology improvements available for new rotor and transmission designs. A summary of lessons from the detailed survey of accident data is appended.

1. Introduction

Safety considerations have been of fundamental concern to aircraft designers from the earliest days of powered flight[1]. The formalisation of safety assessment procedures in a separately specified task is a relatively recent development, arising from the criticality, complexity, and interdependency of modern flight control systems[2]. In parallel with the development of such analysis procedures, airworthiness authorities have introduced requirements for their application to the design of new fixed and rotary wing aircraft[3]. The objective is to demonstrate by analysis, supported where necessary by tests, that the required safety levels can be achieved. Demonstration of compliance requires the determination of failure condition probabilities, expressed in either qualitative or quantitative terms which are defined in advisory material[4]. The broad intention of the requirements is that an inverse relationship should exist between the severity of a failure condition (e.g. 'minor, major, hazardous, and catastrophic') and its probability of occurrence (e.g. 'probable, improbable, extremely remote, and extremely improbable'). Furthermore a catastrophic failure condition should virtually never occur in the fleet life of the type. Until recently these requirements have been restricted to 'equipments, systems, and installations' as defined in subchapter 1309 of the requirements of the USA (FAR), Joint European (JAR), and UK (BCAR) civil authorities. This includes systems such as electrical power and hydraulic flying control systems (all referred to in this paper as '1309' systems), but excludes helicopter rotor and transmission systems. Requirements for design safety assessments of the latter is a more recent development, emanating from the UK CAA[5,6]. In 1985 the CAA re-defined rotorcraft categories in terms of the probability of occurrence of failures from all causes that would prevent safe flight and landing[6]. In the same document they introduced a new failure probability term - Very Remote - with the advisory interpretation of less probable than one per million flying hours. The same safety target was set for the rotorcraft as a whole, and for the rotor and transmission systems considered together[5]. The implication of this is that, in addition to specific targets for '1309' systems and any other systems, all of these considered together should have a critical failure probability at least an order of magnitude less likely - i.e. lower than 10^{-7} per flying hour. The European Joint Aviation Authorities also plan to introduce a requirement for design safety assessment of rotor and transmission systems. The draft material (NPA 29-4) requires a detailed qualitative failure analysis which identifies the means to minimise the likelihood of occurrence of hazardous or catastrophic failures. The attached advisory material advises that the concurrence of the cognisant certificating authority with the proposed compensating provisions should be obtained. In describing the background to the CAA's 'interim' requirements, which affect at least two rotorcraft types currently in course of development, Witham[7] quotes historical accident rates for rotorcraft and for a range of fixed wing aircraft types. The same data was used by the Helicopter Airworthiness Review Panel (HARP) in support of their call for airworthiness improvements, particularly in respect of passenger transport helicopters involved in North Sea operations. Detailed analysis of the historic accident record (investigation reports and summaries) reveals variations in system contributions - with time frame, types, operation/ theatre, fatal/non-fatal, basis of quantification, etc., but common features are apparent[8,9]. In most operations, both civil and military, the majority of accidents (up to 70%) are attributed to operational factors. Surprisingly, perhaps, operational factors in North Sea passenger transport operations appear to be significantly lower - approximately 45%[9]. In general, rotors and transmissions tend to

dominate the airworthiness or systems-related causes, with control systems, propulsion/fuel systems, secondary power systems, and structure together contributing up to a third. It is therefore evident that design safety assessments of rotor and transmission systems could benefit rotorcraft safety significantly, provided that they are executed effectively. To be effective the traditional analysis procedures must be closely examined and revised where necessary to suit rotor and transmission systems.

2. Traditional Design Safety Assessment Procedures

The application of formalised safety assessment procedures to the design of aircraft systems is a fairly recent development[2,10], and the term 'traditional' is used to signify their first aircraft application area - flying control systems and other '1309' systems referred to above. The background, objectives, analysis procedures, and data sources are described in detail in References 2 , 11. A brief summary of the characteristics and limitations of these procedures is given here as a prelude to the discussion of tailoring requirements for application to rotor and transmission systems. The safety assessment comprises two distinct phases:

2.1 Hazard Assessment/Analysis

The purpose is to establish Failure Conditions resulting from functional failures, establish the Safety Objectives associated with the Failure Conditions, and to determine the depth of analysis required in the Detailed Analysis of a particular system. The hazard assessment is performed in three basic steps:

a. define the system boundaries, its interfaces with other systems and with the crew, all required input and output functions, including incidental (self-generated) functions, performance parameters and allowable limits, and the environmental conditions which the system is required to withstand

b. determine the failure condition associated with each functional failure taking into account all operational phases of the aircraft, based on the consequences of the functional failure for other systems, the aircraft, and its occupants

c. classify each functional failure in accordance with its severity and relevant airworthiness requirements, and hence determine the safety objectives in qualitative or quantitative terms as appropriate.

The hazard assessment requirements dictate that combinations of functional failures be considered when adverse events, either internal or external to the system, can increase the severity of effect.

Hazard assessment is thus concerned with system functionality rather than its hardware.

