2014-01-2119

Impact of engine certification standards on the design requirements of More-Electric Engine electrical system architectures

Steven Fletcher, Patrick Norman, Stuart Galloway, and Graeme Burt
University of Strathclyde

Abstract

The development of the More-Electric Engine (MEE) concept will see an expansion in the power levels, functionality and criticality of electrical systems within engines. However, to date, these more critical electrical systems have not been accounted for in existing engine certification standards. To begin to address this gap, this paper conducts a review of current engine certification standards in order to determine how these standards will impact on the design requirements of More-Electric Engine (MEE) electrical system architectures. The paper focuses on determining two key architectural requirements: the number of individual failures an architecture can accommodate and still remain functional and the rate at which these failures are allowed to occur. The paper concludes by discussing how the derived failure rates begin to define a set of design requirements for MEE electrical architectures, considering various operating strategies, and demonstrates their application to example MEE electrical system architecture designs.

Introduction

The development of the More-Electric Engine (MEE) is potentially one of the next key steps in the greater electrification of aircraft systems [1, 2, 3]. The MEE concept focuses on the replacement of mechanically driven engine accessories such as fuel pumps and oil pumps with electrical equivalent systems, with possible benefits including reduction in overall system weight and size, and improved efficiency and maintainability [1, 2]. Clearly these design aspects are of high importance given the targets for increased fuel efficiency improvement for future generations of aircraft [4, 5] and reduction in aircraft maintenance requirements [4, 6] (including a desire for no unscheduled maintenance of aircraft by around 2020 [6]).

The inclusion of these electrical accessories will mean that the engine electrical power is likely to become more extensive than before, both in terms of cabling paths and power levels. The types of electrical devices which could be used within a MEE system are illustrated within Figure 1. These will also be far more critical to the engine's continued operation. However this increasing degree of importance for electrical systems has yetto be accounted for in existing engine certification standards which, with the exception of providing requirements for electrical engine control systems (EECS) design, do not explicitly cover electrical engine accessories. Therefore, there is a timely requirement to consider the certification requirements of MEE systems.

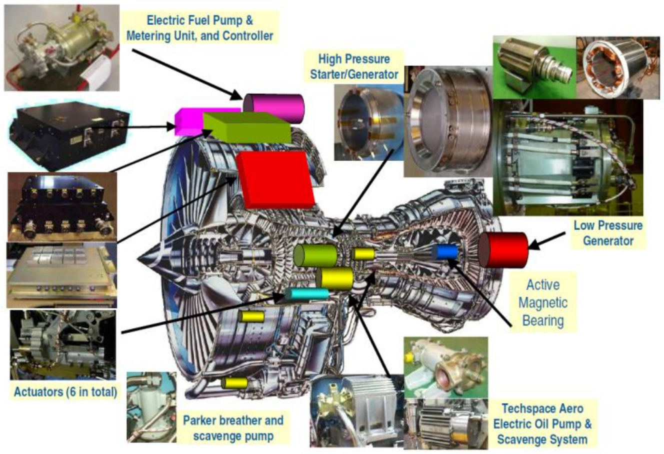


Figure 1. Example More-Electric Engine system with hardware from the ESVR demonstrator [3]

This paper will consider the MEE from the perspective of its electrical system architecture design. Two of the key requirements for the design of a certifiable architecture relate to reliability and redundancy, namely the number of individual failures an architecture can accommodate and still remain functional and the rate at which these failures are allowed to occur. In order to define these design criteria for MEE electrical architectures, the paper conducts an in depth review of relevant engine certification standards, such as CS-E [7]. From this, the paper identifies where clear guidance is given within current standards, and also where they must be further developed to provide adequate coverage on MEE accessories. Where these gaps currently exist, the paper infers design requirements from existing functional descriptions contained within the standards in order to propose necessary design requirements.

The paper concludes by proposing a comprehensive set of design requirements for MEE electrical architectures for various operating strategies. The value of these requirements to future design programs is then demonstrated through their application to the feasibility evaluation of example MEE electrical system architecture designs.

Review of engine certification standards and reliability requirements

In order to properly quantify the certification requirements for new electrical loads it is important to understand the context of existing standards and their high level functional requirements. The following sections will therefore review the key certification standards for engine systems. The European Aviation Safety Agency's (EASA) Certification Specifications for Engines (CS-E) [7] and large aeroplanes (CS-25) [8] are used as the main point of reference within these sections however note that similar certification regulations do exist from the Federal Aviation Administration (FAA), with FAR part 25 [9] referring to transport category airplane and FAR part 33 [10] detailing the FAA regulations for aircraft engines. The sections define acceptable failure rates for various 'engine effects' before consideration is given to which of these main failures may be influenced by the engine electrical system. This enables the derivation of design requirements for the various electrical components within this system as will be illustrated.

Engine Failure Types and Acceptable Failure Rates

Information from the standards related to the classification of different failure types and the maximum acceptable rate at which these are allowed to occur is presented in the following subsections.

Acceptable Maximum Failure Rates

Table 1 describes the acceptable maximum probability of occurrence for various failure classifications. Failures are classified based on their severity and likely impact on the aircraft. Clearly the aircraft should be designed in such a way so the failures of increasing severity occur less frequently.

Note that the reliability specifications within AMC 25.1309 [8] define an additional category. This is:

Extremely Improbable Failure Conditions: Extremely Improbable Failure Conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type, and have a probability of the order of 1 x 10^{-9} or less. Faults classified as 'Catastrophic Failure Conditions' (where loss of hull and/or multiple fatalities would be expected if the fault were to occur [8]) must be shown to meet this target.

For MEE applications, the reliability of the electrical accessories and supporting electrical architecture is shaped by these general targets as described in later sections.

Table 1. Summary of CS-E failure rate specifications [7]

General failure type classification	**Probability (average failures per flight hour)**	**General description**	**Engine specific terminology**
Extremely remote	10^{-7} to 10^{-9}	Unlikely to occur when considering the total operational life of a number of aircraft of the type in which the Engine is installed, but nevertheless, has to be regarded as being possible.	**Hazardous Engine Effects**
Remote	10^{-5} to 10^{-7}	Unlikely to occur to each aircraft during its total operational life but may occur several times when considering the total operational life of a number of aircraft of the type in which the Engine may be installed.	**Major Engine Effects**
Reasonably Probable	10^{-3} to 10^{-5}	Unlikely to occur often during the operation of each aircraft of the type but which may occur several times during the total operational life of each aircraft of the types in which the Engine may be installed.	**Minor Engine Effects**

Examples of various 'Engine Effects'

The following sections provide examples of the types of defined within AMC-E 510 [7] as 'Hazardous', 'Major' and 'Minor'. Whilst these are primarily designed to regulate the performance of non-electrical engine system, various entries may still be relevant to MEE accessories and architectures. For example, the 'non-containment of high-energy debris' is appropriate for electrical machines, particularly any high-speed designs that may be considered.

