SAE Aerospace
An SAE International Group

AEROSPACE RECOMMENDED PRACTICE

ARP5107 | REV. B

Issued 1997-06
Revised 2006-11

Superseding ARP5107A

Guidelines for Time-Limited-Dispatch (TLD) Analysis for Electronic Engine Control Systems

RATIONALE

Revision B has a revised section 6.4 on Recommendations on Items Considered Part of the FADEC System.

TABLE OF CONTENTS

1. SCOPE 4
1.1 Purpose 4
1.2 Summary of Revisions 4
1.2.1 Summary of Revision A 4
1.2.2 Summary of Revision B 5
1.3 Field of Application 5
2. REFERENCES 6
2.1 Applicable Documents 6
2.1.1 FAA Publications 6
2.1.2 EASA Publications 6
2.2 Acronyms and Symbols 6
3. APPLICABILITY 8
4. HISTORICAL PERSPECTIVE 8
5. HISTORY OF INTEGRITY GUIDELINES 8
6. GENERAL ANALYSIS APPROACH 10
6.1 FADEC System Configuration 10
6.2 Repair Categories: Immediate, Short, and Long Time 12
6.3 Classification of FADEC Fault Types 13
6.3.1 No Dispatch (ND) Type Faults 13
6.3.2 Short Time (ST) Type Faults 13
6.3.3 Long Time (LT) Type Faults 13
6.3.4 Combinations of Faults and Uncovered (UC) Faults 14
6.3.5 Aircraft Related Information 15
6.4 Recommendations on Items Considered Part of the FADEC System 15
6.5 Recommendations on In-Service LOTC Reporting 22
7. CALCULATION APPROACHES: SINGLE ENGINE ANALYSIS 22
7.1 A Simple Time-Averaging Approach 22
7.1.1 LOTC Rate for Full-up Electronics 25
7.1.2 Average LOTC Rate for Short Time (ST) Faults 26
7.1.3 Average LOTC Rate for Long Time (LT) Faults 26
7.1.4 Calculations of the Average LOTC Rate Using the TWA Approach 26
7.1.5 An Example Calculation 27
7.2 Markov Model Approach 28
7.2.1 Open Loop Markov Models: 29
7.2.2 Closed Loop Markov Model Approach 32

7.2.3 Examples of Single Fault States 38
7.2.4 Acceptability (and Accuracy) of Single State Models 38
7.3 Comparison of TWA and MM Approaches 38
7.4 A Single State FADEC System MM Example 40
7.4.1 Description of the Excel Spreadsheet Data 40
7.4.2 Validity of the Calculated Data 49
7.5 Second Example: A Single and Dual State Model of a FADEC System 50
7.6 Discussion of Markov Model and TWA Approaches, and the Use of Fault Trees for Determining LOTC Rates When Operating With Faults 50
7.7 Time-Since-Fault (i.e., On-Condition) Repair Versus Periodic Inspection and Repair 53
8. CALCULATION APPROACHES: DUAL ENGINE ANALYSIS 57
8.1 Time-Averaging Approach 57
8.2 Maximum Specific Risk Failure Rates as a Function of Dispatch Configuration 58
9. SUMMARY 59
10. NOTES 59

APPENDIX A EARLY APPLICATIONS 60
APPENDIX B REVISED FAA ANE POLICY LETTER, ANE-1993-33.28TLD-R1, DATED JUNE 29, 2001, POLICY FOR TIME LIMITED DISPATCH (TLD) OF ENGINES FITTED WITH FULL AUTHORITY DIGITAL ENGINE CONTROLS (FADEC) SYSTEMS 61
APPENDIX C DISCUSSION OF SOME TYPICAL FADEC SYSTEM FAULTS AND THEIR APPLICABILITY TO THE LOTC ANALYSIS 88
APPENDIX D DISCUSSION OF THE MMEL, DDG, CMRS, AND THEIR RELATIONSHIP TO FADEC SYSTEM MAINTENANCE (THE HANDLING OF ND, ST, AND LT FAULTS) 90
APPENDIX E PROBABILITY OF A DUAL ENGINE FAILURE WITH DIVERSION AND TURNBACK 93
APPENDIX F REVIEW OF THE COEFFICIENTS USED IN THE TIME-WEIGHTED-AVERAGE (TWA) EQUATION 95
APPENDIX G WHEN IS A SINGLE STATE MODEL OK? 100
APPENDIX H COMPARISON OF THE ASYMPTOTIC VALUE OF {(DP/DT)/(1 – P)] IN AN OPEN LOOP MARKOV MODEL WITH THAT OF THE AVERAGE FAILURE RATE OF THE SYSTEM FROM A CLOSED LOOP MARKOV MODEL. 103

FIGURE 1 SIMPLIFIED FADEC SYSTEM 11
FIGURE 2 SIMPLIFIED FADEC SYSTEM FAULT DIAGRAM 14
FIGURE 3 SIMPLIFIED FLOW DIAGRAM FOR FADEC SYSTEM FAULTS LEADING TO LOTC 15
FIGURE 3.1 ILLUSTRATIONS OF ALL LOTC EVENTS, ALL IFSD EVENTS, AND ENGINE CONTROL SYSTEM ELEMENTS INVOLVED IN A TLD ANALYSIS 16
FIGURE 4 A GRAPHICAL REPRESENTATIONS OF THE FAILURE PATHS OF A SIMPLE FADEC SYSTEM THAT LEAD TO LOTC 23
FIGURE 5 PLOT OF THE LOTC RATE FOR THE EXAMPLE DATA GIVEN IN 7.1.5 FOR BOTH THE ORIGINAL FRACTIONAL COEFFICIENTS (AS GIVEN IN THE ORIGINAL ARP) WITH THE IMPROVED FRACTIONAL COEFFICIENTS GIVEN IN THIS REVISED ARP 28
FIGURE 6 OPEN LOOP MARKOV MODEL WATER FALL DIAGRAM 29
FIGURE 7 OPEN LOOP MARKOV MODEL OF SIMPLE FADEC SYSTEM WITH REPAIR FOR SHORT AND LONG TIME FAULT STATES 29
FIGURE 8 PROBABILITY FLOW INTO AND OUT OF STATE P_J 30
FIGURE 9 CLOSED LOOP MM FOR SIMPLE FADEC CONTROL SYSTEM WITH REPAIR FOR SHORT AND LONG TERM FAULT STATES 33
FIGURE 10 SINGLE STATE MARKOV MODEL 35
FIGURE 11 COMPARISON OF TWA SOLUTIONS USING THE ORIGINAL ARP FRACTIONAL COEFFICIENTS AND THE BALANCED EQUATION 6 COEFFICIENTS OF THIS ARP WITH MARKOV MODEL SOLUTIONS USING EQUATIONS 20, 20C AND 20F (FROM THIS ARP) FOR THE FADEC SYSTEM DATA GIVEN IN 7.1.5 39
FIGURE 12 MM DIAGRAM OF A TYPICAL FADEC SYSTEM (NOTE: ALL λ'S ARE FAILURES PER MILLION HOURS) 41
FIGURE 13 LOTC RATE (TABLE 1 DATA USING EQUATION 20) AS A FUNCTION OF THE LT FAULT REPAIR TIME FOR SIMPLE FADEC SYSTEM EXAMPLE OF FIGURE 12 47
FIGURE 13A COMPARISON OF FIGURE 12 MARKOV MODEL LOTC CALCULATIONS USING EQUATIONS 20, 20C AND 20F 48

FIGURE 14 SECOND EXAMPLE OF SINGLE STATE MARKOV MODEL OF A TYPICAL FADEC SYSTEM, WITH 23 SINGLE FAULT STATES 51
FIGURE 15 FIGURE 14 MODEL WITH 180 DUAL STATES ADDED 52
FIGURE 16 LOTC RATES AS A FUNCTION OF LT REPAIR TIME FOR BOTH THE SINGLE AND DUAL STATE MODELS OF FIGURES 14 AND 15 53
FIGURE 17 ($T_{INSPECT}/T_{TSF}$) VERSUS ($T_{TSF}/T_{MTBF(LT)}$) 55
FIGURE 18 DERIVATION OF APPROXIMATION GIVEN IN EQUATION 24 56

TABLE 1 TYPICAL CATEGORIZATION OF FADEC SYSTEM ELEMENTS 18
TABLE 2 SPREADSHEET SOLUTION FOR FADEC SYSTEM EXAMPLE SHOWN IN FIGURE 12 43
TABLE 3 SPREAD SHEET SHOWING THE CALCULATIONS FOR DETERMINING THE COEFFICIENTS A_0, A_1, B_0, B_1, C_0, C_1, D_0, D_1 USED IN EQUATION 20C 49
TABLE 4 DUAL ENGINE SPECIFIC RISK AS A FUNCTION OF DISPATCH CONFIGURATION 58

1. SCOPE

This SAE Aerospace Recommended Practice (ARP) provides methodologies and approaches which have been used for conducting and documenting the analyses associated with the application of Time Limited Dispatch (TLD) to the thrust control reliability of Full Authority Digital Electronic Control (FADEC) systems. The TLD concept is one wherein a redundant system is allowed to operate for a predetermined length of time with faults present in the redundant elements of the system, before repairs are required. This document includes the background of the development of TLD, the structure of TLD that was developed and implemented on present generation commercial transports, and the analysis methods used to validate the application of TLD on present day FADEC equipped aircraft. Although this document is specific to TLD analyses (for FADEC systems) of the loss of thrust control, the techniques and processes discussed in this document are considered applicable to other FADEC system failure effects or other systems, such as, thrust reverser, and propeller control systems, and overspeed protection systems.

1.1 Purpose

The purpose of this document is to provide guidance on achieving approval of time-limited-dispatch (TLD) for full authority digital electronic (engine) control (FADEC) systems. In this regard, the usage of the term "TLD" refers to the concept that FADEC engine control systems shall be allowed to operate with faults for a specified period of time, after which, appropriate repairs shall be made to bring the system back to a "full up" configuration. For the purposes of this document, the term "full up" is used to indicate that the FADEC system is free of faults which affect its loss of thrust control (LOTC) failure rate as defined in Section 5. Hence, "required repairs" for this application of TLD are limited to only those faults that affect the LOTC rate, and faults that do not affect the LOTC rate, such as faults in sensors used for engine condition monitoring, are not addressed in these guidelines. Sensors that could affect the LOTC rate, such as oil pressure, oil temperature, and exhaust gas temperature (EGT) should be included in the analysis if those sensors are part of the engine's FADEC system.

This document is concerned with LOTC events which are caused by failures and/or faults in the engine's control system. Engine failures from any other causes are not the subject of these guidelines. In addition, this document is not intended to establish specific requirements for FADEC system certification or design. Specific requirements pertaining to certification should be coordinated with the appropriate certifying agency.

1.2 Summary of Revisions

1.2.1 Summary of Revision A

A significant improvement in determining the fractional coefficients of the time-weighted-average (TWA) equation, which is the first approach described herein for estimating the average LOTC rate of the system, has been made and is described in 7.1. The new coefficients allow the TWA method to yield a more balanced solution - one which is closer to the Markov model solution and somewhat simpler to use.

Much has changed in the description of the Markov modeling (MM) analysis approach described in this revision. Since the original release in June of 1997, the authors of this ARP have a better understanding of the MM approach as it applies to FADEC as well as other systems. Unique to this document is the description of MM as either an Open Loop or Closed Loop model. The nomenclature of Open Loop and Closed Loop Markov models is unique to this document. The authors have not seen this terminology used elsewhere, and there is no intention herein to set any type of standard in the using of this terminology. The development of the Closed Loop MM approach has lead to NOT having to solve a set of differential equations to obtain the steady state solution for the overall average failure rate of a system, but rather, simply solving a set of algebraic equations to obtain the solution. This was implied in the original release, because the MMs in that release were solved by integrating the differential equations until a steady state solution was obtained, where all of the time derivatives were essentially zero. However, it was not specifically called out that the derivatives should be set to zero at the onset, and the resulting set of algebraic equations solved to obtain the values of the state probabilities.

In addition, it was not recognized that the values obtained for the state probabilities, which are dependent on the value of the feedback rate from the fully-failed, loss-of-thrust-control (LOTC) state to the full-up state, do not affect the failure rate of the system. Hence, although the original release provides some rational for setting the feedback or repair rate from the fully failed LOTC state to the full-up state to unity (i.e., 1.0), the value of this feedback rate doesn't matter and the rational for setting the feedback rate to unity can be misleading. As the new material shows, the solution is independent of all state probabilities and the value of the fully failed to full-up feedback rate. The solution is only dependent on the failure

rates between the various states of the model and the repair rates used for the short time (ST), long time (LT) states, and if modeled, any no-dispatch (ND) fault states.

Experience has also shown that simulating states representing two or more failures has little influence on the overall LOTC rate of FADEC systems when the repair rates for the various fault states are much more frequent than the failure rates into and out of those fault states. When this is the case, constructing a “single state model” is usually adequate. In single state models, described in 7.2.2.3, only single fault states are modeled, and only those additional single failures that would cause the control system to go from those single fault states to the LOTC state are modeled. Adding additional multiple failure states only affects the answer by small amount, i.e., less than 5%. This is discussed in more detail in Appendix G.

Similar to the above, the use of the terminology “single state model” is unique to this document, and there is no intention to set any terminology standard with the use of this descriptive term. Some who have reviewed this document have commented that the use of the terminology single state model is misleading because a single state model actually models all dual failures that lead to the LOTC state. This is correct. However, the selection of the terminology made because the model explicitly shows only the single failure states. All dual failures that lead to LOTC events are included in the LOTC failure state, and no dual failures that do NOT result in an LOTC event are modeled.

A revised Engine and Propeller Directorate policy letter, reference 2.1.1.3, on time-limited-dispatch for engines fitted with FADEC systems was released on June 29, 2001. Changes from the original policy letter, see references in 2.1.1, to the requirements for TLD operations were minor in nature, but the revised policy letter was expanded greatly to reflect what has been learned of TLD operations from in-service experience. The new policy letter replaces the original one and is included in Appendix B.

A discussion of the elements that are considered part of the engine control system and should be represented in the LOTC analysis, will be added (6.4) in the future.

1.2.2 Summary of Revision B

Section 6.4, on Recommendations on Items Considered Part of the FADEC System, has been significantly expanded to provide more guidance on that subject. Section 6.5, on Recommendations on in-service LOTC Reporting, has been added.

The functions of the system, the elements selected for use in the system, and the design implementation all depend on the overall system architecture. In addition, integration between the engine and the aircraft control systems is constantly changing. All of these factors impact the selection of the elements to include as part of the FADEC system. Therefore, the information included in this section does not provide an absolute answer, but is intended to provide a methodology to use in selecting which elements of the aircraft/engine control system should be included in the analysis.

The added Table 1 in that section illustrates how to consider all elements of the thrust or power control system, the functions and failure modes associated with the element, and then evaluate whether it is or is not part of the TLD restriction envelope depicted in Figure 3.1. The table also shows the most likely result of a failure of the element by identifying the applicable area of Figure 3.1.

1.3 Field of Application

This document applies to redundant FADEC control systems for aircraft engines on multi-engine aircraft. TLD addresses the level of degraded redundancy that is allowable - while still meeting the necessary airworthiness requirements - for FADEC controlled aircraft engines used on multi-engined aircraft. (It is noted that the submittal of a TLD analysis is not a requirement for certification of an engine incorporating a FADEC system. The analysis is a means to substantiate and obtain approval for dispatching and operating a FADEC system - for limited time periods - with faults present in the system.) Although this document specifically applies to FADEC systems on multi-engined aircraft, the methodologies presented herein with regard to achieving an overall average system failure rate can also be applied to other systems.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. However, nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

- 14 CFR Parts 23, 25, 27, 29, 33
- (Original) ANE Policy Letter, on dated October 28, 1993, Time-Limited-Dispatch of Engines Fitted with FADEC Systems
- Revised ANE Policy Letter, ANE-1993-33.28TLD-R1, dated June 29,2001, Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems, given in Appendix B
- Advisory Circular, AC 33.28-1, “Compliance Criteria for 14 CFR §33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems”, issued June 29th., 2001

2.1.2 EASA Publications

Available from European Aviation Safety Agency, Postfach 10 12 53, D-50452 Koeln, Germany, Tel: +49 221 8999 000, www.easa.eu.int.

- CS - 23
- CS - 25
- CS - 27
- CS - 29
- CS - E
- CS - APU

2.2 Acronyms and Symbols

ARP	Aerospace Recommended Practice
CAA	Civil Aviation Authority (FAA of United Kingdom)
CFR	Code of Federal Regulations (aka. FARs)
CPU	Central Processor Unit
CMR	Certification Maintenance Requirement

CS	Certification Specification (EASA nomenclature)
DDG	Dispatch Deviation Guide
EASA	European Aviation Safety Authority
EEC	Electronic Engine Control
FAA	Federal Aviation Administration (or Authority)
FL	Flight Length (in hours)
FADEC	Full Authority Digital Engine Control
FAR	Federal Aviation Requirement
HM (or HMC or HMU)	Hydromechanical (control or unit)
IFSD (or IFSDs)	In-Flight Shut Down(s)
JAA	Joint Airworthiness Authorities (of Europe) (Replaced by EASA)
JAR	Joint Airworthiness Requirement (Replaced by EASA CS publications
LOTC	Loss of Thrust Control
MEL	Minimum Equipment List (airline operator constructed, based on the MMEL)
MM (or MMs)	Markov Model(s)
MMEL	Master Minimum Equipment List (provided by aircraft manufacturer)
MPD	Maintenance Planning Document
MRB	Maintenance Review Board
ND	Non-Dispatchable Fault/Condition
ST	Short Time Fault/Fault State/Repair Interval
LT	Long Time Fault/Fault State/Repair Interval
TLA	Thrust Lever Angle
TLD	Time Limited Dispatch
TWA	Time Weighted Average (see Section 7)
λ	failure rate (failures per million hours)
μ	repair rate, given on a per hour basis
=	equals
$\approx$	approximately equal to

≡	defined as
≥	greater than or equal to
≤	less than or equal to
P	probability
T	time
t	time

3. APPLICABILITY

The applicability of these guidelines is primarily intended for FADEC equipped engines certifying to 14 CFR Part 33 regulations and the application of those engines to aircraft certifying under 14 CFR Part 23, 25, 27, and 29 regulations. The approaches contained herein have been accepted in previous FADEC system approvals for engines installed on aircraft certified under 14 CFR Part 25 regulations. The continued acceptability of these approaches should be coordinated with the appropriate certification agency during any new certification effort.

An objective is to extend the applicability of the techniques discussed herein to certification of FADEC systems under EASA CS-23, 25, 27, 29 and CS - E.

This approach may also be applied to other than FADEC systems.

4. HISTORICAL PERSPECTIVE

The concept of time limited dispatch (TLD) originated during the development and certification of FADEC systems used on the turbine (jet) engines of the Boeing 767 airplane. A brief discussion of some of the early applications of electronics to turbine engine controls is given in Appendix A.

5. HISTORY OF INTEGRITY GUIDELINES

Improved dispatchability for the FADEC engine control systems was a major objective during the design and development of the Boeing 767 airplane. The approach pursued was to have the engine manufacturers conduct an analysis of all control system faults, which would include all electrical/ electronic and hydromechanical/mechanical faults, to determine their influence on control system integrity. This analysis would determine the length of time a fault (or faults) could be allowed to exist - after which repair would be required - to achieve a given level of integrity. Early discussions with Seattle's Northwest Mountain (ANM) Region FAA office, which certified the 767 aircraft; New England's (ANE) FAA office, which certifies the Pratt & Whitney and General Electric engines; Britain's Civil Aviation Authority (CAA) office, which certifies Rolls-Royce engines; and all engine manufacturers ensued. Representatives from the FAA field operations office (Part 121) attended the above meetings also. Although not directly involved in certification matters, the FAA Part 121 group approves airline maintenance and operations policies and procedures, and their concurrence with the proposed approach was needed.

The discussions defined an LOTC event and established some significant integrity requirements for FADEC systems. (These integrity requirements are contained in the recently issued revision to, FAA Engine and Propeller Directorate policy letter, see Appendix B.) For engines intended for Part 25 applications, the LOTC definition and the integrity requirements are as follows:

a. An LOTC event is defined to be one wherein:

   1. the engine cannot be modulated between idle and 90% of maximum rated power (at any flight condition) via normal throttle movement. (Failures that cause the engine to operate at a slightly higher than intended idle thrust or power are generally not considered. They would be if they resulted in the flight crew's having to shutdown the engine to descend and/or land.)

2. the engine cannot meet the operability requirements of Part 33, or

3. engine thrust oscillates in an unacceptable manner. (This definition is provided for guidance only. The level of unacceptable thrust (or power) oscillations will be dependent on the application. Hence, the "unacceptable level" needs to be established in coordination with the installer. Lacking this installer information, a default value of ±5% [i.e., 10% peak-to-peak] of takeoff thrust is suggested. This level was found to be quite difficult to handle during the approach and landing flight phase of flight on a typical 2-engine, wing mounted, aircraft. Higher oscillation values may be tolerable during other phases of flight, but the aircraft still has to successfully transition through the approach and landing phase of flight. Hence, the ±5% of takeoff power is considered to be a reasonable definition for unacceptable thrust oscillation.)

b. The average integrity of the control system has to be better than or equal to 100,000 hours for faults that result in an LOTC event. In other words, the Fleet Average LOTC rate of the FADEC system has to be less than or equal to $10*10^{-06}$ failures per hour. This fleet average is to include all modes of control system operation, and by definition, is the average of all dispatches, including full-up system dispatches.

c. The engine control system is considered to be NOT dispatchable if the instantaneous LOTC rate is greater than $100*10^{-06}$ failures per hour. The instantaneous LOTC rate is defined as the calculated LOTC rate of a given control configuration at dispatch.

d. The control system should have a more restricted (i.e., short time) dispatch period if it has suffered a significant loss in redundancy or its instantaneous LOTC rate is between $75*10^{-06}$ and $100*10^{-06}$ failures per hour. The engine manufacturer may choose to place other dispatchable failures, which have an associated instantaneous LOTC rate less than $75*10^{-06}$ events per hour, in this short time dispatch category as well, as that would be conservative. (Dispatches in these configurations are generally handled via the aircraft's Master Minimum Equipment List (MMEL). See Appendix D.)

e. A longer, but still restricted, dispatch interval is allowable when the instantaneous LOTC rate is less than $75*10^{-06}$, but greater than the $10*10^{-06}$ failures per hour overall target.

It has been generally accepted that if (1) the FADEC installations have been shown to comply with FAR 25.903(b) in the system configurations approved for TLD, and (2) approved TLD methods are used to monitor and govern maintenance of each engine's FADEC system, then the engines may be considered independent of each other when determining dispatch in service. Thus, the airplane could be dispatched with faults present in more than one engine's FADEC system. Since this last item involves application of TLD to the aircraft, the acceptability of this item is at the discretion of the aircraft certification authority.

The initial 10 per million hour LOTC rate integrity requirement for engines intended for Part 25 applications is documented in the revised advisory circular (AC) for FAR 33.28, AC 33.28-1. An analysis to show that the control system is designed to meet this integrity requirement is usually submitted as part of engine certification. This is normally required - even when the applicant is not applying for TLD operations.

Although not a part of the above discussions, a remaining integrity requirement for aircraft certification is to show compliance with FAR(CS) 25.1309. This FAR relates to Systems and Equipment, and the requirement is that the probability of having a catastrophic multi- engine thrust loss event due to independent control system causes must be less than 10^{-9} failures on a "per hour of flight basis". In previous certifications, the FAA has agreed that the use of a fleet-wide average, control system caused LOTC rate is acceptable when showing compliance with this requirement. Using a fleet wide LOTC rate for engine certification of $10*10^{-06}$ per hour results in compliance with the FAR/CS 25.1309 requirement for multi-engined aircraft. This is discussed in more detail for a twin-engined aircraft in 8.1. Thus, the integrity requirements for engine certification are more stringent than those that come from aircraft certification with regard to the application of FAR 25.1309. (Note that single engined aircraft used in commercial service do not certify under Part 25 regulations; thus, FAR 25.1309 requirements do not apply to single engine aircraft.) For a twin engined aircraft, the specific risks for dual engine LOTC events, caused by loss of both engines' control systems due to faults, is given in 8.2 for the various dispatch configurations currently allowed in service. The acceptability of all dispatch configurations needs approval from the aircraft certifying authority as well. Hence, any new aircraft certification application requires coordination with the appropriate aircraft certifying authority to establish the aircraft level allowable dispatch configurations and the acceptability of the associated specific risks for limited time periods requested.

There was no intent to circumvent or establish a more severe requirement for FADEC system integrity during engine certification under 14 CFR Part 33 than would come from the aircraft certification under 14 CFR Part 25, FAR 25.1309, when the integrity requirements for FADEC systems were being established. The intent was merely to require that FADEC system integrity be equivalent to the established reliability of the then current hydromechanical engine control systems. For aircraft certifying under 14 CFR Part 25, FAR 25.901(b)(2) requires the engine control to be reliable between "normal inspections and overhauls". The above engine control system integrity requirements were considered to meet this requirement as well as the fail safe requirements of FAR 25.901(c) and 25.1309(b). For Part 25 applications, TLD is a useful tool for assuring that appropriate instructions for continued airworthiness are provided, as required by FAR 25.1529.

It is interesting to note that since the issue of the original ARP 5107 in June of 1997, there have been significant changes in engine-run reliability as a result of Extended-range Twin-engined OPerationS (ETOPS). In the newly coordinated activity on ETOPS requirements, the overall engine – including those IFSDs caused by aircraft systems, have to show an IFSD rate of 0.02 per 1000 hours to be allowed ETOPS operations with diversions of 3 hours or less, and an IFSD rate of less than 0.01 per 1000 hours for ETOPS operations with diversions of more than 247 minutes. Because of this, the allowance (by the engine manufacturer) for engine control system caused IFSDs has continued to be dramatically reduced. This reduction has not been the result of more restrictive FAA regulations with respect to engine control system caused IFSD's, but rather, the "pressure of ETOPS" IFSD events. Hence, the average overall FAA LOTC rate for transport aircraft engines continues to be limited to 10 events per 10^6 flight hours, although the engine manufacturer would not allow such a high rate (for just the control system) in ETOPS operations. Such an allowance would have too high an impact on the IFSD rate.

6. GENERAL ANALYSIS APPROACH

The general approach is to construct a model of the FADEC system which allows the integrity of the system to be analyzed in its full-up as well as the various fault configurations considered allowable for dispatch, and to "time average" those various states of operation to achieve the required average integrity. The current integrity requirements are listed in Section 5 and given in Appendix B.

In general, the analysis used to determine compliance with the requirements can be completed using any analysis tool(s), provided that the tools and methods used are acceptable to the certifying authority. Hence, it is important to have discussions with the appropriate certifying office concerning the capabilities and limitations of the analysis tools before commencing the actual analysis. Examples of previous tools used include standard fault tree computer programs and Markov models.

The general rule for faults relating to a TLD analysis is; if they affect the LOTC rate, include them in the analysis; if they do not affect the LOTC rate, leave them out. Obviously, a fault does not have to have an immediate affect on the operation of the engine to be included in the analysis. It is sufficient that the 'instantaneous LOTC rate' of the control be influenced for the fault to be included in the analysis. A more detailed discussion of some typical FADEC system faults and whether they should be included in the LOTC analysis is given in Appendix C. Section 6.4 will be updated in a future revision of this ARP to provide recommendations on elements that should be included in the FADEC system's LOTC analysis.

This document addresses two types of repair scenarios. The first type is generally termed "on condition" or "time since fault" repair. In this scenario, the time at which the fault occurs is known, and the fault is repaired within X hours of its occurrence. The second type addressed in this document is the "scheduled inspection and repair" scenario. In this scenario, the time of occurrence of the fault is not known, but rather, a periodic inspection for faults is made, and should a fault be found, it must be repaired at that time or within X hours of the inspection. This document addresses both scenarios and shows the relationship between the two.

6.1 FADEC System Configuration

A typical (simplified) FADEC system configuration is shown in Figure 1. For simplification purposes, it is assumed throughout this report that all electrical/electronic elements of the control have redundant elements, that the redundant elements are identical, and that the control alternates between use of the redundant elements on each engine start. This last item minimizes the exposure time for the existence of latent faults in the electrical/electronic elements. The above assumptions need not be the case for the use of these guidelines, but essentially all the equations used herein would need modification to account for dissimilar redundancy and not alternating electronic element/channel operation.

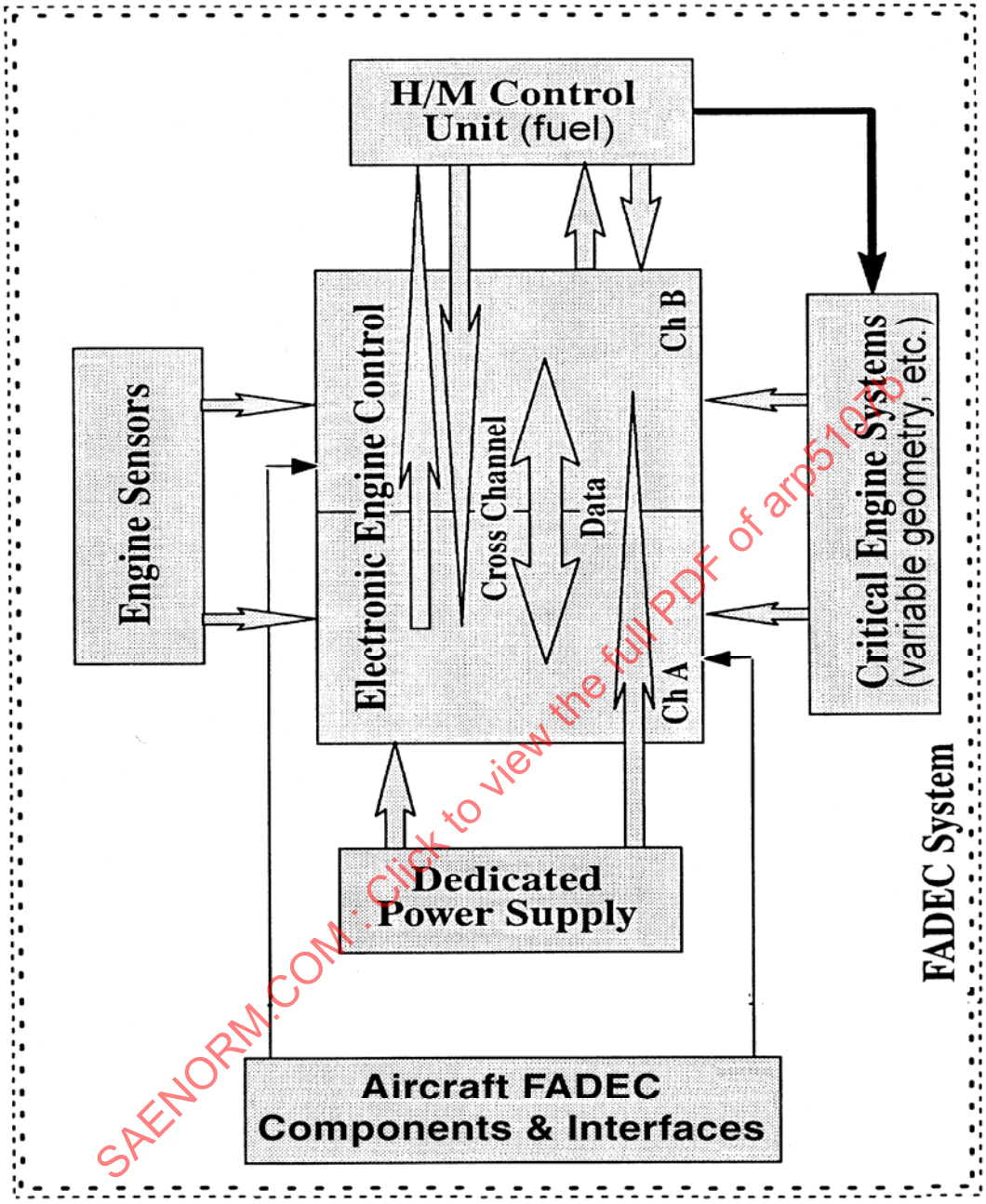

FIGURE 1 - SIMPLIFIED FADEC SYSTEM

6.2 Repair Categories: Immediate, Short, and Long Time

Past certification analyses have chosen to group FADEC system faults into one of three repair categories. The first of these is the immediate, or "no dispatch" category. As the name implies, faults in this category require repair prior to dispatch. The second group is a short time repair requirement of usually less than 500 hours. Repair requirements for these faults are typically handled via the aircraft operator's Minimum Equipment List (MEL). (See Appendix D for further discussion of this item.) The third is a longer repair interval of 500 hours or more. Faults in the long time repair category are typically handled via the operator's maintenance program. The specific allocation of faults to the short or long time category is determined as part of "the conducting" of a TLD analysis. This determination can be influenced by an operator's maintenance policy.

