Aircraft Electric Power System Overview:
System Description and Specifications

Liangpeng Guo, Mehdi Maasoumy, Mohammad Mozumdar, Pierluigi Nuzzo, Necmiye Ozay,
Ufuk Topcu, Huan Xu, Richard M. Murray and Alberto L. Sangiovanni-Vincentelli

1. Introduction

This document focuses on the power distribution system of an aircraft's electric power system as part of the Multiscale System Center (MuSyC) avionics challenge problem. As an aircraft becomes increasingly more electric (i.e., hydraulic and pneumatic systems are replaced with electric systems), the electric power system becomes increasingly critical for safe operation. The electric power system typically consists of a combination of generators, contactors, buses and loads. Primary power generation elements include batteries, auxiliary power units (APU), generators connected to the aircraft engine, and a ram air turbine (RAT) used for emergency power. Power is distributed via one or more buses and connection of generators to loads is routed by way of a series of electronic control switches (contactors). Primary electric loads include communications and computing systems, electrically-driven actuation systems (including electro-hydraulic systems), anti-ice and/or de-ice systems, and lighting systems. In this report, we discuss design specifications, while focusing on the single-line diagram shown in Figure 1.

2. System Description

In what follows, we provide a brief description of the electric power system, starting from its main components.[1]

2.1 Components

- Generators
    - DC generators are regulated by means of a commutator, which enables an AC sine wave output voltage to be full-wave rectified and smoothed to a steady DC voltage.
    - AC generators include a permanent magnet generator (PMG), excitation stator surrounding an excitation rotor containing rotating diodes, and a power rotor

[1] Moir, Ian and Allen Seabridge. *Aircraft Systems: Mechanical, Electrical, and Avionics Subsystems Integration.* 3rd ed. John Wiley and Sons, Ltd.

encompassed by a power stator. The PMG generates variable frequency power sensed by the control and regulation section of the generator controller unit.
    - AC/DC voltage levels should be compliant with the standards (for example, 115-120 VAC, 28 VDC). Higher voltages are not inherently advantageous, as they require more insulation. Transmission of power at higher voltages, however, is better due to lower currents, which lead to lower power losses (proportional to the squared current).
- Buses: AC and DC power buses deliver power to a number of loads or power conversion equipment. A start bus is used for the combined starter/generator.
- Transformer Rectifier Units: Rectifier units are used to convert three-phase AC power to DC power. Transformers are used to step down high voltages to lower voltages. A combined transformer rectifier unit both converts power from AC to DC as well as lowers the voltage.
- Motor Drives: Motors are used to drive a valve or actuator from one position to another. Typical uses for motors include actuation (engine control, trim, flap/slat operations), control valve operation, starter motors (used to start the engine), pumps, gyroscope motors, and fan motors. Motor drives can be used to control doors, windshield wipers, hydraulic pumps. In hybrid systems, hydraulic pumps are only supplemental; there are also electrical alternatives.
- Motor Controllers: These are permanent magnets (induction motors) and require a rotating AC source to operate.
- Contactors: Contactors are high-power switches that control the flow of power and establish connections between components. In particular, contactors can support current level of the order of 1000 A, while relays support current levels of the order of 1 A. Contacts can be 3-phase or single phase. Critical loads lose their functionality when they experience more than 50ms power interruption. Auxiliary contacts are included in each unit to provide an “open” or “closed” contactor status to other aircraft systems.
- External Power: This is a power supply provided when the aircraft is on the ground.
- Batteries: Batteries are used as an electrical storage medium independent of primary generation sources. Their main uses include assisting in damping transient DC loads, providing power in system startup modes, and providing short-term high-integrity power sources during emergency conditions while alternative sources are being brought online. The battery set may not be symmetric.
- Loads: Electrically-driven loads include sub-systems such as lighting, heating, motors, and actuation. Some subsets of loads are critical and cannot be shed, while others can be taken offline in case of emergency.
- Sensors: Sensors are used to monitor the status of the system and to identify possible faults. There are three important classes of sensors, namely, *current* sensors, *voltage*

sensors and *contactor* sensors. Voltage sensors, which consist of a set of resistors, are cheaper than current sensors (hence preferable in terms of cost). Contactor sensors come with the contactors, at no additional cost.

