Fault tolerant drives for aerospace applications

G.J.Atkinson, J.W.Bennett, B.C.Mecrow, D.J.Atkinson, A.G.Jack, V.Pickert
Power Electronics, Machines and Drives Group, School of Electrical Engineering, Newcastle University,NE1 7RU, UK. G.J.Atkinson@ncl.ac.uk

Abstract
This paper will discuss the emerging application of electrical machines and drives within the aerospace sector. The reasons for the implementation of electrical systems in aircraft will be considered, and the necessity for fault tolerance discussed.

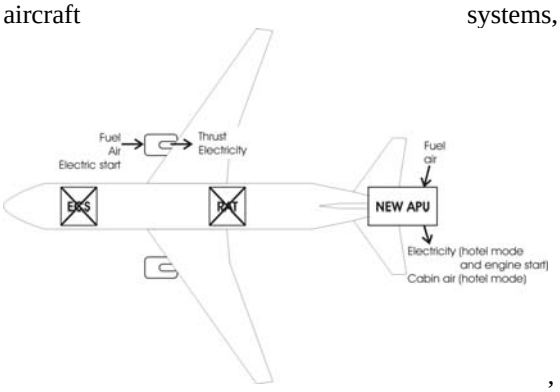
1. Introduction

An aircraft is a self contained system using fuel to provide propulsion and generate all secondary power. Secondary power is electric, hydraulic, pneumatic and mechanical and is used in a plethora of secondary systems. In modern aircraft the secondary systems are broadly split into five categories; flight control, environmental control, anti-icing, galley load and miscellaneous loads [1].
Early aircraft were of such a size that flight control secondary systems could be powered manually, a good example being the direct connection between the flight control surfaces via rods and cables to the control yoke. As the size and speed of aircraft increased it became necessary for many secondary systems to have some form of power assistance.
During the early use of assisted power there was much debate over the power source for each of the secondary systems, but over time the various aerospace manufacturers converged, as summarised in table 1.

Table 1. The five main aircraft systems and their power sources.

Aircraft system	Power source
Flight controls	Hydraulic
Environmental control	Pneumatic
Anti-icing	Pneumatic
Galley loads	Electric
Miscellaneous	Hydraulic

Much research has been carried out on replacing the three individually optimised power systems with one globally optimised electrical power system. It is a commonly held view that this will not only result in less scheduled maintenance, Oman [2], but also a reduction in weight and fuel consumption. Indeed the 1985 NASA case study based an all-electric version of the Boeing 767, indicated a weight saving of 10% and a similar reduction in fuel consumption [1].
Such an improvement is in line with current industrial (and political) thinking, and the recent advances in permanent magnet and power electronic technologies make all-electric systems technologically and financially feasible.
The 'all-electric' aircraft, that is all secondary power being electrical, requires a total redesign, replacing all pneumatic and hydraulic systems with electrical systems in one step. Such a move is not without significant commercial and safety risks and would never 'get off the ground' as far as certification is concerned. It is for this reason that the aerospace industry prefers the more-electric aircraft (MEA) approach, a progressive program in which new electrical systems are adopted one by one, whilst retaining some degree of the original pneumatic or hydraulic system as a backup. As time passes, trust in the new electrical systems will grow, facilitating the removal of the non-electric systems. Once this stage is reached the tried and tested electrical systems can then be used in a totally redesigned all-electric aircraft. The current aircraft systems,



,
can be compared to the proposed all-electric aircraft systems in **Fehler! Verweisquelle konnte nicht gefunden werden.**.
The A380 has demonstrated more-electric technologies including electro-hydrostatic actuators for flight control surfaces. These are hydraulic in operation but fed from an electrical supply rather than a hydraulic network – an inbuilt electrical pump and reservoir pressurises the actuator [3].

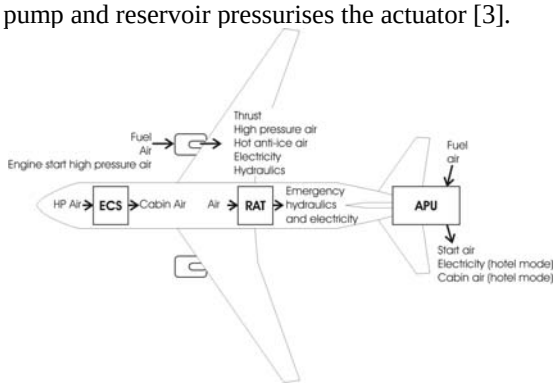


Figure 1. Current aircraft power distribution systems.