See Appendix B, the "Policy Letter from ANE FAA Regarding Time Limited Dispatch (TLD) for FADEC Controlled Engines", for TLD time limit restrictions applicable to "entry level" systems.

As indicated earlier, when complying with FAR 25.903(b) and showing that engine-to-engine isolation is maintained in all TLD approved dispatch configurations, it is not necessary to consider combinations of faults involving multiple engines when determining aircraft dispatch. However, if an applicant found that it was either necessary or "advantageous" to do so, an "airplane level" TLD criteria could be proposed to the aircraft certifying authorities. If both the airplane and engine manufacturer wish to place limitations on TLD operations, the more restrictive of the two, on an item by item basis, should be used. For example, if the engine manufacturer indicates in the Instructions for Continued Airworthiness (ICA's) for the engine that short time faults must be limited to 150 flight hours and long time faults should be limited to 500 hours, and the aircraft manufacturer places the limitation on the aircraft that short time faults should be limited to 100 flight hours and long time fault limited to 750 flight hours, the limitation should be 100 flight hours for short time faults and 500 hours for long time faults, as this is the more restrictive for each of the categories.

It is important to note that these repair categories are applicable to single faults as well as combinations of faults. For example, a mechanical/hydromechanical fault that may not have caused an LOTC event on the last flight might be a stability bleed valve failure, where the bleed valve failed open, but did not cause EGT to increase to a level which would cause the flight crew to have to reduce thrust. Although the condition did not cause an LOTC event on the last flight, this is a single fault that requires immediate repair. (This assumes that the flight crew notes the effects of the failure condition and maintenance investigates and discovers the faulty condition.) An example of a dual electronic fault that would normally require immediate repair is the loss of both channels' (free stream) total temperature sensors. This condition may not have resulted in a LOTC event on the last flight either, because the control may have been configured to accommodate such a fault.

But it may be considered a non-dispatchable configuration for the control; and hence, immediate repair may be required. Immediate repair is required for all combinations of faults that leave the FADEC system in a configuration where the instantaneous LOTC rate is greater than $100*10^{-06}$ failures per hour and/or all combinations of faults that leave the FADEC system with loss of functions that contribute to LOTC.

A similar situation exists for the short and long time repair categories. A single fault, such as loss of the central processor in one channel, is a fault that is generally placed in the short time (i.e., less than 500 hours) repair category because the system suffers a significant loss of redundancy when such a fault occurs. The short time repair category might also be used to repair a condition caused by a combination of faults. For example, assume that the control experiences two independent faults, one in either channel, which by themselves might be placed in the long time (i.e., greater than 500 hours) repair category. The FADEC system could be configured so that when the two faults exist together, the repair requirement is "elevated" to the short time repair interval. This is required if the combination of faults results in a FADEC configuration where the instantaneous LOTC rate is greater than $75*10^{-06}$ failures per hour, but less than $100*10^{-06}$ failures per hour no-dispatch rate.

If two or more faults do not result in a condition of significance or concern, and by themselves, each would only require long term repair, then their combination may be left in the long time repair category as well.

Hence, in summary, the immediate (i.e., no dispatch), short time and long time repair categories can be used for single as well as combinations or multiple faults. The selection of the category is dependent on the condition of the control when operating with the fault(s).

As always, discussions with the appropriate authorities should be held to confirm the acceptability of the various dispatch configurations and their respective operating intervals.

6.3 Classification of FADEC Fault Types

The approach used herein is to take all FADEC system faults, one by one, and determine which repair category is suitable for that fault, assuming that it is the only fault in the system, and that ultimately the fleet average LOTC rate of $10*10^{-06}$ failures per hour is achieved with the defined categorization. If the fleet average is not achieved, it will be necessary to place more restrictive dispatch limits on some of the faults to achieve the required rate.

6.3.1 No Dispatch (ND) Type Faults

Single faults that require immediate repair are termed no-dispatch (ND) type faults. (This should not be confused with combinations of faults that result in a no-dispatch condition.) The assumed FADEC system configuration (Figure 1) consists of redundant elements for all electronic/electrical portions of the system. Because of this assumed redundancy, the configuration has no known single electronic/electrical elements (from a functional perspective) which if failed, would require immediate repair to achieve a dispatchable configuration.

Note, however, that all single faults have to be assessed against the requirement that the instantaneous LOTC rate cannot be greater than $100*10^{-06}$ failures per hour when dispatching with the fault. If a single fault leaves the control in a configuration where the instantaneous LOTC rate is greater than this upper bound, the fault should be placed in the no-dispatch category. Exposure to these faults over a single flight are generally not included in the reliability analysis because the repair interval is so frequent, there is essentially no effect on the estimated LOTC rate.

Since the hydromechanical/mechanical elements of the system are assumed to be non-redundant, all ND type faults in the FADEC system discussed herein are in the hydromechanical/mechanical elements. Only those ND faults which would lead to an LOTC event should be included in the analysis. If some fault redundancy is provided within the mechanical/ hydromechanical elements, these can be treated as additional ST or LT faults provided the detectability and residual system reliability are adequate. The engine manufacturer(s) may elect to place single element items in the ND category that do not lead to an LOTC event. Examples of this might be an air-oil-cooler valve, which if failed open might result in the inability to maintain adequate fire extinguishing capability. Failure of such a valve would not generally lead to an in- flight LOTC event; therefore, these type ND faults should not be included in the TLD analysis.

6.3.2 Short Time (ST) Type Faults

Faults placed in the short time repair category (e.g., less than 500 hours) are termed ST type faults. From the requirements of Section 5, single faults which leave the control in an acceptable dispatch configuration, but one where the instantaneous LOTC rate is between $75*10^{-06}$ failures per hour and $100*10^{-06}$ failures per hour should be placed in this category. In addition, FAA approved TLD operations to date have all single faults which leave the control in essentially single channel operation, such as loss of one channel's CPU or power supply, placed in the ST category - even though the LOTC rate of the remaining channel may be less than $75*10^{-06}$. Again, it is assumed that there are no single electrical/electronic faults which leave the control in a configuration where the instantaneous LOTC rate is greater than $100*10^{-06}$ failures per hour. If this were the case, those faults would have to be placed in the ND category. There are many applications where faults that could be placed in the Long time category (discussed below) are placed in the Short Time category. Obviously, this is always acceptable.

6.3.3 Long Time (LT) Type Faults

Single faults placed in the long time (e.g., longer than 500 hours) repair category are termed LT type faults. Based on the requirements given in Section 5, LT faults must not leave the FADEC system in a configuration where the instantaneous LOTC rate is greater than $75*10^{-06}$ failures per hour. Examples of these faults might be loss of a sensor or any other input or feedback signal for which there is redundancy (or adequate fault accommodation in the case where redundancy is not provided for all electronic elements) - and a suitably low LOTC rate is maintained.

6.3.4 Combinations of Faults and Uncovered (UC) Faults

Figure 2 shows a very simplified FADEC system fault configuration diagram which is used for the LOTC analysis. Figure 3 shows Figure 2 expanded into a flow diagram leading to the LOTC state. "Uncovered faults" have been added to these diagrams. Uncovered faults are faults in the electronic portions of each control channel for which no means of detection or accommodation has been provided. Since these faults are unaccommodated, it is assumed that they would lead to LOTC events. Typical uncovered fault rates are between 0 and 5% of the total of both channels (electronic) failure rates. The analysis should provide substantiation for the value used. (It is noted that undetected faults which result in an LOTC event do not remain "undetected" for long. Some prefer classifying these as simply "uncovered" faults).

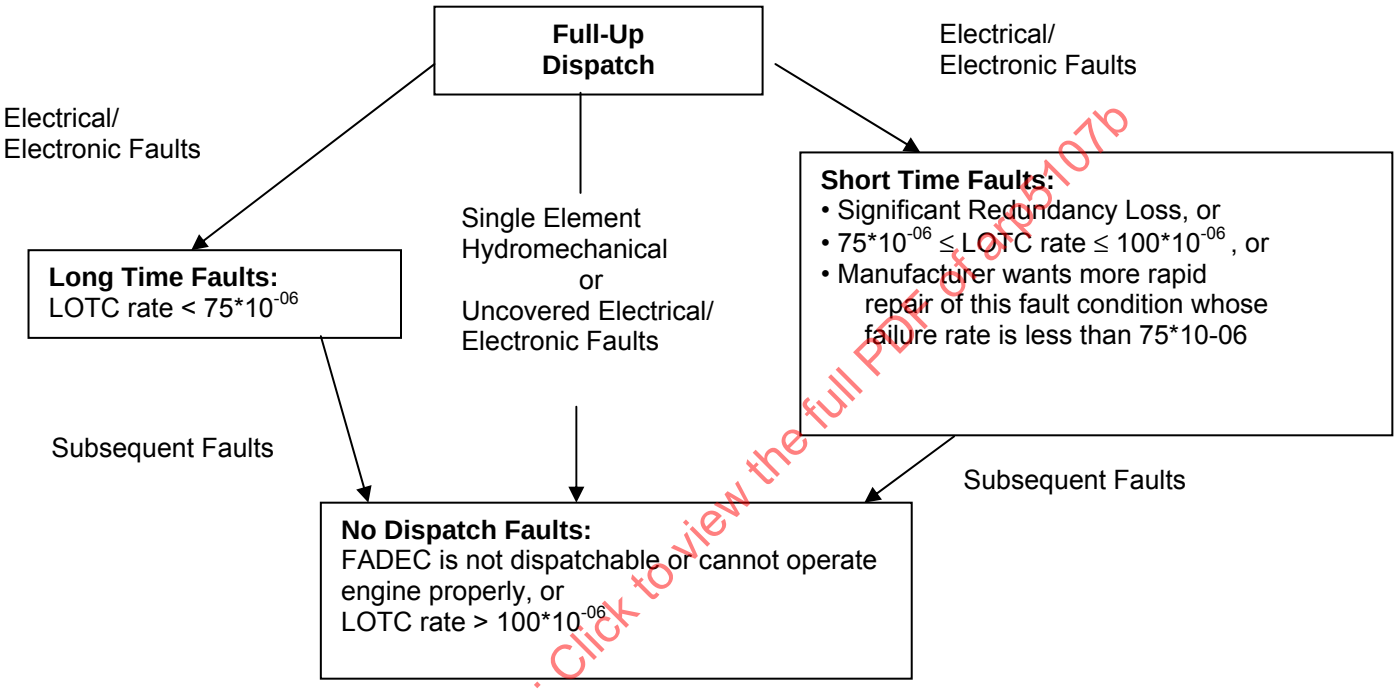

FIGURE 2 - SIMPLIFIED FADEC SYSTEM FAULT DIAGRAM

Figure 3 is not intending to imply that all combinations of ST and LT faults in both channels lead to LOTC events. The analysis has to look at each combination and determine whether they are truly independent and together would lead to an LOTC event. This is the cornerstone of any reliability analysis. The usage of the TLD approach is dependent upon the knowledge that the system has been thoroughly and accurately analyzed for operation with single and combinations of faults - at least to the second fault level. The third fault level does not have to be analyzed if the applicant elects to take the conservative position that all third faults lead to an LOTC event. The analysis will yield the conservative result that the repair intervals will be sooner than those that would have been obtained had third faults been analyzed. Analyzing the combinations of faults is the difficult and tedious part of the analysis, and although these guidelines do not discuss this task, this is where much of the work is. It should be noted if the analysis is only completed to the second fault level, there will be occasions in service when the FADEC systems are actually dispatched and operated with more than two faults present. However, the likelihood of three or more independent faults occurring within the short or long term repair interval - and still having the control function with no discernible effect - is quite small; and therefore, the impact on the fleet average is expected to be negligible. A TLD analysis should include some analysis and documentation to substantiate this assertion.

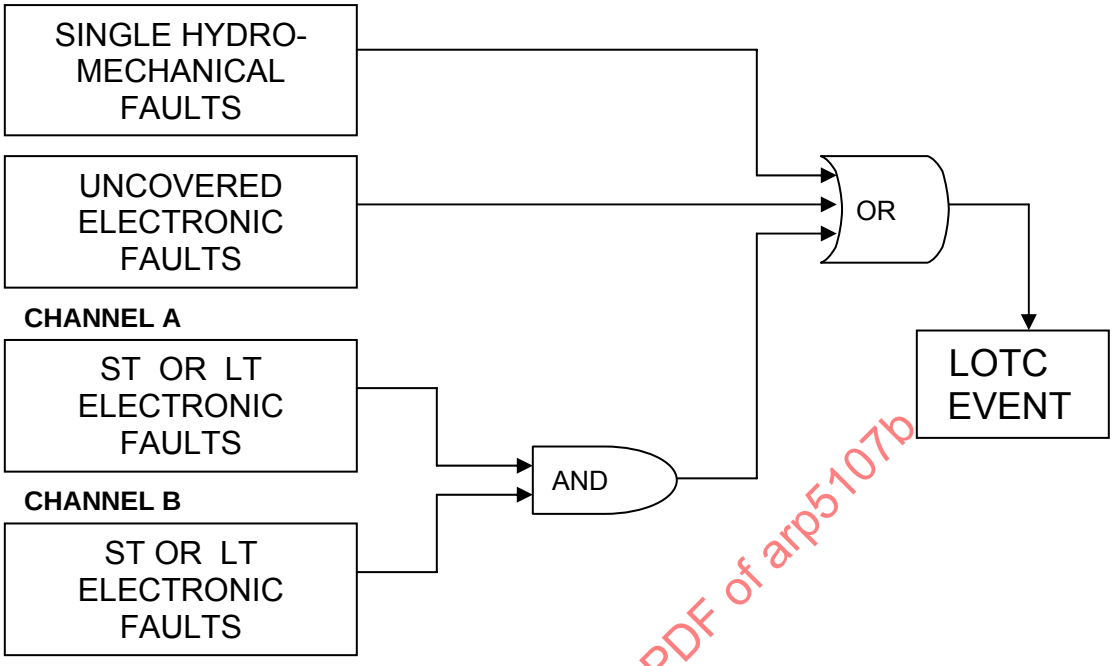

FIGURE 3 - SIMPLIFIED FLOW DIAGRAM FOR FADEC SYSTEM FAULTS LEADING TO LOTC

6.3.5 Aircraft Related Information

A discussion of the aircraft's MMEL, operator's MEL, dispatch deviation guide (DDG), and maintenance review board (MRB) report; how ND, ST, and LT type faults relate to those documents; how LT faults became a certification maintenance requirement (CMR); and some options for handling LT faults to remove them from the CMR classification is presented in Appendix D.

6.4 Recommendations on Items Considered Part of the FADEC System

The question “What elements of the system are to be included?” is frequently raised relative to LOTC analysis and Time Limited Dispatch. This section addresses that question. The functions of the system, the elements selected for use in the system, and the design implementation all depend on the overall system architecture. In addition, integration between the engine and the aircraft control systems is constantly changing. All of these factors impact the selection of the elements to include as part of the FADEC system. Therefore, the information included in this section does not provide an absolute answer, but is intended to provide a methodology to use in selecting which elements of the aircraft/engine control system should be included in the analysis.

In general the analysis used to predict the frequency of an LOTC should include all elements in the thrust or power control system that can contribute to an LOTC event. It is the overall LOTC rate for a given engine and aircraft that is relevant to obtaining and maintaining TLD in service.

Since TLD is a benefit to engine manufacturer customers, the engine manufacturer has a vested interest in obtaining TLD for the installed engine control system. Including the required aircraft elements in the analysis allows the engine certification authority visibility of total LOTC rates. Therefore, the engine manufacturers must include the relevant aircraft supplied control elements as part of the engine control system when seeking approval of TLD operations. The engine manufacturer may provide the airframe information by obtaining it from the airframer or by using data from the engine manufacturer’s applicable prior history. The overall installed engine LOTC rates will also be reviewed and used by the aircraft certification agency in approving TLD operations for the aircraft.

Note that the LOTC analysis and reporting does not include the details, analysis and corrective actions associated with basic engine events. And the engine manufacturer is not expected to (1) substantiate any airframer predictions, (2) explain the details of aircraft element failures which contribute to LOTC events, or (3) monitor and manage any resulting changes to the aircraft systems. Hence, the engine manufacturer may not be in a position to provide detailed information on any aircraft element failures which could lead/contribute to LOTC events, even though those aircraft elements are

considered part of the engine control system. However, it is anticipated that when LOTC events occur, the engine manufacturer will be made aware of them. If those events are caused by aircraft elements which are part of the engine control system, the engine manufacturer is expected to coordinate with the aircraft manufacturer to determine whether corrective actions are needed - so that the engine control system can continue to meet its Continued Airworthiness requirements.

In general the following guidelines apply when selecting the elements to include in the LOTC analysis:

- The LOTC event is related to an engine control failure or malfunction. The engine control system failure may involve aircraft supplied element failures or malfunctions. In some cases the failure may result in flight crew action to reduce power or thrust, or initiate an engine shutdown.
- All In-Flight Shut Downs (IFSDs) are a subset of LOTC events (see Figure 3.1), and all engine control system caused or induced IFSDs and fail fixed rotor speed, thrust or fixed fuel flow conditions are forms of LOTC.
- If a component is part of the control system and its failure or malfunction can contribute to an LOTC event, it should be included in the LOTC analysis.
- If a component is not directly part of the engine control system but has an electrical interface with the EEC, it is a candidate for contributing to an LOTC event and should be considered for inclusion in the analysis.
- If a component is part of the basic engine mechanical system, but not part of the mechanical portion of the engine control system, it is usually not a candidate for an engine control system related LOTC event, and therefore, not included in the engine control system LOTC analysis.
- The FAA TLD policy allows exclusion of the fuel pump from being included as part of the engine control (see ANE Policy Letter given in Appendix B).
- Components to be included are not limited to the redundant electrical parts of the control system.
- If an element can cause an erroneous value to be displayed in the cockpit and the crew might respond by shutting down the engine or reducing thrust or power, the element should be included in the LOTC analysis.

Figure 3.1 attempts to illustrate the concept of selecting the events and causes of the events, and hence, the elements to be included in the TLD analysis.

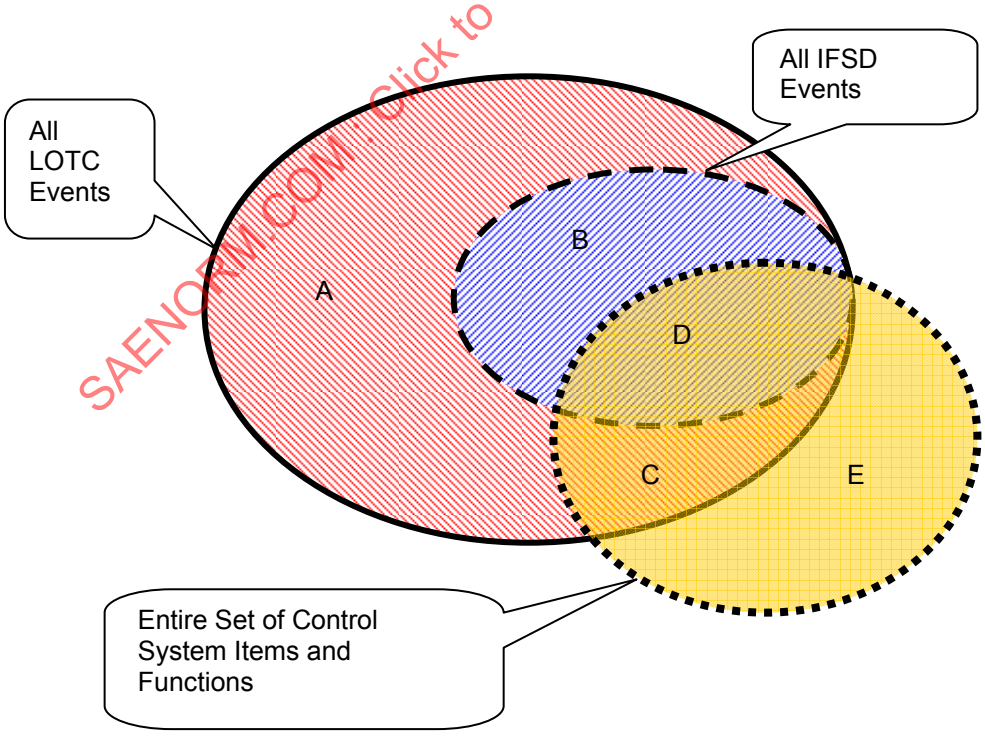

FIGURE 3.1 - ILLUSTRATIONS OF ALL LOTC EVENTS, ALL IFSD EVENTS, AND ENGINE CONTROL SYSTEM ELEMENTS INVOLVED IN A TLD ANALYSIS

Area	Represents
A	All LOTC events not associated with IFSD or engine control system failures.
B	All IFSD events not caused by control system failures.
C	LOTC events not associated with IFSD and resulting from TLD related control system faults
D	IFSD events resulting from TLD related control system faults
E	Control system items not effecting LOTC/IFSD events

Figure 3.1 provides an illustration of the interaction of TLD, LOTC, and IFSD events.

The envelope shown as “Entire Set of Control System Items and Functions” includes some, but not all LOTC events and some, but not all IFSD events. The subset of those events applicable to TLD that overlap the TLD considerations envelope are shown as areas “C”and “D”. Those LOTC and IFSD events not applicable to TLD are shown as areas “A” and “B.

As discussed in 6.3, there are many functions in an EEC system that have no effect on the LOTC rate of the control. These items have to be given consideration as candidates when completing the task of “considering what items should be in the TLD analysis” to document the fact that they have no impact on the control system’s LOTC rate. These items are represented by area “E” in Figure 3.1.

Table 1 illustrates how to consider all elements of the thrust or power control system, the functions and failure modes associated with the element, and then evaluate if it is or is not part of the TLD restriction envelope depicted in Figure 3.1. The table also shows the most likely result of a failure of the element by identifying the applicable area of Figure 3.1.

TABLE 1 - TYPICAL CATEGORIZATION OF FADEC SYSTEM ELEMENTS

Engine Electrical Control System			
Item	*To Be Included*	*Figure 3.1 Failure Area*	*Included Yes / No / If*
EEC	Primary engine control providing power setting, fuel flow setting and splitting, engine operability control, and engine limit protection functions. Auto or continuous ignition may need to be included.	C or D C, D or E	Yes If
Engine Condition/ Health Monitoring	Yes, if impact on LOTC rate No, if no impact on LOTC rate (inspection is presumed to provide adequate analysis.)	C, D or E	If
Other electronic boxes	Yes, if it has impact on LOTC rate. (if not, area “E”) Yes, if it includes processing of signals listed elsewhere that affect LOTC rate. (Area “E” if no affect on LOTC rate) Yes, if it includes processing of fault detection and reporting data related to TLD.	C, D or E C, D or E C or D	If
Ambient temperature and pressure sensors	Yes, for FADEC dedicated sensors. (Unless the system is configured to use the aircraft sensors as primary or only).	C (possible D)	Yes
Engine operating parameter sensors (pressure, temperature, speed)	Yes, sensors that may contribute to LOTC. No, sensors used only for monitoring; e.g. engine performance monitoring or secondary systems.	C E	If
Electrical cables, including airframe cables as appropriate.	Yes, but only for cables that carry a signal applicable to LOTC / IFSD	C	If
Igniters, Ignition exciter and associated cables	No,	N/A	. No
Dedicated EEC alternator	Yes, includes the electrical generation portion of the alternator and any drive shafts/couplings/bearings within the alternator.	C or D	Yes
Alternator Drive Assembly (But not part of alternator)	No	A or B	No
Cockpit throttle position elements	Yes, for electrical throttle position sensor and aircraft electrical cables connecting the sensor to the EEC No, for mechanical parts of throttle system	C or D A or B	Yes
Aircraft data bus inputs to EEC	Yes, if it can contribute to engine control system caused LOTC.	C	If
Rating, configuration, and thrust trim definition (connectors/boxes)	Yes, if it can contribute to LOTC rate	C	Yes

Engine Electrical Control System			
Item	*To Be Included*	*Figure 3.1 Failure Area*	*Included Yes / No / If*
Engine fault detection sensors, conditioners and computers (E.g. Overspeed limiters)	Yes, if effect on LOTC Rate and control system operation / maintenance. Area "E" if no effect on LOTC rate.	C, D or E	If
Engine transient performance	Yes, If caused by failure within the control system. No, If caused by engine damage or deterioration preventing it from operating with correctly implemented control limits	C A	If
Engine transient due to lightning strike	No, if events caused by engine damage due to direct effects or engine surges due to pressure/thermal inlet effects. Yes, if control system upsets caused by EMI, HIRF or the indirect effects of lightning. This is true during all dispatchable configurations. Control related events must be reported	A or B	IF
Inappropriate pilot commanded shutdown	No	B	No
Aircraft auto throttle or auto thrust system	No	A	No

Fuel System			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Mechanical Fuel Pump	No, Excluded per FAA policy. Considered part of basic engine.	A or B	No
Accessory Gearbox elements associated with Fuel Pump or Metering Unit drive	No, Engine mechanical systems are not considered to be part of the control system	A or B	No
Fuel Filter condition sensors	Yes, If fault results in restriction on power setting or time at power	C	If
Flow Meter	Yes, if active part of fuel control	C or D	If
Fuel Metering Unit	Yes	C or D	Yes
Active Fuel Flow Divider Valves	Yes, Assumes fault results in restriction on power setting or time at power. Active refers to any valves that are controlled by the FADEC to divide or stage flow to the burner	C or D	Yes
Combustor Flow Control	Yes, Assumes fault results in restriction on power setting or time at power	C or D	Yes
Other fuel actuated control units	Yes, if unit associated with the control of any function listed elsewhere as applicable	C or D	If
Fuel Nozzles and fuel lines	No, Considered part of basic engine.	A or B	No
Fuel temperature or pressure sensors	Yes, if the fault results in restriction on power setting or time at power	C	If
Fuel lines, manifolds, etc	No, Considered part of basic engine. Fixed position flow distribution or pressure modification devices within the manifolds are included in the same category as fuel lines and manifolds.	A or B	No

Variable Geometry And Bleed Systems			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Compressor Variable Stator Vane Actuators and position sensors	Yes, Assumes fault can impact engine performance to cause a LOTC. Actuator means the device that receives the air or fuel muscle to position the loop.	C or D	Yes
Variable (Bleed) actuators and position sensors	Yes, Assumes fault can impact engine performance to cause a LOTC. Actuator means the device that receives the air or fuel muscle to position the loop.	C or D	Yes
Variable Stator Vane and Bleed Actuation System Unison Rings, links, clevis, vane bearings, etc.	No, Defined as all mechanism(s) connecting the control actuator mechanical output to the variable position air flow device	A or B	No
Air bleed valves (transient or start)	Yes, Assumes fault results in reduction in power or a restriction on power setting or time at power	C	Yes

Engine Oil/Lubrication System			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Oil Tanks and lines	No	B	No
Mechanical Oil Pumps	No	B	No
Electronic Debris sensors and conditioners	No, Assumes there is no control initiated input to power setting	N/A or E	No
Filter condition sensors	No, Assumes there is no control initiated input to power setting	A, B or E	No
Temperature and pressure sensors	Yes, if there is control-initiated input to power setting or if a control system fault leads to erroneous indication which the Engine Operating Instructions would require the pilot to reduce power.	C or D	If

Aircraft Interfaces			
Item	*Comments*	*Figure 3.1 Failure Zone)*	*Included Yes / No/ If*
Vibrations sensors and conditioners	No, Assumes there is no control initiated input to power setting. Yes, if a control system fault leads to erroneous indication which the Engine Operating Instructions would require the pilot to reduce power.	A C or D	No Yes
Engine performance / health monitoring sensors wired direct to cockpit	No	A	No
Aircraft Power	Yes, if the failure of aircraft power can affect LOTC rate	C or D	If

Propulsion System & Installation			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Basic engine turbo-machinery	No	A or B	No
Engine Operability or Performance	No, Includes thrust loss due to engine deterioration, surge, and reduction of power required to stay within limits	A or B	No
Thrust Reverser position sensors	Yes, if a failure of a thrust reverser position sensor can result in a change in thrust setting; e.g. selection of idle thrust.	C	If
Thrust reverser actuation & control systems	No, if fault results in inability to deploy or stow the reverser but does not restrict engine power setting. Yes, if it does restrict engine power.	N/A C	No If
Engine anti-icing sensors, controllers, & control valves	Yes, if these elements are used within the engine control system for automatic engine internal anti-icing	C	If

Propulsion System & Installation			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Sensors, cables, or signal processing elements for aircraft electric or hydraulic power	No	A	No
Cockpit display signals	Yes if erroneous display can lead to flight crew initiated thrust reduction or IFSD; e.g. incorrect rotor speed or EGT displayed. No, if only informational; (e.g. fuel flow)	C or D E	If
Cockpit Display Systems	No, cockpit display systems are not considered part of the engine control system.	A or B	No
Aircraft Bleed Extraction	No	A	No

Engine Configuration			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Brackets/clamps mounting bolts, seals, etc associated with elements listed as applicable.	No.	N/A	No
Thermal shields and insulation blankets	No	A or B	No
Pneumatic lines to sensors	Yes, If fault detection and accommodations can result in an LOTC.	C or D	Yes

Items Unique to General Aviation Applications or Rotorcraft			
Item	*Comments*	*Figure 3.1 Failure Zone*	*Included Yes / No/ If*
Collective Compensation Input	Yes, for electrical compensation sensor and associated electrical cables. No, for mechanical parts of the compensation system.	C N/A	Yes No
FADEC Back up battery	Yes	C or D	Yes
Torque Sensor	Yes, if the system has torque control or limiting	C	If
Turbine temperature sensing system	Yes, if system has temperature limiting or OEI limiting, or pilot reduces power due to false (high) indication.	C	If

6.5 Recommendations on In-Service LOTC Reporting

After TLD approval is obtained and field experience is achieved the FAA policy (Reference Appendix B) requires reporting of the field experience to provide continuing validation of the TLD analysis, identification of emerging trends that require field action, component redesign, etc. As part of this reporting process, the engine manufacturer should collect the data for all LOTCs that occur on an installation, including any that are caused by aircraft systems.