2.2 Single-Line Diagram

The role of primary distribution is to guarantee that primary buses are correctly powered. Figure 1 illustrates an architecture for electric starting, generation, and distribution in a more-electric aircraft. The top of the diagram shows six generators and an external power source. Each engine connects to a high-voltage AC (HVAC) generator (blue) and a low voltage AC emergency generator (purple). Two HVAC APUs can also serve as backup power sources, and an external source can be connected when on the ground.

Each of the three HVAC distribution panels has one or two HVAC buses, which can be selectively connected to the HVAC generators/APUs and to each other via contactors (represented by the double bars in the single-line diagram). Each panel also has its own start bus (green). The start bus can draw power from the motor drive, and is used to power on either the main generator or the APU. Once the generator comes online, the start bus is disconnected, the generator/APU then proceeds to power the main buses. HVAC Bus 1 and 4 contain two types of loads. Loads labeled L are essential loads and must remain powered (subject to the safety specifications detailed in the following section). Loads L_S are sheddable loads and can be dropped if power supplies are insufficient. Loads include, in addition to motors and actuators, lighting, heating and cabin pressurization.

Four Rectifier Units (RUs) are selectively connected to the four HVAC buses. RU 1 and 2 are directly connected to high-voltage DC (HVDC) Bus 1, and similarly RU 3 and RU 4 are connected HVDC Bus 2. Each HVDC bus also has a battery source that can be selectively connected. Additionally, each HVDC bus powers a set of motor drives. HVAC Bus 2 and HVAC Bus 3 are also selectively connected to a set of transformers that convert HVAC to low voltage AC (LVAC). The LVAC system is contained in the green boxes in the diagram. The transformers are connected to a series of four LVAC buses. AC Ess bus 1 and AC Ess bus 2 are essential and should always be powered. These buses are selectively connected to the two emergency generators. Additionally, an external ground source can be applied to the buses for ground services and handling, e.g. operations that are only used when the aircraft is on the ground, and are therefore never powered when in flight.

AC essential buses are connected to RUs converting LVAC to low-voltage DC (LVDC) as shown in the blue panels. There are four LVDC buses each with sheddable and un-sheddable loads, as well as two batteries, which may be selectively connected. Power can also be routed from the HVAC bus through transformer rectifier units to LVDC Main Bus 1 and LVDC Main Bus 2.