2.2 Detailed Failure Analysis

The purpose is to establish the likelihood of occurrence of critical functional failure conditions predicated by the hazard assessment. The value of this analysis is therefore greatly dependent on the rigour employed in the hazard assessment. There are two possible approaches to the detailed analysis of a system, commonly characterised as 'top-down' (deductive) or 'bottom-up' (inductive)[2]. The former starts with a critical failure condition and considers the failure modes and combinations of modes which could result in that failure condition. Fault Tree Analysis (FTA) and Dependence Diagrams are powerful logic models in this category. FTA employs logic symbols (e.g. 'and', 'or' gates) which show the relationship of events needed for the occurrence of a 'higher' event. The limit of resolution of FTA is determined by the primary 'input' events, i.e. those events which are not further developed to a lower level. The method has the advantage of good visual representation of events and their combinations, and is particularly valuable for systems having redundancy or other reasons for combining events. The Dependence Diagram employs interconnected blocks which also start with the 'top event' - a particular failure condition. Each block represents the failure of a particular item or 'assembly', and is interconnected according to the effect that failure has on the system function. In both methods the predicted occurrence rate or probability of each individual event and minimal combinations that could lead to system failure are determined. Finally the overall probability of the particular failure condition is determined.

The 'bottom-up' approach starts with the physical components of a system and systematically examines each one to determine possible failure modes, and the possible effects of those failures. Failure Modes, Effects, and Criticality Analysis (FMECA)[10] is a widely used analysis tool in this category. Using a tabular proforma, for each component all

possible failure modes and causes are recorded together with relevant phases of operation, the possible effects locally, on the system under analysis, and on the aircraft. Also recorded are appropriate failure detection methods and 'compensating provisions' - i.e. means of circumventing or mitigating the effect of the failure. The predicted failure occurrence rate and criticality or severity classification are also recorded. FMECA has the advantage of completeness in consideration of components, but has a number of disadvantages and limitations when used for safety analysis. Firstly it is very manpower intensive and tends to be inefficient because it cannot focus exclusively on safety related failures. The method is used for many other purposes including maintenance and logistic support, and is therefore more cost and time effective if planned and tailored to satisfy all these requirements together. Secondly FMECA is less amenable to the consideration of combinations of failure modes which tend to prevail in safety critical events. Thirdly, because FMECA is focused on hardware design, it is more difficult to address adverse events such as human error and environmental factors.

Both approaches are dependent upon the availability and accuracy of relevant failure data, and engineering experience required for the necessary engineering judgements. The latter is required in determining component and system functionality and interaction, identification of safety critical failure modes, causes, and effects, provision of relevant failure data, identification and evaluation of the compensating provisions, determination of failure condition occurrence probabilities, and identification of any areas requiring design improvement. Application of these procedures has highlighted the difficulty of obtaining accurate numerical predictions. This is primarily associated with the lack of accurate and meaningful baseline data. Where large data samples are available, failure distribution curves such as Weibull or Log Normal can be conveniently applied. Bayesian methods are useful where data samples are small - this permits the range of reasonable failure probability to be determined through the input of subjective engineering judgement. Sensitivity analysis[2] has much to contribute to improved accuracy. Leitch[12] examines sources of error in data and analysis, and suggests ways of reducing them.

3. Constraints Imposed by Rotor and Transmission Systems

Helicopter rotor and transmission systems (R&Ts) are fundamentally flight critical, complex in nature, single-load-path in structure, highly loaded of necessity, and operate in an adverse environment including self-generated vibration and heat. Redundancy in load-paths, and damage-tolerance characteristics can be designed in to an extent, and the consequences of system failure can be influenced by the choice of rotor configuration, but the concept of 'fail-safe' R&T design has yet to become a reality. Much time, cost, and engineering expertise is committed to substantiating the integrity of new and upgraded R&Ts, but unlike the 'fit-and-forget' drive systems in modern automobiles, their continued airworthiness is very much dependent on effective maintenance and reconditioning, and is influenced by actual service usage and environment. Their significant contribution to the historical airworthiness record for transport helicopters is therefore not surprising, but this needs to be examined in some detail before attempting to apply traditional design safety analysis procedures. Whilst R&T related accident *rates* may appear somewhat higher than say turbo-propeller installations in aeroplanes[7], the rates are conditioned by low rate of flying hours accumulation. Factors influencing the latter include the maintenance dependency referred to above (much lower time between removals), usually a single 'main' R&T compared with multi-engines, and the limited operating range of helicopters. Thus the 10 fatal accidents for airworthiness causes in North Sea transport helicopter operations from 1965-1990 resulted in an accident rate of 4 per million flying hours as only 2.5 million hours were accumulated in that time[9]. In absolute terms the numbers are small - 6 attributed to rotors, 2 to transmissions, and 2 to propulsion/fuel systems. Analysed by type and major R&T component, 3 of the accidents were attributed to the same component on one helicopter type, but none of the remaining 5 involved type/component repetitions. Similar analysis of the world wide accident data base (Appendix 1) reveals a relatively small number of design weaknesses which resulted in more than one accident, the majority being 'one-offs'. This reflects to some extent the effectiveness of 'reactive' measures such as mandatory modifications to eliminate a weakness, but these cannot be relied upon to achieve low failure rates in view of the several factors which contribute to repeated occurrences:- components unrecoverable/ cause not discernible, 'concurrent' failures, maintenance/ reconditioning errors, and the difficulties involved in substantial re-design, all of which feature in the data base. Thus there is real scope for design safety assessment methods to support the existing pro-active measures such as substantiation testing. However, the North Sea data quoted above and the world-wide data underline the first difficulty - the zero failure target.