Only actual LOTC events shall be counted for reporting relative to the allowable event numbers provided in the FAA policy. See Appendix B, Sections 12 and 13 for additional discussion. Some failures occur without an LOTC that are identified by system fault detection. Corrective action is taken before an LOTC event has occurred. If those same failures had occurred at a different engine operating condition, an LOTC may have occurred. Since there was no LOTC, none is reported against the allowable number of events criteria. However, the TLD analysis related to these failures should be reviewed to determine if appropriate failure rates for the failures was used in the analysis. Even though it may not have caused an LOTC event, if the failure rate for the in-service faults and their effect on the LOTC rate is considerably greater than the one used in the TLD analysis, corrective action should be considered. Corrective actions may involve a greater restriction on the time allowed for operating with faults that contribute to the failure mode of concern, or redesign and replacement of the parts involved to achieve the desired design reliability for those components.

7. CALCULATION APPROACHES: SINGLE ENGINE ANALYSIS

7.1 A Simple Time-Averaging Approach

Note that the terminology "fleet average" is used synonymously with "time-weighted average". This is appropriate because any given engine may have more or less ST and/or LT faults than the expected number, but these guidelines are intended for use in a large fleet of engines where all possible single faults will occur at or close to their expected rates, and if all faults are allowed to remain in the system for the maximum approved number of hours before repair is accomplished, the LOTC rate of the control will approach the expected value. It is recognized that in practice, many faults are repaired sooner than the maximum allowed time, and therefore, the fleet averaged LOTC rate may be quite a bit lower than the expected value.

A simple "time-weighted-averaged (TWA) LOTC rate" is one wherein the LOTC rate is determined as the sum of (1) the hydromechanical/mechanical failures, (2) the uncovered faults, and (3) a time-weighted-average value of the FADEC system's dual channel, electrical/electronic failures. The failures and failure rates leading to an LOTC event are shown graphically in Figure 4, below.

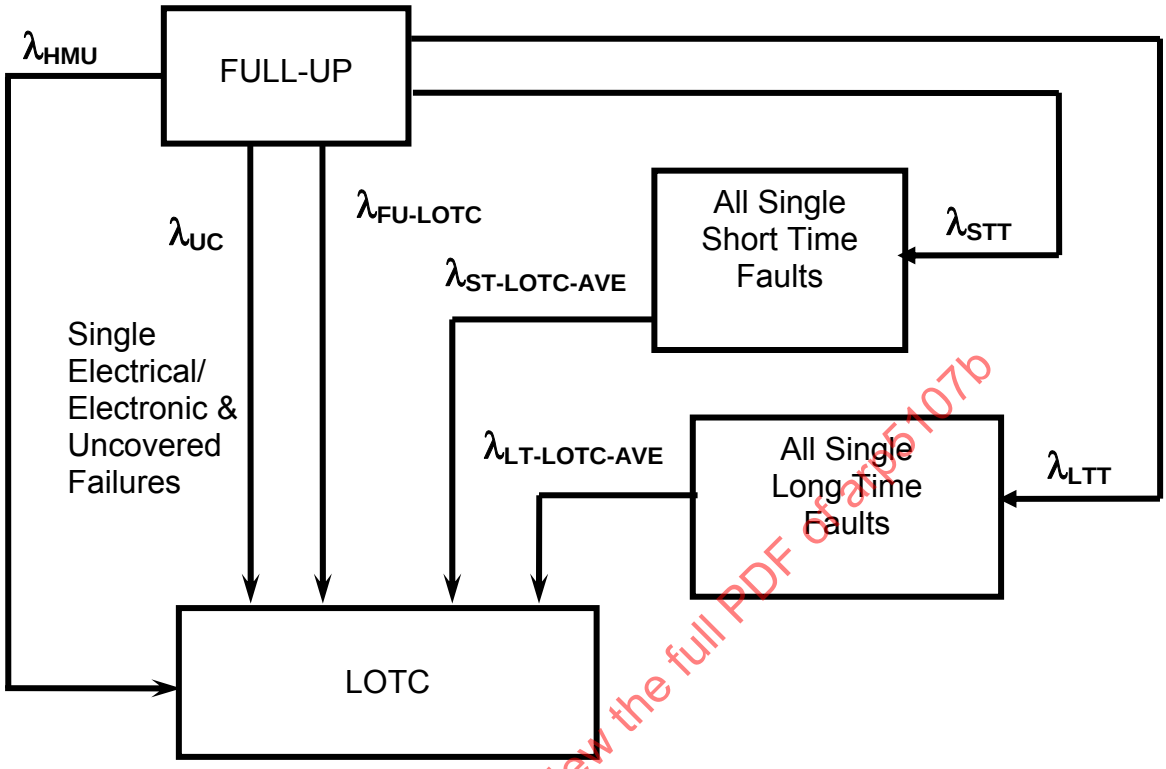

FIGURE 4 - A GRAPHICAL REPRESENTATIONS OF THE FAILURE PATHS OF A SIMPLE FADEC SYSTEM THAT LEAD TO LOTC

The TWA failure rate for the dual channel electronic failures is determined as the sum of single hydromechanical and uncovered electrical/electronic failures that lead directly to an LOTC event plus the percentages of time spent in a given operating configuration multiplied by the average LOTC rate of that configuration. Hence, the fleet TWA LOTC rate for a simple FADEC system is given as:

$$\lambda_{LOTC\text{-}AVE} = \lambda_{HM+UC} + \lambda_{FU\text{-}LOTC} * Fract(FU) + \lambda_{ST\text{-}LOTC\text{-}AVE} * Fract(ST) + \lambda_{LT\text{-}LOTC\text{-}AVE} * Fract\ (LT) \quad \text{(Eq. 1)}$$

where: $\lambda_{HM+UC} = \lambda_{HMC} + \lambda_{UC}$

λ_{HMC} represents the sum of the rates of all single mechanical/ hydromechanical faults which lead to LOTC events.

λ_{UC} represents the sum of the rates of all undetected/uncovered electrical/electronic faults assumed to lead to LOTC events.

$\lambda_{FU\text{-}LOTC}$ is the (average) failure rate from the full-up configuration to the LOTC state caused by failures in the redundant portions of the electronic control system, in one flight. (Single electrical/electronic failures that lead to an LOTC event are contained in λ_{UC}, which is described below.)

$\lambda_{ST\text{-}LOTC\text{-}AVE}$ is the average failure rate of the system due to a second electrical/electronic fault when operating in an ST fault dispatch configuration.

$\lambda_{LT\text{-}LOTC\text{-}AVE}$ is the average failure rate of the system due to a second electrical/electronic fault when operating in an LT fault dispatch confirguration.

The uncovered fault rate, λ_{UC}, is generally expressed as:

λ_{UC} = X*{$\sum\lambda$ of both channel electrical/electronic faults associated with LOTC critical elements)} (Eq. 2)

where:

The "$\sum\lambda$ of all electrical/electronic hardware associated with LOTC critical elements" can be approximated by (λ_{STT} + λ_{LTT}), where λ_{STT} is defined as the sum of the failure rates of all ST type faults in both channels, and λ_{LTT} is defined as the sum of the failure rates of all LT type faults in both channels. Hence,

$\lambda_{STT} \equiv \sum(\lambda_{ST(i)})$, the sum of the failure rates of all ST faults in both channels where $\lambda_{ST(i)}$ represents the failure rate for a particular ST fault. (Eq. 3a)

$\lambda_{LTT} \equiv \sum(\lambda_{LT(i)})$, the sum of the failure rates of all LT faults in both channels where $\lambda_{LT(i)}$ represents the failure rate for a particular LT fault. (Eq. 3b)

And, "X" is a number generally between 0 and 0.05.

(It should be noted that although Equation 2 might imply that the uncovered fault rate is assessed at the "channel" level, in actual practice, it isn't. The uncovered fault rate is usually determined by summing the uncovered fault rates of all LOTC critical elements, on an element-by-element basis - such as the power supply, the CPU, sensors, A/D converters, etc. Equation 2 tends to imply that the uncovered fault rate of each element is between 0 and 5%. This is not intended. Equation 2 is merely a simplification indicating that a channel's overall uncovered fault rate will "generally" be somewhere between 0 and 5% of the channel's total LOTC rate.)

Equation 2 is quite conservative because it assumes that an uncovered fault in either channel would lead to an LOTC event - in any given flight. In practice, many different system architecture's are possible, each of which utilize varying degrees of system resources and each with its own unique level of system coverage. For these systems, Equation 2 can be modified to provide a more accurate representation of the architecture. For example, assume that the system being addressed is an active-standby system, which is currently representative of many of the current designs. In these systems, the controlling channel provides all of the required resources when operating in a full-up condition. Furthermore, the alternating channel scheme (i.e., the process of alternating control channels on each engine start), provides nearly 100% coverage of undetected faults in the standby channel at the next engine start. Hence, an undetected fault in the standby channel in a given flight would not cause an LOTC event unless the operating channel has a fault (in that flight) which requires the system to "switch" channels. The likelihood of this is relatively small for most channel switching schemes. Hence, for these system configurations, the value of λ_{UC} may be reduced by approximately one half (1/2) because the vast majority of uncovered faults that lead to an LOTC event are only those in the active channel.

In any case, knowledge of the system configuration and its operating characteristics should be used when determining the value of the uncovered fault "multiplier".

Continuing with Equation 1:

Fract(FU) is the fraction of time spent in the full-up state,

Fract(ST) is the fraction of time spent in the short time dispatch state,

Fract(LT) is the fraction of time spent in the long time dispatch state.

The following discussion uses the nomenclature “T” to represent repair times. This T repair time is the same time period that the system is allowed to operate with a given fault before repair is required.

Assume a block of time of a million hours. During the million-hour block of time, the system is in the full-up state for Fract(FU)*10^6 hours, the system fails from the full-up state to the ST state at a rate of λ_{STT} per hour, and for each of those failures it remains in the ST state for $T_{ST\text{-}REPAIR}$ hours. Therefore, the fraction of the million hours spent in the ST state is

$$Fract(ST) = Fract(FU)*(\lambda_{STT} * T_{ST\text{-}REPAIR}) \quad \text{(Eq. 4a)}$$

And likewise, the fraction of time spent in the LT state is

$$Fract(LT) = Fract(FU)*(\lambda_{ITT} * T_{LT\text{-}REPAIR}) \quad \text{(Eq. 4b)}$$

Combining these equations with the conservation requirement that

$$Fract(FU) + Fract(ST) + Fract(LT) = 1 \quad \text{(Eq. 5)}$$

leads to the fractions:

$$Fract(FU) = \frac{1}{1 + \lambda_{STT} * T_{ST\text{-}REPAIR} + \lambda_{LTT} * T_{LT\text{-}REPAIR}} \quad \text{(Eq. 6a)}$$

$$Fract(ST) = \frac{\lambda_{STT} * T_{ST\text{-}REPAIR}}{1 + \lambda_{STT} * T_{ST\text{-}REPAIR} + \lambda_{LTT} * T_{LT\text{-}REPAIR}} \quad \text{(Eq. 6b)}$$

$$Fract(LT) = \frac{\lambda_{LTT} * T_{LT\text{-}REPAIR}}{1 + \lambda_{STT} * T_{ST\text{-}REPAIR} + \lambda_{LTT} * T_{LT\text{-}REPAIR}} \quad \text{(Eq. 6c)}$$

As discussed in 7.1.4 and 7.1.5, and shown in Figure 5, the use of these fractional coefficients provides a much improved result as compared with the fractional coefficients as defined in the original release of this ARP. This is because the fractional coefficients defined by Equations 6 of this revised ARP adjust in a more balanced manner to reflect the actual portion of time spent in the various states. The definitions of the fractional coefficients in the original ARP did not do this because the Fract(ST) and Fract(LT) fractional coefficient terms, as developed in original ARP, assume the control is in the full-up state for the full million hour block of time. In this revised ARP, it is recognized that the control is only in the full-up state for Fract(FU)*10^6 hours.

7.1.1 LOTC Rate for Full-up Electronics

For small λT's, the LOTC rate for the full-up electrical/electronics portions of the control at dispatch is approximated as:

$$\lambda_{FU\text{-}LOTC} \leq [(\lambda_{STT} + \lambda_{LTT})/2]^2 * T_{FL} \quad \text{(Eq. 7)}$$

where:

λ_{STT} and λ_{LTT} are defined above and,

T_{FL} represents the length of a flight (in hours).

This full-up channel failure rate is a very conservative estimate because it assumes that all channel faults (both short time and long time) result in loss of that channel. Although this is far from accurate, it surely provides an upper bound. The calculated value of $\lambda_{FU\text{-}LOTC}$ is usually quite small, as it should be. This is because it takes two independent, electrical/electronic failures, one in each channel, to have an LOTC event occur in one flight from the full-up configuration. The small value of $\lambda_{FU\text{-}LOTC}$ serves to show that the redundant electronic portions of the control have little affect on the LOTC rate of the control system when operating in the full-up configuration.

7.1.2 Average LOTC Rate for Short Time (ST) Faults

The certifying authorities have indicated that all faults which deplete a significant portion of the control system's capability should be repaired in a short period of time. Hence, sum the failure rates of the power supply and processor unit elements of both channels, along with any other items that are deemed necessary of requiring short term maintenance, and set the repair interval for these elements equal to (or slightly greater than) the maximum MEL dispatch deviation time allowed in the application.

An average LOTC rate for operation with one of these faults is useful. Grouping the above faults together as ST repair faults, the "average" LOTC rate with a short time (ST) fault is defined as follows:

$$\lambda_{ST\text{-}LOTC\text{-}AVE} = \frac{\sum(\lambda_{ST(i)} * \lambda_{ST-LOTC(i)})}{\sum(\lambda_{ST(i)})} \quad \text{(Eq. 8)}$$

where:

$\lambda_{ST(i)}$ is the failure rate for a given ST fault, and $\lambda_{ST-LOTC(i)}$ is the failure rate to the LOTC state when operating with that particular $\lambda_{ST(i)}$ fault. (Include all faults in the 'other' channel that would lead to an LOTC event, but do not include the hydromechanical and uncovered faults, as they are already accounted.)

7.1.3 Average LOTC Rate for Long Time (LT) Faults

Excepting the "no dispatch" and "short time" faults, group all remaining electrical/electronic faults affecting LOTC of one channel together and place them in the long time repair category. As in the above discussion, an average LOTC rate is useful (for calculation purposes) for these long time faults; this is defined as:

$$\lambda_{LT\text{-}LOTC\text{-}AVE} = \frac{\sum(\lambda_{LT(i)} * \lambda_{LT-LOTC(i)})}{\sum(\lambda_{LT(i)})} \quad \text{(Eq. 9)}$$

where:

$\lambda_{LT(i)}$ is the failure rate to a given LT fault state, and $\lambda_{LT-LOTC(i)}$ is the failure rate to the LOTC state when operating with that given $\lambda_{LT(i)}$ fault. (Again, include all faults of the 'other' channel and cross-talk link faults which would lead to an LOTC event, but do not include HMC or uncovered faults.)

In general, many LT faults have only a minor effect on the control. For example, assume that one channel has a sensor failure, such as one of two actuator feedback position signals. The LOTC rate when operating with this signal would be the sum of the failure rates for (1) the redundant sensor, (2) the other channel's CPU and power supply sources and circuitry, and (3) the cross-talk link between the two channels These are the only failures that would lead to an LOTC event, because these are the only paths that would cause loss of both actuator feedback signals to the control. (It is assumed in this example that an actuator feedback position signal is needed to maintain control of the engine. If controller logic is constructed to re-configure the control laws to work with no actuator position feedback information, this LT fault could well be deleted from the analysis.)

7.1.4 Calculations of the Average LOTC Rate Using the TWA Approach

Having summed all of the ST and LT faults rates to obtain λ_{STT} and λ_{LTT}; and determined the average failure rates $\lambda_{ST\text{-}LOTC\text{-}AVE}$ and $\lambda_{LT\text{-}LOTC\text{-}AVE}$ from Equations 8 and 9, the average overall LOTC rate given by Equation 1 can be calculated.

Using the balanced fractional coefficients given in Equation 6 in Equation 1 yeilds the LOTC rate as:

$$\lambda_{LOTC\text{-}AVE} = \lambda_{HM+UC} + \frac{\lambda_{FU\text{-}LOTC} + (\lambda_{STT}*T_{ST\text{-}REPAIR})*\lambda_{ST\text{-}LOTC\text{-}AVE} + (\lambda_{LTT}*T_{LT\text{-}REPAIR})*\lambda_{LT\text{-}LOTC\text{-}AVE}}{\{\ 1 + \lambda_{STT}*T_{ST\text{-}REPAIR} + \lambda_{LTT}*T_{LT\text{-}REPAIR}\ \}} \quad \text{(Eq. 11)}$$

Using the above TWA equation, which used the balanced fractional coefficients of Equations 6 to estimate the average LOTC rate of the control system, yields a result which is considerably improved as compared with the fractional coefficients defined in the original release of this ARP. It is a more balanced approach because the fractional coefficients are more representative of the amount of time that is spent in each of the three states, i.e., full-up, short time fault (or dispatch), and long time fault (or dispatch). This is illustrated in the following example.

7.1.5 An Example Calculation

Assume the following data:

λ_{HMC} = $4.0*10^{-6}$ (failures/hour)

λ_{STT} = $30.0*10^{-6}$ (failures/hour) (sum of ST electronic faults for both channels)

λ_{LTT} = $70.0*10^{-6}$ (failures/hour) (Sum of LT electronic faults for both channels)

$\lambda_{ST\text{-}LOTC\text{-}AVE}$ = $65.0*10^{-6}$ (failures/hour) (from second electronic faults only)

$\lambda_{LT\text{-}LOTC\text{-}AVE}$ = $50.0*10^{-6}$ (failures/hour) (from second electronic faults only)

X (the fraction of uncovered faults) = 0.02

$T_{ST\text{-}REPAIR}$ = 100 (hours)

$T_{LT\text{-}REPAIR}$ = To Be Determined to achieve an LOTC rate of $10*10^{-06}$ (events/hour)

T_{FL} = 4.5 (hours)

Substituting the above data into Equation 11, which uses the balanced Equation 6 fractional coefficients, yields the TWA average LOTC rate for an ST repair interval of 100 hours of:

$$\lambda_{LOTC\text{-}AVE} = 6.0*10^{-6} + \frac{\{0.20625 + 0.0035*T_{LT\text{-}REPAIR}\}*10^{-6}}{\{\ 1.003 + 70.0*10^{-6}*T_{LT\text{-}REPAIR}\ \}} \quad \text{(Eq. 11a)}$$

A plot showing a comparison of the results from this equation, Equation 11a, with those from the equation used in the original ARP5107 is shown in Figure 5. This plot shows the LOTC rate as a function of the long time repair interval. The short time repair is fixed at 100 hours. As shown, the results using the balanced fractional coefficients from Equation 6 allow a longer LT fault repair interval to be used before the limit (i.e., target) of 10*10-6 LOTC rate in encountered. This is because the fractional coefficients contained in this ARP provide a more balanced solution for the times spent in the various dispatch configurations.

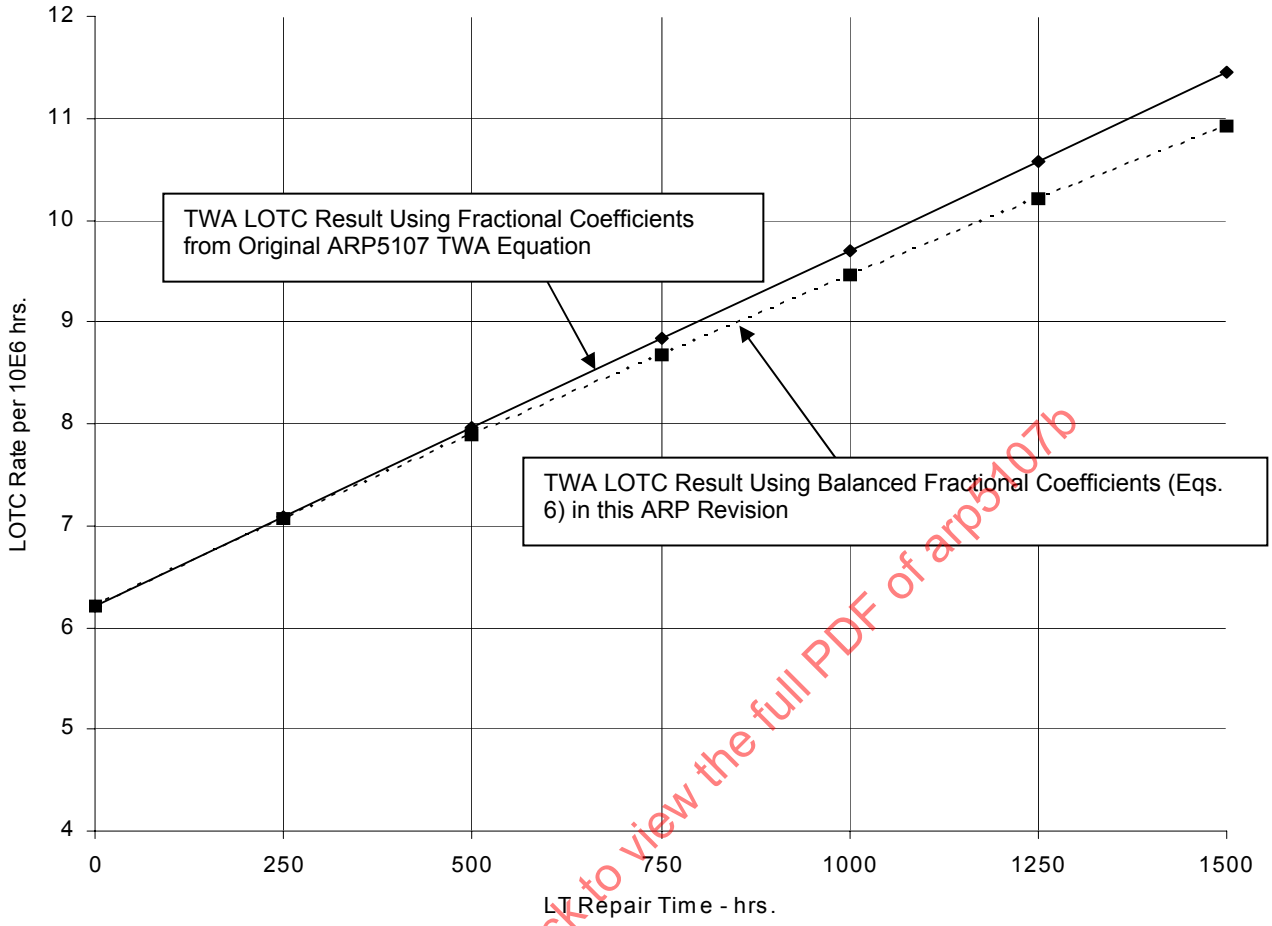

FIGURE 5 - PLOT OF THE LOTC RATE FOR THE EXAMPLE DATA GIVEN IN 7.1.5 FOR BOTH THE ORIGINAL FRACTIONAL COEFFICIENTS (AS GIVEN IN THE ORIGINAL ARP) WITH THE IMPROVED FRACTIONAL COEFFICIENTS GIVEN IN THIS REVISED ARP

7.2 Markov Model Approach

The Markov modeling (MM) approach is somewhat different than the above TWA approach, but all of the same data is still needed and used.

This document is going to use a unique nomenclature when referring to Markov models, and that nomenclature is to refer to the models as either “open loop” or “closed loop” models. For the purposes of this document, an open loop model is one that has no feedback or simulated repair from the final failed state to the full-up state. And in contrast, closed loop models are those that incorporate a feedback or simulated repair from the fully failed state to the full-up state. Both open and closed loop models can incorporate simulated repair paths from the various faulty states leading to the fully failed state, to the full-up state. Examples of both open loop and closed loop models follow.

7.2.1 Open Loop Markov Models:

These models can be visualized as a waterfall system, as shown in Figure 6, below.

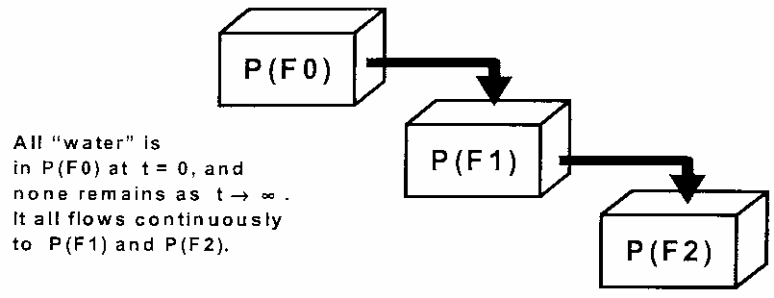

FIGURE 6 - OPEN LOOP MARKOV MODEL WATER FALL DIAGRAM

In this figure, P(F0) represents the probability of being in the full-up state, P(F1) represents the probability of being in the first failure state, and P(F2) is the probability of being in the second failed state, which in this simple model is the final failed state. This is called an "open loop" model herein, because there is no simulated repair path to return any of the water from the fully failed state, P(F2), to the full-up state, P(F0). In open loop models, the initial condition at time zero, is usually to have all the water in the full-up state, that is, P(F0) = 1.0 at t=0.0. As time increases, the water, or probability, will flow into the first, and then the second failure states. Since there is no simulated repair from the fully failed state, P(F2), to the full-up state, all of the water, or probability, will flow to the final failed state, P(F2), as time approaches infinity. Hence, the probability of being in state P(F2) will approach unity (i.e., 1.0) as time approaches infinity. The model could be revised to incorporate a repair path from the first failed state, P(F1), to the full-up state, but it would still be an open loop model because there is no repair path from the fully failed state to the full-up state. An example of an open loop model with repair paths from initial failure states to the full-up state follows.

A simplified open loop Markov model for a FADEC system is shown in Figure 7.

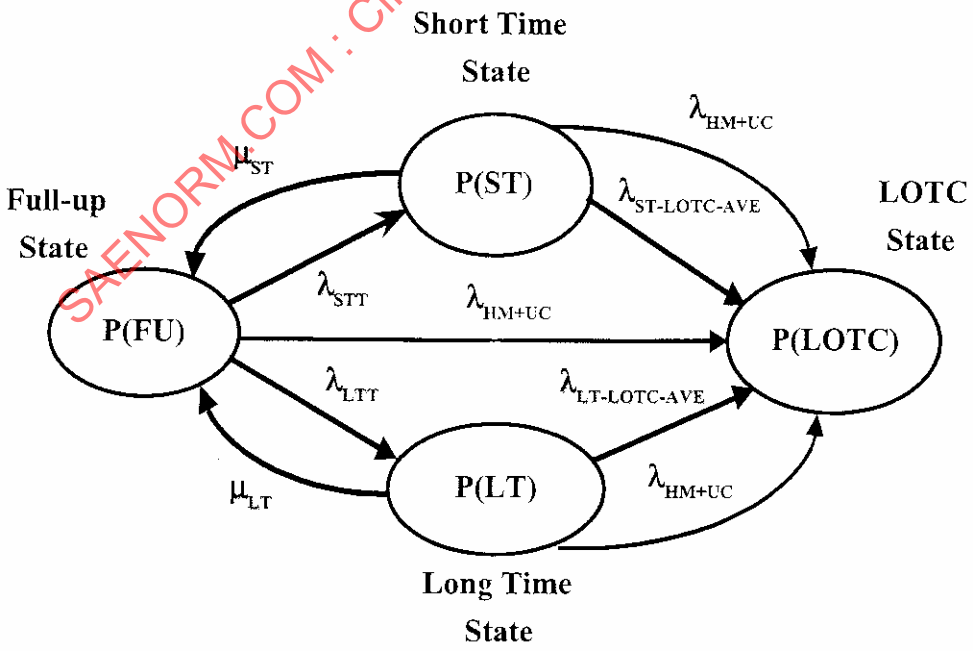

FIGURE 7 - OPEN LOOP MARKOV MODEL OF SIMPLE FADEC SYSTEM WITH REPAIR FOR SHORT AND LONG TIME FAULT STATES

In this model, P(FU), P(ST), P(LT), and P(LOTC) represent the probabilities of being in the full-up, short term fault, long term fault, and loss-of-thrust-control (LOTC) states, respectively. In Markov models, the transition rates from one state to another are simply the failure rates or repair rates between those states. So for example, the failure rate from the full-up state to the short term fault state is simply the failure rate, λ_{STT}. The transition rate from the P(ST) state to the P(FU) state is the repair rate, μ_{ST}.

It should be noted here that Markov models of FADEC systems normally do not aggregate all short time and long time fault states into one short time and one long time fault state. One could do that, but the various short time and long time fault states (or conditions) are generally shown on a MM diagram (and handled) as separate and independent fault conditions, and they have their own “bubble”. If one wishes to aggregate all ST and LT fault states into one ST and one LT state, Equations F7 through F10 in Appendix F show (for single state models) how the λ_{STT}, λ_{LTT}, $\lambda_{ST\text{-}LOTC\text{-}AVE}$ and $\lambda_{LT\text{-}LOTC\text{-}AVE}$ rates would be calculated. It is noted that for large repair rates, μ_{ST} and μ_{LT}, with respect to the failure rates into and out of the various ST and LT fault states, the failure rates, λ_{STT}, λ_{LTT}, $\lambda_{ST\text{-}LOTC\text{-}AVE}$ and $\lambda_{LT\text{-}LOTC\text{-}AVE}$ approach those values calculated by Equations 3a and 3b, and Equations 8 and 9.

For the purposes of the initial Markov model discussion presented here, the same notation of λ_{STT}, λ_{LTT}, $\lambda_{ST\text{-}LOTC\text{-}AVE}$ and $\lambda_{LT\text{-}LOTC\text{-}AVE}$ will be used because it is convenient to show “one” ST state and “one” LT state in these initial model diagrams. As the discussion of Markov models progresses, the actual individual ST and LT states will be shown.

It should also be noted that in a Markov model approach, unlike the TWA approach, the single hydromechanical and uncovered fault rate needs to be added to the LOTC rate of each and every fault state, because those single failures can take the system to LOTC from any (and every) fault state.

The μ’s represent the repair rates for the states. The repair rate for a repair interval of T hours is usually represented as an exponential transition with a rate of 1/T per hour. Hence,

$\mu_{ST} = 1/T_{ST\text{-}REPAIR}$, and

$\mu_{LT} = 1/T_{LT\text{-}REPAIR}$

In open loop MM’s the solution is obtained by solving a set of first order differential equations which represent the probabilities of being in the various "states". The time-rate-of-change of a probability state is equal to the “probability flow into” that state minus the “probability flow out of” that state. The probability flows into and out of a given state are illustrated in Figure 8.