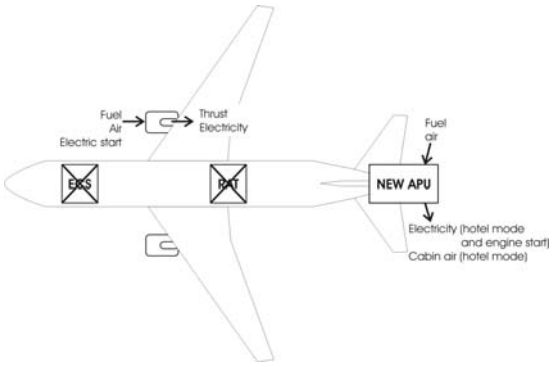


Figure 2. Proposed all-electric aircraft power generation.

2. Examples of fault tolerance

There is always a combination of faults which will lead to the failure of a system, the task of the engineer is to overcome or manage the likely faults and thus provide a system which is predictable and sufficiently reliable, with scheduled servicing.

For any safety critical system the development of an uncontrolled fault may risk property, life and limb: the response to a fault should fall into one of three categories;

A. Benign failure

Mellor *et al.* [4] describe an electrically powered vehicle traction drive designed to fail in a benign manner, where a fault may damage a single module, but is contained. This allows the driver to manoeuvre to a safe position with full use of steering, braking and other necessary systems and makes economic repair possible.

B. Continuous operation with reduced output

In his paper on the design of telecommunication systems, White [5] discusses the desired response of a network server in the event of a fault. Total failure could lead to an entire corporation grinding to a halt until the problem is fixed. However by partitioning the system, the fault is limited to only a few users.

C. Continuous operation with full output

Aircraft primary flight control surfaces such as rudders, elevators and ailerons must maintain operation following actuator, power supply or control signal failure, so parallel arrangements of actuators are typically employed to ensure full operation in the event of any single or even double failure.

An often cited analogy is the spectrum used by White [5] and shown in Figure 3. A system which gives some protection against the most common faults lies to the left, whereas a system designed to overcome all conceivable faults and combinations of faults lies to the right. Increased fault tolerance equals increased complexity and cost.

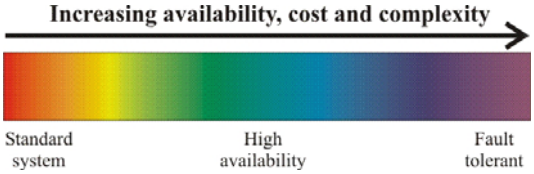


Figure 3. White's spectrum of availability [5]

The reliability of a system is defied by the standards applicable to the application and may be measured in a number of ways, as described by Caplin [6]. For a relatively flight critical system such as an aircraft engine fuel pump, the following reliability standards must be met, Mecrow *et al.* [7];

- There must be no single fault which causes a hazardous failure.
- Any fault which will cause an in flight shutdown must have a failure rate of less than 10^{-7} failures per hour.
- Undetectable faults which could, in combination with a subsequent fault, cause an in flight shut down, must have a failure rate of less than 10^{-8} failures per hour.

These levels of reliability are virtually impossible to achieve with a standard system and as such, flight critical systems have evolved to be fault tolerant by a variety of methods.

3. What is 'fault tolerance'?

For a system to be fault tolerant, White [5] states that: "*no single failure will cause the system to malfunction*". The level of fault tolerance is dependent on the severity of the application, however, for a system to be fault tolerant four principles must be met;

A. Partitioning and redundancy

A fault must be limited to a single component or sub-system. Jahns [8] introduced the concept of partitioning a 370kW AC drive so each phase of the motor is isolated and connected to a separate drive. In the event of a fault, the fault is contained to a single phase ensuring continued, albeit reduced, output. This method results in a statistically more reliable system, as modules are not interdependent.

Where a drop in performance is unacceptable, redundancy is required. This may involve a spare module, in use only during a fault, or the overrating of all modules so in the event of a fault, the healthy modules are capable of providing an increased output. Redundancy comes at a cost, as more components are required and overrating means extra capacity that is not normally in use. Welchko *et al.* [9] apply a "silicon overrating cost factor (SOCF)" to a number of fault tolerant drive strategies. The standard 3-phase AC drive, as shown later in **Fehler! Verweisquelle konnte nicht gefunden werden.**, has a SOCF of 1,

whereas the fault tolerant drives considered in the paper have a SOCF ranging between 1.15 and 2.24 with the general rule that the higher the cost, the greater the fault tolerance.