Zero failure has naturally been the long-standing aim of R&T designers who are well aware of the likely catastrophic consequences of system failure. Few rotorcraft types have accumulated more than 10 million hours throughout their service life, many achieve much less. Such totals require the equivalent of 140 samples flying 200 hours per month for 30 years. A safety target of 10^{-6} per FH, as required by the CAA[5] thus translates into an absolute number less than 10 for the R&T of a particular helicopter type. However, a typical R&T system comprises at least 10 major components which are treated as separate entities in terms of design, manufacture, and testing (2 rotors plus

mechanical control elements, 2 rotor drive shafts, 4 gearboxes plus structural/ dynamic mounting interfaces, 2 input shafts/ flexible couplings, and a rotor brake), the failure of any one of which could result in a catastrophic effect, and be recorded as an R&T failure. In order to achieve a 10^{-6} per FH target for the complete R&T, each major component would be designed to meet a target of 10^{-7} per FH. In absolute terms this translates to less than one failure throughout the service life of the type - which can only be zero. A design safety analysis applied to each major component must therefore be focused on eliminating all possibility of serious failure. A subsequent analysis of the complete R&T system, including component interaction and the influence of failures in other systems, can focus on the elements with the highest failure probabilities for the purposes of obtaining adequate margins, and for demonstrating compliance with the requirements. If this approach is successful it will have a dramatic multiplying effect as more rotorcraft types undergo the discipline. Conceptually at least, what appears to be a relatively small step in terms of aims and requirements (3-fold improvement[7]) promises a much greater reduction in the R&T related accident rate as older types are displaced - falling from $4x10^{-6}$ or worse in rate terms for all transport helicopter types considered together[7,9], towards zero (i.e.$<10^{-8}$ with ten successful types meeting the objectives, and no older types remaining). Whether in compliance with UK CAA requirements, or in satisfying self-motivated goals, the zero failure target has become a clearly identified aim. All effort should be directed at achieving this aim, including the application of best available design/ manufacturing/ maintenance technology and safety analysis methods.

A second difficulty for design safety assessment methods applied to R&Ts is the very different relationship between safety and reliability considerations, compared with systems having functional redundancy. The safety critical nature of R&Ts has led to the development of high levels of reliability in respect of serious failure modes. If this were not the case, helicopters would not be occupying their present pre-eminent position in several areas of passenger transport. Reliability of R&Ts as conventionally measured in terms of component removal rates, relates not to functional failures but to scheduled removals, 'on-condition' removals, and unscheduled removals for non-safety related cause. The purpose of 'condition-monitored maintenance' reliability data is to flag up any abnormally high removal rates.[13] Low mean time between removals (MTBR) or inspection intervals do not necessarily imply high safety risk - they may reflect conservatism applied for safety purposes, noting that R&Ts are inspection-dependent items. The increased risk of maintenance-induced damage will tend to be off-set by the increased opportunity for discovering early signs of failure. Occurrence data, as typified by the UK CAA Mandatory Occurrence Reporting (MOR) scheme addresses safety-related arisings, and is therefore potentially useful for the purposes of design safety assessment. However, only a minority of occurrences are investigated and reported with sufficient detail to permit judgements to be made about underlying causes. Exceptions are repeated occurrences and related accidents which lead to detailed investigations. Also, by definition, an Occurrence is an accident prevented. In many cases the prevention 'mechanism' is one of the compensating provisions for which credit may be sought in a design safety assessment (e.g. health monitoring), and the Occurrence may serve to support the case for that provision. The only data that is both relevant to R&T safety and available in sufficient detail is accident data - from individual accident investigation reports, from published summaries[14], special studies[15], and to a lesser extent from operators and manufacturers (normally classified confidential). This data should form the basis on which functional failure rates are calculated and against which the benefits of compensating provisions are evaluated. In pursuing a zero failure target it is not sufficient to know for example the total historic failure rate of bearings - it is necessary to identify the type of bearing, the standard of materials, manufacture, and installation employed, the status of lubrication, cooling, the response to indications of distress, and the occurrence of any abnormal operating conditions. Such data is required in sufficient breadth to cover all critical R&T components, and engineering experience is required in sufficient depth to interpret and apply the data.

4. Safety Assessment Procedures Developed for Rotor and Transmission Systems

4.1 Hazard Assessment:

The purpose of the hazard assessment is identified in paragraph 2.1, together with the three essential elements of the activity. Application to R&Ts involves no additional elements, but does require extreme rigour in all aspects - in identifying R&T functions and potential functional failures; in identifying the most critical operating phase relating to each loss of function; in identifying all interfacing systems and the effect of R&T functional failure on them; in determining the consequent rotorcraft failure condition, and the appropriate classification - from 'minor' to 'catastrophic'. It follows directly from the safety objectives for R&Ts set in some of the airworthiness requirements reviewed earlier - from their equality with those of the rotorcraft as a whole - that far more hazardous and catastrophic failure conditions can be expected to be postulated than in '1309' systems, or in propulsion systems. Furthermore R&Ts are particularly vulnerable to single element failures in addition to all of the other categories of failure - dormant, combination, common mode, cascade, and environmental/external. Thus R&T systems are fundamentally

less tolerant to any departures from extreme rigour in the hazard assessment. It is helpful to bear in mind that the hazard assessment is no more than a postulation of potential failure conditions in the most generic sense - it does not address the strengths or weaknesses of the particular project design. The latter is the function of the Detailed Analysis. It is conceivable that 'textbook' hazardous assessments could be published independently, covering the relatively modest number of variations in R&T functional configurations. Space limitations prohibit the inclusion of the authors' generic hazard assessments in this paper. However, we offer a number of suggestions which we consider important to the effectiveness of design safety assessment of rotor and transmission systems:

a. Conduct the hazard assessment as early as possible in the conceptual design phase to ensure that all hazards are eliminated or controlled in subsequent design stages. Most R&T components have long lead times from design to development hardware, and the slightest improvement required in a major component can result in significant delays and additional costs.

b. All known historical functional failures and failure conditions should be considered. There is no excuse for replicating known errors of the past, regardless of their source or nature.