Hazardous Engine Effects

Hazardous engine effects include:

1. Non-containment of high-energy debris

2. Generation and delivery of toxic products caused by abnormal engine operation sufficient to incapacitate the crew or passengers during the flight.

3. Significant thrust in the opposite direction to that commanded by the pilot.

4. Uncontrolled fire.

5. Complete inability to shut the engine down.

Major Engine Effects

Major engine effects include:

1. Controlled fires (i.e., those brought under control through engine shutdown or onboard extinguishing systems).

2. Case burn-through where there is no propagation to Hazardous Engine Effects.

3. Release of low-energy parts where there is no propagation to Hazardous Engine Effects.

4. Thrust in the opposite direction to that commanded by the pilot (below the level defined as hazardous).

5. Generation of thrust greater than maximum rated thrust.

6. Significant uncontrollable thrust oscillation.

Minor Engine Effects

A minor engine effect is an engine failure which only results in a partial or complete loss of thrust and associated secondary engine services. As these failures are expected to occur in service, the aircraft should be capable of controlled flight following an event of this nature.

Failure conditions and operating strategies influenced by the electrical architecture design

Based on the above review of failure types, two general design aspects have been identified which drive the reliability requirements of an engine system. These can be broadly categorised as:

- The reliability of the engine itself and the components it contains (*physical failures*)

- The reliability of control systems within the engine (‘*control failures which lead to unwanted physical effects*’)

The following sections will identify and describe two key failure cases which are influenced by the MEE electrical system architecture design. In each case, two important pieces of information are sought after from an architectural perspective. These are:

- What is the maximum allowed rate of occurrence for the given failure condition?

- How many redundant electrical supply paths are required to loads/supply points to prevent this failure occurring?

The following review will be carried out with these questions in mind.

Single engine in-flight shutdown

ETOPS regulations define performance requirements for any aircraft flying long distance routes or beyond certain distances from a suitable airport. The FAA ETOPS requirements are summarised in [9], with the equivalent EASA requirements published within [12]. Both sets of standards are primarily concerned with the operation of twin engine aircraft and stipulate performance requirements of the remaining healthy engine following the failure of the other engine. Approval for ETOPS is based on the time within which a second engine failure would be extremely remote, where the time relates to the flight time to the nearest suitable airport with the aircraft travelling at a single engine speed.

These regulations can influence an electrical architecture in two main ways: the provision of backup electrical supplies and the engine in-flight shutdown (IFSD) rate. The relevant sections from the regulations are discussed below.

ETOPS electrical system requirements

The following relevant ETOPS electrical system requirements are derived from [9] (Chapter II, section 7). Note that paragraph numbers have been retained for ease of cross referencing with [9]. These requirements are:

(6) During extended duration single-engine operation, the remaining secondary power (electrical, hydraulic, pneumatic) will continue to be available at levels necessary to permit continued safe flight and landing.

(7) In the event of any single failure, or any combination of failures not considered Extremely Improbable, electrical power should be provided for essential flight instruments, warning systems, avionics, communications, navigation, required route or destination guidance equipment, supportive systems and/or hardware as well as any other equipment deemed necessary to continue safe flight and landing at an ETOPS en-route alternate aerodrome. Information provided to the flight crew should also be of sufficient accuracy for the intended operation (typical functions are described in [9]).

(8) Three or more reliable and independent electrical power sources should be available. As a minimum, following failure of any two sources, the remaining source should be capable of powering the items specified above [in (7)]. When one of the 3 independent electrical power sources is time-limited (e.g. batteries), this power source should have a capability to provide sufficient power for the items listed above for continued flight and landing to an ETOPS en-route alternate aerodrome.

(9) For ETOPS approvals above 180 minutes, the following additional requirements exist:

1. Unless it can be shown that the failure of all 3 independent power sources required by paragraph (8) above is extremely improbable, following failure of these 3 independent power sources, a fourth independent power source should be available that is capable of providing power to the essential functions referred to in paragraph (7) for continued safe flight and landing to an adequate ETOPS en-route alternate aerodrome.

Depending on the criticality of engine accessories, these requirements may impact the necessary level supply path redundancy.

ETOPS engine IFSD rates

Both [9] and [12] provide examples of the average IFSD rate which engines on a twin engine aircraft should achieve in order to meet certain ETOPS authorisation levels. The clearest definition (in the opinion of the authors) for the different ranges of applications is provided by EASA [9] (although the FAA and EASA guidance is generally consistent). These various levels are summarised below within Figure 2 and Figure 3.

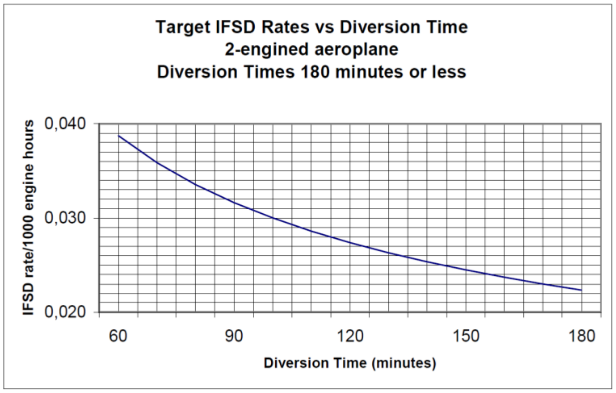


Figure 2. EASA derived ETOPS curve for IFSD rates against diversion time for diversions of less than 180 minutes [9]