B. Fault isolation

Partitioning alone is not sufficient, as certain types of fault will propagate throughout the system, affecting previously healthy modules. Isolation may be through a simple fuse or switch, or managed by a complex control system.

C. Fault detection and annunciation

Fault isolation generally requires detection. For electric motors, Nandi and Toliyat review the fault detection methods available [10]. Methods ranging from signal based to infra-red monitoring and chemical detection are considered. A versatile method, capable of detecting a variety of faults, both mechanical and electrical, uses continuous harmonic analysis of a line voltage, current or other signal. Changes to the system are detected by an alteration of the harmonic spectrum. This harmonic signature indicates the type of fault and may be used to predict a slowly developing fault, allowing remedial action to be taken.

D. Online repair

Certain systems should not be shutdown for servicing or repair, an example may be a safety system in a nuclear power plant. In the event of a fault, the faulted module should be removed without a halt in operation.

An alternative is to overcome a fault using a different control strategy. Wallace and Spee [11] postulate a number of failure symptoms and remedial control strategies for a brushless DC drive. With suitable drive technology and fault detection a highly available fault tolerant system can be developed.

4. Considerations in fault tolerant drives

The most important decision to be made in the design of a fault tolerant drive is the type of machine, as each machine has its own characteristics, which make it more or less fault tolerant and this has an impact upon the topology of the electrical drive. The power density of each machine type will also vary and weight is an important consideration in aerospace.

A. Brushed machines

Wound field machines only offer power density advantages at very high power levels, hence their use in power generation. At aerospace power levels these machines are larger and less efficient than their counterparts. There is the additional set of failure possibilities associated with the brushes, and electrical arcing is most definitely not suited to an aerospace application in which the air pressure can be very low.

B. Synchronous reluctance machines

These benefit from a rugged rotor, however the overlapping winding mean that there is mutual coupling between phases and thermal overload is likely to affect more than one phase. Fault tolerance is possible by using groups of isolated phases; however this comes at the cost of a much larger machine.

C. Induction machines

As with the synchronous reluctance machines, the induction machine (IM) benefits from a simple rotor, however this requires careful design to avoid failure due to differential thermal expansion of the rotor bars and rotor laminations. Mutual coupling between phases and between the rotor and phases mean fault tolerance with complete magnetic and thermal isolation is only possible if a series of separate IMs are used.

D. Switched reluctance machines

SRMs are a natural candidate for fault tolerance and much work has been done by Richter et. Al. [12-14]. The rotor is robust and will withstand large mechanical and thermal stresses. The phases are decoupled electrically and mechanically, but only slightly coupled thermally and magnetically – a problem that can be overcome by the use of a spacer tooth between phase windings.

E. Permanent magnet synchronous machines

While considered the most power dense at lower power levels, PMSMs have a number of disadvantages over SRMs. Their magnets make for a mechanically challenging design and place limits on the thermal capability of the machine. More notably, the rotor field will drive a current in an armature winding, even in the event of a power converter or winding fault. In the case of a winding or power device short-circuit, this can result in additional damage, including excessive heating of the motor windings.

However, it has been shown [15-17] that these problems can be overcome with careful mechanical and thermal design, fault detection and appropriate drive response. In particular, a high per unit reactance in the motor will limit fault currents in shorted armature turns by the remedial application of a terminal short-circuit by the control electronics. This will induce a drag torque which must be overcome by the remaining active phases, but despite this, a well designed PMSM is considered to be the smallest and most efficient machine topology, a definite attraction for aerospace applications.

F. Considerations for the electric drive

Phase isolation must continue back to the electrical drive through the use of isolated modules. These may take the form of a set of isolated H bridges each supplying a single isolated winding, or a multiple set of three phase drives supplying multiple isolated sets of three phase windings. It is necessary to employ independent control electronics for each module and, unless the reliability can be assumed far in excess of the drive, independent power supplies and control signals to each module. A fully independent drive configuration is shown in Figure 4.