c. R&Ts have a large number of functions in addition to the obvious ones. Care should be taken to include all of them, including all incidental functions such as lubricant containment, where appropriate. It helps to divide R&Ts into major sub-systems based on functional considerations (e.g. main rotor, main rotor drive, tail rotor drive systems etc.) and to start with a description of each sub-system which is focused on functionality.

d. In considering interfaces with other systems for functionality and failure consequences, note that potentially all such interfaces involve reciprocal action. For example a rotor system may impose lift, shear, and bending moment loads on a gearbox casing. It is a function of the gearbox to react those loads and thereby to adequately locate the rotor in all planes at all times and operating conditions. Also, whilst the function of a sensor is to extract a condition signal from a gearbox or oil system, the sensor installation can give rise to stress concentrations in the host component, or result in oil loss if it loosened or detached.

e. For each potential functional failure consider the operating condition that would give rise to the most adverse rotorcraft failure condition / classification.

f. Functional failure of monitoring provisions or safety devices should be considered in conjunction with the relevant functional failure of the R&T sub-system, both in terms of loss of output and of spurious output.

Matters which should be excluded from the Hazard Assessment and considered only in the Detailed Analysis include:

g. Component failure modes and combinations of element failures.

h. Probability of occurrence of functional failure, component failure, operating condition, or any other event.

i. Compensating provisions, including detailed design features / materials, testing, manufacturing quality control, maintenance actions, and monitoring provisions.

4.2 Detailed Analysis:

The purpose of the Detailed Analysis of each major sub-system is to identify and substantiate the compensating provisions, evaluate their safety benefit, and thence determine, in either numerical or qualitative terms, the probability of occurrence of each failure condition postulated in the Hazard Assessment, and classified as Catastrophic, Hazardous, or Major. Functional failures which could give rise to a particular failure condition are also identified in the Hazard Assessment. For each of these, all possible failure modes and causes must be identified and their likelihood determined. To satisfy the CAA requirements[6], numerical probabilities of occurrence are required for each potential failure condition classified as Catastrophic, together with the overall value for the R&T, which should be less than 10^{-6} per FH. Otherwise likelihood of failure could be expressed in qualitative terms (e.g. 'Extremely Remote' = Unlikely to occur when considering the total operational life of a fleet of rotorcraft of the type, but nevertheless has to be considered as being possible).

If the Hazard Assessment has been conducted in a 'generic' fashion as recommended above, the first task of the Detailed Analysis should be to check the Hazard Assessment document for compatibility with the project design - in particular for possible omissions of potential functional failures. No item in the Hazard Assessment should be arbitrarily deleted or reclassified - all items should be dealt with in a traceable manner.

The complexity of R&Ts necessitates a combination of 'top-down' and bottom-up' procedures in the Detailed Analysis. Proformas that we have produced to facilitate this approach are shown in Figs 1, 2, one set being devoted to each functional failure postulated for each major sub-system (e.g. Main Rotor). The same formats are applicable to qualitative and quantitative analysis - the examples given relate to the latter. Table 1a (Fig 1) identifies the critical components, failure modes, and causes. Also identified are the compensating provisions, or the means by which the effect of failure is circumvented or mitigated and the occurrence probabilities for the project R&T assessed, and the declared values justified. In the first part of this table the 'top-down' and 'bottom-up' procedures are reconciled. The items (components, assemblies, or systems) the failure of which could result in the particular functional failure (e.g. failure of drive to the main rotor) are first determined by 'top-down' considerations - by applying Fault Tree Analysis methods where necessary, or by systematic scrutiny of the system hardware in the form of general arrangement drawings. This involves systematic examination of each component and assembly which contributes to the particular function under consideration, starting at the 'point of delivery' and working backwards to the relevant 'input boundaries' e.g. from rotor shaft to engine shaft, and from oil jets to oil sump. Failure modes are then identified at functional failure level - e.g. complete fracture or complete disengagement of part of the drive in the case of 'failure to drive the main rotor'. The possibility of cascade type failures is considered for each component - e.g. oil supply interruption leading to bearing damage/overheating, leading to elevated temperatures in critical sections of a driveshaft. The potential causes of each possible failure mode are then determined in a systematic manner by applying the 'error checklist' shown in Fig 3 to the particular item and its supporting features (e.g. casing, bearings, oil supply, clamping features). The error checklist comprises four sections - design/material/manufacture, assembly/reconditioning, maintenance, and operation. Examples of all the items in the checklist relating to several different components are to be found in the incident data base which goes back to 1958 (Appendix - Table A1). Whilst quality control of manufacture, assembly, reconditioning, and operations may be outside the direct control of R&T design, these activities are open to design influence in terms of requirements shown on drawings, and in maintenance and operating manuals. In addition, design features and attention to design detail can reduce R&T vulnerability to these factors. Application of the checklist to each item in the Detailed Analysis ensures that the great majority of potential causes of failure are included. It is also necessary to consider the possibility of other causes, not experienced hitherto, that may be pertinent to a particular item, especially if it contains any elements which are particularly complex or novel - radically new materials, manufacturing processes, or configurations, for example. Space is provided for cross-reference to the results of the FMECA or 'bottom-up' analysis. In addition to providing a space-saving cross-reference to component part numbers, this permits a correlation check of the 'top-down' and 'bottom-up' procedures. Any gaps in the FMECA reference column will indicate that a particular combination of component, failure mode, and cause have not been considered in the FMECA. Any 'unused' items from the FMECA will indicate either an omission of a relevant failure mode/cause combination, or that they are not considered appropriate to the loss of function under examination. Engineering judgement is required in this reconciliation of 'top-down' and 'bottom-up' analyses.