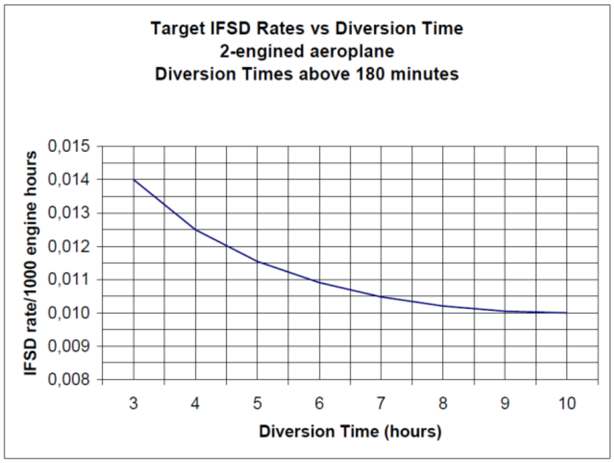


Figure 3. EASA derived ETOPS curve for IFSD rates against diversion time for diversions above 180 minutes [9]

Interpreting the above per engine IFSD rates from EASA; these are generally derived from two main influencing factors: the target reliability for twin engine failure and the diversion time to a safe landing area. The relationship between these factors can be simply represented as

$$IFSD\ rate = \sqrt{\frac{overall\ probability\ target}{Diversion\ time}} \qquad (1)$$

Within (1), the overall reliability target will be around a probability of 1×10^{-9} failures per flight hour – this being the maximum probability for the occurrence of any catastrophic failures (although this target appears to vary at different points - for example two different targets are provided for the 3 hour diversion within Figure 2 and Figure 3). Within Figure 3, for 10 hours diversion time to be acceptable the overall probability target is equal to 1×10^{-10} failures per flight hour (i.e. a rate of 1×10^{-10} failures per flight hour for 10 hours). A plot based on (1) (which is the authors' simplification of the IFSD rate calculation) with an overall target of 1×10^{-9} failures per flight hour is shown in Figure 4 for reference. Note that the resultant IFSD rate is lower (for the shorter diversion times at least) than the EASA plot in Figure 2 highlighting that this overall target can be higher than 1×10^{-9} failures per flight hour.

The impact of these various failure rates will be to place different requirements on the engine reliability, and hence on the components responsible for maintaining continued engine operation.

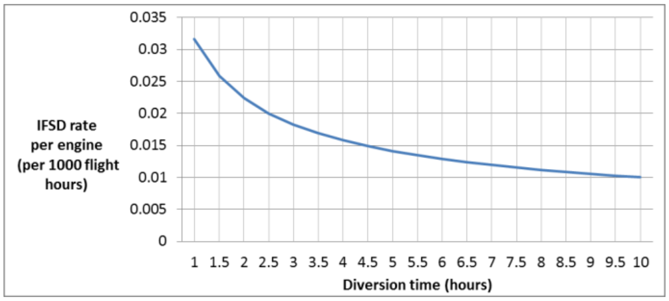


Figure 4. Example IFSD rate based on equation (1) with a twin engine failure target of 1×10^{-9}

Summary of requirements for prevention of engine IFSD

The above sections have shown that there is some variability in the allowed IFSD rate of engines, with this mainly depending on the whether ETOPS certification is required and if so, the desirable 'diversion time' of the given aircraft.

CS-E classes engine failure (provided no additional external issues occur) as a minor engine effect and so on this basis its allowed failure rate ranges anywhere between 1×10^{-3} to 1×10^{-5} failures per flight hour. Bringing in the requirements for ETOPS from Figure 2, Figure 3 and Figure 4 narrows this range to 3.9×10^{-5} to 1×10^{-5} failures per flight hour, depending on required diversion time. This is this allowed failure rate of the overall engine system inclusive of the combined failure rate of relevant electrical components along with all other engine components which would contribute to an engine failure.

To determine the impact this has on the engine electrical system and its components requires two main steps:

1. A qualitative failure analysis of the electrical system to assess which fault types will cause an engine IFSD to enable the allowed probability of these occurring to be assessed and quantified.

2. A quantitative failure analysis of the non-electrical engine parts which could result in an engine shutdown to enable the allowed electrical system failure rate to be determined.

In the absence of the information in which to carry out step 2 above, an alternative approach, or "rule of thumb", could be to design the electrical system such that the probability of failures in step 1 are insignificant compared to the overall engine failure rate (by say an order of magnitude).

The review of the standards did not present clear guidance on the need for redundant supply paths for engine accessory loads, with specific reference only being made to loads such as flight instruments and avionics. However some provision is made for additional flight critical equipment where the standards state '*any other equipment deemed necessary to continue safe flight*'. Therefore a judgement will need to be made as to whether, following the failure of one engine, electrical engine loads critical to its ongoing operation would come into this category. It worth noting that in either case it may be challenging to achieve the quantitative reliability requirement with a single channel electrical supply.

Engine control system failure

The main means of engine control is provided by the Electric Engine Control System (EECS). Therefore much of the certification standards on engine control relate to the operation of this system. One failure mode which the standards make specific provision for is loss of thrust/loss of power control (LOTC/LOPC). Reference [13] defines LOTC/LOPC (hereafter just referred to as LOTC) event as either:

- The loss of ability to modulate power or thrust from idle to 90% maximum rated power or thrust at given flight condition *or*
- The oscillation of engine thrust in an unacceptable manor

Reference [13] and AMC E 1030 within CS-E [7] state that these events should not *on average* (although the *instantaneous* rate can be temporary higher as discussed in the following section) occur at a greater rate than 10 in every million flight hours (1×10^{-5} failures/flight hour) or an alternative appropriate rate for the given application. Whilst LOTC is not directly referred to within the above examples of 'Engine Effects', the above failure rate and the reference to '*unacceptable thrust oscillation*' would suggest that it is a 'Major Engine Effect'.

As the engine thrust is controlled via the EECS and it is this system (and its electrical supply) which should ensure these conditions are met. This is reflected in CS-E where all statements which refer to the prevention of LOTC relate to the performance and reliability of the EECS.

In addition to the quantified failure rate for EECS (with respect to LOTC), prescriptive statements are made within [13] regarding the requirement for redundant channels in the EECS regardless of the failure rate of any single channel. Those relevant statements and their potential impact on a system's architecture are discussed below.

CS-E 50 (c) *Engine Control System Failures.* The Engine Control System must be designed and constructed so that:

(1) The rate for Loss of Thrust (or Power) Control (LOTC/LOPC) events, consistent with the safety objective associated with the intended aircraft application, can be achieved.

(2) In the Full-up Configuration (*i.e. the system without any faults present*), the system is essentially single fault tolerant for electrical and electronic failures with respect to LOTC/LOPC events.

(3) Single Failures of Engine Control System components do not result in a Hazardous Engine Effect.