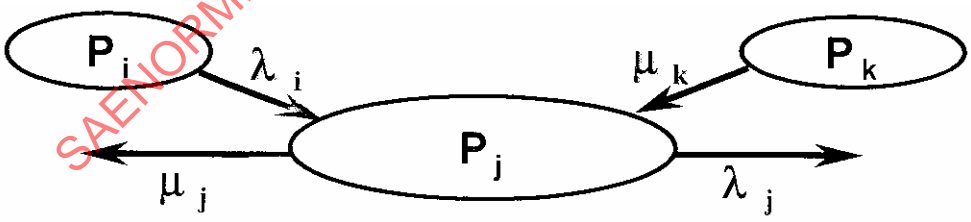

FIGURE 8 - PROBABILITY FLOW INTO AND OUT OF STATE P_j

In this figure, the “i” subscript ranges over all of the states that have failures which cause the control to transition into a given P_j state, and the “k” subscript represents all of the states where a repair returns the system to the given P_j state. Referring to this figure, the probability flow into a state is the sum of the failure rates and repair rates into that state multiplied by the respective probabilities of the states driving those failure, and the probability flow out of a state is the sum of the failure rates and repair rates leaving that state multiplied by the probability of the state, itself. Hence, referring to Figure 8:

Prob. flow into state $P_j \equiv \sum (\lambda_i * P_i) + \sum (\mu_k * P_k)$

Prob. flow out of state $P_j \equiv (\mu_j + \lambda_j) * P_j$

The time dependent differential equation for the P_j state is then, simply:

dP_j/dt = Prob. flow into state - Prob. flow out of state

or, $dP_j/dt = \{ \sum (\lambda_i * P_i) + \sum (\mu_k * P_k) \} - \{ (\mu_j + \lambda_j) * P_j \}$

Referring to the MM given in Figure 7, the probability flow into the ST state is $\lambda_{STT}*P_{FU}$, which is the transition rate into that state (i.e., λ_{STT}) multiplied by the probability driving that rate, P_{FU}, and the probability flow out of the state is the transition rates, $(\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC} + \mu_{ST})$, multiplied by the probability of the state itself, P_{ST}.

Hence, the time rate of change equation for the ST state shown in Figure 7 is:

$dP_{ST}/dt = \lambda_{STT}*P_{FU} - (\lambda_{ST\text{-}LOTC\text{-}AVE} + \mu_{ST} + \lambda_{HM+UC})*P_{ST}$

The first order differential equations for the P_{FU}, P_{LT}, and P_{LOTC} states are:

$dP_{FU}/dt = \mu_{ST} * P_{ST} + \mu_{LT} * P_{LT} - (\lambda_{STT} + \lambda_{LTT} + \lambda_{HM+UC}) * P_{FU}$

$dP_{LT}/dt = \lambda_{LTT} * P_{FU} - (\lambda_{LT\text{-}LOTC\text{-}AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT}$

$dP_{LOTC}/dt = \lambda_{HM+UC} * (P_{FU} + P_{ST} + P_{LT}) + \lambda_{ST\text{-}LOTC\text{-}AVE} * P_{ST} + \lambda_{LT\text{-}LOTC\text{-}AVE} * P_{LT}$

These equations define the system.

NOTE: In all Markov models presented herein (and virtually all Markov probability models), one of the probability state equations is redundant and can be derived from the others. To establish an independent set of equations, always eliminate one of the equations - it doesn't matter which one - and add the conservation equation:

The sum of the probabilities of all of probability states must equal unity.

In this example:

$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0$

Arbitrarily eliminating the first equation, dP_{FU}/dt, and substituting the conservation yields the set of equations representing the MM shown in Figure 7 as:

$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0$ (Eq. 12a)

$dP_{ST}/dt = \lambda_{STT} * P_{FU} - (\lambda_{ST\text{-}LOTC\text{-}AVE} + \mu_{ST} + \lambda_{HM+UC}) * P_{ST}$ (Eq. 12b)

$dP_{LT}/dt = \lambda_{LTT} * P_{FU} - (\lambda_{LT\text{-}LOTC\text{-}AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT}$ (Eq. 12c)

$dP_{LOTC}/dt = \lambda_{HM+UC} * P_{FU} + (\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}) * P_{LT}$ (Eq. 12d)

It is interesting to note that in many papers written on the use of Markov models for solving probability problems, there is no mention of the need to delete one of the equations and substitute the conservation equation to obtain an independent set of equations. Not doing this is acceptable when using the differential equation approach to compute a solution, because the initial conditions for the differential equations would contain the information that the sum of the state probabilities must equal unity, and if the integration algorithm (with time) is accurate, the sum of all state probabilities should remain close to unity. It is still considered that a more robust approach is to eliminate one of the differential equations and replace it with the conservation equation. In the discussion of closed loop Markov models given in 7.2.2, eliminating one of the equations and replacing it with the conversation equation is necessary to achieve a solution.

Using the initial conditions: $P_{FU} = 1.0$, and $P_{ST} = P_{LT} = P_{LOTC} = 0.0$, the set of equations is easily solved to determine the probability states as a function of time.

The overall failure rate of the system, λ_{LOTC}, is then determined from the definition of the hazard rate, which is:

λ_{LOTC} = (Probability Flow into the P_{LOTC} State)/$(1 - P_{LOTC})$ (Eq. 13)

NOTE: Most references define the "hazard rate" only for non-repairable failure states, in which case the value of "probability flow into a state" equals dP/dt, so the hazard rate takes the familiar form (dP/dt)/(1-P). However, in this document we consider repairable failure states, so it is necessary to use the strict definition of "hazard rate" that distinguishes between the probability flow into and out of the failure states.

Using the Probability flow into the LOTC state, the LOTC rate for this example is:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} * P_{FU} + (\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}) * P_{LT}}{(1 - P_{LOTC})} \quad \text{(Eq. 13a)}$$

When solving Equations 12 and calculating the instantaneous LOTC rate from Equation 13a at each point in time, the probabilities of the various states will continuously change with time, but as time approaches infinity (∞) the value of λ_{LOTC}, will approach a constant value. It can be shown that this value asymptotically approaches the smallest eigenvalue of the system, which happens to approximate the long term failure rate under certain conditions. However, in general, it can differ from the true average failure rate of the system by a significant factor, particularly if the repair rates, μ_{ST} and μ_{LT} are not significantly greater than the failure rates into and out of the ST and LT fault states, respectively. This is discussed and illustrated for a simple 2-unit model in greater detail in Appendix H.

Because of these difficulties, an open loop Markov model is not the preferred modeling approach for determining the average failure rate of a system.

The above difficulties as well as the difficulty of having to solve a set of differential equations is circumvented by using the closed loop Markov model approach.

7.2.2 Closed Loop Markov Model Approach

The closed loop MM approach differs from the open loop approach, ONLY in that a feedback is added from the fully failed state to the full-up state. In this example, from P_{LOTC} to P_{FU}.

The closed loop Markov model diagram for the system is shown in Figure 9.

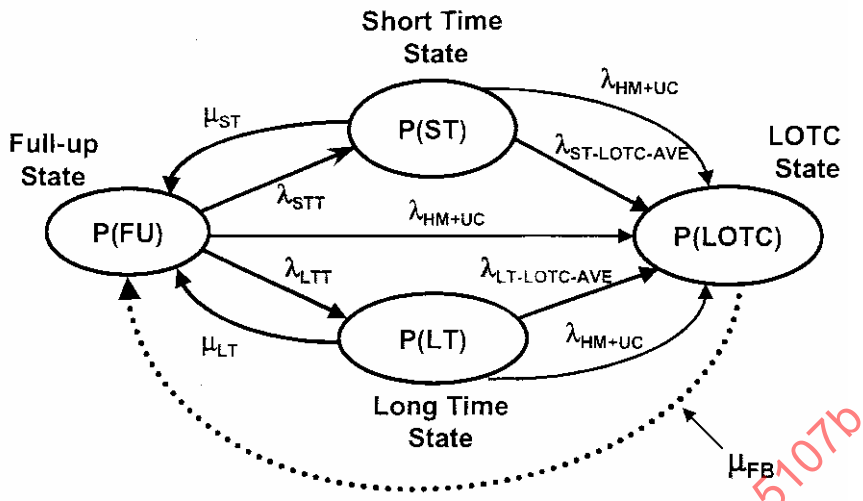

FIGURE 9 - CLOSED LOOP MM FOR SIMPLE FADEC CONTROL SYSTEM WITH REPAIR FOR SHORT AND LONG TERM FAULT STATES

The dotted line in Figure 9 represents the feedback path, μ_{FB}, which has been added from the fully failed, PLOTC, state, to the full-up, PFU, state.

Substituting the conservation equation for the dP_{FU}/dt state equation, the system of differential equations for the system is:

$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0$

$dP_{ST}/dt = \lambda_{STT} * P_{FU} - (\lambda_{ST\text{-}LOTC\text{-}AVE} + \mu_{ST} + \lambda_{HM+UC}) * P_{ST}$

$dP_{LT}/dt = \lambda_{LTT} * P_{FU} - (\lambda_{LT\text{-}LOTC\text{-}AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT}$

$dP_{LOTC}/dt = \lambda_{HM+UC} * (P_{FU} + P_{ST} + P_{LT}) + \lambda_{ST\text{-}LOTC\text{-}AVE} * P_{ST} + \lambda_{LT\text{-}LOTC\text{-}AVE} * P_{LT} - \mu_{FB} * P_{LOTC}$

The only difference between these closed loop equations and those for the open loop MM diagram (Figure 7) is the addition of the $\mu_{FB} * P_{LOTC}$ term to the dP_{LOTC}/dt equation. This term has a negative sign in front of it because it represents the probability flow out of the P_{LOTC} state.

In closed loop models the solution of interest is the steady state solution, because it is the solution which has all of probability states contributing to the fully failed, P_{LOTC} state in a balanced manner, as would be the case in a large fleet of engines.

The steady state solution is obtained by setting all of the dP/dt terms to zero and solving the resulting set of algebraic equations. This makes the calculation of a solution much simpler.

For this example, the set of algebraic equations to be solved is:

$P_{FU} + P_{ST} + P_{LT} + P_{LOTC} = 1.0$ (Eq. 14a)

$0 = \lambda_{STT} * P_{FU} - (\lambda_{ST\text{-}LOTC\text{-}AVE} + \mu_{ST} + \lambda_{HM+UC}) * P_{ST}$ (Eq. 14b)

$0 = \lambda_{LTT} * P_{FU} - (\lambda_{LT\text{-}LOTC\_AVE} + \mu_{LT} + \lambda_{HM+UC}) * P_{LT}$ (Eq. 14c)

$0 = \lambda_{HM+UC} * P_{FU} + (\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}) * P_{ST} + (\lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}) * P_{LT} - \mu_{FB} * P_{LOTC}$ (Eq. 14d)

Having estimated the failure rates for the various short time and long time faults, and the failure rates to the LOTC state when operating with those faults, one selects the desired repair rates for short time and long time faults, and solves the above set of algebraic equations to determine the probabilities of being in the various states. A value for μ_{FB} is needed to calculate a solution. Arbitrarily set μ_{FB} to 1.0. The value selected for μ_{FB} will effect the solution, such that different values of μ_{FB} will yield different values for the calculated probabilities of being in the various states, but as is shown below, although the probabilities of being in the various states is a function of μ_{FB}, the failure rate into the LOTC state, λ_{LOTC}, is not a function of μ_{FB} or any of the values of the state probabilities. (An intuitive explanation for why the "feedback" rate doesn't matter is that the overall average failure rate of a fleet of engine control systems is not affected by the length of time a control system is absent from the operational fleet following its failure.)

7.2.2.1 Hazard (or Failure) Rate for a Closed Loop Markov Model

The failure rate equation for the closed loop model of Figure 9 is the same as that (Equation 13a) given for the open loop model of Figure 8. It is repeated here as:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC}*P_{FU} + (\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC})*P_{ST} + (\lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC})*P_{LT}}{(1 - P_{LOTC})} \quad \text{(Eq. 15)}$$

It would certainly appear that failure rate given by Equation 15 is a function of the state probabilities, but the following will show that it isn't.

7.2.2.2 Reorganizing the Failure Rate Equation

Rearranging Equation 14a yields

$$1 - P_{LOTC} = P_{FU} + P_{ST} + P_{LT}$$

Substituting this into the denominator of Equation 15 yields

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC}*P_{FU} + (\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC})*P_{ST} + (\lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC})*P_{LT}}{P_{FU} + P_{ST} + P_{LT}} \quad \text{(Eq. 16)}$$

And, Equations 14b and 14c can be rearranged to solve for P_{ST} and P_{LT} as a function of PFU:

$$PST = \lambda STT * PFU / (\mu ST + \lambda ST\text{-}LOTC\text{-}AVE + \lambda HM+UC)$$

$$PLT = \lambda LTT * PFU / (\mu LT + \lambda LT\text{-}LOTC\_AVE + \lambda HM+UC)$$

Substituting Equations 17a and 17b into Equation 16 for PST and PLT yields:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} + \dfrac{\lambda_{STT} * (\lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC})}{\mu_{ST} + \lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}} + \dfrac{\lambda_{LTT} * (\lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC})}{\mu_{LT} + \lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}}}{1.0 + \dfrac{\lambda_{STT}}{\mu_{ST} + \lambda_{ST\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}} + \dfrac{\lambda_{LTT}}{\mu_{LT} + \lambda_{LT\text{-}LOTC\text{-}AVE} + \lambda_{HM+UC}}} \quad \text{(Eq. 18)}$$

Note that this equation only involves the failure rates and repair rates of the system, and that it is independent of the feedback rate μFB and all state probabilities. This is a highly desirable characteristic of closed loop, single state MM's.

7.2.2.3 Single State Closed Loop MMs

For the purposes of this ARP a single state MM is one which shows only single fault conditions as individual states. All second faults from the single states lead to the LOTC state. Second faults, which do not lead to the LOTC state, are not modeled. Hence, no dual state fault conditions are shown as separate states Therefore, the transition rates from the single failure states represent only those additional single failures that would take the system from the single faulty states to the LOTC state. A generic single state MM for a FADEC system is shown in Figure 10.

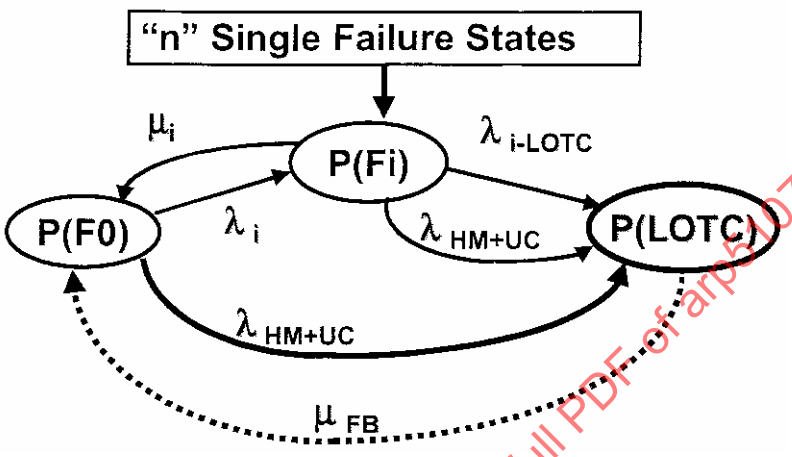

FIGURE 10 - SINGLE STATE MARKOV MODEL

The n single fault states can be ST or LT states, or No Dispatch states, when the No Dispatch (ND) condition does not result in an LOTC event. The repair rates, μ_i, for the ST and LT states are the reciprocals of the ST and LT repair times. For the ND states, the repair time is normally set to the reciprocal of ½ of the average flight time. This is because it is assumed that the system would enter an ND state approximately half-way through the flight. There are control systems that have single failures which result in an ND state, but do not necessarily lead to an LOTC event. Examples of these control systems are ones with only one P_B (i.e., burner pressure) or P_{amb} (i.e., ambient pressure) sensor. Loss of these sensors may not cause an LOTC event, but may result in an ND condition. However, in most systems ND states are usually not modeled in a single state Markov model because it would normally take two independent fault conditions to get into a non-dispatchable state (or configuration), and hence, a single state model would not, by definition, model these conditions.

7.2.2.4 Two Generalized Solution Equations for Single State Models

The general form of the solution for this model is given by Equation 19.

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} + \sum\{ (\lambda_i * (\lambda_{i\text{-}LOTC} + \lambda_{HM+UC}) / (\mu_i + \lambda_{i\text{-}LOTC} + \lambda_{HM+UC}) \}}{1.0 + \sum\{ \lambda_i / (\mu_i + \lambda_{i\text{-}LOTC} + \lambda_{HM+UC}) \}} \quad \text{(Eq. 19)}$$

where:

λ_{HM+UC} represents the hydromechanical plus uncovered fault rate.

λ_i represents the failure rate from the full-up state to a given fault state, and

$\lambda_{i\text{-}LOTC}$ is that failure rate from that given single fault state to the LOTC state, due to additional single faults in the redundant portions of the electronic control. (This failure rate does not include the single element hydromechanical and uncovered faults, as these faults are accounted in the λ_{HM+UC} term.)

μ_i is the repair rate for the fault state.

A slightly different nomenclature is often used. In this representation, the failure rate from the single failure states to the LOTC state, $\lambda_{i\text{-}LOTC}$, includes the additional λ_{HM+UC} failure rate term. That is,

$$\lambda_{i\text{-}LOTC+HM+UC} = \lambda_{i\text{-}LOTC} + \lambda_{HM+UC}$$

When this is done, Equation 19 takes the form:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} + \sum\{ (\lambda_i * \lambda_{i\text{-}LOTC+HM+UC}) / (\mu_i + \lambda_{i\text{-}LOTC+HM+UC}) \}}{1.0 + \sum\{ \lambda_i / (\mu_i + \lambda_{i\text{-}LOTC+HM+UC}) \}} \quad \text{(Eq. 20)}$$

Equation 20 and Equation 19 are exactly the same. They just use different nomenclature for the failure rates from the single failure states to the LOTC state.

7.2.2.5 First Order Approximation to the Single Fault Markov Model LOTC Equation (Equations 20)

A difficulty with Equations 19 and 20 is that when computing the LOTC rate using a spread sheet approach, which is done in the example FADEC system discussed in 7.4 and shown in Table 1, one has to continually re-do the summations shown in the numerator and denominator of those equations for each new value of μ_{LT} to obtain the data for plotting the LOTC rate as a function of the long time repair interval. This difficulty can be eliminated by approximating the summations $\sum\{ (\lambda_i * \lambda_{i\text{-}LOTC+HM+UC}) / (\mu_i + \lambda_{i\text{-}LOTC+HM+UC}) \}$ and $\sum\{ \lambda_i / (\mu_i + \lambda_{i\text{-}LOTC+HM+UC}) \}$ with simple, first order expansions.

First, replace the repair rate, μ_i, with the repair interval, T_i. Equation 20 then becomes:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} + \sum\{ (\lambda_i * \lambda_{i\text{-}LOTC+HM+UC} * T_i) / (1 + \lambda_{i\text{-}LOTC+HM+UC} * T_i) \}}{1.0 + \sum\{ \lambda_i / (1 + \lambda_{i\text{-}LOTC+HM+UC} * T_i) \}} \quad \text{(Eq. 20a)}$$

The first order approximations for the summations are:

$$\sum\{(\lambda_i \lambda_{i\text{-}LOTC+HM+UC} * T_i)/(1 + \lambda_{i\text{-}LOTC+HM+UC} * T_i)\} \approx \sum(\lambda_i * \lambda_{i\text{-}LOTC+HM+UC} * T_i) - \sum(\lambda_i * (\lambda_{i\text{-}LOTC+HM+UC} * T_i)^2)$$

$$\sum\{ \lambda_i / (1 + \lambda_{i\text{-}LOTC+HM+UC} * T_i) \} \approx \sum(\lambda_i * T_i) - \sum(\lambda_i * \lambda_{i\text{-}LOTC+HM+UC} * T_i^{\,2})$$

Substituting these approximations into Equation 20a yields the approximation:

$$\lambda_{LOTC} \approx \frac{\lambda_{HM+UC} + \sum(\lambda_i * \lambda_{i\text{-}LOTC+HM+UC} * T_i) - \sum(\lambda_i * (\lambda_{i\text{-}LOTC+HM+UC} * T_i)^2)}{1.0 + \sum(\lambda_i * T_i) - \sum(\lambda_i * \lambda_{i\text{-}LOTC+HM+UC} * T_i^2)} \quad \text{(Eq. 20b)}$$

Equation 20b may not look any simpler than Equation 20a, but when T_i is a fixed value for a group of faults, the summations for the "λ" terms for that group of faults only has to be done once. For example, if all single fault states are to be grouped into a short time or long time repair group with repair intervals of T_{ST} and T_{LT}, respectively, approximation 20b becomes:

$$\lambda_{LOTC} \approx \frac{\lambda_{HM+UC} + a_0 * T_{ST} - a_1 * T_{ST}^{\,2} + c_0 * T_{LT} - c1 * T_{LT}^{\,2}}{1.0 + b_0 * T_{ST} - b_1 * T_{ST}^{\,2} + d_0 * T_{LT} - d_1 * T_{LT}^{\,2}} \quad \text{(Eq. 20c)}$$

where:

$a_0 = \sum(\lambda_{STi} * \lambda_{STi\text{-}LOTC+HM+UC})$

$a_1 = \sum(\lambda_{STi} * (\lambda_{STi\text{-}LOTC+HM+UCi})^2)$

$b_0 = \sum(\lambda_{STi})$

$b_1 = a_0$

$c_0 = \sum(\lambda_{LTi} * \lambda_{LTi\text{-}LOTC+HM+UC})$

$c_1 = \sum(\lambda_{LTi} * (\lambda_{LTi\text{-}LOTC+HM+UC})^2)$

$d_0 = \sum(\lambda_{LTi})$

$d_1 = c_0$

These coefficients only have to be calculated once for the fault states in the ST and LT fault groups, and then the repair intervals, T_{ST} and T_{LT} can be varied to determine the effect on the LOTC rate.

7.2.2.6 Simplified Approximations When Using High Repair Rates (i.e., Short Repair Intervals)

In Equations 19 and 20, the $(\lambda_{i\text{-}LOTC} + \lambda_{HM+UC})$ and $\lambda_{i\text{-}LOTC+HM+UC}$ terms, which represent the same failure rates, are usually less than $50*10^{-06}$, and the repair rates, μ_i, are generally greater than 0.001 (i.e., repair times of less than 1000 hours in a time-since-fault-model). Therefore, the μ_i's are approximately 10 times greater than the $\lambda_{i\text{-}LOTC+HM+UC}$ failure rates. This being the case, Equations 19 and 20 can be simplified to:

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} + \sum\{ (\lambda_i * (\lambda_{i\text{-}LOTC} + \lambda_{HM+UC}) / \mu_i \}}{1.0 + \sum\{ \lambda_i / \mu_i \}} \quad \text{(Eq. 19a)}$$

and

$$\lambda_{LOTC} \approx \frac{\lambda_{HM+UC} + \sum (\lambda_i * \lambda_{i\text{-}LOTC+HM+UC} / \mu_i)}{1.0 + \sum(\lambda_i / \mu_i)} \quad \text{(Eq. 20d)}$$

Again, these two equations yield the same answer. The only difference in the equations is whether the HMU plus uncovered fault rate is included in the failure rates from the single faulty states to the LOTC state, as it is in Equations 20, 20a, 20b, etc., or whether the HMU plus uncovered failure rate is not included in the $\lambda_{i\text{-}LOTC}$ failure rate but handled separately, as is done in Equations 19 and 19a.

Since $(1/\mu_i)$ is simply the repair time for a particular fault repair interval, $T_{i\text{-}REPAIR}$, Equation 20d can be written as:

$$\lambda_{LOTC} \approx \frac{\lambda_{HM+UC} + \sum (T_{i\text{-}REPAIR} * \lambda_i * \lambda_{i\text{-}LOTC+HM+UC})}{1.0 + \sum(T_{i\text{-}REPAIR} * \lambda_i)} \quad \text{(Eq. 20e)}$$

When the dispatchable faults are allocated to two fault groups, a short time fault group with a repair time of T_{ST} and a long time fault group with repair time T_{LT}, Equation 20a can be written as:

$$\lambda_{LOTC} \approx \frac{\lambda_{HM+UC} + T_{ST} * \sum (\lambda_{STi} * \lambda_{STi\text{-}LOTC+HM+UC}) + T_{LT} * \sum (\lambda_{LTi} * \lambda_{LTi\text{-}LOTC+HM+UC})}{1.0 + T_{ST} * \sum(\lambda_{STi}) + T_{LT} * \sum(\lambda_{LTi})} \quad \text{(Eq. 20f)}$$

Generally, when the time-since-fault repair times are less than 1000 hours, Equation 20e (and Equation 20f when there are just two fault groups) yield reasonably good approximations for the estimated LOTC failure rate. If repair times of 1000 hours or more are to be considered, the analyst can revert to the use of Equation 20, 20a, or 20b. (NOTE: The 1000 hour long time repair time is not to be considered an absolute number. It's a relative number. As discussed in section 7.2.4, the repair rate, which is the reciprocal of the repair interval, has to be at least 10 times greater than the failure rates into and out of the various fault states for single state models to be reasonably accurate.)

7.2.3 Examples of Single Fault States

Examples of single failure states in an engine FADEC system are operation with one item, such as a T2, $P_{ambient}$ or other sensor failed; a fuel metering valve or variable geometry feedback failed; a CPU or power supply in one channel failed; or any other single failure being modeled.

7.2.4 Acceptability (and Accuracy) of Single State Models

In general, single fault state models are acceptable when the repair rate for the single fault states are approximately 10 times (or more) greater than the maximum failure rate into or out of those fault states. Most Markov models group the dispatchable faults conditions into either a short time (ST) or long time (LT) repair category. For these models to be reasonably accurate (i.e., approximately 5%), the repair rate for all ST fault states should be at least 10 times greater than the maximum failure rate into or out of any given ST fault state, and similarly, the repair rate for all LT fault states should be at least 10 times greater than the maximum failure rate into or out of any given LT fault state. Making the repair rates for the 1st fault states high translates into making multiple faults so improbable that they are negligible contributors to the shutdown rate. This is why high repair rates ensures that a "single state" model is reasonably accurate. See Appendix G for further discussion of this subject.

7.3 Comparison of TWA and MM Approaches

A comparison of the TWA and MM solutions for the example system given in 7.1.5 is shown in Figure 11.

The two TWA solutions shown in Figure 11 are the same as those shown in Figure 5. The MM results using Equations 20, 20c and 20f are also shown. Note that the TWA solution using the balanced fractional coefficients from this ARP (Equation 6) is virtually the same as the simplified (Equation 20f) Markov Model solution - and both the balanced fractional coefficient solution and the simplified MM solution from Equation 20e (i.e., Equation 20f for a system for two fault groups) are easier to calculate than the MM solution given by Equation 20, as the coefficients only have to be calculated once.

If one desires a very good match to the full Markov model solution given by Equation 20 - but without the need to re-do the spread sheet when the repair times are changed - the first order approximation given by Equation 20c should be used. The coefficients a_0, a_1, b_0, b_1, c_0, c_1, d_0, and d_1 used in the approximation, Equation 20c, only have to be calculated once, and there are only two more of these coefficients than in the simplified Equation 20f solution.

All of the solution methods provide acceptable accuracy. The preferred approach is to use the first order approximation given by Equation 20c. It provides an excellent approximation to the full Markov model solution equation with significantly less effort.

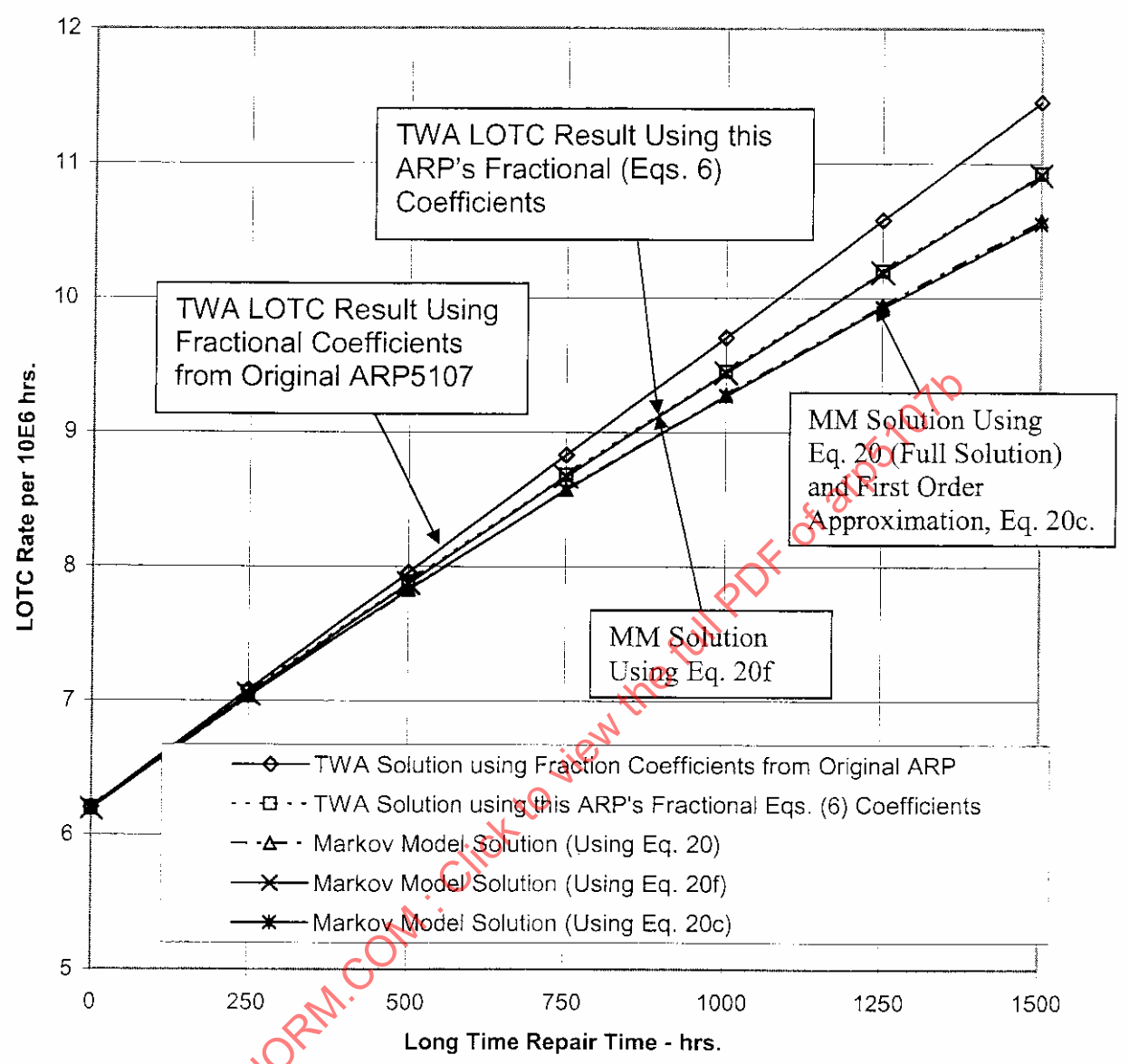

FIGURE 11 - COMPARISON OF TWA SOLUTIONS USING THE ORIGINAL ARP FRACTIONAL COEFFICIENTS AND THE BALANCED EQUATION 6 COEFFICIENTS OF THIS ARP WITH MARKOV MODEL SOLUTIONS USING EQUATIONS 20, 20C AND 20F (FROM THIS ARP) FOR THE FADEC SYSTEM DATA GIVEN IN 7.1.5

7.4 A Single State FADEC System MM Example

A single state MM for an example FADEC system is shown in Figure 12. In this system, the bleed valves account for much of the single element mechanical failure rate, and since they are all controlled separately by the electronics, they contribute a significant portion to the electrical/electronic system's failure rate. The ECU and alternator were put into the ST repair state because when either is failed, it takes away a significant amount of redundancy. All other items were placed into the LT category.