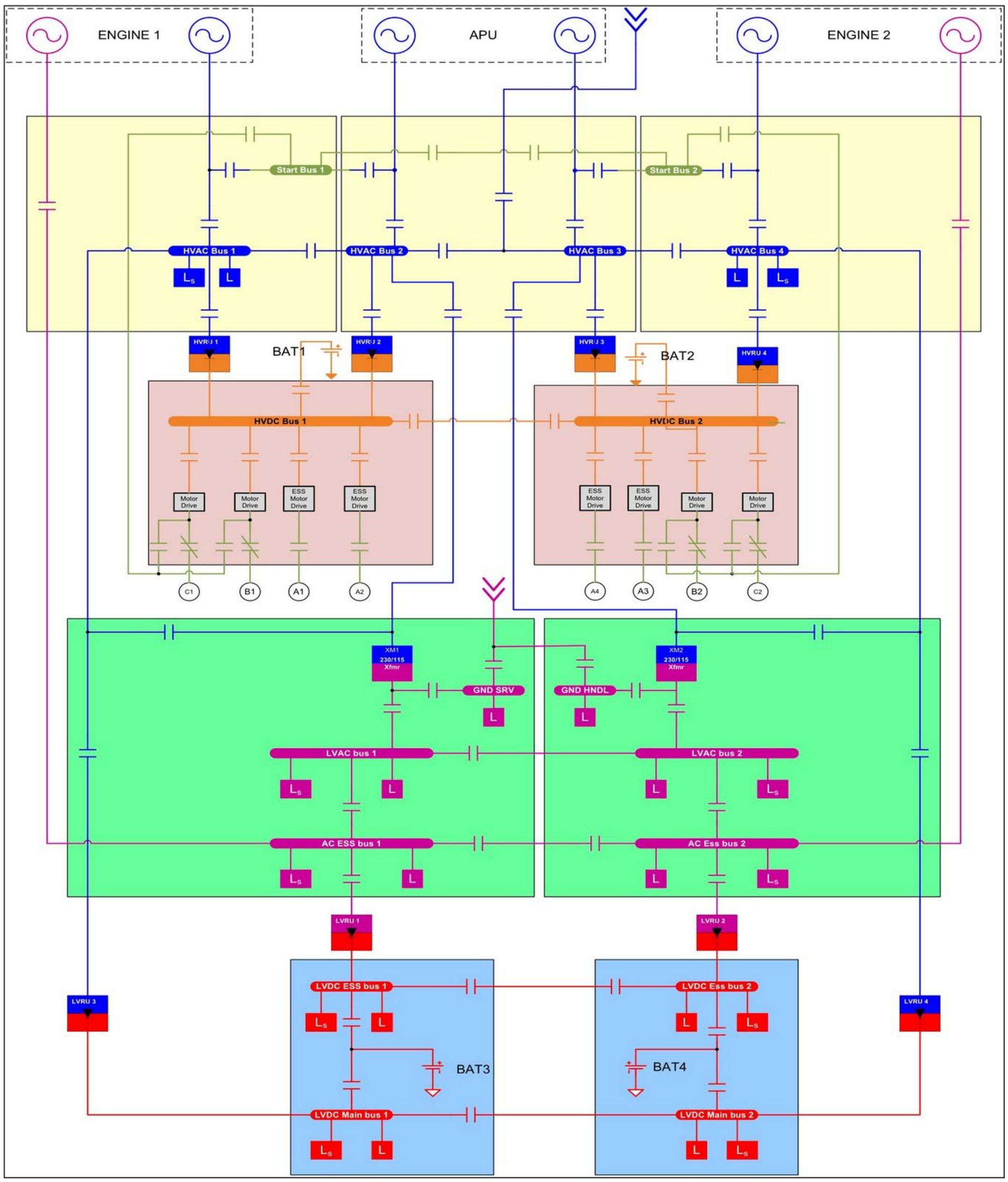

Figure 1: Single line diagram of an electric power system adapted from Honeywell Patent US 7,439,634 B2. Figure courtesy of Rich Poisson, Hamilton-Sundstrand.

3. Specifications

The requirements of the power system are generally expressed in terms of safety, availability (reliability) and performance (e.g., power quality and voltage and current levels needed for the system to function properly). Defining specifications is an iterative refinement process. Specifications defined by the customers and the related single-line diagram are merged into a document together with the “internal specifications” originating from the experience of the company that is in charge of integrating the power system. Such a document is compiled in English text, and may be hundreds of pages in length. On this reference document both the customer and the company agree for future development. Afterwards, specifications are partitioned among the main building blocks such as generators, primary distribution, secondary distribution and load management. The organization of the components into panels occurs also at this stage. In general, different components may come from different providers. The task of defining the specifications and possibly partitioning them may require a good number of experts interacting on several issues and taking decisions, mostly based on experience and a limited amount of tool support. At the level of the component, further refinement steps include, for instance, partitioning between mechanical and electrical domains, and in the electrical case, between hardware and software. Supporting tools may include, for instance, Doors (which allows managing requirements, but is not useful for formalizing requirements) as well as advanced (in-house) differential equation solvers for cyber-physical system simulation.