CS-E 50 (h) *Aircraft Supplied Electrical Power*

(1) The Engine Control System must be designed so that the loss or interruption of electrical power supplied from the aircraft to the Engine Control System will not:

(i) Result in a Hazardous Engine Effect.

(ii) Cause the unacceptable transmission of erroneous data.

The effect of the loss or interruption of aircraft supplied electrical power must be taken into account in complying with CS-E 50 (c)(1).

Two key messages can be taken from the above statements:

1. Dual redundancy as a minimum is required in the EECS itself
2. Dual redundancy as a minimum is required in the supply of electrical power to the EECS

Whilst this redundancy is critical to meeting overall reliability standards, the multiple channels can actually increase the probability of a single failure occurring (although not one which would interrupt the operation of the EECS). In order to prevent an increase in system downtime and maintenance, the EECS can be dispatched with an existing fault for a limited period of time [14]. The approach to managing this dispatch is described in the following section.

Management of control system faults through time limited dispatch

Time limited dispatch (TLD) describes an operating philosophy whereby aircraft are allowed to dispatch with faults present for a set period of time [14]. Within CS-E, specific reference is made to the EECS and the use of the redundancy present within these systems to continue aircraft operation (albeit with reduced levels of redundancy) for a limited period of time whilst still meeting appropriate reliability targets.

CS-E 1030 (a) states that "*if approval is sought for dispatch with Faults present in an Electronic Engine Control System (EECS), a time limited dispatch (TLD) analysis of the EECS must be carried out to determine the dispatch and maintenance intervals*". In particular, the system architect must consider all fault types to assess whether the system is capable of meeting certain design criteria with that fault present. As well as continuing to meet all the usual functional requirements of the engine operation, the additional rules which apply to systems which would be dispatched with faults present include:

CS-E 1030 (b) For each dispatchable configuration it must be shown by test or analysis that a further single failure in the EECS will not produce a Hazardous Engine Effect.

CS-E 1030 (c) The time-weighted-average of the Full-up Configuration and all allowable dispatch configurations with faults, must meet the Loss of Thrust Control / Loss of Power Control (LOTC/LOPC) rate for the intended application(s).

These rules present new requirements for the engine:

1. An additional layer of redundancy over and above that provided to meet failure and LOTC requirements may be required to meet TLD conditions.

2. Following a single failure, the remaining healthy portion of the engine systems must be able to meet a dedicated TLD probability requirement.

AMC E 1030 provides further guidance to help quantify some of the additional design constraints. First it describes four general categories to describe a faulted or degraded system with respect to dispatch. These categories are:

(a) **No Dispatch**. Configurations that do not comply with CS-E 1030 (b) and/or (c) or do not qualify for another category should be categorised as No Dispatch.

(b) **Short Time Dispatch**. Configurations that comply with CS-E 1030 (b) and/or (c) and satisfy the following condition should be categorised as Short Time Dispatch: the computed LOTC/LOPC rate with the Fault(s) present is less than or equal to an upper limit that has been set at 10 times the fleet-wide average reliability criteria or “average LOTC/LOPC rate” for the installation. (The LOTC/LOPC rates for different installations may be found in AMC 20-3.) However, even if the Long Time Dispatch LOTC/LOPC rate is met, configurations where the EECS has reverted to essentially single channel operation or has lost a significant degree of redundancy should be categorised as Short Time Dispatch.

(c) **Long Time Dispatch**. Configurations that comply with CS-E 1030 (b) and/or (c) and satisfy the following condition should be categorised as Long Time Dispatch: the computed LOTC/LOPC rate with the Fault(s) present is less than or equal to 75 percent of an upper limit that has been set at 10 times the fleet-wide average reliability criteria or “average LOTC/LOPC rate” for the installation. (The LOTC/LOPC rates for different installations may be found in AMC 20-3.)

(d) **Applicant defined dispatch**. This category is for faults that do not have an impact on the LOTC/LOPC rate.

Information is also given on the acceptable length of time which these various fault types may be present on a system. This is shown in Table 2. These repair times give an impression of allowable maintenance periods following any system failure. Guidance on how these times impact the required reliability of system components within a ‘dispatchable’ system with respect to LOTC is provided within AMC E 1030 section (4) on Time Limited Dispatch Analysis. Alternatively, part (b) above states that the maximum LOTC rate for the dispatched system is 10 times the fleet-wide average. For the example figures given, the maximum ‘instantaneous’ (as it called in [14]) LOTC rate is therefore 100 events per million flight hours.

Table 2. An Example of Operating Times for TLD Operations [7]

Experience Level	No dispatch category	Short time faults (max operating time)	Long-time fault category – max operating time
Entry Level	No Flight Allowed	125 Engine flight hours.	250 Engine flight hours.
Mature Level	No Flight Allowed	Depends on system analysis	Depends on system analysis

Finally, AMC E 1030 provides a simplified decision making process to give guidance on how various system fault types may be dealt with. This is presented in Figure 5. Note that the Master Minimum Equipment List (MMEL) is the collective equipment required for take-off.

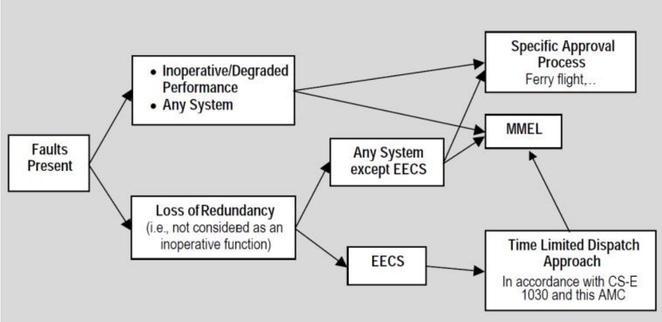

Faults Present
• Inoperative/Degraded Performance
• Any System
Loss of Redundancy
(i.e., not consideed as an inoperative function)
Any System except EECS
EECS
Specific Approval Process
Ferry flight,..
MMEL
Time Limited Dispatch Approach
In accordance with CS-E 1030 and this AMC

Figure 5. Different possible ways of managing dispatch with engine faults [7]

Within Figure 5 it can be seen that all initial EECS faults are considered to cause a loss of redundancy rather than any performance degradation. This is the key factor will enables the system to continue to operate correctly and safely with faults present. For TLD to be applied to anything other than the EECS then, similar levels of redundancy must be available.