In this particular system, the N1 and N2 sensor systems are triple and quad redundant, respectively, and the control is not dispatchable without 2 of each of these signals present, so the impact on the LOTC rate from a complete loss of N1 or N2 is negligible.

7.4.1 Description of the Excel Spreadsheet Data

The following is an example of using a spread sheet to obtain the estimated LOTC rate for the FADEC system represented by the single state Markov model shown in Figure 12. The spread sheet solution uses Equation 20 to approximate the LOTC rate.

In referring to the Excel spread sheets shown in Table 1 below:

Column A is simply the row # (this has nothing to do with any of the calculation

Column B lists the fault states:

Column C is λ_i , the failure rate from the full-up state into that fault state

Column D is $\lambda_{i\text{-LOTC+HM+UC}}$, the failure rate from that state into the LOTC state. This rate includes the single element HMU and uncovered failure rate, as well as the additional (single) electrical/electronic failures in the redundant elements of the control that would take the system to the LOTC state (i.e., result in an LOTC event).

Column E is $\lambda_i/(\mu_i + \lambda_{i\text{-LOTC+HM+UC}})$, where μ_i is the appropriate repair rate (i.e., $1/T_{REPAIR}$) for that state

Column F is $(\lambda_{i\text{-LOTC+HM+UC}} * \lambda_I)/(\mu_i + \lambda_{i\text{-LOTC+HM+UC}})$, which is simply col. D times col. E.

The rate for the single mechanical/hydromechanical element failures and electrical/electronic failures that cause the system go directly from the full-up state (and any other fault state) to the LOTC state is 7.6 per million hours.

The short time repair interval used in the analysis is fixed at 250 hours. (This is because the applicant wishes to obtain an ST dispatch interval of 125 hours, and since the system being analyzed is for an "initial FADEC system application", the analysis is completed using a margin of 2, which is required by the current FAA TLD Policy Letter referred to in section 2.1.1 and attached herein as Appendix B).

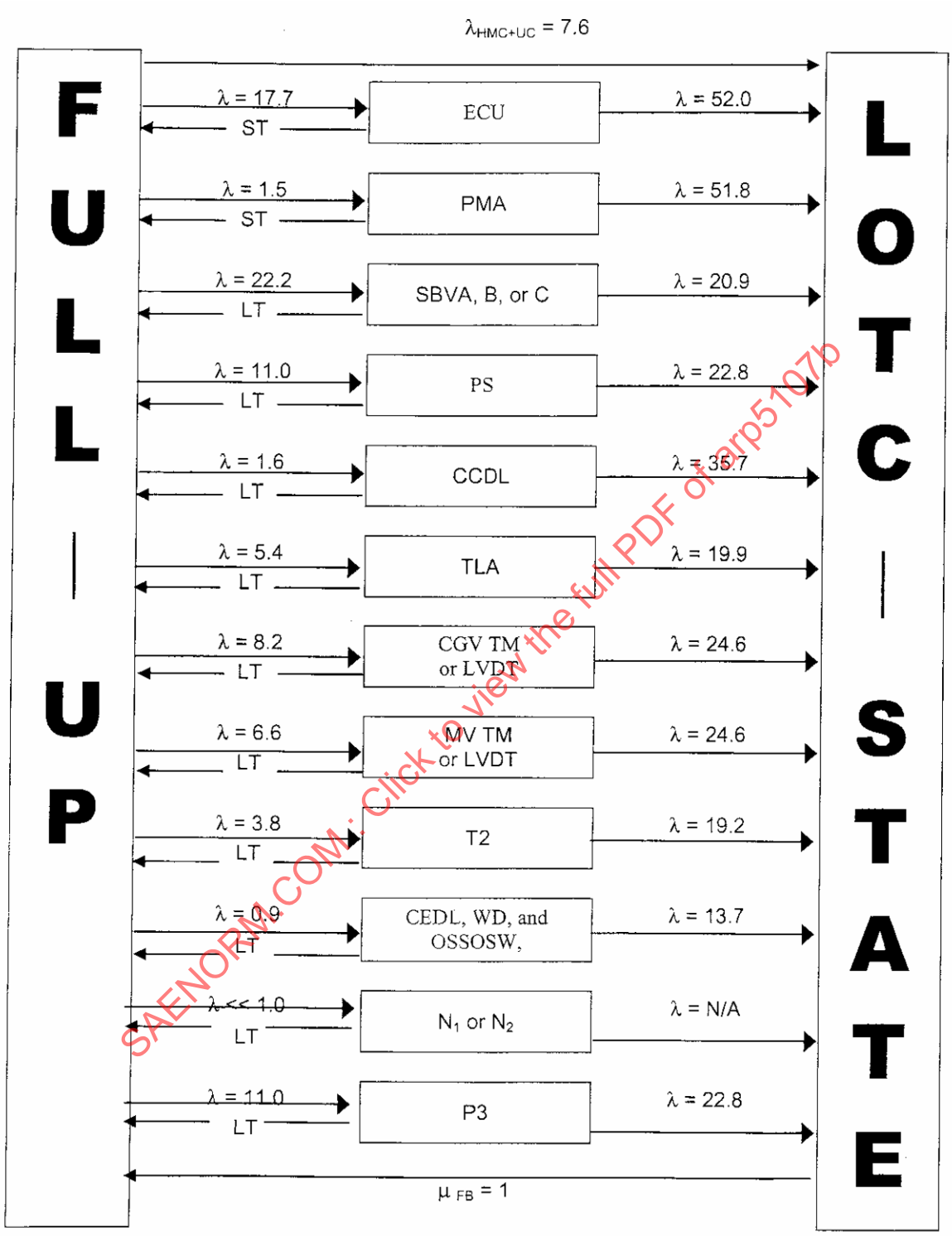

FIGURE 12 - MM DIAGRAM OF A TYPICAL FADEC SYSTEM
(NOTE: ALL λ'S ARE FAILURES PER MILLION HOURS)

$$\text{Column G, LOTC rate is} = \frac{[0.0000076 + \sum((\lambda_{i\text{-LOTC+HM+UC}} * \lambda_i)/(\mu_i + \lambda_{i\text{-LOTC+HM+UC}}))]}{1 + \sum(\lambda_i / (\mu_i + \lambda_{i\text{-LOTC+HM+UC}}))}$$

for example, G22 = [0.0000076 + F8 + F22] / [1. + E8 + E22]
and G37 = [0.0000076 + F8 + F37] / [1. + E8 + E37]
and G52 = [0.0000076 + F8 + F52] / [1. + E8 + E52]
and G67 = [0.0000076 + F8 + F67] / [1. + E8 + E67]
and G82 = [0.0000076 + F8 + F82] / [1. + E8 + E82]

The F8 and E8 terms always stay the same because those terms are for the short time repair faults and the time for those fault states is fixed at 250 hours.

TABLE 2 - SPREADSHEET SOLUTION FOR FADEC SYSTEM EXAMPLE SHOWN IN FIGURE 12

$T_{ST\text{-}Repair}$ = 250 hours (μ_{ST} = 0.004 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{ST} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{ST} + \lambda_{i\text{-}LOTC+HM+UC})$	
4	CPU (system)	1.77E-05	5.20E-05	4.37E-03	2.27E-07	
5	PMA	1.50E-06	5.18E-05	3.70E-04	1.92E-08	
6						
7				SUM	SUM	
8				4.74E-03	2.46E-07	

$T_{LT\text{-}Repair}$ = 1 hour (μ_{LT} = 1.0 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
11	SBV A,B,C	2.22E-05	2.09E-05	2.22E-05	4.64E-10	
12	PS	1.10E-05	2.28E-05	1.10E-05	2.51E-10	
13	CCDL	1.60E-06	3.57E-05	1.60E-06	5.71E-11	
14	TLA	5.40E-06	1.99E-05	5.40E-06	1.07E-10	
15	CGV	8.20E-06	2.46E-05	8.20E-06	2.02E-10	
16	MV	6.60E-06	2.46E-05	6.60E-06	1.62E-10	
17	T2	3.80E-06	1.92E-05	3.80E-06	7.30E-11	
18	4 SUMS	9.00E-07	1.37E-05	9.00E-07	1.23E-11	
19	P3	1.10E-05	2.28E-05	1.10E-05	2.51E-10	
20						
21				SUM	SUM	
22				7.07E-05	1.58E-09	7.81E-06

$T_{LT\text{-}Repair}$ = 1000 hours (μ_{LT} = 0.001 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
26	SBV A,B,C	2.22E-05	2.09E-05	2.17E-02	4.54E-07	
27	PS	1.10E-05	2.28E-05	1.08E-02	2.45E-07	
28	CCDL	1.60E-06	3.57E-05	1.54E-03	5.52E-08	
29	TLA	5.40E-06	1.99E-05	5.29E-03	1.05E-07	
30	CGV	8.20E-06	2.46E-05	8.00E-03	1.97E-07	
31	MV	6.60E-06	2.46E-05	6.44E-03	1.58E-07	
32	T2	3.80E-06	1.92E-05	3.73E-03	7.16E-08	
33	4 SUMS	9.00E-07	1.37E-05	8.88E-04	1.22E-08	
34	P3	1.10E-05	2.28E-05	1.08E-02	2.45E-07	
35						
36				SUM	SUM	
37				6.92E-02	1.54E-06	8.74E-06

$T_{LT\text{-}Repair}$ = 2000 hours (μ_{LT} = 0.0005 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
41	SBV A,B,C	2.22E-05	2.09E-05	4.26E-02	8.91E-07	
42	PS	1.10E-05	2.28E-05	2.10E-02	4.80E-07	
43	CCDL	1.60E-06	3.57E-05	2.99E-03	1.07E-07	
44	TLA	5.40E-06	1.99E-05	1.04E-02	2.07E-07	
45	CGV	8.20E-06	2.46E-05	1.56E-02	3.85E-07	
46	MV	6.60E-06	2.46E-05	1.26E-02	3.09E-07	
47	T2	3.80E-06	1.92E-05	7.32E-03	1.41E-07	
48	4 SUMS	9.00E-07	1.37E-05	1.75E-03	2.40E-08	
49	P3	1.10E-05	2.28E-05	2.10E-02	4.80E-07	
50						
51				SUM	SUM	
52				1.35E-01	3.02E-06	9.53E-06

$T_{LT\text{-}Repair}$ = 3000 hours (μ_{LT} = 0.000333 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
56	SBV A,B,C	2.22E-05	2.09E-05	6.27E-02	1.31E-06	
57	PS	1.10E-05	2.28E-05	3.09E-02	7.04E-07	
58	CCDL	1.60E-06	3.57E-05	4.34E-03	1.55E-07	
59	TLA	5.40E-06	1.99E-05	1.53E-02	3.04E-07	
60	CGV	8.20E-06	2.46E-05	2.29E-02	5.64E-07	
61	MV	6.60E-06	2.46E-05	1.84E-02	4.54E-07	
62	T2	3.80E-06	1.92E-05	1.08E-02	2.07E-07	
63	4 SUMS	9.00E-07	1.37E-05	2.59E-03	3.55E-08	
64	P3	1.10E-05	2.28E-05	3.09E-02	7.04E-07	
65						
66				SUM	SUM	
67				1.99E-01	4.44E-06	1.021E-05

$T_{LT\text{-}Repair}$ = 4000 hours (μ_{LT} = 0.00025 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
71	SBV A,B,C	2.22E-05	2.09E-05	8.19E-02	1.71E-06	
72	PS	1.10E-05	2.28E-05	4.03E-02	9.19E-07	
73	CCDL	1.60E-06	3.57E-05	5.60E-03	2.00E-07	
74	TLA	5.40E-06	1.99E-05	2.00E-02	3.98E-07	
75	CGV	8.20E-06	2.46E-05	2.99E-02	7.35E-07	
76	MV	6.60E-06	2.46E-05	2.40E-02	5.91E-07	
77	T2	3.80E-06	1.92E-05	1.41E-02	2.71E-07	
78	4 SUMS	9.00E-07	1.37E-05	3.41E-03	4.68E-08	
79	P3	1.10E-05	2.28E-05	4.03E-02	9.19E-07	
80						
81				SUM	SUM	
82				2.60E-01	5.79E-06	1.079E-05

$T_{LT\text{-}Repair}$ = 5000 hours (μ_{LT} = 0.0002 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
86	SBV A,B,C	2.22E-05	2.09E-05	1.00E-01	2.10E-06	
87	PS	1.10E-05	2.28E-05	4.94E-02	1.13E-06	
88	CCDL	1.60E-06	3.57E-05	6.79E-03	2.42E-07	
89	TLA	5.40E-06	1.99E-05	2.46E-02	4.89E-07	
90	CGV	8.20E-06	2.46E-05	3.65E-02	8.98E-07	
91	MV	6.60E-06	2.46E-05	2.94E-02	7.23E-07	
92	T2	3.80E-06	1.92E-05	1.73E-02	3.33E-07	
93	4 SUMS	9.00E-07	1.37E-05	4.21E-03	5.77E-08	
94	P3	1.10E-05	2.28E-05	4.94E-02	1.13E-06	
95						
96				SUM	SUM	
97				3.18E-01	7.09E-06	1.130E-05

$T_{LT\text{-}Repair}$ = 6000 hours (μ_{LT} = 0.0001667 events/hour)

A	B	C	D	E	F	G
		λ_i	$\lambda_{i\text{-}LOTC+HM+UC}$	$\lambda_i / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	$(\lambda_{i\text{-}LOTC+HM+UC} * \lambda_I) / (\mu_{LT} + \lambda_{i\text{-}LOTC+HM+UC})$	λ_{LOTC}
101	SBV A,B,C	2.22E-05	2.09E-05	1.18E-01	2.47E-06	
102	PS	1.10E-05	2.28E-05	5.81E-02	1.32E-06	
103	CCDL	1.60E-06	3.57E-05	7.91E-03	2.82E-07	
104	TLA	5.40E-06	1.99E-05	2.89E-02	5.76E-07	
105	CGV	8.20E-06	2.46E-05	4.29E-02	1.05E-06	
106	MV	6.60E-06	2.46E-05	3.45E-02	8.49E-07	
107	T2	3.80E-06	1.92E-05	2.04E-02	3.93E-07	
108	4 SUMS	9.00E-07	1.37E-05	4.99E-03	6.84E-08	
109	P3	1.10E-05	2.28E-05	5.81E-02	1.32E-06	
110						
111				SUM	SUM	
112				3.74E-01	8.34E-06	1.174E-05

Figure 13 shows a plot of the Table 1 data for the LOTC rate as a function of the time-since-fault, repair time for long time faults, T_{LT}. The short time repair interval in this analysis is fixed at 250 hours. This 250 hour repair time is also a time-since-fault repair time.

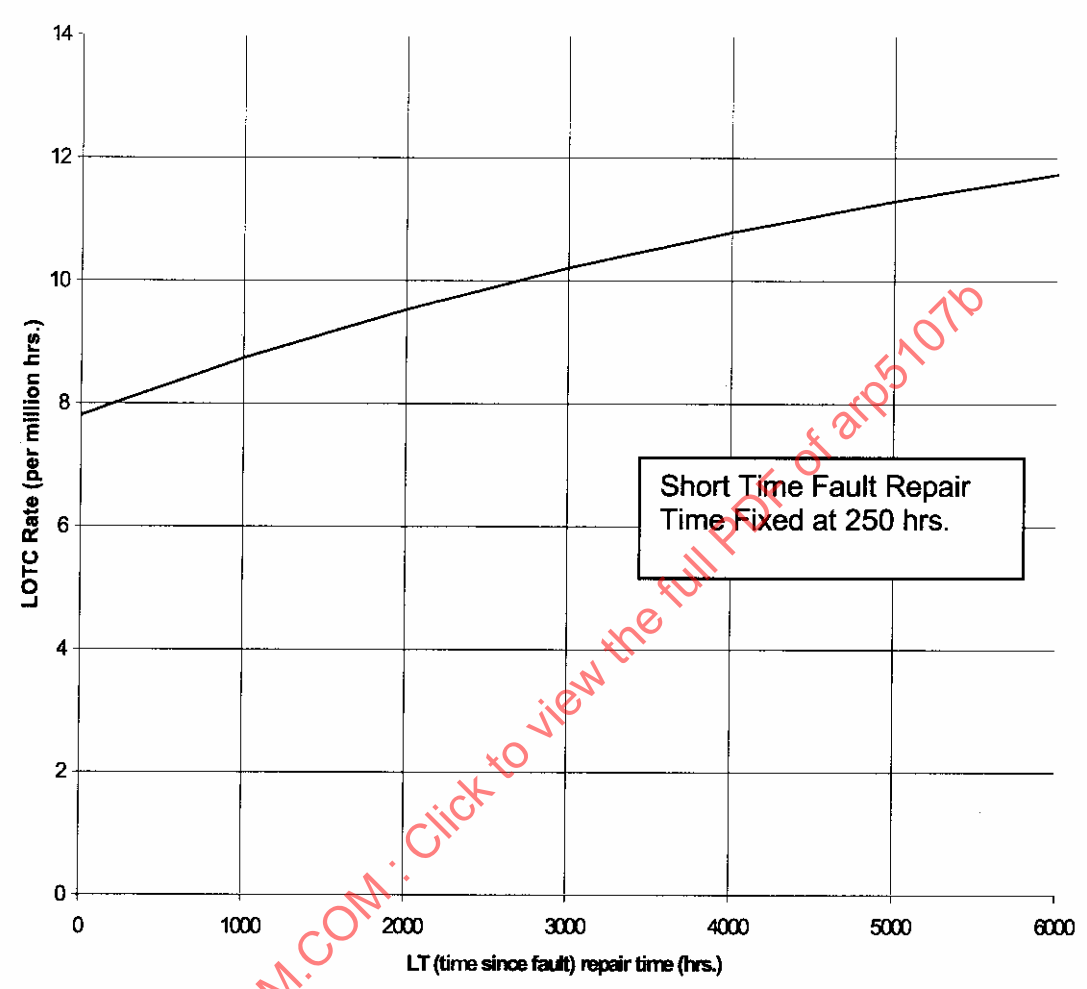

FIGURE 13 - LOTC RATE (TABLE 1 DATA USING EQUATION 20) AS A FUNCTION OF THE LT FAULT REPAIR TIME FOR SIMPLE FADEC SYSTEM EXAMPLE OF FIGURE 12

The 10 per million LOTC rate (for engines installed on transport category aircraft) is achieved by repairing ST fault within 250 hours of their occurrence and LT faults within approximately 2700 hours of their occurrence. If this is an initial application of a FADEC system, the FAA's policy letter for LOTC analyses requires a 2:1 margin in the repair times simulation, with a maximum time-since-fault repair time of 125 hours for ST faults and 250 hours for LT faults. Thus, if this were an in initial FADEC system application, those would be the maximum allowed limits, even though the analysis shows that a longer than 250 hour LT repair time would yield an LOTC rate less than 10 per million hours.

Figure 13A shows a comparison of the LOTC solution results (Table 1) for the Figure 12 Markov model using the complete single state Markov model equation (Equation 20) along with the first order approximation Equation 20c and the simplified solution equation given by Equation 20f.

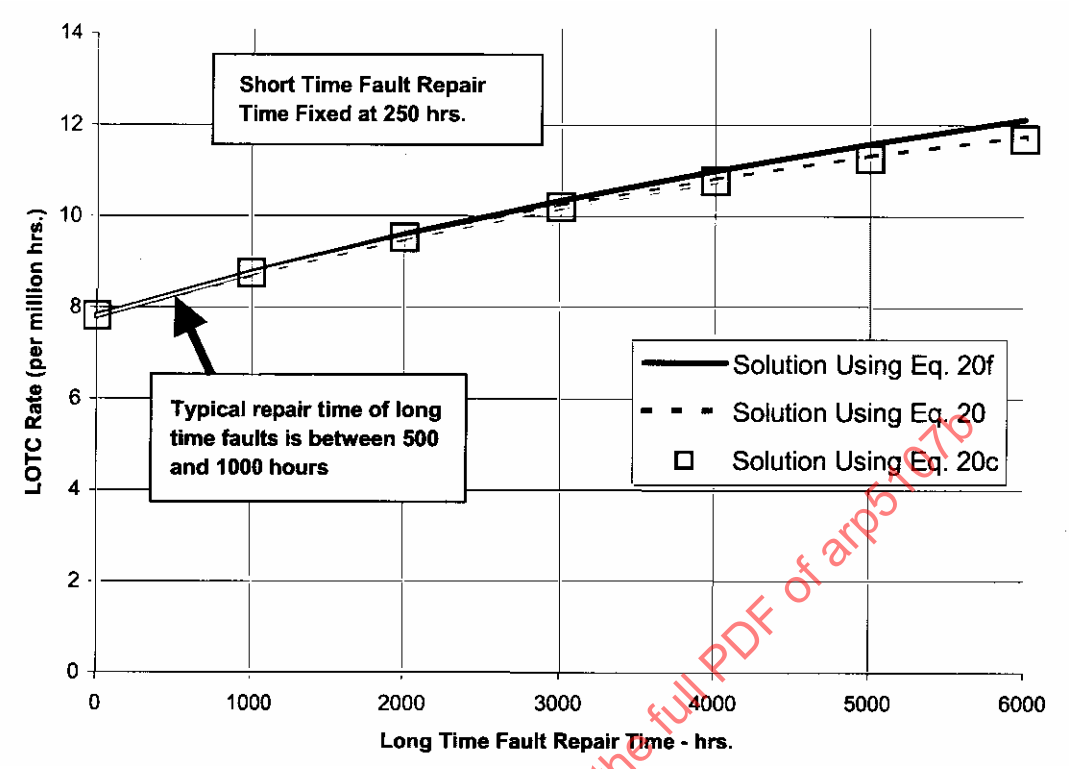

FIGURE 13A - COMPARISON OF FIGURE 12 MARKOV MODEL LOTC CALCULATIONS USING EQUATIONS 20, 20C AND 20F

Table 2 shows a spread sheet of the calculations involved in determining the coefficients; a_0, a_1, b_0, b_1, c_0, c_1, d_0, and d_1, which are used in Equation 20c. Note how easy it is to calculate the coefficients, and the coefficients only have to be calculated once for the ST and LT fault states. This is much easier than doing the spread sheet layout of Table 1, and the first order approximation provided by Equation 20c is in excellent agreement with the more complex solution given by Equation 20 (and Table 1).

TABLE 3 - SPREAD SHEET SHOWING THE CALCULATIONS FOR DETERMINING THE COEFFICIENTS a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1 USED IN EQUATION 20C

	λ_{STi}	$\lambda_{STi\text{-}LOTC}$	$\lambda_{STi} * \lambda_{STi\text{-}LOTC}$	$\lambda_{STi} * \lambda_{STi\text{-}LOTC}^2$
ECU	1.77E-05	5.20E-05	9.20E-10	4.79E-14
PMA	1.50E-06	5.18E-05	7.77E-11	4.02E-15
	SUM		SUM	SUM
	b0 =		a0 = b1 =	a1 =
	1.92E-05		9.98E-10	5.19E-14
	λ_{LTi}	$\lambda_{LTi\text{-}LOTC}$	$\lambda_{LTi} * \lambda_{LTi\text{-}LOTC}$	$\lambda_{LTi} * \lambda_{LTi\text{-}LOTC}^2$
SBVA,B,C	2.22E-05	2.09E-05	4.64E-10	9.70E-15
PS	1.10E-05	2.28E-05	2.51E-10	5.72E-15
CCDL	1.60E-06	3.57E-05	5.71E-11	2.04E-15
TLA	5.40E-06	1.99E-05	1.07E-10	2.14E-15
CGV	8.20E-06	2.46E-05	2.02E-10	4.96E-15
MV	6.60E-06	2.46E-05	1.62E-10	3.99E-15
T2	3.80E-06	1.92E-05	7.30E-11	1.40E-15
4 SUMS	9.00E-07	1.37E-05	1.23E-11	1.69E-16
P3	1.10E-05	2.28E-05	2.51E-10	5.72E-15
	SUM		SUM	SUM
	d0 =		c0 = d1 =	c1 =
	7.07E-05		1.58E-09	3.58E-14

When the repair rates are high with respect to the failure rates into and out of the single fault states, the use of Equation 20f is certainly adequate.

High repair rates mean short repair times. Equation 20f is much simpler to use than Equation 20 because it only requires a one time calculation of the terms:

$\Sigma(\lambda_{STi})$, $\Sigma(\lambda_{LTi})$, $\Sigma(\lambda_{STi} * \lambda_{STi\text{-}LOTC+HM+UC})$, and $\Sigma(\lambda_{LTi} * \lambda_{LTi\text{-}LOTC+HM+UC})$.

The use of Equation 20c only requires two more terms to be calculated in addition to the above. They are:

$\Sigma(\lambda_{STi} * (\lambda_{STi\text{-}LOTC+HM+UC})^2)$, and $\Sigma(\lambda_{LTi} * (\lambda_{LTi\text{-}LOTC+HM+UC})^2)$.

When the repair times are relatively short, such that the repair rates (i.e., the reciprocal of the repair times) are approximately 10 time or more greater than the failure rates into and out of the various fault states, the use of Equation 20f should be adequate. From its ease of use and accuracy, Equation 20c is preferred.

7.4.2 Validity of the Calculated Data

As discussed in 7.2.4, single state Markov models are representative of a system when the repair rates for the states are frequent with respect to the failure rates into and out of the states. Having a frequent repair rate simply reduces the probability of having a second ST or LT fault occur during the time period that a ST or LT fault is allowed to exist. It is suggested that the repair time be at least 10 times greater than the highest of the failure rates into or out of all states in a given (i.e., ST or LT) group.

In the above example, the highest failure rate in the ST fault group is the failure rate out of the CPU (system) fault state, which is 52.0 * 10^{-6} failures per hour. The repair rate for all ST states – there are only two ST fault states in the example model – is 0.004 units per hour. This repair rate is 77 times greater than the highest failure rate of 52 per million hours, and therefore, the model is accurate with regard to using a single state model for ST faults.

The highest failure rate for LT faults is the failure rate out of the CCDL fault state, which is 35.7*10^{-06} failures per hour. Using this number, the repair rate for all LT faults states should be no less than 357.*10-6 units per hour. This equates to a repair interval, which is the reciprocal of repair rate, of 2800 hours. Hence, the data shown in Figure 13 for the LOTC rate of the system is increasingly inaccurate for LT repair times greater 2800 hours. In this particular model, the highest failure rate of 35.7 per million hours is a bit less important because the failure rate into the CCDL state is only 1.6 per million hours, and therefore, this state does not contribute significantly to the LOTC rate and it is unlikely to have this failure coupled with another LT fault in the 2800 hour period. The next highest failure rate is 24.6 failures per million hours and occurs from both the “CGV TM or LVDT” and “MV TM or LVDT” states. Multiplying this by 10 and taking the reciprocal yields a maximum repair time of 4064 hours. The model is reasonably accurate up to this time period.

In summary, although data is calculated and shown in Figure 13 for LT repair times up to 6000 hours, the data beyond 4000 hours is increasingly inaccurate in this particular single state model. Most FADEC system LT repair times are 1000 hours or less, and for these shorter repair times, a single state MM is usually quite adequate.

7.5 Second Example: A Single and Dual State Model of a FADEC System

A major engine manufacturer provided this second example. Without showing all of the failure rates and the particular failure states, Figure 14 shows a second example of a single state Markov model of a typical FADEC system. State #1 is the full-up state, states 2 through 24 are the single failure states, and state 300 is the LOTC state. Dual failure states, which are combinations of the single states, were added to the model, as shown in Figure 15. The dual states are numbered from 30 to 209, so there are 180 dual states represented. In both models, there are only three short time (ST) states. They are states numbered 2, 3, and 4. Using a fixed ST repair interval of 250 hours for these three states, the LOTC rates for both the single and dual state models are shown in Figure 16 as a function of the LT fault repair time. Note that at an LT repair time of 2000 hours, which is a long LT repair time, the single and dual state models only differ by about 3%, and at an LT repair time of 1000 hours, the two differ by less than 1%. This is an example which shows how small the contribution of the dual states is to the estimated LOTC rate.

7.6 Discussion of Markov Model and TWA Approaches, and the Use of Fault Trees for Determining LOTC Rates When Operating With Faults

As stated above, in comparing the MM approach with the TWA approach, the MM approach has the advantage of being able to balance the various states of a redundant system slightly better than the TWA approach. The use of Equation 20c allows an accurate MM result to be determined in a simple manner (i.e., the coefficients only have to be calculated once. See Table 2). Using the definitions for the fractional coefficients given by Equations 6 in this revised ARP significantly improves the “balancing” of the TWA approach. The TWA approach, with either the original fraction coefficients or the new defined ones, yields a conservative answer for the LOTC rate and is an acceptable method for completing the LOTC TLD analysis.

The use of fault trees to calculate the average failure rates of the system when operating with faults is quite acceptable, but the fault tree of the system needs to be completed with considerable care. Markov models tend to be a functional representation of the system. Fault trees tend to be more of a hardware representation of the system. For example, assume that one channel is operating with one thrust level angle (TLA) signal failed. Whether control remains in that channel or not, the only next failures that would cause the system to go to the LOTC state is the loss of the other channels CPU, power supply, or remaining TRA signal. (If control remains in the channel with the failed TLA signal and the cross-talk bus, which contains the remaining TLA signal, fails, the control can simply revert to the good TLA signal channel.) There have been examples of very complex fault tree models which calculated a very incorrect failure rate for this simple situation. Hence, if fault trees are used to calculate the failure rates of the system when operating with faults, do simple reasonableness checks on the results to see if they agree with what is logical. This is reasonable easy to do in a single state model.