Compensating provisions are identified under the headings: design, monitoring, manufacture, testing, and maintenance. In order to keep hard copy outputs within manageable bounds, a cross-referencing system is used to indicate substantiation material relating to each line item. This material is referenced separately in the form of drawings, design reports, test reports, etc. Further saving of space and repetition is obtained by means of a common data set associated with the error checklist. Individual line items can then indicate additional supporting material or the most significant compensating provisions relating to that particular combination of item/ failure mode/ cause.

Table 1b (Fig 1) records the occurrence probability data in numerical form, but a similar format can be used for qualitative analysis. For each line entry corresponding to Table 1a, columns are provided for accident or occurrence data from alternative sources. All relevant incident data is considered, and where more than one set exists the most critical case is recorded in the table, in terms of helicopter type and event occurrence rate. This may be the case with the highest historical occurrence rate, or the one with the most recent R&T technology, or any between the two. Where such information is available from more than one source, the most adverse case is recorded in the 'datum' column. For numerical analysis, the rate data is based, wherever possible, upon the world wide flying hours for that type, but where the incident(s) apply to particular operator(s) with the possibility that similar incidents may have been experienced by other operators but not published, then the flying hours accumulated by the particular fleet(s) is used.

Where no accidents or occurrences are recorded for a particular failure mode, the 'safety rate' is used - i.e. a rate less than the reciprocal of the total flying hours accumulated by all transport helicopter types in the data base.

The compensating provisions relating to the project R&T for each event is then evaluated and expressed as a 'beneficial' factor. This requires engineering knowledge and judgement - knowledge of the relevant technology employed in the datum type and in the project design, and judgement of the likely long term safety benefits of the enhanced technology, based upon test results and possibly experience elsewhere. This can vary from the fairly straight forward (e.g. avoidance of non-symmetrical thrust bearings in the case of reversed assembly incidents) to the more difficult (e.g. locking features omitted, or over / under-tightened on assembly). An 'adverse' factor is also enumerated for elements of the project R&T having novelty, complexity, or any other cause for uncertainty about long term service effects. The task of assessing the beneficial factor is simplified by considering the boundary values corresponding to 'negligible improvement' (= 1) and 'total elimination' (= maximum), and by dividing the range into a small number of increments corresponding to say 'modest', 'significant', and 'major' improvement. Since no passenger transport helicopter type could conceivably accumulate more than 10^9 hours in service, the maximum numerical value of the factor can be readily bounded. The task of selecting the appropriate increment can be simplified by restricting the judgement to say the 'top three' compensating provisions, having first assessed their relative merits. The adverse factor can be determined on a similar basis, but in this case the likely range is expected to be very much less. In a qualitative analysis, the likelihood of the event is determined by applying the beneficial and adverse considerations to the datum case expressed in qualitative terms. For quantitative analysis, the resultant probability of occurrence for the event is obtained by dividing the datum rate by the beneficial factor and multiplying by the adverse factor.

These procedures and formats permit a ready audit of an unavoidably large number of component / potential failure mode / cause combinations. This facility is important both for compliance demonstration, and for managing improvements in overall system integrity.

5. Rotor and Transmission Design/Technology Improvements and Safety Compensating Provisions

In addressing R&T design/technology improvements it should be noted that the majority of incidents in the incident data base relate to helicopter types designed in the 1950s and 60s (see Appendix), and that considerable advances have since been made in respect of most of the causes of those incidents. It is beyond the scope of this paper to review these advances in detail, but references are given where available to sources of more detailed discussion. Items of a general nature that apply to both rotor and transmission systems include:-

Advanced computational design analysis facilities and materials data bases
Advanced materials with improved fatigue damage tolerance
Computer aided drafting, manufacture, and metrology
Total Quality Management
Computer-controlled test facilities permitting more representative load cycles, etc., with advanced diagnostics
Electronic instrumentation/display systems with clear pre-flight/ in-flight cautions; accurate solid state sensors
R&T Health and Usage monitoring systems on-board/ on test rigs; operator commitment to support
Advanced vibration diagnostics/reduction facilities

In addition to the advances in design, production, and operation listed above and below, the discipline of design safety assessment using the procedures described in this paper leads designers to a detailed awareness of historic failure data, and the more general implications of their circumstances. New R&T designs will avoid the historic weaknesses which led to repeat occurrence situations, and will address the less well-known errors or weaknesses which could otherwise frustrate the achievement of the zero failure objective. The procedures will also greatly reduce the possibility of hitherto unknown failure modes.

Several technology improvements which represent potential compensating provisions in a 1990s project design are summarised below under the compensating provisions headings, but with reference to the error checklist.

5.1 Rotors:

a. Design:

Reduced number of parts.
Damage tolerant design: - multiple load paths
- extensive use of composite materials

- metallic elements in super clean steel and titanium
- reduced stress concentration in critical areas
- design for low crack propagation rate.

Replacement of conventional bearings with elastomeric bearings.
Design for low vibration.

b. Monitoring:

Advanced vibration analysis techniques.
Blade spar integrity monitoring.

c. Manufacture/Assembly (New and Reconditioning)

'Critical Parts' control procedures.
Design for manufacture and assembly; prevention of incorrect assembly.
Design standards for bought-out parts; source control.

d. Substantiation Testing (Advanced facilities -see above):

Static and Fatigue tests with representative load cycles and high load factors; multi-specimens.
Tests for dynamic behaviour.
Endurance tests.
Environmental tests with representative environments.
Type tests.
Reliability enhancement tests/fleet leader programmes.

e. Maintenance:

Preventive maintenance based on MSG3 or Reliability Centred Maintenance procedures.
Retirement/removal based on measured torque exposure/duty cycles and health monitoring.
Operator support - ground station analysis of monitoring data; advanced off-line analysis methods.
Design for maintenance.
Simulator/interactive training facilities.

