An improved aircraft electric power testbed for validating synthesis methods

Linnea Persson[1], Scott C. Livingston[2], and Richard M. Murray[2]

[1] KTH Royal Institute of Technology, Stockholm, Sweden,
laperss@kth.se
[2] California Institute of Technology, Pasadena, CA, USA,
slivingston@cds.caltech.edu

Abstract. We present substantial improvements to a testbed for validating control protocols in aircraft electric power systems (EPS). The testbed is a simplified EPS that captures many salient features of actual aircraft EPS: control switching delays, decay times of suddenly unpowered voltage rectifiers, and uncertainty about the healthiness of power sources. The motivating context is synthesis of strategies for routing power sources to loads in response to changing conditions, e.g., when a power source becomes unavailable. These changes are modeled adversarially, and reactive synthesis methods are brought to bear. This work builds on a previous testbed design by developing a Python (rather than MATLAB) interface, creating a model of the testbed in the simulation tool Ptolemy II, and validating an estimation method on the testbed.

1 Introduction and summary

Aircraft power systems have traditionally been powered by hydraulic, pneumatic and electrical subsystems. Advancements in technology have enabled a shift from traditional aircraft power systems towards systems built up of electrical subsystems to a higher degree than before, increasing the complexity of the architecture and the number of components in the electric power system (EPS) [2]. This makes the fulfillment of reliability and safety requirements more demanding and presents a challenge to historically heuristic design techniques. Furthermore, the requirements may be in written English and incomplete or contain contradictions. Thus we are motivated to bring formal methods to bear.

The success of the flight depends on the ability of the system to power essential loads at all times, even when some components have failed. This is ensured by a control protocol that opens and closes electromagnetic switches, called contactors, so as to route power and isolate failed sources. This immediately leads to a reactive synthesis problem in which a specification in LTL can precisely express assumptions about failures and recoveries among available power sources, as well as requirements about how and where power must be routed. Synthesis methods can then be used to obtain a protocol, as described by Xu et al. in [6] for the GR(1) fragment and by Nuzzo et al. [3] for a contract-based method.

Aircraft EPS exhibit hybrid dynamics, e.g, contactors do not switch instantaneously, and changing voltage sources involve nontrivial decay times (cf. Section 3.4). Thus a testbed for experimenting is well motivated. In this paper we describe recent developments made to a testbed design originally presented in [5]. We develop infrastructure and examples in Python code (rather than the original MATLAB) and validate a state estimation method for EPS that had previously only been studied in simulation [1]. Finally a model of the testbed is developed in Ptolemy II [4]. The code and assembly instructions for this testbed will soon be released open source.

2 Graphical model of the aircraft electric system

As a graph, the EPS is modeled as $\mathcal{G} = (\mathcal{N}, \mathcal{E})$, in which generators, rectifiers and loads are represented as nodes $\mathcal{N}$, and edges $\mathcal{E}$ represent contactors $\mathcal{C}$ or fixed wired connections. A subset $\mathcal{U} \subset \mathcal{C}$ of the contactors may be *uncontrollable* in the sense that their configuration is fixed and possibly unknown or chosen adversarially during execution.

In this section we outline a model of the EPS that is amenable to estimation and control. This notation also provides a basis for expressing requirements. E.g., the safety property of never connecting AC power sources in parallel is expressed as always configuring contactors to ensure no path exists between AC generator nodes in $\mathcal{G}$.

2.1 States and actions

The state of the total electric power system is defined as the state of all generators and all rectifier units, together with the state that the contactors are in.

$$x : \mathcal{N} \cup \mathcal{C} \to \{0, 1\}. \tag{1}$$

The state of a particular component c when the system is in state x is denoted $x(c)$. The set of all states is denoted X. The states of the individual components are interpreted as follows. Generators and rectifiers may take the state of *healthy* (1) or *unhealthy* (0), where the former indicates that they satisfy their supposed function and the latter indicates that they are not able to fulfill their purpose in a sufficiently good way. Each contactor assumes the state of *open* (0) or *closed* (1). The controllable contactors have a state which is always known and controlled by the user. An *action* is a function on the controllable contactors

$$u : (\mathcal{C} \setminus \mathcal{U}) \to \{0, 1\}. \tag{2}$$

Taking an action u causes the state x to change to fulfill $\forall c \in \mathcal{C} \setminus \mathcal{U}\ x(c) = u(c)$.