Summary of requirements for the prevention of engine control system failure

The need to prevent LOTC events places requirements on the EECS load and its electrical supply. These requirements are both qualitative (in terms of required layers of redundancy) and quantitative (in terms of prescribed failure rates under different conditions).

The main quantitative certification requirement is that LOTC events should on average occur at a rate no greater than 10 in every million flight hours (although there is some scope for this to change based on the application as discussed in [15]). Therefore any failure mode of the EECS which causes this to occur must have a probability of this or lower for normal system design. This design specification is referred to as the time weighted average rate, which allows some scope for temporarily greater LOTC event rate which is a maximum of 10 times the average LOTC rate, which is 100 events per million flight hours for the general allowed LOTC rate. This higher rate would occur under TLD operation and all dispatchable configurations would be required to meet this specification.

The failure rate of the electrical supply to the EECS would also need to meet this requirement to ensure continued availability of this system. Therefore it can be derived that the EECS electrical supply should have an average failure rate of no greater than 1×10^{-5} failures/flight hour. As the failure of the EECS load itself would also need to be accommodated within this rate, it is reasonable to assume that the failure rate of the electrical supply would have to be even lower.

In terms of qualitative design requirements, single fault tolerance is required in the 'full-up configuration'. However this is not a stipulation for TLD. Instead any single channel operation would be placed in the 'short-term dispatch/repair' category, which for entry level systems is 125 hours. This single channel would also be required to match the instantaneous LOTC event rate which is a maximum of 100 events per million flight hours.

Electrical supply options to achieve these design objectives can vary with application as discussed in [15]. These include the use of dedicated engine power sources for EECS, aircraft supplied power (or at least engine power sources also connected to the aircraft) or a combination of both options.

Outstanding questions on the certification of MEE electrical systems

It is clear from the reviews in the previous sections that, with the exception of the EECS supply, direct information regarding the required failure rate of the engine electrical system is not explicitly provided within the certification standard. This puts an onus on the architecture designer to infer requirements from the more general functional specifications. As discussed previously, this requires a full failure analysis of the engine electrical system to ensure all failure modes are accounted for.

Furthermore, the optimal means of managing these electrical system faults (from an aircraft dispatch perspective) requires investigation. CS-E provides 3 general options (as shown in Figure 5) for this and these are:

1. No dispatch
2. Master Minimum Equipment List (MMEL) – where all equipment required for take-off must be functional
3. Time limited dispatch – as described for EECS systems

Within this list, AMC 1030 suggests that the MMEL approach should be taken for anything other than EECS faults. However, in a similar way to that of the EECS, there may be an opportunity to maximise the availability of the electrical system and make best use of redundant supply paths through a TLD type operating approach. This would also provide guidance on the duration which failure electrical equipment is allowed to remain on the engine before maintenance is requirement. More specifically, provided there is no impact on the LOTC rate, some 'Applicant defined dispatch' time intervals could be defined by the systems integrator in terms of maintenance scheduling for the electrical system.

The following section provides examples of how a degraded electrical system might compare to certification requirements.

Comparison of example MEE architecture with derived reliability requirements

In order to assess the compliance of a MEE electrical system architecture with the above requirements, it is necessary to carry out a reliability study of the architecture being considered. An example of how this can be carried out will be presented within this section. The analysis will also consider some degraded architectures, where certain supply routes are inoperable, in order to establish the feasibility of any TLD operation of the electrical system.

The outline electrical architecture to which this analysis will be applied is shown in Figure 6. This architecture contains two generators, which supply both the airframe and the engine accessory loads (supplying independent channels within each). Two loads (L1 and L2) are considered for the purpose of this analysis. It is assumed that both of these loads are critical to the continued operation of the engine (an electrical engine fuel pump for example) and the failure of these loads, or the electrical supply to them, would cause an IFSD event. Each load has two supply routes (S_2 and S_3 for L1, S_1 and S_4 for L2) via the two intermediate busbars (Bus_1 and Bus_2) and bus-tie contactor (BT_1). Finally, it is assumed that each load would require its own custom AC power supply and therefore to provide this, power converters would need to be integrated into this architecture at appropriate locations (also accommodating the needs of the airframe). Different conversion options are discussed within a later section.

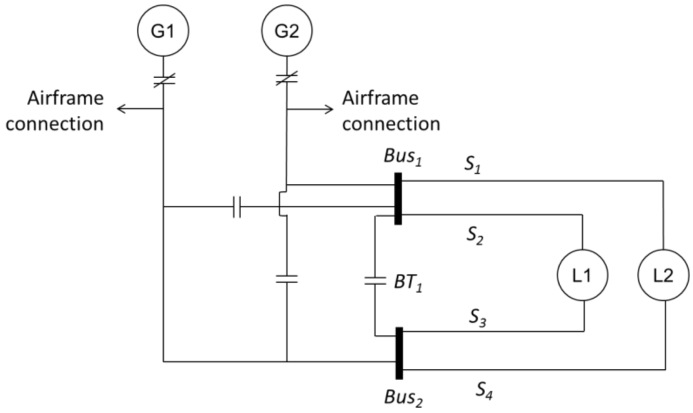


Figure 6. Outline MEE electrical system architecture

Reliability analysis of full-up electrical architecture

Analysing a network with multiple but dependent backup paths such as that in Figure 6 this can be complex, particular when accommodating the large number of potential failure events. To analyse these failure conditions, this section will employ fault tree analysis and will apply Boolean reduction to simplify the developed equations describing the main failure modes of the architecture. These techniques for fault analysis are described within [16]. More specifically, the application of Boolean reduction allows the 'minimal cut set' to be determined

– this being the minimum number of individual failures which must occur in order to cause the event of interest.

The purpose of the examples within this section is to illustrate the methodology for analysing electrical networks. Therefore to simplify this illustration, contactor failures (except from the bus tie contactor) and cable failures have been excluded. Note these should however be considered at a later stage for an entirely accurate calculation of failure rate. Applying this analysis to the architecture in Figure 6 to the failure of the fuel pump supply initially gives a minimal cut set of

$$P(L_1) = G_1.G_2 + Bus_1.Bus_2 + S_2.S_3 \qquad (2)$$

Probability of failure to where all terms refer the failure rate of the components labelled in Figure 6 and G_1 and G_2 include the failure rate of the associated generator control unit and/or power electronic interface. From (2) a fault tree can be drawn and this is shown in Figure 7.