5.2 Transmissions:

More detail on many of the topics listed below is given in Ref 8.

a. Design:

Avoidance of intermeshing rotors.
Avoidance of multi-stage planetary gearing; off-loading of ring gear.
Large diameter drive shafts with minimised stress concentrations.
Established gear tooth forms; avoidance of bolted flange joints.
Reduced number of parts in gear support/clamping arrangements.
Avoidance of plain journal bearings; also of taper roller bearings in difficult situations.
High accuracy rolling element bearings with steel cages.
Super-clean steels; temper-resistant steels.
Effective emergency lubrication systems and avoidance of external oil pipes.
Fine filtration, disposable elements, damage resistant assembly, impending blockage indicators.
Oil jet filters; internal oil feed to bearings; oil flow management.
Oil lubricated splined couplings and freewheel units; toothed clutch design.
Adequate cooling; cooler integrity/protection; high integrity fan drives.
Adequate venting; desiccated breathers; carbon face seals.
Casings with borescope and monitoring sensor provisions, inspectable oilways, minimum stress concentrations, means for off-loading rotor loads, means for reducing casing vibration levels.

b. Monitoring:

Oil pressure and temperature indications - only when outside normal limits.
Quantitative on-line wear debris monitoring - rolling contact fatigue/fracture debris.
Vibration monitoring - advanced techniques for shafts, gears, bearings.
Usage monitoring - cumulative damage and limit exceedances (accurate torque).
Cruise guide indicator - accurate torque measurement.
Metal temperature monitoring - critical bearings.

Application to rig tests - validation and adjustment of rejection criteria.

c. Manufacture/Assembly (New and Reconditioning):

'Critical Parts' control procedures.
Design for manufacture and assembly; prevention of incorrect assembly.
Design standards for bought-out parts; source control.
Computer controlled gear grinding/shot-peening/surface and pitch measurement.
Super-cleaning facilities - removal of build debris.
Gearbox QA: 100% testing (under load); recorded meshing pattern checks; advanced diagnostics.
Lubrication system tests; oil jet checks.

d. Substantiation Testing (Advanced facilities -see above):

Static and Fatigue tests with representative load cycles and high load factors; multi-specimens.
Endurance and oil-loss tests.
Environmental tests with representative environments.
Type tests.
Reliability enhancement tests/fleet leader programmes.

e. Maintenance:

Preventive maintenance based on MSG3 or Reliability Centred Maintenance procedures.
Retirement/removal based on measured torque exposure/duty cycles and health monitoring.
Operator support - ground station analysis of monitoring data; advanced off-line analysis methods.
Design for maintenance; borescope inspection provisions; extended time between overhaul.
Oil reservoir contents gauging (remote indicating); high contrast, cleanable sight gauges.
Simulator/interactive training facilities.

6. Conclusions

1. Design safety assessment procedures tailored for rotor and transmission systems as described in this paper offer a significant enhancement of the safety record of helicopters, provided that they are applied rigorously, and at an early stage of project design.

2. The procedures and document formats described are appropriate to both qualitative and quantitative analysis.

3. The design safety assessment of rotor and transmission systems can benefit from a generic approach to the Hazard Assessment, with no consideration being given to likelihood of the failure condition, or to compensating provisions relating to the project design.

4. Determination of likelihood of critical failure conditions arising from rotor or transmission failure should be based on accident and incident data, rather than removal rate data. The latter generally has little relevance to critical failure.

5. Examination of rotor and transmission related accident data reveals their sensitivity to errors in manufacture, assembly, maintenance, and operation, in addition to shortcomings in design. The proposed method provides a systematic consideration of these factors in design safety assessment.

6. Two factors in particular give grounds for optimism in achieving improved airworthiness in respect of rotor and transmission systems:

   a. The wide range of technology improvements in design, manufacture, maintenance, and operation relative to the levels employed in the majority of rotorcraft that feature in the accident database.

   b. The availability of design safety assessment procedures which encourage full cognisance of lessons from the past, and offer a structured approach to the analysis of potential failure circumstances not experienced hitherto.