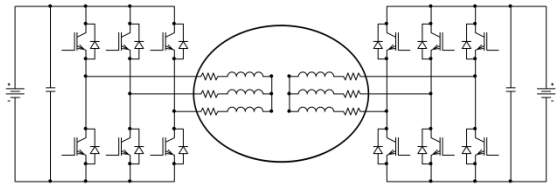


Figure 4: Dual three-phase electric drive.

The drive must rapidly detect a power device or motor winding fault and act accordingly (within a PWM cycle) to avoid the fault propagating through the power devices.

Appropriate actions [18-19] may be complete disconnection of the faulted phase from the DC supply, open circuiting the faulted phase in the case of an open circuit fault, or short circuiting the phase in the case of a turn-turn short. In addition the drive may need to be capable of supplying a shaped current to the remaining healthy phases to overcome any alteration to the quality of the output torque [20].

5. Recent Fault tolerant drive applications

Below are a few examples of these fault tolerant principles applied to electrical drives for aerospace applications carried out by the authors.

A. Prototype Electrical Actuator for Aircraft Flaps and Slats.

Aircraft wing surfaces consist of a system of flaps and slats. The controlled position of the flaps is not flight critical, however ensuring their symmetry across both wings is. The current system uses two hydraulic motors, mechanically summed via a shaft running the length of the wing span, and connected to two separate hydraulic supplies with an electrical pump to pressurise each hydraulic system. The relative position of all flaps is monitored (to maintain symmetry), and any small amount of asymmetry will result in the system locking all flaps in position, likewise if the pump system fails.

An electrical version of the flap actuation system was sought [21] in which the conventional system of a centralised dual hydraulic motor and drive shaft across the wing span, is replaced with an individual actuator at each flap surface. Such an approach would give greater functionality (independent flap control which may be aerodynamically desirable), reduced maintenance (due the removal of hydraulics) and most importantly, a reduction in mass due to the removal of the shafting, hydraulics and all associated ancillaries such as torque limiters and pipework.

Although the flaps may be locked in the event of a failure, failure may require an emergency landing and trade studies showed a level of fault tolerance is required in the actuator electronics to ensure this has a 10^{-5} per flight hour probability of occurring.

1) Choice of drive

The choice of motor type was between SRM and PMSM. With the actuator motors requiring rated torque at all angles in the event of a fault, the PMSM was felt to offer the simplest solution. In addition the PM machine offered the highest power density at the ~2kW level – important, given the limited space available for the system and the multiple number of actuators.

A number of power electronic and motor phase fault tolerant topologies were assessed with two basic types of motor topology identified – multiple single phase drives and multiple three-phase drives, described as;

- n+1 phase drives (eg. 2+1, 3+1 etc.)
- 3n+3 phase drives (eg. 3+3, 2×3+3 etc.)

In all cases the performance, component count, reliability and mass of each topology were considered and the worst case from high and low speed operation. The result, shown in Figure 5, suggests that a 2+1 or 4+1 topology, supplied from single phase bridges, provides the best combination of component count, converter size and machine size. For the flap actuator a 2+1 was deemed the optimum choice for the lower complexity, including a requirement for only 3 power supplies and sets of control electronics.

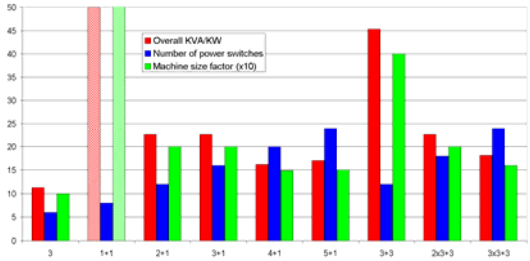


Figure 5: Fault tolerant drive sizes and complexity.

2) Prototype actuator system

The system specification is based on that used in a mid-sized commercial aircraft. The aircraft has two flaps per wing and a maximum load per flap of 34kNm. The flaps must be synchronised to within 0.25% of their full travel when retracted and 0.5% at all other times. Any asymmetry exceeding these limits may result in an uncontrollable roll of the aircraft so a mean time between failures of 10^{-9}

failures per flight hour is specified (less than once every 100,000 years). This is considerably more than the 10^{-5} specified for loss of operation, however fail-safe power-off brakes can be used to lock the system to avoid any excessive asymmetry, a technique employed in conventional flaps. The three sets of control electronics in each flap actuator and a three-lane flap control computer are sufficient to monitor flap position sensors and guarantee shutdown of the system in a severe failure or asymmetry.