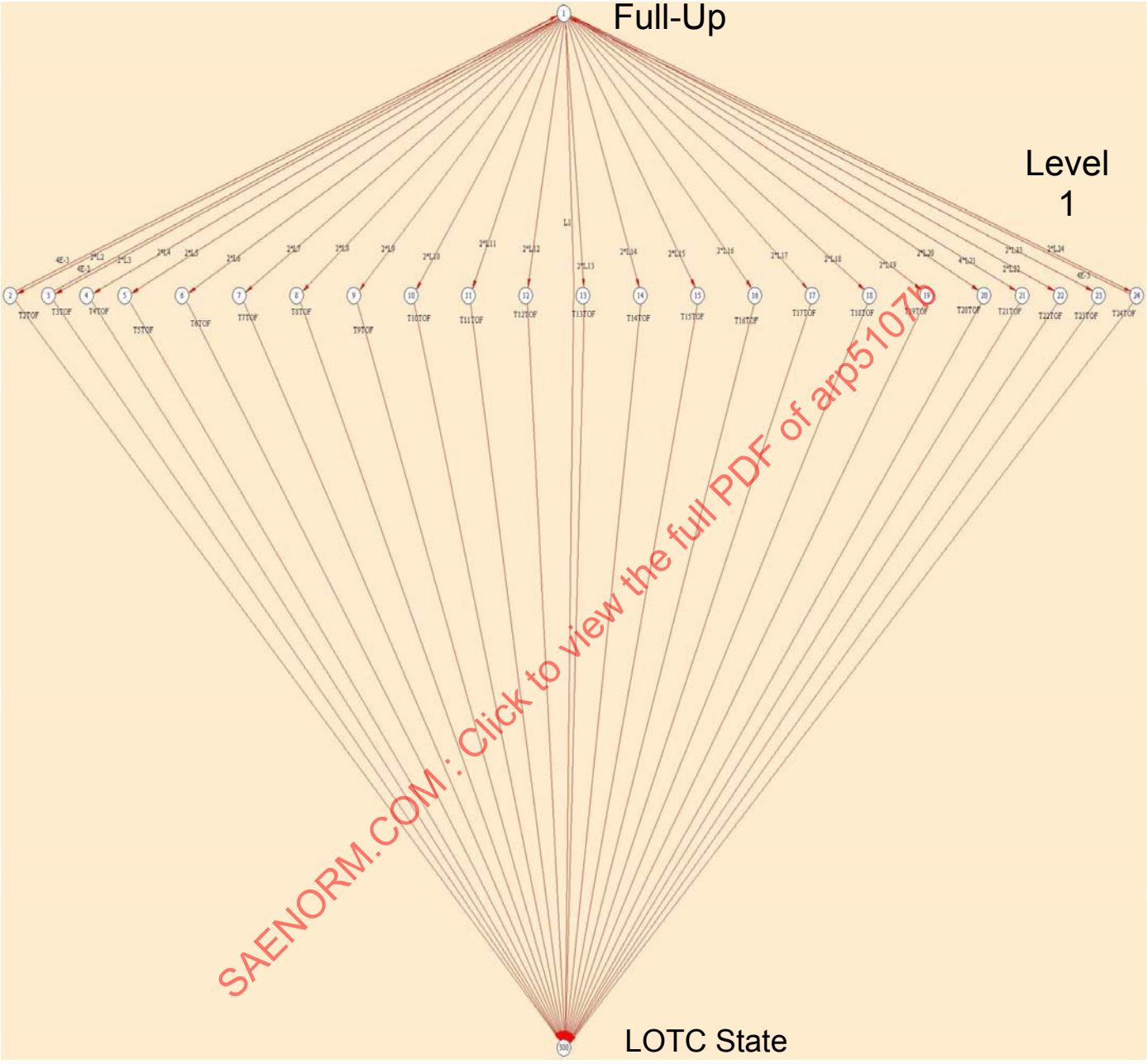

FIGURE 14 - SECOND EXAMPLE OF SINGLE STATE MARKOV MODEL OF A TYPICAL FADEC SYSTEM, WITH 23 SINGLE FAULT STATES

Cross-channel resource-sharing

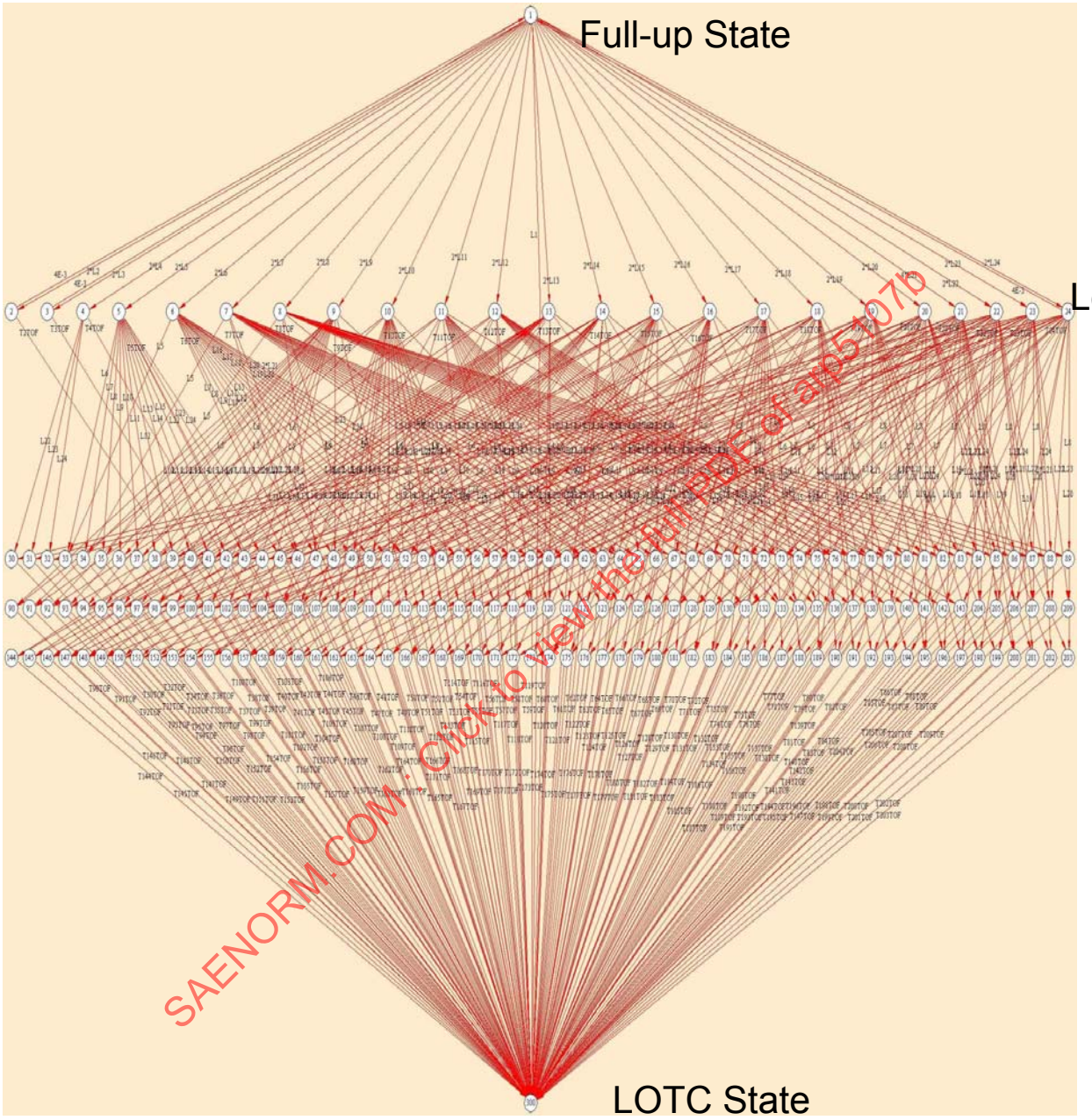

FIGURE 15 - FIGURE 14 MODEL WITH 180 DUAL STATES ADDED

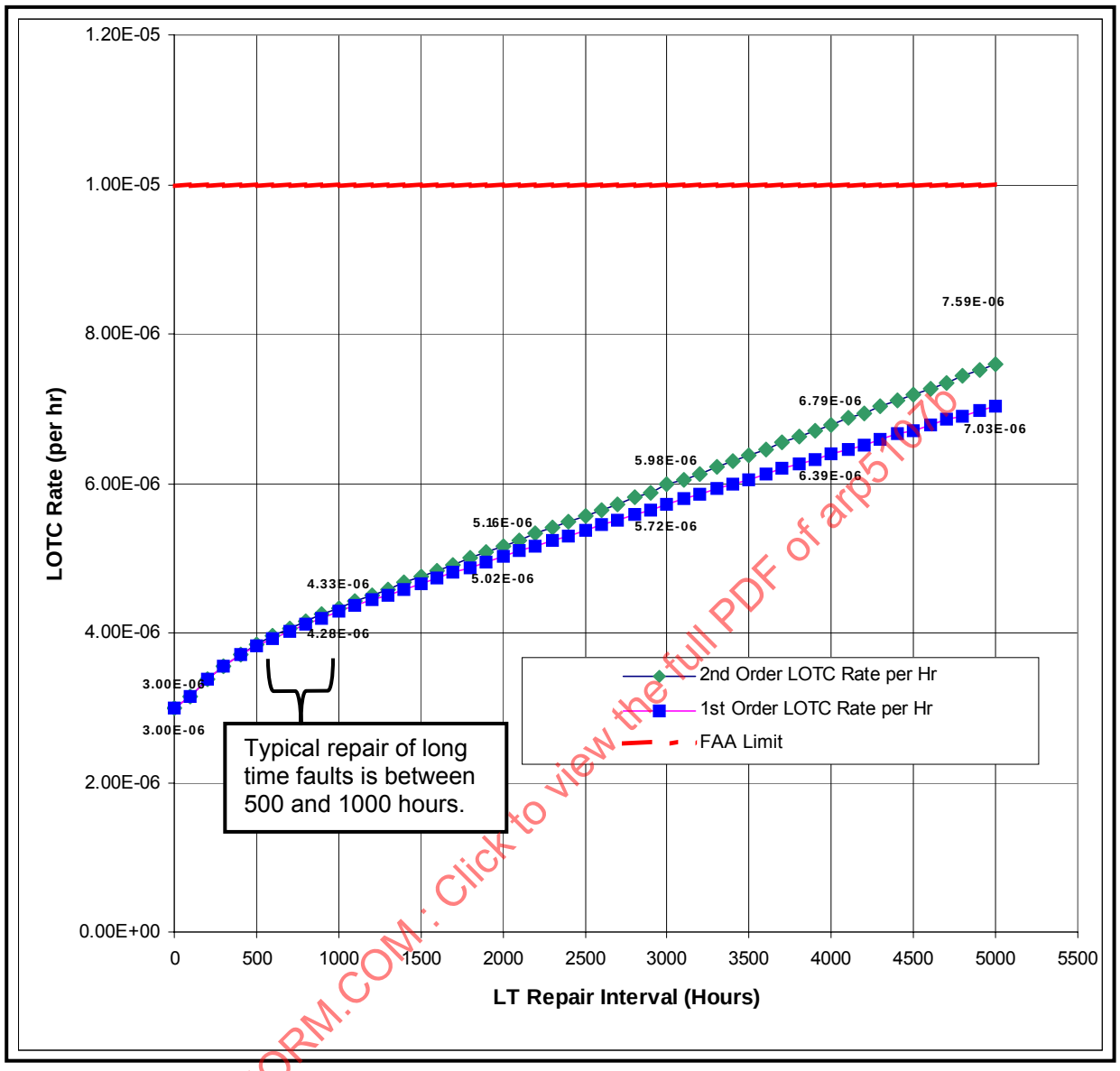

FIGURE 16 - LOTC RATES AS A FUNCTION OF LT REPAIR TIME FOR BOTH THE SINGLE AND DUAL STATE MODELS OF FIGURES 14 AND 15

7.7 Time-Since-Fault (i.e., On-Condition) Repair Versus Periodic Inspection and Repair

In all of the above discussion, the repair intervals for ST and LT faults are based on time-since-fault repair. (This is also referred to as 'On Condition' repair. The two nomenclatures are herein considered synonymous.) In this repair scenario, a 'clock' is started when the fault occurs, and after a certain number of hours have elapsed - like 100 hours for ST faults - the fault is repaired. This repair strategy can be employed when airline operator maintenance is immediately notified or aware of the occurrence of a fault. This works reasonably well for ST faults, because there is (generally) an aircraft 'flight deck indication' presented to the flight crew of an ST fault condition, and maintenance can 'start the clock' and track the fault to see that it is repaired within the required period. LT faults, however, are generally handled in a different manner. Most airline operators do not wish to have a 'flight deck indication' for something that is allowed to be in existence for 500 hours or more. Hence, LT faults are generally handled via an "inspection and repair" activity. This activity involves a periodic inspection of the FADEC system for LT type faults, and if LT faults are found, they must be repaired.

If an inspection and repair activity is used to implement fault maintenance, the inspection/repair interval should not be greater than twice the on-condition, time-since-fault time limit. This is because the fault could have occurred at any time during the interval, and "on average" the fault will have occurred half way through the interval. Hence, the fault has been "On Condition" for approximately 1/2 the interval. This is true when the inspection interval is short with respect to the mean-time-between-failure (MTBF) of the sum of the items in the fault group.

The following presents a derivation for determining the periodic inspection interval time as a function of the time-since-fault repair time and the MTBF of the sum of the items grouped in the LT repair category.

The average time-since-fault, T_{TSF}, that a fault has been present (if found at inspection) is given by the following expression:

$$T_{TSF} \quad T_{Inspect} \quad T_{Mean\ LT} \tag{Eq. 21}$$

where:

TInspect is the length of time between periodic inspections in hours.

TMean-LT is the mean time in hours (from the start of the interval) where a LT fault is expected to occur.

$T_{Mean\text{-}LT}$ is evaluated as:

$$T_{MEAN\text{-}LT} = \frac{\int (t * e^{-\lambda(LTT)*t})\, dt}{\int (e^{-\lambda(LTT)*t})\, dt} \tag{Eq. 22}$$

The integrations are from t=0 to $T_{Inspect}$, and again, the term, λ(LTT) represents the total sum of all long term (i.e., LT) faults in both channels.

Completing the Equation 22 integration, substituting the result for $T_{Mean\text{-}LT}$ into Equation 21, and simplifying yields:

$$\frac{T_{TSF}}{Tinspect} = \frac{1 - (1 - e^{-R})/R}{1 - e^{-R}} \tag{Eq. 23}$$

where:

$R = T_{Inspect}/T_{MTBF(LTT)}$

$T_{MTBF(LT)} = 1/(\lambda_{LTT})$

This can be solved iteratively to obtain values for $(T_{Inspect}/T_{TSF})$ as a function of $(T_{TSF}/T_{MTBF(LT)})$. The results are shown in Figure 17. Note from this figure that if the value for the time-since-fault repair time is greater than approximately one-tenth the MTBF of the LT fault group (i.e., values greater than 0.1 on the “x” axis in Figure 17), the approximation of having the periodic inspection interval time be twice the time-since-fault repair time becomes increasingly inaccurate.

As shown in the derivation given in Figure 18, for $(T_{Inspect}/T_{MTBF})$ less than 2.0, a good approximation to Equation 23 is:

$$\frac{T_{TSF}}{T_{Inspect}} \quad 1/2 \quad (1/12) * (T_{Inspect} / T_{MTBF(LT)}) \tag{Eq. 24}$$

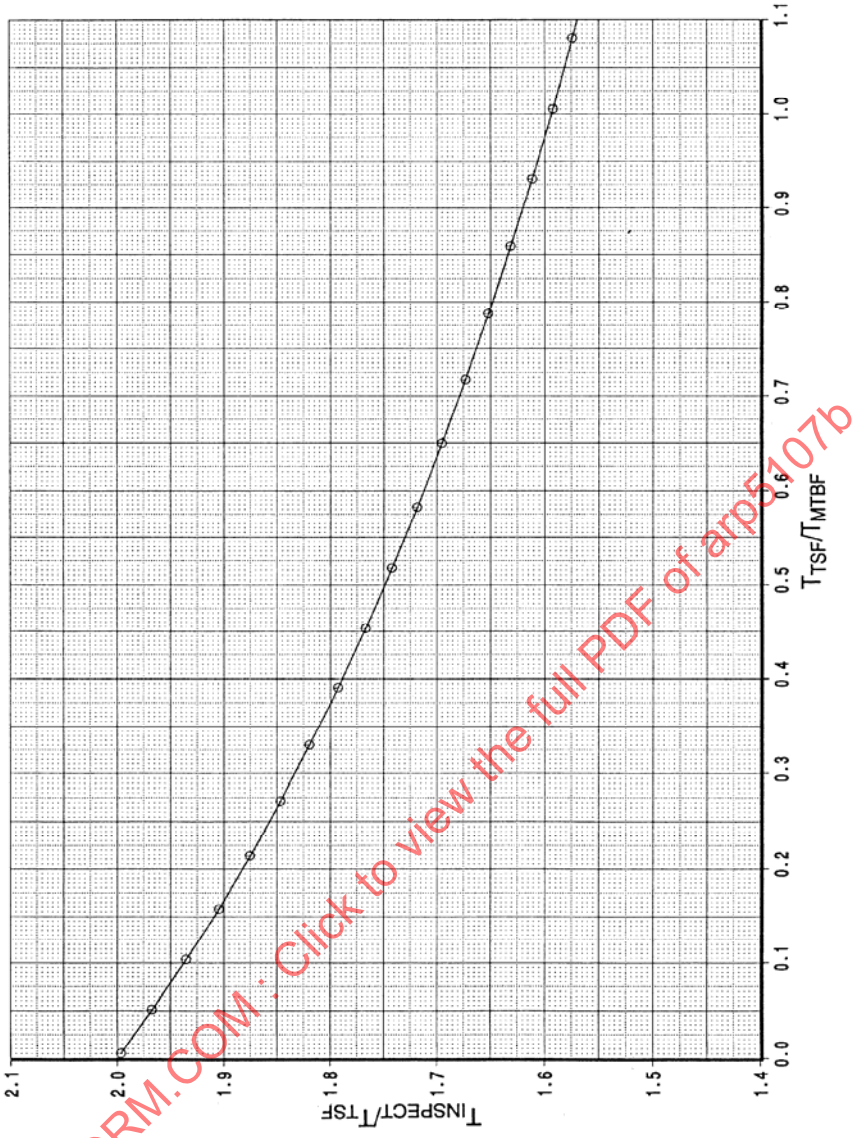

FIGURE 17 - ($T_{INSPECT}/T_{TSF}$) VERSUS ($T_{TSF}/T_{MTBF(LT)}$)

Using the Maclaurin series expansion for e^{-R} of

$e^{-R} = 1 - R + R^2/2! - R^3/3! + R^4/4! + ...$

$$\frac{R-(1-e^{-R})}{R(1-e^{-R})} \approx \frac{R^2/2! - R^3/3! + R^4/4! + ...}{R(R - R^2/2! + R^3/3! - R^4/4! + ...)}$$

Dividing through by R^2 simplifies this to:

$$\frac{R-(1-e^{-R})}{R(1-e^{-R})} \approx \frac{1/2! - R/3! + R^2/4! + ...}{1 - R/2! + R^2/3! - R^3/4! + ...}$$

Dividing the right-hand side numerator by the denominator yields

$$\frac{R-(1-e^{-R})}{R(1-e^{-R})} \approx 1/2 + R/12 - R^3/720 + R^5/30240 - R^7/1209600 + ...$$

For R less than approximately 2.0, the above is simplified to

$$\frac{R-(1-e^{-R})}{R(1-e^{-R})} \approx 1/2 + R/12$$

Inserting this approximation into Equation 23 yields

$$\frac{T_{TSF}}{T_{Inspect}} \approx 1/2 + T_{Inspect}/(12 * T_{MTBF(LT)})$$

This is Equation 24.

FIGURE 18 - DERIVATION OF APPROXIMATION GIVEN IN EQUATION 24

Solving Equation 28 for $T_{Inspect}$ as a function of T_{TSF} and $T_{MTBF(LTT)}$ yields:

$$\frac{T_{Inspect}}{T_{MTBF(LT)}} \quad 3 * \{ \ 1 \quad [1 \quad (4/3) * (T_{TSF}/T_{MTBF})]^{0.5}\} \qquad \text{(Eq. 25)}$$

As in the above examples, most reliability tools are constructed to analyze systems with faults being repaired on a time-since-fault basis. Hence, having determined T_{TSF} from the analysis, the inspection interval corresponding to that T_{TSF} is determined from Figure 15 (or if applicable Equation 25).

For example, if there are 10 faults in the long term (LT) category and the failure rate for each is 20 x 10^{-6} failures/hour, the total LT failure rate would be 200 x 10^{-6} failures/hour, and the T_{MTBF} for the group would be 5000 hours. If a reliability analysis yields the result that the maximum on-condition operational time for an LT should be limited to 3000 hours, Equation 29 can be used to calculate a corresponding inspection interval of 5125 hours - which is significantly less than twice the “on condition” repair interval of 3000 hours. In this case, the time-since-fault or "on condition" length of time that an LT fault is allowed to exist (before requiring repair) is long in comparison to the expected time, $T_{MTBF(LT)}$, of a LT fault; and therefore, the approximation of using twice the calculated T_{TSF} interval as the periodic inspection interval would not be a good one (see Figure 15).

8. CALCULATION APPROACHES: DUAL ENGINE ANALYSIS

8.1 Time-Averaging Approach

The dual engined LOTC rate analysis is not significantly different than the single engine analysis. The "average" dual LOTC rate is given as:

$$\lambda_{DUAL\text{-}ENG\text{-}LOTC\text{-}AVE} = \frac{2*T_{DIV}*(T_{FL}-T_{DIV})*(\lambda_{LOTC\text{-}AVE})^2}{T_{FL}} \quad \text{(Eq. 26)}$$

where:

T_{FL} is the flight length
T_{DIV} is the diversion time on one engine

For the equation to be valid, (T_{DIV}/T_{FL}) must be less than 0.5

(A derivation of Equation 26 is given in Appendix E.)

Using an average λ_{LOTC} of 10^{-5} per hour, T_{FL} as 4.5 hours, and T_{DIV} as 1 hour, the dual engine LOTC rate is calculated as:

$$\lambda_{DUAL\text{-}ENG\text{-}LOTC\text{-}AVE} = \{2*1*(4.5-1)*(10^{-5})^2\}/4.5 \quad \text{(Eq. 27)}$$
$$= 0.155*10^{-9} \text{ events per flight hour}$$

The reason that the result is small is that the twin-engined aircraft does not proceed to destination after the first engine failure. It diverts to the nearest suitable airport. Hence, the exposure time for the second engine failure is limited. If an extended operations (ETOPS) scenario is simulated, T_{FL} could be up to 16 hours and T_{DIV} is approximately 3 hours.

In this case:

$$\lambda_{DUAL\text{-}ENG\text{-}LOTC\text{-}AVE} = \{2*3*(16-3)*(10^{-5})^2\}/16$$
$$= 0.488*10^{-9} \text{ events per flight hour}$$

Hence, using an average engine control system failure rate of $10*10^{-06}$ is consistent with meeting the FAR/CS 25.1309 requirement for meeting a 10^{-9} per hour failure rate for a dual engine failure event (caused by control system failures).

8.2 Maximum Specific Risk Failure Rates as a Function of Dispatch Configuration

The probability of a dual engine LOTC event during any given flight is generally termed "the specific risk" of that flight. Since the FADEC control systems for each engine are independent of each other, the specific risks for a twin-engined aircraft are calculated from:

$$\lambda_{DUAL\text{-}ENG\text{-}LOTC\text{-}AVE} = \frac{2*T_{DIV}*(T_{FL}-T_{DIV})*\lambda_{SPEC.\text{-}LOTC\text{-}ENG\#1}*\lambda_{SPEC.\text{-}LOTC\text{-}ENG\#2}}{T_{FL}} \quad \text{(Eq. 28)}$$

Using a full-up to LOTC fault rate of $6*10^{-06}$ for the mechanical/hydromechanical elements plus the uncovered faults, and the maximum allowed ST- and LT-to-LOTC rates of $100*10^{-06}$ and $75*10^{-06}$ respectively (these values include the hydromechanical and uncovered faults), the specific "worse case" dual engine LOTC rates for the various dispatch states for a flight of 4.5 hours with a 1 hour diversion are shown in Table 3.

TABLE 4 - DUAL ENGINE SPECIFIC RISK AS A FUNCTION OF DISPATCH CONFIGURATION

Dispatch States (eng1/eng2)	Dual LOTC Rate (failures/hour)
Full up/Full up	$0.056*10^{-9}$
Full up/ST	$0.933*10^{-9}$
Full up/LT	$0.700*10^{-9}$
LT/LT	$8.750*10^{-9}$
ST/LT	$11.667*10^{-9}$
ST/ST	$15.556*10^{-9}$

The above calculations assume that the engine control systems on the two engines are in the fault condition state listed in the table at dispatch.

Dispatches of configurations with dual engine LOTC rates greater than 10^{-9} failures per hour are allowed by the FAA, but only for limited periods of time. Any dispatch allowance should be determined via discussions with the FAA concerning the specific configurations and the integrity of the FADEC system(s) when operating in those configurations.

There has been occasional indications from the European Aviation Safety Agency (EASA) that each and every dispatch should meet the "systems requirement" for catastrophic failures (i.e., be less than 10^{-9} failures per hour). Should this be the case, it (most likely) will not be possible to dispatch twin engined aircraft with faults in more than one engine's FADEC system.

9. SUMMARY

The concept of Time Limited Dispatch (TLD) for FADEC systems has worked well in service. Prior to the release of the FAA's Engine and Propeller Directorate policy letter (Appendix B) governing certification of FADEC systems, there were no FAA "rules" or "guidelines" governing dispatch of redundant systems in non-full-up configurations, and even though many systems on modern day commercial transports are using electronic redundancy, the FADEC system is still the only one (currently) employing the use of TLD. The approach has provided engineering guidance to maintenance and dispatch policies.

The three large turbine engine manufacturers, Pratt & Whitney, General Electric Aircraft Engines, and Rolls-Royce have all endorsed and use TLD for their FADEC systems. All three pursue the Markov Modeling approach when analyzing their systems.

The MM approach appears to be the better approach to analyzing FADEC systems. It's flexible and reasonably easy to use. The capability to implement and easily change "transition paths" and rates, as well as repair intervals, is a distinct advantage. The first order differential equations are easily solved.

Two items should be recognized when using the approach:

a. Maintenance becomes a certification item. The airline operators do not like this. They do not like maintenance, which is traditionally an FAA field operations Part 121 issue, to be controlled by an FAA Engine or Aircraft certification group(see Appendix D for more discussion).

b. It brings to the "front" the issue of dispatching systems (for limited periods of time) in configurations where the specific risk of a catastrophic event on a given flight may be greater than 10^{-9} failures per hour.

The first of these tends to be a "political issue". There isn't much the aircraft or engine manufacturers can do to help this situation. As electronic systems continue to grow in usage, FAA aircraft certification groups associated with finding compliance with 14 CFR Parts 23,25,27,29, and 33 and the Flight Standards groups associated with Part 121 operations will both be involved in "certification" and "operations" decisions, and trying to draw a distinct line between the two areas will become increasingly difficult. FADEC redundancy is not simply provided for economic purposes. It's there for integrity also. This needs to be recognized.

The second item is always controversial; however, the use of "fleet averages" to show compliance with the FAA FAR 25.1309 Systems and Equipment requirement (that failures which lead to catastrophic events be “extremely improbable”) has been accepted by the FAA Transport Airplane Directorate (Part 25).

10. NOTES

10.1 The change bar (l) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document.

APPENDIX A - EARLY APPLICATIONS

A.1 EARLY ELECTRONIC APPLICATIONS

For the most part, early turbine engine powered aircraft used hydromechanical controls. There were electronic systems on early turbine engine applications, but generally they were limited to simple functions, such as rotor speed limiters and prop speed synchronizers. In most cases these were single channel, analog type systems. Since the engine had a "full" hydromechanical control system as basic equipment, the FAA generally allowed the aircraft to be dispatched for a period of time with the electronically controlled function(s) inoperative. An example of such a case was the electronic fan speed limiter used on the Rolls Royce RB211 engine used on the Boeing 747 and Lockheed L- 1011 aircraft. The FAA generally determined the "allowable" dispatch interval based on the importance of the function. In the case of the RR limiter, the function was considered to be relatively important, and therefore, the FAA limited the "electronics inoperative" time to 25 hours.

A.1.1 Supervisory Engine Controls

The use of electronics widened as the engines became more complex to control and an improved interface with the engines (by the flight crew) was desired. This led to the use of what were termed "supervisory controls". These control systems employed much more electronics to achieve the desired control/interface functions, but they still generally employed a "full" hydromechanical controller for backup. The electronic supervisory controls were constructed in both analog and digital versions. Examples were the electronics used on the PW JT9D, GE CF6-80A/-80C2, GE- SNECMA CFM 56-2/-3, and RR RB211-535 engines. Although the hydromechanical controllers on these engines generally contained all of the functions needed to operate the engines, the aircraft on which they were installed began using signals from the supervisory electronics portion of the control to achieve improved engine/aircraft integration and operation during "electronic system" operation. For example, autothrottle operation was significantly simplified and improved during electronic engine controller operation, and the increase in crew work load in 2-crew cockpits was always a discussion issue when the engine electronics were inoperative. Hence, the "allowable" time period of electronics inoperative operation always received considerable discussion. In (approximately) 1982 the FAA instituted a policy change that required most items affecting basic aircraft operation/crew interfaces to be repaired within 10 days. The supervisory electronic controls were considered to be in this category, and therefore, the aircraft manufacturer's master minimum equipment list (MMEL), which is the FAA approved document controlling maximum allowable non-full-up dispatch operations, contains this time limitation.

A.1.2 FADEC Engine Controls

As the commercial transport turbine engines became more complex, it became apparent that the hydromechanical controllers were becoming incapable of providing all of the desired functions as well as the "full time" (i.e., electronics always operative) interface desired by the crew. Hence, FADEC engine controllers were developed by the engine manufacturers. These were dual channel electronic control systems that provided complete engine operation and the desired crew interface, even with one channel inoperative. It was anticipated that the dual-channel architecture would achieve excellent engine control system integrity. However, when the first engine, the PW 2037, with such a system was certified on the Boeing 757 aircraft, there were no guidelines in place to allow operation with faults in the electronic portions of the control. Lacking guidelines, the FAA took the very conservative approach of allowing the aircraft to be dispatched with faults in only one of the channels of one engine. In addition, the FAA did not allow the aircraft to leave a station where "repairs could be made". Hence, the aircraft was not allowed to dispatch with engine controller faults if there was a "spare" controller available at that station. This limitation on aircraft dispatchability is a concern to the airline operators.

APPENDIX B - REVISED FAA ANE POLICY LETTER, ANE-1993-33.28TLD-R1, DATED JUNE 29, 2001, POLICY FOR TIME LIMITED DISPATCH (TLD) OF ENGINES FITTED WITH FULL AUTHORITY DIGITAL ENGINE CONTROLS (FADEC) SYSTEMS

REVISION 1 CHANGES:

Section 5. Definitions. Removed the reference to “On-Condition” and “Condition Monitoring” maintenance strategies and revised the applicable text to address the maintenance strategies in terms of “task oriented” strategies. Added a definition of software integrity.

Section 6. Background. Added this section to provide information on TLD and describe the various ways in which TLD has been approved during previous engine and aircraft certification programs; how it has been approved for in-service operations; and the approach to be used for future TLD approvals.

Section 8. Discussion. Revised this section to indicate the documentation for TLD approval at engine certification, aircraft certification, and in-service operations.

Section 9. System Model. Rewritten extensively to provide a more complete description of the full-up and single-fault system models used in the TLD analysis and their outputs.

Section 13. Dispatch Intervals. Revised to add the fourth category of faults, manufacturer/operator defined dispatch, introduced after the issue of the original TLD policy. Simplified the maximum operating time allowance for short time faults in Entry Level applications from “150 flight hours or 10 days, whichever occurs first,” to “125 flight hours.”

Section 14. Maintenance Strategies. Revised to remove reference to “On-Condition” and “Condition Monitoring” maintenance strategies. Also, revised to emphasize that the authorization for the Principal Maintenance or Avionics Inspector (PMI/PAI) to temporarily extend the approved dispatch interval must be stated in the TLD authorization notes. The section has been considerably expanded to address the various maintenance approaches that can be used in conjunction with TLD operations.

Section 16. Engine-Aircraft Interface. Considerably revised and expanded to provide guidance to the engine manufacturer to include TLD information in the engine installation manual and provide guidance to the installer regarding the part 25 development assurance integrity requirements relating to any installer-provided fault recording devices.

Section 17. Field Experience. This section has been deleted from this policy because most of the information is no longer applicable or useful. The information that is still useful has been moved to Section 13 of this policy.