The basic safety principle prescribes that *no single failure can cause to lose important features*. Failures can be classified as in Table 1.

Failure	Probability of occurrence per operational hour	Informal Description	Examples
Catastrophic (level A)	10^{-9}	The pilot cannot do anything about it	Loss of airplane, wing cuts (falls) off, cabin pressurization
Hazards (level B)	10^{-7}	The pilot has to work hard to solve the problem	Fault in the gear
Critical (level C)	10^{-5}	Pilot can easily fix the problem	One engine shuts off

Table 1: Failure Classification

Operational hours denote the “hours of flight”. A probability of occurrence of 10^{-9} can also be interpreted as a Mean Time Between Failure (MTBF) of 10^{9} hours. These probability levels are estimated via fault tree analysis and reached by using redundancy of paths in the control loop. In fact, safety constraints translate into the architecture in terms of independence between hardware and software components that is needed to guarantee a certain fault probability. Independence is mostly implemented, for instance, by using redundancy and parallelism of components. As an example, some contacts have a *dual controller* (Master-Slave) or two controllers may be used to control the same subsystem to be robust against hardware problems. Similarly, sensors may include duplicate auxiliary contactors as shown in Figure 2, or contactors can be used in groups for redundancy, as represented in Figure 3.[2] We summarize the set of safety, reliability and performance specifications as follows.

3.1 Safety

- Each generator shall be controlled by one and only one controller.
- To avoid paralleling of AC sources, no AC bus can be powered by multiple generators at any point of time.
- Contactor closure times are between 15-25 ms and opening times are between 10-20 ms.
- Essential AC buses can never be unpowered for more than 50 ms. This requirement is necessary in order for contactor switches to open or close to avoid paralleling of sources. DC buses shall never be unpowered under no fault conditions.
- Never lose more than one bus for any single failure.
- At least half of each type of motor drive must be working at all times. In Figure 1, there are four A motors, which means that at least two of those motors must be powered.
- Total load must be within the capacity of the generators.
- Other safety specifications include no arcing and personal safety.

3.2 Reliability

- Every component comes with a reliability level. A level of 10^{-5}, for example, means that one failure will occur every 10^{5} hours. The desired system will satisfy the following probabilities:
    - The probability of losing one bus must be less than 10^{-5}.
    - The probability of a component failure ranges between 10^{-4} and 10^{-7}. With these components, the system must be designed to be safe up to 10^{-9} under all conditions. That is, the systems must be capable of tolerating any combination of component faults that has a joint probability more than 10^{-9}.
- Erroneous processors: Components could be functioning correctly, but a processor might also fail due to hardware or software faults.

[2] We refer to the following web page for further discussion on safety constraints from the Federal Aviation Administration (FAA):
http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/Chap3_120 0.PDF

- Every level of failure should be considered in the controller - from individual components to everything connected to the controller.

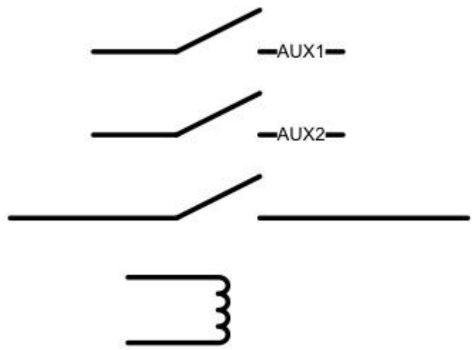

Figure 2: Example of auxiliary contactors for reliability

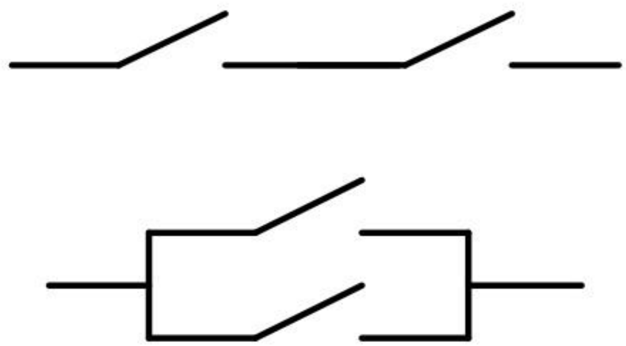

Figure 3: Contactor implementing the AND (top) and OR (bottom) functions

Table 2: Bus Prioritization

Priority	HVAC1
1	Eng 1 HV_VFG
2	Eng 2 HV_VFG
3	L_APU_VFG
4	R_APU_VFG
5	Eng 1 LV_VFG
6	HV_EXT_PWR