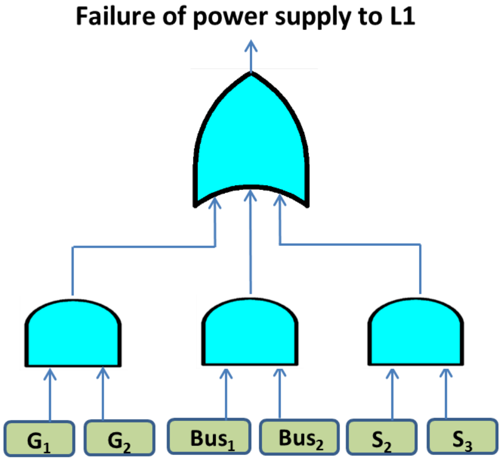
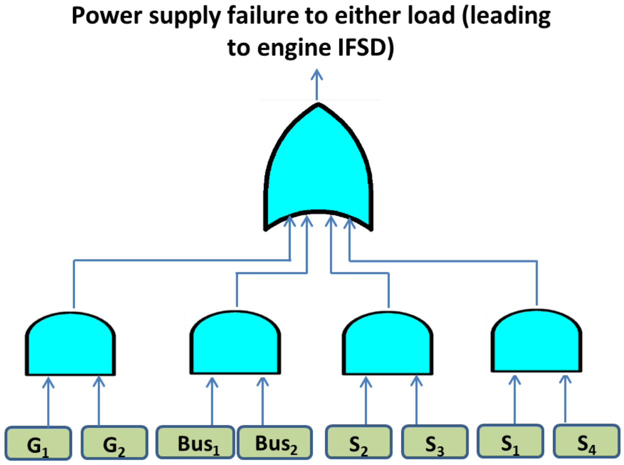


Figure 7. Simplified fault tree for the failure of electrical supply to L1

A similar fault tree can be drawn for L2, with the substitution of supply paths as appropriate. Finally, an equation for the rate of either of these events occurring can be developed, which for the purpose of this analysis would also cause an engine IFSD event. This equation is

$$P\ (L_1\ or\ L_2) = G_1.G_2 + Bus_1.Bus_2 + S_2.S_3 + S_1.S_4. \qquad (3)$$

The fault tree based on (3) is shown in Figure 12. Later sections demonstrate how these fault tree and/or equations can be used to compare the network failure rate with the certification requirements.



Power supply failure to either load (leading to engine IFSD)
G_1
G_2
Bus_1
Bus_2
S_2
S_3
S_1
S_4

Figure 8. Simplified fault tree for the failure electrical supply to L1 or L2

Reliability analysis of degraded electrical architectures

The following two sections provide analysis to describe how the calculations for a fuel or oil pump electrical supply failure vary with certain supply path inoperable. These cases will highlight changes in system reliability under possible time limited dispatch scenarios.

Single inoperable supply path - dispatch scenario 1

The first dispatch scenario which has been analysed is, as illustrated in Figure 9, the failure of one of the redundant supply path, S_1.

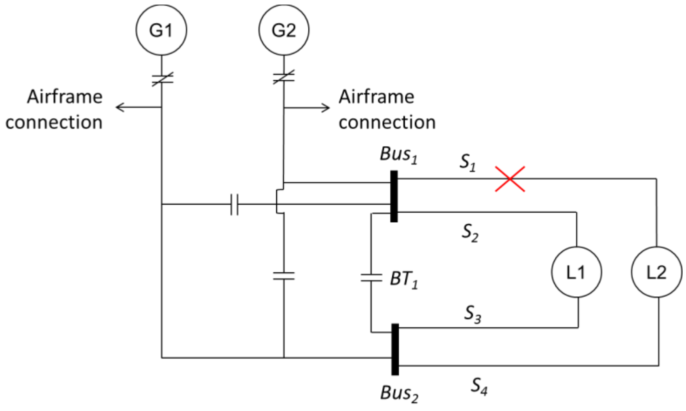


Figure 9. Outline MEE electrical system architecture with one supply path inoperable (dispatch scenario 1)

The equation to describe the probability of supply failure in this new configuration can be developed by simply removing the S_1 term from (3). This equation becomes

$$P\ (L_1\ or\ L_2) = G_1.G_2 + Bus_1.Bus_2 + S_4 + S_2.S_3 \qquad (4)$$

The fault tree based on (4) is shown in Figure 10. Note that the removal of S_1 means that it no longer multiplies the parallel path of S_4, which in turn is likely to increase the overall failure rate.

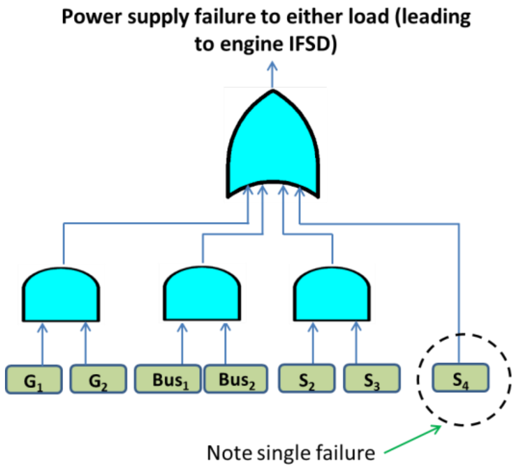

Power supply failure to either load (leading to engine IFSD)
G_1
G_2
Bus_1
Bus_2
S_2
S_3
S_4
Note single failure

Figure 10. Simplified fault tree for the failure electrical supply to either L1 or L2 with supply path S1 inoperable

Two inoperable supply paths - dispatch scenario 2

The second dispatch configuration considered looks at further degradation of the architecture, with both supply paths S_1 and S_2 inoperable. This configuration is illustrated in Figure 11.