7. References

1. K.J. Meekoms, The origins and evolution of Design Requirements for British military aircraft, HMSO. Dmd 8273293. 11/83, June 1983.
2. E. Lloyd and W. Tye, Systematic Safety, Civil Aviation Authority, London, ISBN 0 86039-141-9, July 1982.
3. U.S. Federal Aviation Administration (FAA), Equipments, systems, and installations, sub-chapter 1309 of Part 25: Airworthiness Standards: Large Aeroplanes, Dept of Transportation, FAA, Washington D.C., (see FAR 29.1309 for Transport Category Rotorcraft, and JAR 25.1309/JAR 29.1309 for European Joint Aviation Authority equivalents).
4. U.S. FAA, Equipments, systems, and installations) interpretative material and acceptable means of compliance, AC No. 1 to FAR 25.1309 (also ACJ No. 1 to JAR 25.1309), sources as Ref. 3.
5. UK Civil Aviation Authority (CAA), Rotor and Transmission Systems (design and construction), chapter G4-9, British Civil Airworthiness Requirements (BCAR), Paper G778, Oct. 1985.
6. UK CAA, Rotorcraft Categories (definitions), chapter G1-2, BCAR, Paper G780, Oct. 1985.
7. J. E. Witham, Safety standards for helicopter and engine transmissions, Paper 1, IMechE Seminar: Pushing back the frontiers of failure in aerospace transmissions, London, Dec. 1986.
8. D.G. Astridge, Helicopter transmissions-design for safety and reliability, chapter 1, Rotorcraft drivetrain life, safety, and reliability, AGARD report No. 775, ISBN 92-835-0540-9, June 1990.
9. D.G. Astridge, Diagnostics for helicopter safety, paper presented to AIRDIAG '91, 2nd International Conference: Aircraft Diagnostics, Warsaw, May 1991.
10. U.S. Department of Defense, Procedures for performing a Failure Mode, Effects, and Criticality Analysis, MIL STD 1629A, Nov. 1980.
11. A.J. Wilson and F. Cortellini, The safety analysis approach for the EH101, Paper 42, Fourteenth European Rotorcraft Forum, Milan, Sept. 1988.
12. R.D. Leitch, Sources of errors in safety predictions, Paper 4, IMechE Seminar: Safety Assessment methods for Transmission Systems, Solihull, April 1992.
13. UK CAA, Condition monitored maintenance: an explanatory handbook, CAP 418, London, July 1978
14. UK CAA, World helicopter accident summary, WHAS, CA12 Supplement 89, Jan. 1993.
15. G.S. Campbell and R.T.S. Lahey, A survey of serious aircraft accidents involving fatigue fracture, Aeronautical Note: NAE-AN-8, National Research Council, Ottawa, April 1983.

TABLE 1. SUMMARY - DETAILED ANALYSIS RESULTS FOR MAIN ROTOR DRIVE SYSTEM HAZARD ASSESSMENT LINE ITEM: 1.1

Table 1a. Summary of FMEA sheet data appropriate to a Hazard Assessment Line Item, plus Compensating Provisions

HAZARD ASSESSMENT DOCUMENT: xxyy FUNCTIONAL FAILURE: Failure of drive to the Main Rotor Classification: FAR/BCAR: Catastrophic

FMEA Sheet No. *	Tab.1a Ref.	Item/ Sub-Item	Failure Mode	Failure Cause	Design Provisions Notes: (A)	Monitoring Provisions Notes:(B)	Manufacture Provisions Notes:(C)	Testing Provisions Notes:(D)	Maintenance Provisions Notes:(E)
	1.1.1 1.1.1.1	Main rotor driveshaft shear sections-notches, prox-imity to brgs)	Fatigue fracture - possibly hot with brg damage/overheat	a. Design/Material/Manufacture:					
xx				a.1.1 shaft design;					
yy				a.1.2 bearing/clamping, design					
zz				a.1.3 lubrication system, design					

Table 1b. Failure Occurrence Probability Analysis appropriate to a Hazard Assessment Line Item: MRDS 1.1

Tab.1a Ref	Item	Failure Mode	Failure Cause	Failure Data Base - Catastrophic failure rate per 10^6 hrs. (No off)			Probability of Occurrence per 10^6 hrs.			
				source 1	source 2	source 3	Datum	Factors Adverse	Factors Beneficial	Project X
1.1.1 1.1.1.1	Main rotor driveshaft shear sections-notches, prox-imity to brgs)	Fatigue fracture - possibly hot with brg failure/overheat	a.1.1 shaft design;	<.025 (0)			<.025(0)	1.0	2	.012
			a.1.2 bearing/clamping, design	1.4 (5) Type Ia			1.4 (5) Type Ia	1.0	100	.014
			a.1.3 lubrication system design	8.9 (8) Type Ib			8.9 (8) Type Ib	1.0	1000	.009

Figure 1 Example Extracts from Detailed Analysis Tables for Rotor and Transmission Systems

Table 2a. Main Rotor Drive System Hazard Assessment Line Items Classified as 'CATASTROPHIC'

Hazard Assessment Line Item (See Hazard Assessment for operating condition)		Qualitative Failure Probability	Quantitative Failure Probability (from Table 1b)	Justification (Principal Compensating Provisions)
1.1	Failure of drive to Main Rotor			
2.1	Failure of Main Rotor retention			
2.2	Failure of location of Main Rotor in axial/radial planes			

Figure 2 Example Extract from Detailed Analysis Summary Tables for Rotor and Transmission Systems

(a) Materiel Factors	(c) Maintenance Factors
a 1: Design	c1: Misinterpretation of Maintenance Manual
a 2: Material	c 2: Servicing errors/omissions/damage
a 3: Manufacture (inc. bought-out parts)	c 3: Inspection errors/omissions (inc. misinterpretation of health monitoring indications/ wear manifestations)
(b) Assembly Factors (new build or reconditioning)	(d) Operational Factors
b 1: Misassembly/omission/mis-locking/mis-protecting	d 1: Overload/excessive duty cycles
b 2: Use of incorrect/unauthorised/damaged parts	d 2: Excessive exposure to damaging external environment (including sand, brine, lightning strike)
b 3: Damage caused in assembly/handling/transport/storage	d 3: Incorrect response to cockpit warnings/ cautions/ indications of R&T systems health.

Figure 3 Error Checklist for Determining Failure Cause

APPENDIX

SUMMARY OF ROTOR & TRANSMISSION RELATED ACCIDENT DATA BASE

Sources

Much of the data was obtained by detailed examination of the World Helicopter Accident Summary[14], which relates to civil transport helicopters with a maximum authorised weight greater than 4550 Kg. The ICAO definition of an accident, used in that document, relates to injuries sustained and to damage to the helicopter. Other sources of accident and occurrence data used include individual accident investigation reports, a study of fatigue related accidents[15], the Safety Data Analysis unit of the UK CAA, and several military operators, the source details of which are required to be kept confidential.