The electric actuator is designed to deliver 3.4Nm at 10,000rpm into an inbuilt 37:1 gearbox and then to a conventional flap gearbox (already integral on a rotary flap system). A permanent magnet fault tolerant motor was designed with a 2+1 phase topology and fault-tolerant characteristics. This motor can deliver full torque with 2 out of 3 phase operational, and the magnetic design ensures that each phase is thermally, magnetically and mechanically isolated. This phase isolation is maintained by the three converters .

A full scale demonstrator has been built and tested, featuring two flaps actuators. This was shown to operate with a variety of faulted conditions at a motor drive and actuator level and to meet symmetry requirements. The actuator test-rig is shown in figure 6 and the reshaping of current waveforms when operating on two out of three phases to reduce output torque ripple is shown in Figure 7.

Figure 6: DEAWS flap actuator test rig.

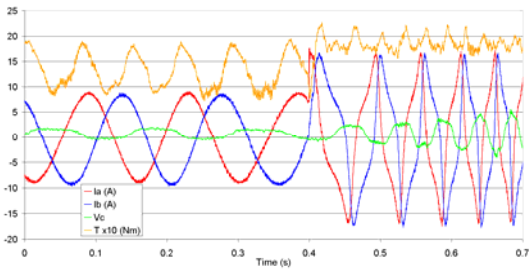


Figure 7: Reshaping of waveforms to reduce torque ripple.

B. High power fault tolerant machine design

Aircraft fuel pumps are conventionally a mechanical pump, coupled to an engine output shaft via a gearbox.

The benefits of an electric fuel pump are the removal of the mechanical gearbox (less maintenance and the removal of equipment from the space-limited engine region) and independence between the speed (hence fuel flow rate) of the fuel pump and the speed of the engine allowing the fuel delivery to be matched precisely to the engine conditions.

An aircraft fuel pump has strict reliability requirements so an electrical alternative must be fault tolerant.

A fault tolerant prototype has been built and tested by the authors [23]. The machine has a specification of 100kW at 30,000rpm. To produce the most power dense machine possible a fuel cooled PMSM was used. Fuel cooling allows for current densities in excess of $20A/mm^2$ without overheating.

The motor is a multiple single-phase design, with 4 concentrated windings isolated mechanically, thermally and magnetically, as shown in Figure 8 .

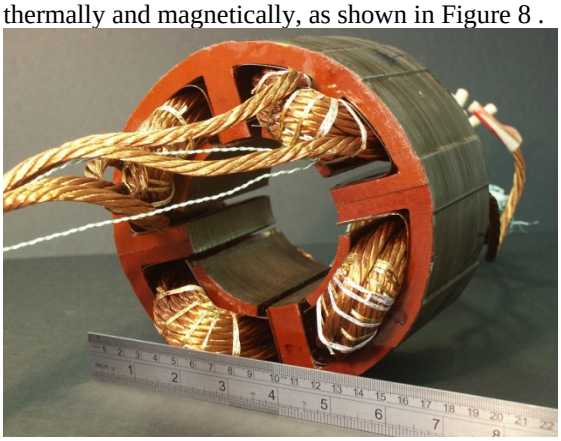


Figure 8. 100kW Fault tolerant four phase PMSM stator.

Fault tolerance is via a 3+1 topology, i.e. the 4 phase machine can operate to meet specification with only 3 phases working. Electrical isolation at the power electronics level is maintained through the use of four independent phase modules.

This 3+1 topology implies an over-rating of 33% on the motor phases and the converter, i.e. under normal conditions each phase delivers 25kW, rising to 33kW under faulted conditions.

The high power level demanded a great deal of design effort into avoiding excessive losses. Due to the high speed of the rotor an Inconel retaining sleeve was required to hold the samarium cobalt magnets in place. This electrically conducting sleeve and magnet arrangement is very susceptible to induced eddy currents and their associated losses.

The concentrated winding arrangement results in a high degree of non-synchronous airgap magnetic

fields. A great deal of effort went into the electromagnetic design of the stator to diminish these, with the result of a reduction in rotor loss of 29% [24].

C. A Prototype Electric Landing Gear Nose Wheel Steering System

Aircraft landing gear is currently hydraulically powered. This poses a fire risk as the hydraulic fluid is in close proximity with the brakes, to mitigate this problem there is a minimum turn-around time after landing in order for the brakes to cool sufficiently before takeoff again.