Table 1. TLD Approval. Added Table 1 to indicate the various documentation associated with FAA Engine Certification Office approval of TLD as part of engine certification; FAA Flight Standards Aircraft Evaluation Group approval of TLD at aircraft certification; and FAA Flight Standards Field Inspectors approval of TLD operations for a particular operator.

Table 2. Typical ALS Entry for TLD Limitations. Added Table 2 to show a typical Airworthiness Limitations Section entry that might be used for the TLD associated limitations.

Table 3. Maximum Operating Times for TLD Operations. Changed the short time limitation to be specified in flight hours only; changed the long time interval to have the limitation specified in exposure time in flight hours - so that the short time and long time limitations are both given in flight hours; added the fourth dispatch category to the figure with an accompanying Note 2.

Table 4. Maximum Operating Times for TLD Operations Associated with the “MEL Maintenance Approach” and “Inspection/Repair Maintenance Approach.” Added Table 4 to show the time limitations for both the short time and long time fault conditions associated with the maintenance approach used to address those fault categories.

Figure 1. Typical Data Presentation Showing LOTC Rate as a Function of Short Time and Long Time Operating Hours. Added Figure 1 to show the typical graph used to substantiate the analysis for compliance with the requirement for equivalent or better reliability than the hydromechanical technology of early systems.

Figure 2. Typical Aircraft System Configurations. Added Figure 2 to show the typical aircraft avionics system associated with FADEC system maintenance information and displays.

FEDERAL AVIATION ADMINISTRATION (FAA) POLICY FOR
TIME LIMITED DISPATCH (TLD) OF ENGINES FITTED WITH FULL
AUTHORITY DIGITAL ENGINE CONTROL (FADEC) SYSTEMS

TABLE OF CONTENTS

SECTION PAGE (as printed herein)

1. PURPOSE 64
2. SCOPE 64
3. CANCELLATION 64
4. RELATED SECTIONS 64
5. DEFINITIONS 64
6. BACKGROUND 66
7. DISPATCH CRITERIA 67
8. DISCUSSION 68
9. SYSTEM MODELS 69
10. UNCOVERED FAULTS 70
11. COMPONENT FAILURE RATES 70
12. FLEET-WIDE AVERAGE LOTC RATE 71
13. DISPATCH INTERVALS 71
14. MAINTENANCE STRATEGIES 73
15. SYSTEM REPAIR 77
16. ENGINE-AIRCRAFT INTERFACE 77
17. REPORTING SYSTEM 80

TABLE 1 TLD APPROVAL 82
TABLE 2 TYPICAL ALS ENTRY FOR TLD LIMITATIONS 83
TABLE 3 MAXIMUM OPERATING TIMES FOR TLD OPERATIONS 85
TABLE 4 MAXIMUM OPERATING TIMES FOR TLD OPERATIONS ASSOCIATED WITH THE “MEL” AND “INSPECTION/REPAIR" MAINTENANCE APPROACHES 85

FIGURE 1 TYPICAL DATA PRESENTATION SHOWING LOTC RATE AS A FUNCTION OF SHORT TIME (ST) AND LONG TIME (LT) OPERATING HOURS 86
FIGURE 2 TYPICAL AIRCRAFT SYSTEM CONFIGURATION(S) 87

1. PURPOSE. This document provides FAA policy for obtaining type design approval for an airworthiness limitation under part 33 of Title 14 of the Code of Federal Regulations (14 CFR part 33), relating to dispatch of engines with full authority digital engine control (FADEC) systems in a degraded condition with respect to redundancy. This airworthiness limitation is commonly referred to as time limited dispatch (TLD) for engines with electronic engine control systems, which have some level of redundancy. This policy does not constitute a new regulation and does not establish a binding norm.

2. SCOPE. This document applies to type design approval for TLD for engines fitted with FADEC systems, when these systems are to be dispatched with faults present for limited time intervals before maintenance actions are required. The objective of this policy is to define the various dispatch categories and corresponding maintenance intervals to provide a control system that achieves overall compliance with the applicable airworthiness requirements of part 33. TLD operations have been applied to FADEC-equipped engines used in multi-engine aircraft applications, particularly those engines used in part 25 aircraft. The TLD requirements and limitations for those multi-engine aircraft discussed in this policy should be acceptable in single engine aircraft applications. However, the criteria used to establish acceptable TLD operations may need to be reviewed for those other applications. For example, it has been accepted that single or multi-engine aircraft certified to part 23 requirements (and not certified to part 25 requirements) may only have to achieve a 40,000 hour “average reliability” for the engine control systems. This reliability level is considered equivalent to the mechanical engine control systems currently being used in part 23 aircraft. Thus, it may be acceptable for part 23 aircraft to dispatch with faults in the FADEC engine control systems that result in a control system loss-of-thrust-control (LOTC) or loss-of-power-control (LOPC) rate of less than the 10,000 hour lower limit allowed in part 25 applications. For part 23 applications, a lower limit for the LOTC rate of approximately 4,000 hours may be acceptable. The Engine and Propeller Directorate is currently reviewing the criteria for these other applications. The Engine and Propeller Directorate may issue additional or revised TLD policy to include the appropriate information for these other applications after the requirements have been established. This review of control system reliability and availability requirements for single engine aircraft applies to both reciprocating and turbine engines. The engine control system reliability and availability requirements should be the same for both turbine and reciprocating engines when those engines are targeted for the same type of aircraft application. The FAA is developing a separate TLD policy for engines targeted for airplanes certified under part 23 and operated under part 91 or part 135.

3. CANCELLATION. This document supersedes FAA policy on TLD of engines fitted with FADEC systems issued on October 28, 1993.

4. RELATED SECTIONS. Sections 33.4, 33.5, 33.19, 33.28, 33.91(a), 43.16, 91.213(d), 121.303(d), 121.627, 121.628, and 135.179.

5. DEFINITIONS.

a. Adequate Software Integrity. For the purposes of this policy, “adequate software integrity” level means that the software level used in the particular electronic unit being discussed is equivalent to DO-178B, level C, unless a higher level is specified.

b. Central Processor Unit (CPU). The CPU is the main processor(s) within the electronic engine control that receives conditioned input data, processes and manipulates the data, and provides output commands to control the engine in accordance with stored algorithms.

c. Cross-Channel Data Link (CCDL). The CCDL is the digital data link that transfers data between the functionally redundant CPUs in their respective channels.

d. Dispatch Interval. The dispatch interval is the maximum time interval approved by the FAA for dispatch with faults present in the system before corrective maintenance is required.

e. Entry Level System. An entry level system is a FADEC system that has not reached maturity as defined in this policy.

f. FADEC Family. FADEC systems can be considered to be a FADEC family when the electronic engine controls are related due to an overwhelming majority of common parts, similar design and manufacturing technology, and similar engine installation.

g. FADEC System. The FADEC system controls the operation of the engine over the entire operating range, usually from engine start to maximum power or thrust. The FADEC system consists of the electronic engine control (EEC), fuel metering unit (hydromechanical control), sensors, actuators, valves, alternator and interconnecting electrical harnesses. In some installations the system may include hardware and/or software propeller or reverser functions; in others it may include ignition elements and other control system components common to reciprocating engines.

h. Fault Exposure Time and Average Fault Exposure Time.

(1) When a Minimum Equipment List (MEL) Maintenance Approach is used, the time of occurrence of the fault is known (generally there is a flight deck indication of the failure condition). The fault exposure time is the time that the fault remains present in the system before it is repaired.

(2) When the Periodic Inspection/Repair Maintenance Approach is used, the time of occurrence of the fault may not be known. The average fault exposure time when the fault is found during a periodic inspection is one-half of the periodic inspection interval, since the fault could have occurred at any time during the interval. This assumes that the fault rate of occurrence is constant throughout the interval. If the fault rate is not constant throughout the interval, the average exposure time should be adjusted accordingly.

i. Fleet-Wide Average Loss-of-Thrust-Control (LOTC) Rate. This rate is the “time weighted LOTC rate” of the FADEC system in all modes of operation and dispatch configurations. When in-service data is available, the fleet-wide average is the total number of LOTC events of a family of FADEC systems divided by the total number of flight hours for the FADEC family.

j. Hours. In this document, hours are engine flight hours.

k. In-Flight Shutdown (IFSD). An IFSD occurs when an engine ceases to function in flight and is shutdown. The shutdown could be self-induced, initiated by the crew, or caused by other external influences. An IFSD caused by the FADEC system is considered an LOTC event.

l. Loss-of-Thrust-Control (LOTC). The LOTC is the loss of ability to modulate power or thrust from flight idle to 90% maximum power or thrust. This is the definition used for part 25, 27, and 29 applications. The FAA is developing different definitions for other applications.

m. LOTC Rolling Average. The rolling average is the sum of LOTC events for a given period divided by the in-service hours for the same period; a three month period gives a three month rolling average.

n. Maintenance Interval. In this document, this is a scheduled maintenance interval such as a repetitive periodic maintenance action or an aircraft maintenance letter check (for example, “A” check).

o. Mature Level System. A FADEC system reaches maturity as defined in this policy after 250,000 hours of in-service operation in the particular installation or its equivalent. In addition, to qualify as a mature system data must be provided to demonstrate that the FADEC system has achieved a stable in-service LOTC rate that is consistent with the analysis on which TLD approval is based.

p. Maximum Allowed Fault Exposure Time and Maximum Allowed Average Fault Exposure Time. The maximum allowed fault exposure time limitations in this policy apply to the following situations:

(1) When the time of occurrence of the fault is known, a suitable generic flight deck display of the condition is provided, and the fault category is addressed using the MEL Maintenance Approach; and

(2) When the time of occurrence of the fault may not be known, and the fault category is addressed using the Periodic Inspection/Repair Maintenance Approach.

q. Redundant. This term refers to an alternate, backup, or equivalent method for providing a parameter or function so that the parameter or function can be provided even though one source of the parameter or function is lost or unavailable.

r. Uncovered Fault. An uncovered fault is a faulted parameter or function of the FADEC system that cannot be provided by another means because either the fault is not detected or the fault is detected but no accommodation means is provided.

6. BACKGROUND. This background section is based on part 33 certificated engines installed on aircraft operating under part 121 regulations. Initial FADEC system reliability analyses were essentially based on full-up system configurations; these analyses provided little information in the area of system integrity with faults present. As a result, dispatch criteria for the early FADEC systems entering revenue service was determined by the selection criteria used when establishing the aircraft's Master Minimum Equipment List (MMEL). This criteria follows the traditional path of considering the consequences of the next failure. Due to the complexity of FADEC systems, it was difficult to consider the various failure combinations and the consequences of the next failure. There was little or no supporting safety analysis or field experience on which to base a dispatch decision. This resulted in a somewhat limited dispatch criteria that, in some cases, had a more negative impact on the aircraft delay and cancellation performance than might result from an analysis performed according to this policy.

Aircraft and engine manufacturers recognized that the redundancy features and reliability of the FADEC systems could provide a means for improving (that is, reducing) aircraft delay and cancellation events by enabling redundant systems to dispatch with faults present. The FADEC systems would also improve control system reliability compared to the technology they replace. The dispatch configurations would have to meet engine and aircraft airworthiness standards and demonstrate that the use of non-full-up dispatch configurations would be acceptable over a specified dispatch interval. The manufacturers proposed TLD intervals that would enable aircraft to complete their regularly scheduled route structure. The FADEC faults could then be repaired on a normal maintenance schedule for the aircraft. This work resulted in the original TLD policy, issued by the FAA Engine and Propeller Directorate (EPD) in October 1993. Since that time, the FAA Engine and Aircraft Certification Offices and the Flight Standards Aircraft Evaluations Groups (AEG) have agreed on a revised approach to TLD approval and operations. The changes associated with this revised approach, which is currently being applied, have prompted this revision to the 1993 TLD policy.

The revised approach to TLD approval is appropriate because the FADEC system is not considered "inoperative" when operating with its various system related faults; the system merely loses some of its redundancy. The following factors suggest that the FADEC system does not readily fit the traditional definition of an inoperative system, as addressed by an aircraft MMEL.

a. A maintenance procedure pertinent to TLD is not required before releasing the aircraft for service (in the case of part 121 operations, this may be referred to as 'dispatch');

b. There is usually no operational impact on crew procedures; and

c. Generally, an aircraft performance penalty does not need to be applied before releasing the aircraft for service (or dispatch, for part 121 operations).

The revised approach to TLD approval transfers the authority for the initial approval of FADEC system TLD operations from FAA Flight Standards to FAA Engine Certification. The FAA Flight Standards organizations, however, are still very much involved. The implementation of the maintenance activities required under TLD is done through the operator's MEL and/or the operator's maintenance plan for the aircraft; both of these activities require FAA Flight Standards approval before implementation. Note: Operators under other regulations, such as part 91 operations, may not have MELs or approved maintenance plans.

In TLD applications prior to the issuance of the original TLD policy, FADEC systems were listed in the aircraft's MMEL; this was driven by the operators. The operators did not want any maintenance tasks that were more frequent than an aircraft "A" check. Initial aircraft "A" checks are generally between 250 and 400 hours. The initial periodic inspection for FADEC system short time faults - for entry level FADEC systems - was set at 150 flight hours or 10 calendar days, whichever occurred first. Since this is a shorter time interval than the aircraft "A" checks, the operators wanted an indication on the flight deck that a short time fault condition was present. The operators used the indication to "start the clock" and schedule the appropriate repair(s). Since the flight crew would see the indication, a means to allow dispatch with the indication present became necessary. Thus, an item to address the indication and allow dispatch with short time FADEC faults present was added to the MMEL. However, as indicated in section 14 of this policy, it is acceptable to NOT have any flight deck indications for FADEC short time or long time faults. If an operator prefers, FADEC system short and long time faults may be addressed using a Periodic Inspection/Repair Maintenance Approach.

When the FAA Engine Type Certificate Holding Office (TCHO) approves a TLD limitation, the time limits relating to TLD operations must be included in the FAA-approved Airworthiness Limitations Section (ALS) of the engine's Instructions for Continued Airworthiness (ICA). At aircraft certification and delivery, the part 121 and 135 operators are required to have an established maintenance plan that shows compliance with the engine ALS items. The FAA Flight Standards (FS) organization is responsible for the review and acceptance of the operator MEL and maintenance program. The FS organizations have generally accepted the FAA-approved TLD limitations for MEL purposes, but they have the option to be more restrictive, if necessary, due to other aircraft or operational considerations. For engines installed on aircraft intended to operate under part 121 or 135 regulations, the engine TC holder and the aircraft manufacturer should coordinate before submitting the FAA-approved TLD limitations to the appropriate FS organizations for inclusion into the aircraft manufacturer's MMEL, recommended maintenance plan, or both, and subsequent inclusion in the operator's specific MEL, maintenance program, or both.

To substantiate the reliability goal for the FADEC system under TLD operations, an analysis, such as a Markov Analysis or fault tree analysis, must be applied to estimate the average reliability of the system during normal and TLD operations. The objective of the reliability analysis is to demonstrate that the time-weighted-average of all allowable dispatch configurations meets the reliability requirements associated with FAA engine certification. Analysis techniques are discussed in section 9 of this policy.

The TLD policy established specific requirements for entry level FADEC system TLD approval. These requirements have essentially not been changed. The FAA revised the short time dispatch interval (time limitation) for entry level applications from "150 flight hours or 10 calendar days, whichever occurs first," to "125 flight hours." This is not a significant change and was prompted by operator request. Since TLD operations are being implemented and becoming a standard for small operators and business aircraft operations, in addition to transport operations, the 10 calendar days requirement is considered overly restrictive. The requirement to achieve 250,000 hours of engine operation to be considered a mature level system still applies. After 250,000 hours of engine operation, the FAA will consider applications for extending the TLD short and long time limitations when field service data supports the request.

7. DISPATCH CRITERIA.

a. Dispatchable Configurations. Each dispatchable configuration must:

(1) Meet the part 33 airworthiness operating requirements

(2) Have at least one channel operating on its dedicated power source; this channel should be capable of being the channel in control;

(3) Maintain the capability of critical engine protection, if provided by the control, (for example, overspeed protection). For additional information, see section 13.a.(1)(c) of this policy;

(4) Maintain a means to provide necessary signals to identify system faults;

(5) Be supported by a statistical analysis for the proposed dispatch intervals;

(6) Not exceed a computed LOTC rate of 100 events per million hours;

(7) Not have additional single failures in the FADEC system that could prevent continued safe flight and landing of the aircraft; and

(8) Meet all aircraft level requirements, when the aircraft installation is known, such as those relating to engine performance, operability, acceleration, etc., unless compensating operational or maintenance procedures are approved.

b. Fleet-Wide Reliability Requirement. The applicant must show by a suitable analysis that the fleet-wide average reliability criteria or "average LOTC rate," which includes full-up as well as degraded system dispatches and uncovered faults, is less than 10 LOTC events per million flight hours.

c. Environmental Requirements. The applicant must demonstrate by analysis, test, or both that all dispatchable configurations continue to meet the environmental certification levels for the system, including those effects associated with high intensity radiated fields (HIRF) and lightning.

8. DISCUSSION. The objective of the TLD approach is to preserve suitable FADEC system integrity while minimizing dispatch delays and cancellations caused by the system. The FADEC system may continue to operate with faults present if the resulting system operation and reliability are adequate and operating exposure in this degraded state is appropriately time limited. The applicant must submit a TLD analysis that substantiates the reliability of the proposed allowable faulted configurations for the associated dispatch intervals. The TLD analysis report must define the dispatchable configurations in terms of the faults, usual degraded redundancy, and the associated dispatch intervals.

The following is a method for linking the approved TLD time limits and operations to the engine:

a. The engine TCDS must indicate that the engine control system has been approved for TLD operations.

b. For all engines, the FAA approved ALS of the engine ICA must also include the restrictions and time limits associated with TLD operations.

c. The FAA recommends that the TLD restrictions, time limitations, and other related installation requirements be included in the engine Installation Instructions. This is described in section 16 of this policy.

Table 1 shows the TLD documentation required and the appropriate FAA approval organization for each type of documentation.

Table 2 provides an example of the TLD limitations as they might appear in the ALS of the engine ICA. The FAA requires an in-service reporting system because unpredicted factors could invalidate the analysis. This reporting system should compare service experience of component failures with the modes, effects, rates, and exposure times predicted in the statistical analysis. In addition, this reporting system is used to support future applications for changing dispatch time intervals. Section 18 of this policy provides details of the reporting requirements.

While developing this TLD policy, the FAA has taken into consideration certain aircraft level certification requirements that are significant for this subject. However, the appropriate FAA Aircraft Certification Office (ACO) will make the final determination of the aircraft certification issues. This policy is not intended to prevent the ACO or FS organizations from determining that more restrictive TLD requirements are warranted. Furthermore, any TLD limitation incompatible with aircraft certification or operational approvals will be resolved within the FAA. The FAA may require an amendment to the engine design, ALS, and Installation Instructions, as necessary, to resolve the situation.

9. SYSTEM MODELS. The FAA must approve the FADEC system model used in the statistical TLD analysis.

a. Components of the FADEC System. The FADEC system includes, but is not limited to, the EEC, fuel metering unit (hydromechanical control), sensors (including the throttle or power lever sensor elements), actuators, valves, alternator and interconnecting electrical harnesses. In some installations, the system may include propeller or reverse functions; in others it may include ignition elements and other control system components common to reciprocating engines. The fuel pump is considered part of the fuel system and does not need to be included.

It should be noted that, in keeping with the EPD objective that the engine should be independent from the aircraft, LOTC credit should generally not be taken in the system model for the use of aircraft power as a backup power source, unless the FADEC system has been designed to accommodate the interrupts and power transients that can occur in those systems. For example, if aircraft power interrupts associated with bus transfers between the battery source and other generated power sources would cause the FADEC system to shut down the engine, LOTC credit for the use of aircraft power as a backup power source should not be taken. If, however, the FADEC system can successfully operate through all expected aircraft bus transfers and transients within the aircraft's electrical power quality specification, then LOTC credit for use of aircraft power as a backup power source can be taken. When credit is taken for aircraft backup power, the assumed aircraft electrical power quality should be included as an installation limitation in the engine's Installation Instructions.

Data provided from the aircraft may be used as a means to provide fault detection and isolation coverage. If failure or malfunction of aircraft data signals can lead or contribute to LOTC events, the engine's Installation Instructions must state the assumed reliability for that data, and the engine's LOTC analysis must include the failure effects of that data loss or malfunction.

b. Control System Fault Models. The following discussion on modeling the control assumes that the system is a conventional type FADEC system (that is, a dual channel system in which both electronic channels are essentially the same). In the TLD statistical analysis, the applicants have used both full-up and single-fault models to establish the maximum dispatch intervals allowed for the various control system faults. Section 14 of this policy discusses the concept of fault exposure times and their effect on maintenance strategies. The Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 5107, Time Limited Dispatch (TLD) Analysis, dated June 1997 provides guidance for performing the TLD analysis.

(1) Full-up Model. A full-up model is one that models all control system states from full-up to LOTC. The model starts in the full-up state, generally called the 0^{th} state, at time zero, and as time progresses, predicts the transfer of the system through the various fault condition states to the LOTC state. These models represent fault conditions to at least the first fault level. When only the first fault conditions are modeled, the model shows only those second fault conditions that cause the system to transition from a first fault condition state to the LOTC state. More complex models show a second fault condition level. These models show the relevant second fault conditions that cause the system to transition from a single fault condition state to the LOTC state, as well as all of the relevant third fault conditions that cause the model to transition from a second fault condition state to the LOTC state. A second fault condition level model is much more complex than a single fault level model. If there are "n" first fault states, there are approximately n(n-1) second fault condition states. Therefore, the number of possible states increases considerably when modeling second fault condition states. It is generally accepted that the modeling of second fault condition states has a small effect on improving the accuracy of the answer of interest, which is the predicted average LOTC rate. This is because the probability of two fault conditions occurring in the system in a given time period is much greater than the probability of three or more fault conditions occurring in that same time period. A conservative assumption for a two fault condition state model is that all third faults lead to an LOTC state. This assumption does not significantly penalize the resultant calculation. For that reason the system's LOTC rate consists primarily of the combinations of two fault conditions that lead to LOTC events, and not the combinations of three or more faults that lead to LOTC events. Adding the second fault state generally increases the accuracy of the predicted LOTC rate by less than 5%; therefore it is acceptable to complete the analysis using a single fault level model. When doing this, the applicant should provide an analysis to show that the modeling of second fault conditions (fault states in which two fault conditions exist together without resulting in an LOTC event) has a small effect (less than 5%) on the predicted LOTC rate. Repair actions can be modeled. The repair actions for given faults or fault categories should be modeled to occur at specified time intervals. Depending on whether the model is an "open loop" or "closed loop" model, as discussed in SAE ARP5107, the result of the analysis will be either: (a) the

instantaneous LOTC rate of the control system at any given point in time; or (b) the average LOTC rate of the system. If an open loop modeling approach is used, the instantaneous LOTC data can be used to determine the average LOTC rate of the control for the modeled fault repair times. If a closed loop modeling approach is used, the result is the average LOTC rate for the fault repair times contained in the model. In either case, the average LOTC rate increases (as expected) with increasing fault repair times. These models are based on repair scenarios in which the time of occurrence of the fault condition(s) is known. Therefore, the repair times modeled actually represent the maximum lengths of time (exposure time) that fault conditions are allowed to be present in the system (before repair is required) and have the system achieve the predicted LOTC rate.

(2) Single-fault Level Model. A single-fault level model is a FADEC system model in which the individual fault conditions are sequentially assumed to exist in the model at time equal to zero, and only those ensuing fault conditions involving that first fault and leading to LOTC events are modeled. Using this modeling approach, the 0^{th} state is not the full-up state; it is the first (assumed) fault condition. The model would show all of the relevant fault conditions that would cause the system to transition from the assumed first fault state to the LOTC state. If modeled, an "in-between first fault level" would show (as separate states) those combinations of two faults that do not result in LOTC events, and the model would show the relevant third fault conditions that cause the model to transition from the first fault level (a dual fault condition state) to the LOTC state. By themselves, each of the single-fault state models is much simpler than a full-up model. However, since all single-fault states have to be modeled, the total task of assembling and analyzing all of the single-fault models is essentially the same as that of doing a full-up model. The single-fault models yield the LOTC rates of the control system (when it starts with that fault present) versus time, for various "modeled" repair times. The data for all of the single-fault states is then "weighted" by the probability of being in that given fault state, to produce an average LOTC rate for the entire control for a given (modeled) repair time. As in the full-up model, the repair times are actually based on knowing when the fault occurs. Again, the repair times modeled actually represent the maximum length of time that the fault is allowed to be in the system before repair is required and still have the system achieve the predicted LOTC rate. If only single-fault conditions are modeled (that is, the model does not show combinations of two or more fault conditions that could exist simultaneously without the system being in the LOTC state), the applicant should show by analysis that neglecting these higher level states has a small effect (less than 5%) on the result.

Although the mathematical models are generally based on knowing when a given fault occurred (in-service FADEC systems generally "know" when a fault occurs), the specific time that the faults occur is not required to establish a maintenance plan that allows compliance with the time limitations specified in the ALS of the engine ICA. In this case, compliance with the ALS time limitations can be accomplished using a Periodic Inspection/Repair Maintenance Approach for FADEC system faults; section 14.b. of this policy discusses this approach.

10. UNCOVERED FAULTS. In the analysis, all uncovered faults must be assumed to lead to LOTC unless they can be shown not to directly result in an LOTC. The analysis must provide the rationale and substantiation for the failure rates used for uncovered faults in the analysis.

11. COMPONENT FAILURE RATES. The failure rates for components used in the analysis should be based upon those listed in a data source accepted by the FAA. When the component failure rate is not listed in an acceptable industry source, the failure rate data used in the analysis should be supported by service experience or other equivalent data. In-service data may be used in place of an acceptable industry source when suitable in-service data is available.

12. FLEET-WIDE AVERAGE LOTC RATE. The FAA requires that FADEC systems demonstrate an equivalent or better reliability than the hydromechanical technology of early systems. Based on available in-service data, the FAA, in coordination with industry, determined that the IFSD rate attributable to the hydromechanical controls used on engines intended for part 25 transport aircraft applications was approximately ten events per million hours. Therefore, the FAA requirement has been to demonstrate by analysis that the FADEC system would be chargeable for fewer than or equal to ten LOTC events per million flight hours. The analysis for TLD must demonstrate that the fleet-wide average LOTC rate continues to comply with this requirement. The average LOTC rate is the time weighted average of all allowable dispatch states. The analysis to substantiate compliance with this requirement should be summarized in a graph. The ordinates of the graph should be in terms of fleet-wide average LOTC caused by the FADEC system per million hours versus the dispatch time interval in hours. The ordinate of the graph should be extended to show a dispatch time interval of at least twice the length of time of the long time repair interval being requested. Data should be shown for both the short time repair interval being requested and twice the length of the short time repair interval being requested. An example of such a graph is shown in Figure 1. A system may be designed to have only one fault group for TLD dispatchable faults. In this case there would only be one data line. An example of this is shown by the ST=LT line in Figure 1.

13. DISPATCH INTERVALS. The applicant must submit a TLD analysis that substantiates compliance with this policy for the desired dispatch configurations and dispatch intervals for the four categories, as applicable, defined in this section. These four dispatch categories are classified as follows:

- No Dispatch
- Short Time Dispatch
- Long Time Dispatch
- Manufacturer/Operator Defined Dispatch

a. Category Definitions.

(1) No Dispatch. No dispatch configurations are those in which the FADEC system has a fault or faults that result in any of the following:

(a) The performance and operation of the engine does not meet its approved type design, which has been shown to comply with part 33 requirements;

(b) The system has suffered a complete loss of a critical resource or a critical function;

(c) The system does not have engine overspeed* or a critical limit protection function* (applicable when the control system is providing such a function); or

(d) The computed LOTC rate of the system (with the fault(s) present) is greater than 100 events per million hours.

*Note: Exhaust Gas Temperature/Inter Turbine Temperature (EGT/ITT) is not considered a critical limit protection function, even though some engine control systems are configured to provide that function. The EGT/ITT display is considered sufficient for indication of an over-temperature condition. In addition, a loss of rotor over-speed protection may not be of major concern in some rotorcraft operations. In practical applications, such as rescue operations or evacuations from distressed areas, the lack of turbine overspeed protection may be a lesser concern. In these installations it may be better to have a separate cockpit indication for loss of the protective function and save the no dispatch indication for conditions in which the control does not have the resources to provide minimally acceptable engine operation. The phrase “minimally acceptable” will always generate discussion. The simple question to be answered, in some scenarios, is if there is a greater risk in staying vs. leaving the area. In difficult situations, the flight crew has to make that decision. In these particular applications, the failure conditions that initiate a no dispatch indication should be carefully reviewed and minimized as necessary.

(2) Short Time Dispatch. Short time dispatch configurations are defined by all of the following:

(a) The system has a fault or faults that do not fall into the no dispatch category;

(b) A fault or faults that cause a significant loss of FADEC system signal redundancy, such as loss of a channel CPU; and

(c) The computed LOTC occurrence rate with the fault(s) present is less than 100 events per million hours but greater than 75 events per million hours.

(3) Long Time Dispatch. Long time dispatch configurations are defined by all of the following:

(a) The system has a fault or faults that do not fall into the no dispatch or short time dispatch categories; and

(b) The computed LOTC rate is less than 75 events per million hours.

(4) Manufacturer/Operator Defined Dispatch. This category is for faults that do not fall into any of the other three categories (no dispatch, short time dispatch, and long time dispatch), and do not have an impact on the LOTC rate. These faults do not have to be included in the LOTC analysis; however, they should be included in the TLD report, and it should be substantiated that these fault conditions do not have an impact on the LOTC rate. The repair interval for these faults may be agreed upon between the engine and aircraft manufacturers, the operators, or both.

b. Statistical Analysis Results. Table 3 illustrates the allowed dispatch intervals. The dispatch intervals for entry level and mature level FADEC systems have been separated to consider factors not included in the statistical analysis. The statistical analysis is based largely on electronic component databases that consider components to be mature. Because the components are assumed to be mature, only random failures are considered in these databases. Failures due to design, manufacturing and quality are not included in the database.