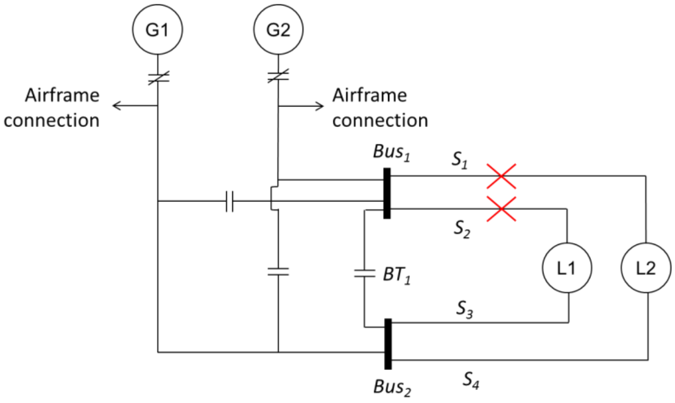


Figure 11. Outline MEE electrical system architecture with two supply paths inoperable (dispatch scenario 2)

Similarly to the previous case, the equation for the supply failure in this configuration can be developed by removing terms S_1 and S_2 from (3). This equation becomes

$$P\ (L_1\ or\ L_2) = G_1.G_2 + Bus_1.Bus_2 + S_3 + S_4 \qquad (5)$$

The fault tree based on (5) is shown in Figure 12. The figure highlights that the removal of both S_1 and S_2 now means that the failure rates of S_3 and S_4 now sum to increase the overall failure rate.

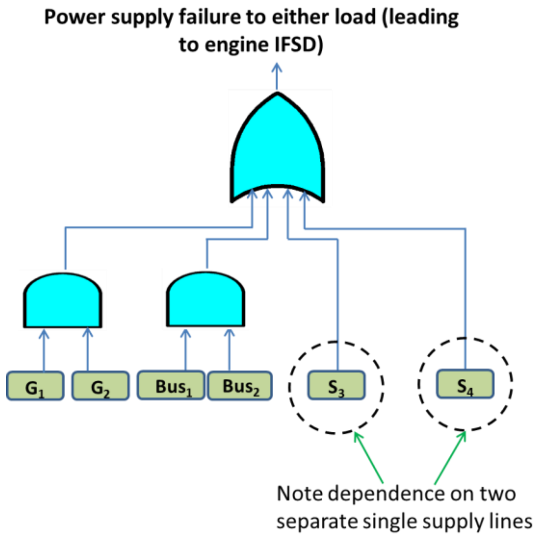

Power supply failure to either load (leading to engine IFSD)
G_1
G_2
Bus_1
Bus_2
S_3
S_4
Note dependence on two separate single supply lines

Figure 12. Simplified fault tree for the failure electrical supply to L1 or L2 with supply paths S_1 and S_2 inoperable

Application of example failure rate data and comparison with requirements

To enable a comparison to be made between the derived electrical system requirements and the architectures analysed previously, this section will define the components within the architectures and apply example failure probability data to the fault tree equations.

Two configurations of the general architecture from Figure 6 will be considered. Configuration 1 is a central conversion architecture, where Bus_1 and Bus_2 represent rectifier stages on to a DC bus and S_{1-4} represent inverter stages, each providing a custom AC supply to the connected load. Configuration 2 is a more localised conversion strategy where $Bus_{1,2}$ are AC distribution busbars and S_{1-4} represent back to back rectifier-inverters, again providing a custom AC supply to the loads. The full up and degraded conditions are assessed for each configuration.

The representative failure probability data used to analyse the architectures is shown in Table 3. This data is derived from a range of sources, as indicated by the references within the table. These have been applied to equations (2) to (5) in order to estimate the probability of the failure events, enabling a comparison with requirements. The data is applied differently for the two architecture configurations. For Configuration 1: $G_{1,2}$ are the sum of the generator and GCU failure rates, $Bus_{1,2}$ are equal to the rate of a rectifier or inverter failure (with a rectifier stage here) and lines S_{1-4} are also equal to the rate of a rectifier or inverter failure (with the inverter stage here). For Configuration 2: $G_{1,2}$ are the same as above, $Bus_{1,2}$ are equal to the rate of the conductor failure and lines S_{1-4} are equal to the rate of a rectifier or inverter failure squared (with both the rectifier and inverter stages now on this line). Note that AC and DC contactors are included in this table to accommodate either an AC or DC bus tie. Results are presented in Table 4.

Table 3. Summary of applied component failure rate data

Component type	Failure Rate (failures per flight hour)
Wound field generator	5 x10^{-4} [17]
Generator control unit (GCU)	2 x10^{-4} [17]
Rectifier/Inverter	2 x10^{-5} [18]
AC contactor	2.30x10^{-5} [19]
DC contactor	1.53x10^{-5} [19]
Conductor	1.01x10^{-6} [20]

Table 4. Summary of failure rates for full up and degraded electrical architectures

Architecture configuration	Architecture condition	Failure event	Probability of failure (failures per flight hour)
1	Full up	L_1 supply	4.908×10^{-7}
		L_1 or L_2 (leading to engine IFSD)	4.912×10^{-7}
	Dispatch Scenario 1	L_1 or L_2 (leading to engine IFSD)	2.05×10^{-5}
	Dispatch Scenario 2	L_1 or L_2 (leading to engine IFSD)	4.05×10^{-5}
2	Full up	L_1 supply	4.916×10^{-7}
		L_1 or L_2 (leading to engine IFSD)	4.932×10^{-7}
	Dispatch Scenario 1	L_1 or L_2 (leading to engine IFSD)	4.05×10^{-5}
	Dispatch Scenario 2	L_1 or L_2 (leading to engine IFSD)	8.05×10^{-5}

The results in Table 4 highlight that the rate of occurrence of a particular failure event tends to be dominated by one or two individual components (note that this has been calculated per flight hour and so would need to be adjusted to determine the likelihood of a failure occurring for longer flight times). For the full up condition for both configurations, the table shows that the engine IFSD rate is very similar to the L1 supply failure rate despite containing a number of additional terms in the failure equation. In this case the overall failure rate is dominated by the combined rate for failure of the two generators. Within the two ‘dispatch’ cases, failure rate becomes dominated by the probability of the single converter or converters supplying the engine accessories. The failure rate of Configuration 2 almost doubles compared to Configuration 1 as it has two converters connected in series to the load input, again highlighting the dominance of the converters in determining this failure rate. Therefore it is clear from this that the results of this analysis are very sensitive to these components’ failure rate.