The elimination of this risk would be beneficial to the safety of the aircraft and also to the airline in terms of a faster turn-around.

A research project looked at replacing the hydraulically actuated nose wheel steering system with an electrical system. The safety requirements for the steering system are less than the aforementioned flap system and fuel pump, although operation must be possible following any single electrical fault. In addition the system must be able to be "free to castor" in the event of a serious failure or when landing or taking off. In 'free to castor', control of the steering is removed and natural corrective forces on the wheels keep the wheels straight on the runway.

The drive employed a dual lane electric drive and a dual 3-phase motor. The system operates in an active-active configuration with both drives simultaneously on, requiring that both control lanes are in agreement for position demands, position feedback and motor torque. In the event of a single electrical fault, the system can operate in active-standby configuration, disabling the failed lane and operating from its own position sensors. In the event of a disagreement both lanes will disable, a power-off clutch will allow 'free to castor' and the pilot or steering control computer can elect to operate the drive from either lane, with the aid of fault signals. Figure 9 shows the prototype actuator. The electric motor is housed at the top of the actuator, resulting in considerably lower forces on the extension and retraction mechanism than conventional hydraulic nose wheel steering.

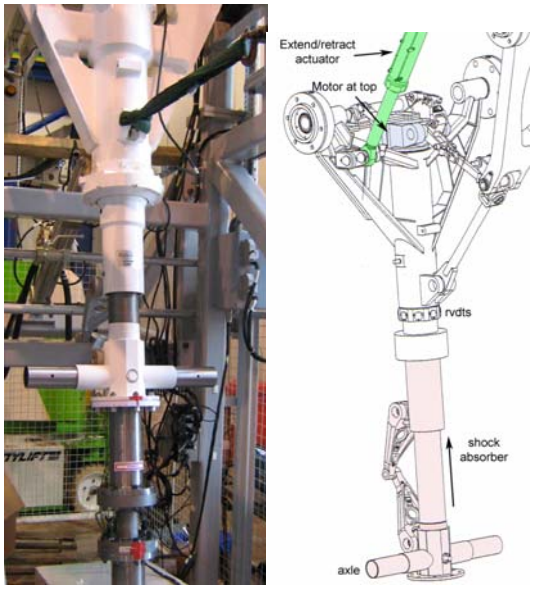


Figure 9: Electric nose wheel steering actuator.

6. Conclusions

Considerable research has been undertaken in the drive towards an all-electric aircraft. This paper details some of the systems investigated by the authors. Fault-tolerance is crucial in attaining the safety requirements for aerospace components, and the prototype systems described can be shown to attain aerospace safety requirements in their suggested applications.

Throughout the prototype systems discussed, the principles of partitioning, isolation and redundancy have been applied to give fault tolerance. For a truly fault tolerant system these design principles must be applied at the motor, converter and controller level.

7. References

[1] Hoffman A.C, Hansen, I.G. Beach, R.F. Plencher, R.M. Dengler, R.P. Jefferies, K.S. Frye, R.J. "Advanced secondary power system for transport aircraft" NASA technical paper 2463, 1985.

[2] Oman, H. "Replacing Hydraulics with electric power" IEEE AES Magazine, March 1998, pp 38-39

[3] Churn, P.M. Maxwell, C.J. Schofield, N. Howe, D. Powell, D.J. "Electro-Hydraulic Actuation of Primary Flight Control Surfaces", IEE Colloquium on All Electric Aircraft (Digest No. 1998/260), 17 Jun 1998, pp. 3/1-3/5

[4] Mellor, P.H. Allen, T.J. Ong, R. Rahman, Z. "Faulted behaviour of permanent magnet electric vehicle traction drives" IEEE Internatioal Electrical Machines and drives Conference, IEMDC 2003, Madison USA, pp. 554-558

[5] White, R.V. "Fault Tolerance In Distributed Power Systems", 6th European Conference on Power Electronics and Applications, EPE'95, Sevilla, Spain, 19-21 September 1995, pp. 2.851-2.857.

[6] Caplin, R.H. "A Practical Approach to Reliability", Business Books Limited, 1972. ISBN 0-220-66809-4.