2.2 State estimation

The system is observed using sensors, which abstractly indicate voltage levels as being sufficiently high ("healthy") or not. In general taking measurements at

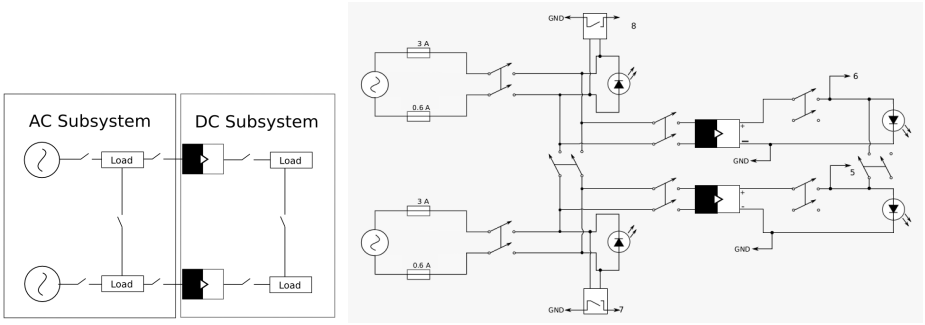

Fig. 1. On the left is an illustration of major components in the considered EPS. It is divided into analogous top and bottom sides because of the two engines of the aircraft. On the right is a schematic of the testbed. The black and white components in the middle represent the rectifier units that separate the AC and the DC sides.

sensors will return a set of states compatible with the measurement. It is then possible to further rule out states that are not compatible with the configuration of controlled contactors. Subsequent actions can further restrict this set of states. We have implemented and demonstrated on the testbed an algorithm for configuring contactors so as to estimate the state by Maillet et al. [1], as described further in Section 3.3.

3 Testbed

3.1 Testbed Characteristics

A schematic of the current setup is given in Figure 1, a photograph of it is shown in Figure 2, and a video demonstration is at http://vimeo.com/112469771. The AC power supplies for the testbed are represented by transformers taking 120 VAC down to 24 VAC. The rectifiers in the testbed that separate the AC and DC sides are represented by DC power supplies that generate a configurable voltage between 1.5 V and 27 VDC. The loads are LEDs on both the AC and the DC side. Later resistors were added close to the LEDs of the DC side that each had resistance of 150 Ω. Contactors are implemented in the testbed as relays. To enable control from a computer via USB, an off-the-shelf board that provides an array of 16 relays is used. In the current design, 8 relays are in use.

The testbed is equipped with four different voltage sensors. The admissible sensor levels for the DC side is 3.2-3.3 V when the DC voltage is set to be 3.3 V. The sensors on the AC side do not measure voltage directly but rather check whether a relay that is attached to an AC line is closed, which only occurs when the line is sufficiently powered. Ports 7 and 8 in Figure 1 provide measurements of the states of these relays, which drive those ports to ground when closed.

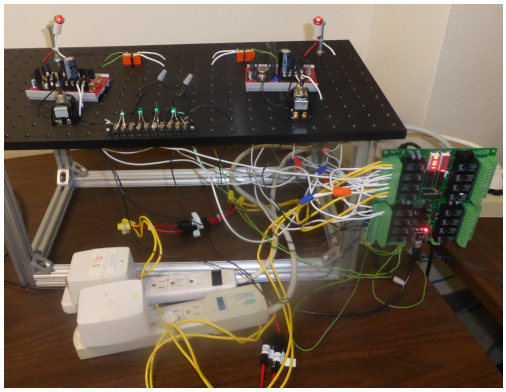

Fig. 2. The physical testbed. The LEDs in the back represent AC loads, and the LEDs in the front represents DC loads. Pictured is also the relay board (to the right), the two transformers functioning as generators (bottom), and rectifiers (between the AC and DC loads). A video demonstration is available at http://vimeo.com/112469771.

3.2 Fault Injection

Faults of three different types can be injected. To simulate generator failure, the transformers providing the circuit with power can be unplugged. Rectifier failure is achieved with external switches that opens the circuit on the DC side of the rectifier. Faults on the uncontrollable contactors can be added by opening or closing the relays corresponding to the uncontrollable contactors.

3.3 Implementation

Physically the testbed is set up according to Figure 1, but it is possible to change its behavior by deactivating components in the state detection script. It is possible to set each relay to behave as a controllable contactor, uncontrollable contactor, or by setting it to always closed, to behave as a normal wire. Sensors can be set to active or passive during the estimation depending on the sensor placement that is being considered in a particular state detection test.

The sensing is repeatedly performed while changing the configuration of the controllable contactors in between each sensing. This is repeated for k steps, and the resulting set of possible states is then the intersection of the possible states for each measurement. All combinations are calculated offline and saved into a database from which the next action is loaded during the actual state detection. While a general method for sensing actions subject to LTL formulae is future work, the current implementation avoids the known safety requirement of avoiding configurations of contactors that place AC sources in parallel.