Design Technology Baselines

The principal indicator of the design technology pertinent to accident case histories is the date or period of design. It is difficult to be precise about the date at which safety-critical design decisions on a particular type were frozen, but for the purposes of summarising this important information in this paper, the date of first flight is used. Rotor and transmission designs tend to be upgraded at least once during the 30 years or so service lifetime of a type, but usually at different stages corresponding to different Mk numbers. The types which feature in the accident data base are divided into four age groups: I = pre-1960, II = 1960-69, III = 1970-79, and IV = post-1980.

Summary of Cause Information

The narrative information relating to the accidents was examined for indications of cause - in terms of the cause groups listed in the error checklist. It is emphasized that the cause group definitions are aimed at assisting safety assessment, and have nothing to do with attribution of responsibility or blame to individuals or companies / entities. Most of the cause groups encompass a number of potentially responsible entities, and their isolation is beyond the scope of the data available and of the purposes of safety assessment. The results, expressed in terms of the number of accidents attributed to each cause group, are summarised in Table A-1. Also shown against each cause group are the age groups of the contributing types. Those cause groups that include the more recent age groups III and IV require particular attention in the design safety analysis, and in the compensating provisions employed. It should be noted that many of the accidents are attributed to multiple causes, either directly in the source narratives, or by inference from the identification of the failure mode. Thus where 'fatigue' failure is identified without cause group attribution, all potential cause groups for fatigue failure of that particular item should be considered in a rigorous safety assessment. Thus the number of accidents recorded against each cause group in Table A-1 may be biased towards rigorous safety assessment.

Lessons From Rotor-Related Data

The data base for rotor-related accidents contains nearly 50 entries, covering 11 types, spanning the period 1958 - 1992. Four types made their first flight before 1960, three between 1960 and 1969, four between 1970 and 1979, and one post-1980. The proportions of accidents corresponding to the four age groups are 46%, 25%, 27% and 2% respectively. The number of rotors related accidents recorded for the eleven helicopter types ranges from 1 to 10, the average being 4.4. The accident occurence rate tends to reduce with increasing flying hours. Design safety assessment which give numerical predictions of occurrence rates should therefore be qualified with the total service flying hours assumed in the calculations.

Several of the accident are attributed to one cause group only, but many have multiple attributions. Not shown in the table are three accidents, for which a cause group was not identified. For the remainder the largest cause group was the Design. Whilst several entries identified cause groups other than design, many of them indicated scope for pre-emptive design action to prevent critical errors in these activities in the future. The next three cause groups in order of significance were Manufacture, Servicing errors and Overload in service.

Lessons From Transmission-Related Data

The data base for transmission-related accidents contains over 100 entries, covering 19 types, spanning the period 1958 - 1992. Four types made their first flight before 1960, six between 1960 and 1969, seven between 1970 and 1979, and two post-1980. The proportions of accidents corresponding to the four age groups are 40%, 31%, 27%, and 2% respectively. The number of transmission related accidents recorded for eleven passenger transport helicopter types ranges from 1 to 18, the average being 6.7. There is much wider variation in accident rate by type (more than two orders of magnitude), and a tendency for the rate to reduce markedly with increasing type total flying hours. Design safety assessments which give numerical predictions of occurrence rates should therefore be qualified with the total service flying hours assumed in the calculations.

Several of the accidents are attributed to one cause group only, but many have multiple attributions. For one accident at least, two independent failure modes were recorded (freewheel wear and gear misassembly). Not shown in the table are the ten accidents for which a cause group was not identified. For the remainder (95 accidents) the largest cause group is Design. Whilst many of the entries identified cause groups other than design, very many of them indicated scope for pre-emptive design action to prevent critical errors in these activities in the future.The next three cause groups in order of significance were Inspection errors (including misinterpretation of health monitoring indications), Servicing errors, and Manufacture.

Failure Cause Group	Rotor Systems		Transmission Systems	
	Types*	No of Accidents#	Types*	No of Accidents#
(a) Materiel Factors				
a 1: Design	I, II, III	23	I, II, III, IV	72
a.2: Material	I	1	I, II, III	10
a.3: Manufacture (inc. bought-out parts)	I, II, III	11	I, II, III	17
(b) Assembly Factors (new build or reconditioning)				
b 1: Misassembly/omission/mis-locking/mis-protecting			I, II, III	14
b 2: Use of incorrect/unauthorised/damaged parts			I, II	2
b 3: Damage caused in assembly/handling/transport/storage				@
(c) Maintenance Factors				
c.1: Maintenance Manual omissions/misinterpretation	II, III	2	II	1
c.2: Servicing errors/omissions/damage	I, II, III	7	I, II, III	23
c.3: Inspection errors/omissions (inc. misinterpretation of health monitoring indications/ wear manifestations)	I, III	2	I, II, III	36
(d) Operational Factors				
d.1: Overload/excessive duty cycles	I, II, III, IV	6	I, II, III	14
d.2: Excessive exposure to damaging external environment (including lightning strike, sand, brine)			II	1
d.3: Incorrect response to cockpit warnings/ cautions/ indications of R&T systems health.			II, IV	4
(e) Uncontained Failures of Other Systems (inc. engines)			II, III, IV	6

Note multiple cause attributions. * Key to rotorcraft types by period of design: I = pre-1960; II = 1960-69; III= 1970-79; IV = 1980-89

@ Several occurrences of bearing installation damage resulting in failure of aircraft Ram Air Turbines.

Table A-1 Summary of Accident Data Relating to Rotors and Transmissions