Table 3: Load Shed Prioritization for HVAC Bus 1

Non-Sheddable Load (W)	Sheddable Load (W)	Shed Priority
1000	1000	1
1000	1000	5
2000	1000	7
2000	1000	10
5000	2000	4
5000	2000	8
500	2000	9
500	2000	3
1000	5000	6
1000	5000	2

3.3 Performance

- **Priority:** Each bus has a priority list by which it can be determined which active generator should be selected to power it. If the first priority generator is unavailable, then it will be powered from the second priority generator, and so on. A hypothetical prioritization list is shown in Table 2. For instance, the priority list for the HVAC Bus 1 prescribes that it should be powered from the first available power source from this ordered list: high voltage left generator (Eng 1 HV), high voltage right generator (Eng 2 HV), left APU (L APU), right APU (R APU), low voltage left generator (Eng 1 LV) and high voltage external source (HV_EXT_PWR). No bus has priority over another bus, i.e. there is no notion that HVAC1 needs to be powered based on its list before satisfying HVAC2. In addition, no bus should be able to downgrade another bus's priority source.
- **System loads:** The system has two kinds of loads, i.e. non-shedable (critical) loads and shedable (non-critical) loads. Avionics components, DC loads, fuel boost pump, hydraulics and window heating are considered as non-sheddable loads. Fuel override pump, fuel jettison pump, ice rain protection unit, cooling fans and lights are considered as sheddable loads.
- **Load management policies:** The load management controller distributes available power to system loads and, if there is no adequate power, it shall shed the loads based on their priorities. Power is always first allocated to the non-sheddable loads and then to the sheddable loads by respecting, in all cases, the load priorities. Loads that are allowed to be shed are those labeled with L_S in Figure 1. Table 3 provides a hypothetical list of sheddable loads for HVAC Bus 1. A higher shed priority number represents a load that should be shed first.
- **Aircraft electric voltage levels:** The electric power system shall provide electric power so that the AC voltage level is between 115 and 120 V and the DC voltage level is 28 V.
- **Power quality:** Each generator is equipped with a generator control unit (GCU) that monitors and regulates the generators output voltage and controls a contactor, called

generator control breaker, which is used to isolate a faulty generator from the rest of the system. GCUs should be designed to meet power quality constraints.

- **Pilot operation:** The pilot performs engine starts/shutdown, monitors run-up and can manage loads.
- **Bus Power Control Unit (BPCU):** There can be one or more BPCU to control the switches (contactors) and provide power to AC and DC buses. The BPCU shall be in charge of enforcing priority list as discussed above. It is also desirable for the BPCU logic to minimize the number of changes of the contactor status (closed/open), while reconfiguring the system due to faults, so that the wear and tear of the contactors can be kept to a minimum.
- **Limit contactor switches:** Contactor switches should be kept to a minimum to extend the life of the component. In a power transfer sequence, if a contactor starts sequence closed and ends sequence closed, then it cannot be opened in the middle of the sequence.

Design rules for the controller are presented in terms of scenarios and priority tables. The entry point of a design process will then include: amount of load, number of generators and criticality of power in the loads.

Acknowledgements

These notes are based on a meeting held at Caltech on October 26-27, 2011 with Rich Poisson (Hamilton-Sundstrand) and on continued interaction with him. The authors gratefully acknowledge the feedback from Rich Poisson on this write-up.