[7] Mecrow, B.C. Atkinson, D.J. Jack, A.G. Green, S. Haylock, J.A. "The Need for Fault Tolerance in an Aeroengine Electric Fuel Control System" IEE Colloquium on Electrical Machines and Systems for the More Electric Aircraft, 1999, London UK, pp. 9/1-9/5

[8] Jahns, T.M. "Improved Reliability in Solid State AC Drives by Means of Multiple Independent Phase Drive Units", IEEE Transactions on Industry Applications, Vol. 16, No. 3, May/June 1980, pp. 321-331.

[9] Welchko, B.A. Lipo, T.A. Jahns, T.M. Schulz, S.E. "Fault Tolerant Three-Phase AC Motor Drive Topologies: A Comparison of Features, Cost, and Limitations" IEEE Transactions on power electronics, Vol. 19, No. 4, July 2004, pp. 1108-1116.

[10] Nandi, S. Toliyat, H.A. "Fault Diagnosis of Electrical Machines – A Review" IEEE International Electrical Machines and Drives Conference, IEMDC 1999 Seattle USA. pp219-221

[11] Spee, R. Wallace, A.K. "Remedial Strategies for Brushless DC Drive Failures", IEEE Transactions on Industry Applications, vol. 26, no. 2, July/August 1996, pp. 259-266.

[12] Richter, E. Radun, A.V.E. Ferreira, C. Ruckstader, E. "An integrated electrical starter/generator system for gaqs turbine application, design and test results", Proc.ICEM Conf, Paris, 1994.

[13] Richter, E. "High temperature switched reluctance motors and generators for future aircraft engine applications" Proc. Arerican Control Conference, Atlanta, June 1998, pp 1846-1851

[14] Richter, E. "Switched reluctance machines for high performance operations in a harsh environment – A review paper" Proc. ICEM, Boston, MA. 1990, pp 18-24

[15] [15] T. M. Jahns, "Improved reliability in solid state a.c. drives by means of multiple independent phase-drive units," IEEE Trans. Ind. Applicat. Soc., vol. IA-16, pp. 321–331, May 1980.

[16] A. G. Jack, B. C. Mecrow, and J. Haylock, "A comparative study of permanent magnet and switched reluctance motors for high performance fault tolerant applications," IEEE Trans. Ind. Applicat., vol. 32, pp. 889–895, July/Aug. 1996.

[17] B. C. Mecrow, A. G. Jack, and J. A. Haylock, "Fault tolerant permanent magnet machine drives," Proc. Inst. Elect. Eng. B, Nov. 1996.

[18] J. A. Haylock, B. C. Mecrow, A. G. Jack, and D. J. Atkinson, "On-Line detection of winding short-circuits in inverter fed drives," in Proc. 9th Int. Conf. Elect. Mach. Drives, Canterbury, U.K., Sept. 1–3, 1999, pp. 258–262.

[19] Haylock, J. Mecrow, B.C. Jack, A.G. Atkinson, D.J. "Operation of fault tolerant machines with winding failures," in Proc. IEEE Int. Electric Machines Drives Conf., Milwaukee, WI, 1997.

[20] Bennett, J.W. Jack, A.G. Mecrow, B.C. Atkinson, D.J. Sewell, C. Mason, G. "Fault-Tolerant Control Architecture for an Electrical Actuator", IEEE 35th Annual Power Electronics Specialists Conference, 20-25 June 2004, pp.4371- 4377 Vol.6.

[21] Bennett, J.W.; Jack, A.G.; Mecrow, B.C.; Atkinson, D.J.; Sewell, C.; Mason, G.; "A prototype electrical actuator for aircraft flaps and slats", IEEE International Conference on15 Electric Machines and Drives, 15 May 2005, pp. 41 - 47 .

[22] Atkinson, G.J. Mecrow, B.C. "High power fault tolerant machines for aerospace applications" UK Magnetics Society seminar, Bristol, April 2007

[23] Atkinson, G.J. Mecrow, B.C. Jack, A.G. Atkinson, D.J. Sangha, P. Benarous, M. "The analysis of losses in high power fault tolerant machines for aerospace applications" Trans. IEEE Industry applications, Sept 2009, Vol. 42, Ho. 5, pp 1162-1170

[24] Thomas, J. Maxwell, C. Benarous, M.; "Electrically Actuated Landing Gear for a Civil Aircraft Application" UK Magnetics Society, More Electric Aircraft, one day Seminar, University of Bristol, 2 April 2009,