Table 5. Estimated allowed failure rate of electrical system for full up and degraded electrical architectures to prevent IFSD with various diversion time

Architecture condition	Estimated allowed failure rate of electrical system (failures per flight hour) with ETOPS diversion requirement of:		
	1 hour	5 hours	10 hours
Full up	1×10^{-5}	5×10^{-6}	1×10^{-6}
Time limited dispatch (assuming 10 times greater than full up)	1×10^{-4}	5×10^{-5}	1×10^{-5}

Comparing these rates to the requirements derived in earlier sections (the estimations of electrical system requirements assuming an failure rate which is an order of magnitude below the overall requirement are shown again in Table 5), and in particular the IFSD rate required for ETOPS certification, reveals some interesting findings. These include:

- In the full up condition of each configuration, the failure rate is almost two orders of magnitude below the maximum permitted IFSD rate and so electrical supply failures (even incorporating cable and contactor failures) should not have any impact on this rate (and there may be some scope for reduction in redundancy).

- In the degraded states, the failure rate is similar to that of the normal IFSD rate of the engine. Therefore the potential for loss of electrical supply to the engine accessories will have a significant impact on the overall engine’s IFSD rate.

- If the allowed engine IFSD is temporarily increased following a single failure in the electrical system (the assumed temporarily increased rate for TLD conditions is shown in in Table 5) then the current results show compliance with the derived requirements.

The second and third points highlight that if it was desirable to dispatch the aircraft with known failures on the engine electrical system (as is very likely to be the case) then careful consideration would have to be given to how this impacts ETOPS certification. No clear guidance was found on the application of the TLD to electrical systems with regard to ETOPS within the standards. However some relevant questions for this purpose are:

- Can ETOPS certification targets still be met with one healthy engine and one engine with a degraded electrical system?

    - Can the failure of both engines still be considered as extremely remote when one engine’s electrical system is in a degraded state?

- Or do ETOPS regulations require the IFSD rate of individual engines to be a certain level (worst case scenario in this case being a failure of one engine with the other having been dispatched with an electrical system in a degraded state)?

- Should the allowed ‘diversion time’ be shortened for specific flights in order to comply with regulations while an engine’s electrical system is in a degraded state and what would the impact of this be on aircraft availability for all intended routes?

- Should the allowed IFSD rate be increased on one engine on a time-limited basis (such as the 10 fold increase in the allowed LOTC rate) for non-EECS related failures?

Addressing these points will enable the suitability of different architectures and operating approaches to be determined with far more assurance.

Conclusions

The interpretation of relevant certification standards is a critical step in defining a system’s design requirements. This paper has outlined a review of engine certification standards, with key redundancy and reliability requirements for normal operation, Time Limited Dispatch (TLD) and Extended Range Twin Operation (ETOPS) being defined. Comparison of MEE architectures with these defined requirements helps to both assess an architecture’s compliance with standards as well as determine the necessary reliability of certain supply paths or components.

The paper also identifies that the optimal means of managing electrical system faults (from an aircraft dispatch perspective) requires investigation. In particular, it is highlighted that there may be an opportunity to maximise the availability of the electrical system and make best use of redundant supply paths through a TLD type operating approach. Exploration of such operating approaches is important in ensuring maintainability targets are met and unnecessary downtime is minimised within future more-electric platforms.

References

1. Richard Newman, “The more electric engine concept,” SAE Technical Papers, document number: 2004-01-3128
2. Lixin Ren, “Should Aero Engines be More Electric,” IEEE Transportation Electrification, September 2013
3. Hirst, M.; McLoughlin, A.; Norman, P.J.; Galloway, S.J., "Demonstrating the more electric engine: a step towards the power optimised aircraft," *Electric Power Applications, IET* , vol.5, no.1, pp.3,13, January 2011
4. European Commission, ‘Flightpath 2050 - Europe’s Vision for Aviation’ 2011, doi 10.2777/50266
5. NASA, “Advanced Concept Studies for Subsonic and Supersonic Commercial Transports Entering Service in the 2030-35 Period”, in NASA Research Announcement, Pre-Proposal Conference, Washington DC, November 2007.
6. Gareth Williams, ‘Future Airbus - Aerospace Growth Partnership’ presentation, London, February 2014
7. European Aviation Safety Agency, “CS-E: Certification Specifications for Engines – Amendment 3”, 23 December 2010.
8. European Aviation Safety Agency, “CS-25: Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes – Amendment 13”, 10 June 2013.
9. Federal Aviation Administration, “FAR part 25 – Airworthiness Standards: Transport Category Airplanes” available online from: http://www.faa.gov/
10. Federal Aviation Administration, “FAR part 33 – Airworthiness Standards: Aircraft Engines” available online from: http://www.faa.gov/
11. Federal Aviation Administration, “Advisory Circular on Extended Operations (ETOPS and Polar Operations)”, Document number 120-42B, June 2008.
12. European Aviation Safety Agency, “AMC 20-6 rev 2 – Extended Range Operation with Two-Engine Aeroplanes ETOPS Certification and Operation” 23 December 2010.
13. Mike James, “Aircraft Electronics: Safety Assurance in Product Design/Development/Certification and Methods for Monitoring and Evaluating Safety Performance Engine Control System Perspective”, November 2010. Accessible at http://onlinepubs.trb.org/onlinepubs/UA/111610Honeywell.pdf
14. Prescott, D.R. and Andrews, J.D., “A comparison of modelling approaches for the time-limited dispatch (TLD) of aircraft,” Proceedings of the 16th ARTS (Advances in Reliability Technology Symposium), Loughborough University, UK, April 2005, pp. 259-276
15. European Aviation Safety Agency, “AMC 20-1: Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems - Amendment 2”, December 2007
16. Michael Stamatelatos, William Vesely, Joanne Dugan, Joseph Fragola, Joseph Minarick, Jan Railsback, “NASA – Fault tree handbook with Aerospace Applications, Version 1.1”, August 2002
17. Ian Moir and Allan Seabridge, ‘Aircraft Systems: Mechanical, electrical, and avionics subsystems integration’, Third Edition, chapter 11, 2008 John Wiley & Sons, Ltd. ISBN: 978-0-470-05996-8
18. Kamiar Karimi, ‘Role of Power electronics in More-Electric-Airplanes’, Keynote presentation at the European Power Electronics conference 2011, Birmingham
19. US Department of Defense, ‘MIL-HDBK-217F – Reliability Prediction Of Electronic Equipment’, section 14.2, December 1991
20. US Department of Defense, ‘MIL-HDBK-217F – Reliability Prediction Of Electronic Equipment’, section 15.1, December 1991

Contact Information

Dr Steven Fletcher, Research Associate, University of Strathclyde, UK

Email: steven.fletcher@.strath.ac.uk

Acknowledgments

This work has been carried out as part of the Rolls-Royce UTC program.