Because system faults attributable to design, manufacturing, quality and maintenance errors are not covered by the statistical analysis, this document introduces a factor related to service experience (see section 13.c. of this policy). The experience factor provides a safety margin for faults in the fleet resulting from latent design, manufacture and quality deficiencies and maintenance errors, because these faults tend to be exposed and corrected as in-service time is accumulated. This safety margin is addressed by providing more conservative criteria for dispatch intervals for entry level systems compared to mature level systems, even though the statistical analysis may support dispatch for a longer dispatch interval for entry level systems.

c. Margins. The predicted fleet-wide average LOTC rate analysis should comply with the fleet-wide average LOTC rate criteria at a time equal to two times the long time dispatch interval for which the applicant requests approval. The predicted LOTC rate, considering full-up as well as all allowable dispatch conditions, should be equal to or less than 10 events per million hours, assuming short and long time exposure intervals that are twice as long as those being requested. The FAA provides this 2:1 margin to cover uncertainties in the analysis.

d. Entry Level Systems. A FADEC system is classified as an entry level system if it has less than 250,000 flight hours of field experience. The applicant may request alleviation from this classification if it has sufficiently similar systems operating in the field that have accumulated greater than 250,000 flight hours. The FAA will review such an application on a case-by-case basis. Table 3 gives the maximum exposure time limitations for the short and long time fault categories for entry level systems.

e. Mature Level Systems. For mature level systems, the FAA engine TCHO approves the short and long time dispatch intervals on a case-by-case basis, depending upon the system, analysis, and service experience. After a FADEC system has accumulated 250,000 flight hours in-service operation, an applicant may request a change in FADEC system status from entry level to mature. The applicant must provide data to support this change. The data must demonstrate that the FADEC system has achieved a stable in-service LOTC rate that is consistent with the analysis on which TLD approval is based. Derivatives of similar FADEC systems can be considered to be part of a FADEC family. If the engine TCHO approves, the summation of a family of FADEC systems in-service flight operation times can be used in the maturity evaluation.

f. Substantiation Data for Dispatch Levels. The applicant must submit the TLD statistical analysis report to the FAA engine TCHO. The report must include a tabulation of the various proposed dispatch configurations that provides: (1) the expected frequency of occurrence of the faults leading to those dispatchable configurations; and (2) the LOTC rate of the system when operating in those configurations. The report must tabulate the chosen category for each fault covered in the analysis and show that the exposure time chosen for the short and long time fault categories allows the control system to meet its reliability requirements. The analysis should substantiate that faults classified in the new fourth category, manufacturer/operator defined faults, do not impact the LOTC analysis. The analysis must also provide a substantiation or justification, including failure rates, exposure times, and other assumptions, for fault(s) that impact engine operability, reliability, or durability.

Based on a positive review of the analysis and data provided in the report and discussions with the applicant, as required, the TCHO may grant approval for the requested TLD. The FAA-approved ALS of the engine ICA must include the TLD approval information.

14. MAINTENANCE STRATEGIES. Applicants have proposed the use of two different maintenance strategies to implement the TLD time limitations. Either strategy or a combination of both may be used; one may be used for the short time faults, and the same or different strategy may be used for the long time faults. In either case, the approved dispatch interval must be substantiated by a TLD statistical analysis that uses a full-up model, a single-fault system model, or the equivalent. Section 9 of this policy discusses system models. This section discusses the differences in TLD maintenance activities when applying these strategies.

a. No Dispatch. Regardless of the maintenance strategy, there will be non-dispatchable configurations. The presence of a no dispatch fault condition must be indicated in the flight deck by essential equipment. Essential equipment is equipment available for every aircraft dispatch.

b. MEL Maintenance Approach. When using this maintenance strategy, the fault occurrence time is known because there is a generic flight deck indication of the condition, and the fault must be repaired before the end of the approved interval. For this strategy, the fault exposure time is the time from when the fault occurred to when it is repaired. For example, if the fault condition is indicated and the fault is not repaired until 100 hours after its occurrence, the entire 100 hour period is the fault exposure time. The short time fault category is generally handled using this approach; however, this is not a requirement. Short time faults could be addressed with a Periodic Inspection/Repair Maintenance Approach. When using the MEL Maintenance Approach, the presence of a fault condition in this category is generally indicated in the flight deck on essential equipment so that the flight crew and/or maintenance personnel can “start the clock” when the fault condition first occurs. This is called the MEL Maintenance Approach because the flight deck indication is generally apparent to the flight crew; therefore, an MEL entry is needed to allow dispatch with the fault indication present. Many applications using this approach “start the clock” at midnight on the day the fault indication occurred; this practice has been reviewed with Flight Standards and is acceptable.

When an MEL Maintenance Approach is used, the item should be listed in the aircraft’s MMEL. An operator reflects that item in its MEL. The MEL Maintenance Approach is generally used for fault conditions that require repair within a relatively short time period, such as 125 flight hours, although longer time periods, such as 300 flight hours, have been approved. This approach is not normally used for fault categories in which the allowed dispatch interval is greater than 300 flight hours. Flight crews must disposition all MEL items before every dispatch because dispositioning a given MEL item of more than 300 flight hours is burdensome.

Note: When using the MEL Maintenance Approach, the aircraft's MMEL may not list the specific time period associated with a given fault category. Instead, the MMEL may reference the ALS of the engine ICA or an engine manufacturer's document that contains the FAA-approved time limitations. The operator's MEL, however, should show the specific time period of allowable dispatch. The flight crews need to know the allowable dispatch times; a reference to a document that is not readily available is not useful.

The aircraft MMEL is developed by the Flight Operations Evaluations Board (FOEB) for a given type design aircraft. An FAA FS Operations Inspector from the AEG assigned to the aircraft serves as chairperson of this board. The board is usually made up of FAA airworthiness inspectors for maintenance and operations and an assigned flight test pilot. The FOEB accepts input from FAA engineering, the aircraft and engine manufacturers, as well as the operators. Evidence of TLD approval by the part 33 TCHO and the listing of the time limitations in the ALS of the engine's ICA, combined with the appropriate generic flight deck indication, is usually sufficient to substantiate the acceptability of the desired MMEL listing. However, the FOEB can be more restrictive if they consider it necessary.

Though unlikely in a reliable system, it is possible for more than one short time fault to occur in a system during a short time interval. An example of a first short time fault might be the loss of one channel's dedicated power supply. The "clock" would be started for this fault condition. If the channel does not have a back-up power source, the remaining channel would have to sense the channel loss and report the fault condition. Although it is unlikely, a second failure that could occur is a failure in the affected channel's CPU. The exact cause of the first short time fault condition (in this example, the loss of one channel's power supply) may or may not be known because a generic indication is usually displayed in the cockpit to indicate the presence of a fault in this category, rather than an indication that identifies the specific fault. But, the "exposure clock" must be started when the first fault occurs. Maintenance personnel will find the existence of the second short time fault before or during the repair of the first fault. If the date of the second fault can be adequately determined by using a system that has been developed and certified to the appropriate software development assurance level (see section 16 of this policy), the MEL "clock" for the second fault can be back-calculated, and the second fault condition may not have to be repaired when the first fault condition is repaired. The second fault can have its own time period. However, if there is no suitable (acceptable to the FAA) media to indicate when the second fault occurred, all short time faults must be corrected at the time of the first fault repair. In the above example, if there is no suitable media for determining when the second short time fault (CPU failure) occurred, both faults (the power supply and the EEC unit, which contains the CPU) must be repaired within the time interval established by the first fault (power supply fault).

c. Periodic Inspection/Repair Maintenance Approach. This maintenance approach applies a periodic inspection and repair strategy to manage FADEC system faults. The approach is generally used for FADEC system faults allowed to remain for time periods greater than 300 flight hours before requiring repair. This approach is normally only applied to long time faults, but it has been applied to short time faults if a generic flight deck indication is not available for the presence of a short time fault condition. When using this approach, the time at which the fault first occurs does not have to be known. The FADEC system must be interrogated by maintenance for the presence of faults during periodic inspections, and the faults found must be repaired within a specified time period or interval, so that the average exposure time of a fault in a particular category does not exceed the maximum average allowed exposure time for that category. The average exposure time of the system to a fault is simply the average length of time that a fault is present in the system before it is repaired.

The following assumption should be used when applying this strategy. If a fault is found during a periodic inspection, the fault could have occurred at any time throughout the interval; therefore, assume that the fault occurred, on average, half-way through the interval. This assumption is acceptable when the failure rates for the faults in a particular category are essentially constant with time, and the periodic inspection interval (in hours) is less than the mean time between failures (MTBF) of the sum of the failure rates of that particular fault category. If either of these conditions is not true, the periodic inspection/repair interval should be adjusted accordingly.

Consider the following example:

A Periodic Inspection/Repair Maintenance Approach is being applied to long time faults, and the limitation relating to those faults is that they must be repaired within a time period sufficient to ensure that the maximum average exposure time of the system to the long time fault does not exceed 250 flight hours. With this information, an operator might arbitrarily establish a task to periodically inspect for long time faults every 400 flight hours. If faults are present when the system is inspected, the applicant can assume that those faults occured half-way through the interval and are on average 200 flight hours old. If the maximum average exposure time of the system to these faults must be limited to 250 hours, then faults found during the 400 hour periodic inspection must be repaired within 50 flight hours to meet the maximum average exposure requirement.

With this approach, the time limitation in the ALS could be met using an inspection period that is twice as large as the maximum allowable exposure time limitation given in the ALS for those faults. This is shown in Table 4; the right columns of the two columns under the "Short Time Faults" and "Long Time Faults" give the maximum periodic inspection/repair interval. However, if the maximum inspection/repair time is chosen, there would be no time to schedule the repairs of those faults to a future date because the faults found, on average, would be at the maximum average allowable exposure time limit. The faults found would have to be repaired before the aircraft could be returned to service. This is why the operators would normally interrogate the system at a periodic interval that is less than the maximum inspection/repair time.

In the above example, the time limitation for the maximum allowed average exposure time to faults was assumed to be 250 flight hours. A maximum inspection/repair time of 500 hours could be used for the inspection/repair interval, but if a 500 hour interval is used, all faults found at that inspection would have to be repaired before the aircraft could be returned to service. By doing the inspection at a shorter interval (400 hours), any faults found would be on average 200 hours old, and the faults would not have to be repaired immediately. An additional 50 flight hours of operation could be allowed before the repair of those faults is required. This example results in a total inspection/repair time of 400 hours for the inspection and 50 hours for the repair, or 450 hours. This reduces the maximum inspection/repair time of 500 hours by 50 hours, but is more flexible because faults found do not have to be repaired immediately; the repair can be scheduled to a more convenient time.

In summary, when using the Periodic Inspection/Repair Maintenance Approach, inspecting at a periodic interval less than the maximum inspection/repair time allows the repair actions for faults to be deferred to an appropriate future date. If the repair of those fault(s) found at inspection is deferred, the faults' average exposure time would consist of half of the inspection interval (in hours) PLUS the operating time between the inspection and when the fault(s) are repaired. The repair actions must be scheduled so that the faults do not exceed their maximum allowed average exposure time limit.

Maintenance personnel usually defer faults found during an inspection by completing a Non-Routine Maintenance/Inspection Card after the inspection. All faults in the category being inspected should be listed on the card in the "DISCREPANCY" field. The following may be used in the "ACTION TAKEN" field: "Deferred in accordance with the Airworthiness Limitations Section of the engine's ICA, chapter xx, page xx, date xx. Repairs to be completed by calendar date "xxx." The planned date of repair, "xxx," should not cause the faults to remain in the system longer than the maximum average allowed exposure time."

It should be noted that dispatch with these faults is not part of an operator's MEL system. These faults are addressed as part of the operator's scheduled maintenance program; an MEL entry for faults being handled in this manner is not necessary.

If the repair of faults is deferred, maintenance personnel may find new faults during the repair that would not have been recorded on the last inspection's Non-Routine Maintenance/Inspection Card. If the date of these new faults can be "acceptably" determined, their repair can be deferred to a future date by completing a new Non-Routine Maintenance/Inspection Card. (See the discussion on "Impact of Software Integrity of the Maintenance Computer or Display Media on the Periodic Inspection/Repair Maintenance Approach" in section 16.c. of this policy.) If the date of the newly found faults cannot be "acceptably" established, all faults in the subject category must be repaired by the date established at the previous inspection.

d. Faults Found During Non-FADEC System Scheduled Inspections. Invariably, FADEC system fault conditions are found during other maintenance inspections of the aircraft or engine. How should these faults be addressed? The recording of these faults is required; maintenance personnel must complete a Non-Routine Maintenance/Inspection Card for the faults found. This card enters the faults into the operator's maintenance program system.

The following scenario may occur in service: A short time fault category is being handled using the MEL Maintenance Approach or the Periodic Inspection/Repair Maintenance Approach. Upon inspecting the aircraft's maintenance system as part of a short time fault related task (or other engine related maintenance activity) maintenance personnel find the presence of a fault in the long time category. The FAA recommends that the maintenance personnel complete a Non-Routine Maintenance/Inspection Card for all fault(s) found. The "ACTION TAKEN" field on the card should indicate that the long time fault would be repaired as if it had been found at the next periodic inspection for this category. If, when using the Periodic Inspection/Repair Maintenance Approach, a fault is found during other engine related maintenance activity, the card should indicate that the fault would be repaired as if it had been found at the next periodic inspection for this category.

e. Examples of Operator Approaches to FADEC System, TLD Related Maintenance. In-service applications of TLD have used these maintenance approaches individually and in combinations. The following examples are approaches used in service:

(1) Some operators want all FADEC TLD faults except the manufacturer/operator defined dispatch faults to be placed in the short time category; they use an MEL item to allow dispatch with those faults present (for the approved time period). They have a flight deck indication associated with the presence of a fault condition. The flight deck indication is usually a generic indication, such as a light or message that indicates short time fault(s) are present. If a previous fault in that category is still in existence, successive faults do not generate a "new" indication.

(2) Some operators use a combination of the two approaches. They have an MEL listing for short time faults (with an associated generic flight deck indication of the presence of a short time fault), and they use a periodic inspection/repair task for long time faults. The long time faults do not have an associated flight deck indication.

(3) Some operators use two separate periodic inspection/repair tasks to address the short and long time TLD faults. These applications have no flight deck indication associated with the presence of either a short or long time fault condition.

Whatever approach is used, the time limits associated with short and long time operations must be integrated into the ICA for the aircraft. Appendix H of part 25 requires that engine Airworthiness Limitations be included as part of the aircraft ALS. Both Appendix A to part 33 and Appendix H to part 25 require that the FAA approve the ALS and specify required maintenance under §§43.16, 25.1529, and 91.403, unless the FAA has approved an "alternative" program. As shown in Table 2, which lists the time limitations associated with short and long time fault categories, the following note should be included with the ALS entries relating to TLD: "The time limitations specified above may only be changed with approval of the FAA engine Type Certificate Holding Office."

f. Engine TLD Limitations Associated with the MEL and Periodic Inspection/Repair Maintenance Approaches. The engine TLD limitations for short time and long time faults, shown in Table 3, are given in terms of the maximum exposure times for those faults. Table 4 shows this data for the MEL Maintenance Approach or the Periodic Inspection/Repair Maintenance Approach.

g. Extension of Long Time Dispatch Interval. If indicated in the FAA-approved ALS of the engine ICA, the FAA Principal Maintenance or Avionics Inspector (PMI/PAI) may authorize a temporary extension of the long time dispatch interval of up to ten percent of the interval, not to exceed fifty hours, to avoid an aircraft-on-ground (AOG) situation. An example of such an unexpected situation is if the aircraft is diverted because of weather and a revenue flight cannot be made back to the maintenance base because time has run out on the long time dispatch interval. This extension is intended to cover unexpected situations, not to routinely extend the approved interval.

15. SYSTEM REPAIR. When two long time faults combine to yield a short time dispatch category, one of the faults can be repaired, resulting in an upgrade to a long time dispatch category. This flexibility is not intended to relieve the operator from repairing the remaining FADEC fault within the approved interval for long time faults. Similarly, when two short time faults combine to yield a no-dispatch condition, one of the faults may be repaired as long as the remaining short time fault is repaired within the approved short time fault interval.

16. ENGINE - AIRCRAFT INTERFACE. The FADEC system is required to supply fault status and dispatch information to the aircraft. This data must satisfy both engine and aircraft dispatch policies. This policy defines the dispatchable configurations and associated dispatch intervals at an engine level. These configurations and criteria are in accordance with the certification basis for the engine. However, this engine dispatch policy does not prevent the ACO from imposing more restrictive aircraft dispatch criteria if necessary.

a. FADEC System Software Changes Affecting TLD Operations. The TLD fault status and dispatch information is part of the engine ALS. The engine TCHO must review and approve proposed changes to TLD limitations. Changes to the FADEC system software that affect TLD operations must be coordinated as follows:

Changing the fault classifications by adding faults or modifying a given fault category should be done in conjunction with software updates to the EEC. The engine TCHO must review and approve these changes as part of the requirements validation in the software process. TCHO approval and incorporation of the software change constitutes approval of the TLD fault classification change. Changes in fault classification may or may not require changes to the ALS; however, they will always require a change to the engine manufacturer's TLD report if the approved TLD report does not support the classification in a less restrictive dispatch category. The engine manufacturer should coordinate changes to the TLD basis with the aircraft manufacturer. The aircraft manufacturer should coordinate the changes with the responsible ACO.

When an engine manufacturer obtains TLD approval for the engine's FADEC system, the FAA recommends that the manufacturer modify the engine's Installation Instructions to include the following information:

(1) FADEC system fault information relating to TLD;

(2) Time limits associated with the various dispatch allowed, fault categories. The time limits information should indicate if the engine manufacturer assumes a given fault maintenance strategy (MEL Maintenance Approach or Periodic Inspection/Repair Maintenance Approach). The time limits information could also be provided in a manner that allows the installer (and operator) to choose either the MEL or Periodic Inspection/Repair Approach to address FADEC system short time and long time fault maintenance; and

(3) The certification of and a reference to the associated maintenance requirements relating to engine, aircraft or ground support equipment used to store and display fault information and/or FADEC system messages related to TLD operations. Section 16.c. of this policy provides information on associated maintenance requirements.

If information relating to TLD fault categories and time limits is included in documents other than the Installation Instructions, the Installation Instructions should reference those documents.

The FAA also recommends that the engine manufacturer reference the FAA Transport Aircraft Directorate Part 25 Policy Letter, TAD-95-001, dated February 22, 1995, in the engine Installation Instructions or other appropriate documents. The policy discusses the use of an aircraft central maintenance computer (CMC) as the sole means of completing FADEC system maintenance and the certification requirements applying to such a system.

The engine manufacturer may not know the specific applications for the engine at the time of engine certification. Therefore, the engine Installation Instructions should recommend a meeting between the engine and aircraft certification authorities, the AEG, and the engine and aircraft manufacturers. This meeting would be held when the installer chooses the engine and the engine is approved for TLD operations. The meeting would determine if the aircraft manufacturer's approach for complying with this TLD policy is acceptable.

b. Software for FADEC System Fault Messages and Displays.

(1) FADEC system "no dispatch" indications must be provided in the aircraft's flight deck by equipment available for every dispatch. If that display equipment involves the use of software, that software must have a development assurance level equivalent to DO-178B, level A if subsequent operation of the aircraft could lead directly to a catastrophe, or level B otherwise.

(2) When the MEL Maintenance Approach is used for either short time or long time faults, the flight deck display system used to show that the FADEC system has those faults present (for which MEL relief is provided) must be provided on essential equipment. If that equipment involves the use of software, the software must have a development assurance level equivalent to DO-178B, level C.

(3) If a generic message is displayed by an aircraft avionics system, or other media involving the use of software, to show that the FADEC system has either short time or long time faults present, and that category (one or both) is being addressed with a Periodic Inspection/Repair Maintenance Approach, then that generic message must be displayed on essential equipment. If that equipment involves the use of software, the software must have a development assurance level equivalent to DO-178B, level C. (This does not necessarily apply to detailed fault information, discussed in paragraph c. of this section.)

c. Impact of Software Integrity on the Periodic Inspection/Repair Maintenance Approach. When using the Periodic Inspection/Repair Maintenance Approach, engine and aircraft manufacturers and operators have had many questions about the media used to store and/or display information concerning FADEC system faults and how to use that information. These questions focus on the software assurance level used for the aircraft's CMC or other device that stores and/or displays a generic FADEC system fault message and the associated FADEC system fault information.

When using the MEL Maintenance Approach, the flight deck indication (a generic message or light indicating that there is a fault in a particular category) is usually provided by a media with a satisfactory level of software development. When the indicator is a light, software is usually not involved.

FAA Policy Letter TAD-95-001 requires that the media used to store and display maintenance information for critical systems, such as FADEC systems, must have a software assurance level equivalent to DO-178B, level C. Software designers indicate that this could have a significant cost impact on developing many of the current complex CMC systems. Due to this, some applicants have pursued the approach of FADEC systems reporting a generic "long time (and short time, if applicable) fault present" message(s). The details of the particular fault(s) could be reported by a media such as a dumb display (a display not driven by software).

This display may be either connected directly to the FADEC system data buses or it may utilize a "hand shake" with the FADEC system that ensures the integrity of the displayed information. However, if the media that displays the generic message uses software, that software must have adequate software integrity. If this requirement is not met, the FADEC system could report faults, and the maintenance personnel could inspect for faults, but the faults may never be found because the device that stores and displays that information does not have adequate software integrity. Therefore, the FAA recommends that the engine manufacturer include this requirement for adequate software integrity in the engine Installation Instructions.

d. Detailed Fault Information. Maintenance personnel need detailed information about the particular fault(s) present to perform repairs. The following example illustrates the difference between systems that do and do not have adequate software integrity:

Example:

A TLD time limit for the average exposure of the FADEC system to faults in a particular category is 300 flight hours. A periodic inspection at 200 hours is used to find the faults. If faults are found, they are on average 100 flight hours old. Maintenance personnel then schedule their repair within the next 200 flight hours at the next inspection/repair interval. At the time of the repair they confirm that the repair was completed. When confirming the repair, maintenance personnel could find a "new" fault in the particular category being worked. Does this new fault have to be repaired immediately, or can the repair be deferred until the next periodic inspection/repair activity?

(1) When the system that stores and displays the details of the particular faults causing the generic fault indication or message has adequate software integrity, the new fault does not have to be repaired immediately. Repair of the new fault can be deferred until the next periodic inspection/repair activity. This allows inspections and repairs to be completed on a continuous cycle. Faults found at the last inspection/repair activity are repaired during the next periodic inspection/repair activity; any new faults found can be scheduled for repair during the subsequent periodic inspection/repair activity.

Using this approach, if the inspection/repair interval is equal to or less than 2/3 of the maximum allowed average exposure time limit, the average length of time that a fault would be present in the system before repair would be equal to or less than the maximum allowed average exposure time specified for those faults. In this scenario, the system never has to be "cleared" of all faults in a particular category at a particular time. There could always be a fault in the system, and it would be acceptable.

(2) A concern arises when the system that stores and displays the details of particular faults that cause the generic fault indication or message does not have adequate software integrity. In this situation, the maintenance reporting system may not be storing and/or displaying one or more faults in a particular category; those faults could be present in the system, and maintenance personnel would not be aware that there are faults needing repair. In this case, maintenance personnel can still use an overlapping inspection/repair approach, but another requirement is added.

Maintenance personnel must bring the system full-up with respect to all faults in a particular category, at an interval that does not exceed twice the maximum allowed average exposure time for those category faults. This can be done, even though the maintenance reporting system(s) for the fault details may not record and/or display some detailed fault information properly, because the media used to display a generic message for a fault in a particular category is an essential display and has adequate software integrity. This is the reason that a generic indication or message must be displayed on essential equipment. If there is a generic message for a fault category and the aircraft maintenance system does not have details of the fault condition(s), maintenance personnel will start changing components to eliminate the generic fault message. The instructions in the engine maintenance manual (and, if appropriate, the aircraft maintenance manual) must indicate that the aircraft cannot be returned to service until the FADEC system faults causing the generic fault message are repaired, and the generic indication or fault message is no longer displayed.

e. In-Flight Faults. Some faults or fault conditions may only occur in-flight. If this is the case, the engine maintenance manual instructions should indicate that, regardless of whether these faults are in a category addressed by the MEL Approach or an Inspection/Repair Approach, it is to the operator's advantage to begin the repair of these faults several flight hours before the end of the interval. This will allow several flights to be completed and will allow maintenance to verify that their repair actions have been successful before the end of the approved exposure interval.

Example:

Using an inspection/repair maintenance approach to address long time (LT) faults, assume that the maximum average exposure time limit is 500 flight hours. In this case the system must be cleared of all LT faults within a time interval that does not exceed 1000 flight hours. To meet this requirement, the operators should begin the inspection and repair of LT faults at a shorter interval, such as 800 flight hours. After repair actions are taken, the system can complete several flights and be re-inspected to ensure that there are no in-flight LT faults present in the system at the 1000 flight hour point.

f. Configuring the FADEC. Figure 2 shows typical aircraft system configurations involving the aircraft's engine indicating and crew alerting system (EICAS), which may or may not include a multi-function display or maintenance page. It also shows a typical CMC system, which may or may not receive FADEC maintenance data. The following information may be helpful for configuring the FADEC when applying the Periodic Inspection/Repair Maintenance Approach.

(1) The display media for indicating the presence of FADEC inspection/repair category faults must have adequate software integrity. (See section 5 of this policy for the definition of “adequate software integrity.”)

(2) If a generic type message is shown on a multi-function display or maintenance page of EICAS and the CMC does not have adequate software integrity, the information for the generic message must be transmitted through EICAS (shown as a solid line in Figure 2) or directly from the FADEC EEC units (shown as dashed lines in Figure 2).

(3) If the generic type message is displayed on a laptop, the laptop’s processing and/or display of that information must have a software assurance level equivalent to DO 178B, level C. Figure 2 illustrates this as well.

(4) If detailed fault information is displayed on a media, including the data path to that media, that does not have adequate software integrity, the FADEC system must be cleared of all faults in that category without exceeding the maximum allowed average exposure time for those category faults. (This is done by making the necessary repairs until the generic fault message, which shows that there are still faults present, is no longer displayed. If software is involved in the display of the generic fault message, that software must be developed in a manner equivalent to DO-178B, level C standards.)

(5) If the detailed fault information is displayed on a media, including the data path to that media, that does have adequate software integrity, those new faults found during the periodic inspection/repair maintenance activity do not have to be repaired in this period. They may be repaired at a future date, provided that the average exposure time of all faults does not exceed the approved maximum average exposure time for that group of faults.

17. REPORTING SYSTEM.

a. General Reporting Requirements. The applicant must institute a formal, auditable reporting system that will provide periodic reports that will be available to the FAA engine TCHO. The reporting system is a requirement for the TLD approval for the applicant’s engine. Failure to maintain the required reporting system could affect the continued approval of TLD. The FAA will use the reported data to assure that the in-service reliability of the FADEC is consistent with the analysis on which the TLD approval is based. The reporting system should also provide the FAA with an early warning of component trend failures. The applicant’s TLD performance will be reviewed periodically to determine if the reporting system should be modified. Also, the FAA will determine through the periodic review(s) if corrective action relating to TLD, such as adjusting dispatch intervals, is required.

b. Report Contents. The reports must include the following:

(1) A plot of three and twelve month rolling averages of LOTC events per million hours versus accumulated FADEC system hours.

(2) An assessment of the FADEC reliability versus that predicted by the TLD analysis. The assessment should cover the report period and the entire period since initiation of TLD. The assessment should also consider individual component failure rates and other assumptions used in the statistical analysis, for continued validity.

In addition, the assessment should report any unpredicted component failure modes or effects and any recurring problems with detecting, isolating, and repairing faults within the required interval. Items b.(1) and b.(2) may be simplified when a system reaches maturity and the in-service data has substantiated the accuracy of the system model and the results of the statistical analysis.

c. Problem Reporting. The applicant should inform the FAA engine TCHO, as soon as practicable, of potential in-service airworthiness concerns resulting from design, manufacturing, quality or maintenance errors that may affect FADEC system operation or reliability. This information should be transmitted to the FAA even if LOTC rates are not currently affected. This does not change or affect the obligation of type certificate holders or operators to report in-service problems under the CFR.

d. Reporting System Life. Since the factors of concern are not necessarily time dependent, the reporting system for a given FADEC system will be continued as long as the TLD operations are in use. For mature FADEC systems, the frequency of the reporting may be reduced if approved by the TCHO.

Original signed by JJP on 6/29/01
Jay J. Pardee

TABLE 1 - TLD APPROVAL

	APPROVAL ORGANIZATION/GROUP		
	Engine Certification Office	Flight Standards – Aircraft Evaluation Group (AEG)	Flight Standards – Field Inspectors (Principle Maintenance Inspectors (PMI), Principle Avionics Inspector (PAI), Principle Operations Inspector (POI))
Documentation ====>	ICA and TLD Analysis Report as part of engine certification	MMEL and/or Maintenance Review Board Report entries relating to TLD. (Entries must be compliant with TLD Limitations as given in engine ICAs.)	MEL and/or Operator's Maintenance Plan entries relating to TLD. (Entries must be compliant with TLD limitations as given in engine ICAs.)
Part 121 & 135 Operators	N/A	✓	✓
Part 91 Operators	N/A	N/A **	N/A **

** Compliance with the engine ICAs is an Operator responsibility under Part 91 Operations.

TABLE 2 - TYPICAL ALS ENTRY FOR TLD LIMITATIONS

TASK 05-xx-xx-xxx This page block gives the FAA-approved time limits to operate this engine (identify engine manufacturer and model) with control system faults present. These limits are also defined in engine report (identify report number and date), the Engine Control System Time-Limited-Dispatch report.	
Fault Category	Operational Limitation
NO DISPATCH FAULTS	DISPATCH NOT ALLOWED WITH THIS CONDITION PRESENT. Note 1: There must be a flight deck display of the presence of a no dispatch condition.
SHORT TIME FAULTS	DISPATCH IS ALLOWED WITH SHORT TIME FAULTS PRESENT. THE MAXIMUM (AVERAGE – IF APPLICABLE) EXPOSURE TIME OF THE SYSTEM TO THESE FAULTS MUST BE LIMITED TO (insert XXX) FLIGHT HOURS. Note 2: All faults in this short time category must be corrected within a time period, such that (a) each fault in the group does not have an exposure time greater than (insert XXX) hours, OR (b) the average exposure time for short time faults does not exceed (insert XXX) hours. Also, it is noted that the time limitations contained herein with respect to short time FADEC system faults may only be changed with approval of the FAA engine TCHO. • If an MEL Maintenance Approach is used for this fault category, there should be an appropriate generic flight deck display of the presence of a short time fault condition(s). • If a Periodic Inspection/Repair Maintenance Approach is used, the system should be inspected for short time faults at an interval, such that if faults are found, they can be repaired so that the average length of time that a fault is present in the system (average exposure time) does not exceed the specified (insert XXX) hour limitation.

TABLE 2 - TYPICAL ALS ENTRY FOR TLD LIMITATIONS (CONTINUED)

LONG TIME FAULTS	DISPATCH IS ALLOWED WITH LONG TIME FAULTS PRESENT. THE MAXIMUM (AVERAGE – IF APPLICABLE) EXPOSURE TIME OF THE SYSTEM TO THESE FAULTS MUST BE LIMITED TO (insert YYY) FLIGHT HOURS. Note 3: All faults in this long time category must be corrected within a time period, such that (a) each fault in the group does not have an exposure time greater than (insert YYY) hours, OR (b) the average exposure time for long time faults does not exceed (insert YYY) hours. Also, it is noted that the time limitations contained herein with respect to long time FADEC system faults may only be changed with approval of the FAA engine TCHO. • If an MEL Maintenance Approach is used for this fault category, there should be an appropriate generic flight deck display of the presence of a long time fault condition(s). • If a Periodic Inspection/Repair Maintenance Approach is used, the system should be inspected for long time faults at an interval, such that if faults are found, they can be repaired so that the average length of time that a fault is present in the system (i.e., average exposure time) does not exceed the specified (insert YYY) hour limitation.
Note 4: The FAA Principal Maintenance or Avionics Inspector may approve an extension, not to exceed 50 flight hours, to the long time dispatch limitation if repairs cannot be made due to extenuating circumstances.	
Note 5: The applicant to add the following words here: “THE TIME LIMITATIONS SPECIFIED ABOVE MAY ONLY BE CHANGED WITH THE APPROVAL OF THE FAA ENGINE TYPE CERTIFICATE HOLDING OFFICE.”	