3.4 Time delay

The capacitors of the rectifier units together with resistive loads on the DC side provide a time delay T_{RU} during which the rectifiers can remain unpowered

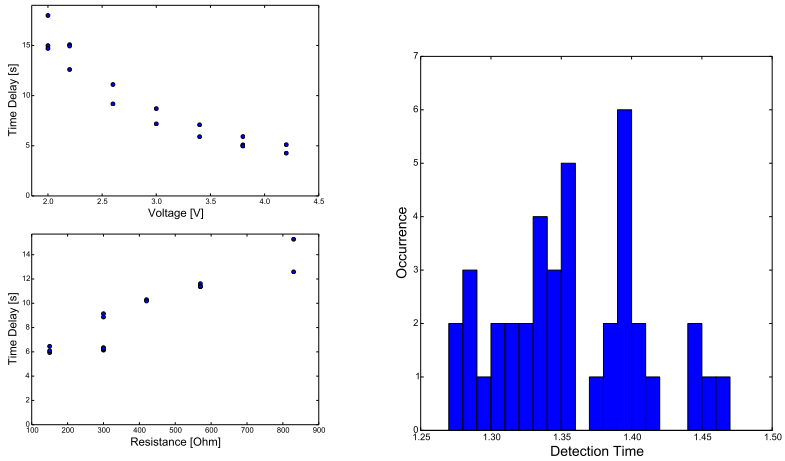

Fig. 3. The two plots on the left show time delay with respect to changes in load resistance (lower subplot) and RU output voltage (upper subplot). The time delay is taken as the time it takes for the voltage to drop to 95% of the starting value. The upper-left subplot has 18 measurements; the lower-left has 18. The histogram on the right is of time taken to estimate the state of the AC side with 3 steps for 40 tests.

without causing any change to the DC output power. For a sufficiently large delay, it is possible for a component failure and recovery to occur on the AC side without any apparent error being sensed on the DC side. In the presence of such large delay, the AC and the DC systems can be approximated as separate systems with their own control and fault detection. The control is divided into two parts, state detection (T_{estim}) and finding and taking a final action to route power such that all loads are powered ($T_{control}$). If $T_{estim} + T_{control} \ll T_{RU}$, then a fault on the AC side will not affect the DC side since alternative power will be provided to the rectifier before the output power of the rectifier is influenced. Alternatively, if T_{RU} is small, it is possible to add an artificial delay in the state estimation method to let the DC side adjust to the AC side values at every step of the fault detection algorithm. This would affect the overall performance since the time it takes from when a fault happens to when it has been discovered and fixed will increase.

While we have some control over the input voltage, resistance, and capacitance, it is not possible to give them arbitrary values so as to make the time delay small since the loads have a minimum power requirement. Tests made on the testbed, with results plotted to the left in Figure 3, show how the DC power time delay depends on the input voltage and the load resistance. For some typical values, it varies between 5 and 15 seconds. This time delay is considerably higher than the time it takes to complete one state detection cycle on the testbed shown on the right of Figure 3, which varies between approximately 1.27 and

1.47 seconds. This makes the distributed version of the system preferable, since the centralized version would require a time delay of several times the order of the state detection time to be added at each step of the detection algorithm.

4 Model in Ptolemy II

As a complement to the physical testbed, a model representing it has been made in Ptolemy II (http://ptolemy.eecs.berkeley.edu/ptolemyII/) [4]. Having this model makes it possible to test protocols before they are used on the testbed, where there is the risk of permanently damaging components. The estimation for the Ptolemy model works in the exact same way as described for the testbed above. The model uses the same scripts, though now communication is via a HTTP server rather than over a serial connection to the relay board.

5 Future Work

We are currently exploring interleaving state estimation with protocols synthesized using the Temporal Logic Planning (TuLiP) toolbox (http://tulip-control.org). This includes sensing in a manner consistent with specified LTL formulae, as well as hybrid models using, e.g., signal temporal logic (STL). Current work includes separation of the AC and DC state detection from each other, motivated by timing effects like those described in Section 3.4.

Acknowledgements

This work was partially supported by United Technologies Corporation and IBM, through the industrial cyberphysical systems (iCyPhy) consortium.

References

1. Q. Maillet, H. Xu, N. Ozay, and R. M. Murray. Dynamic state estimation in distributed aircraft electric control systems via adaptive submodularity. In *Proc. of the IEEE Conf. Decision and Control (CDC)*, pages 5497–5503, Dec 2013.
2. I. Moir and A. Seabridge. *Aircraft Systems: Mechanical, Electrical and Avionics Subsystems Integration*. Aerospace Series. Wiley, 2008.
3. P. Nuzzo, H. Xu, N. Ozay, J. Finn, A. Sangiovanni-Vincentelli, R. Murray, A. Donzé, and S. Seshia. A contract-based methodology for aircraft electric power system design. *IEEE Access*, 2:1–25, 2014. http://dx.doi.org/10.1109/ACCESS.2013.2295764.
4. C. Ptolemaeus, editor. *System Design, Modeling, and Simulation using Ptolemy II*. Ptolemy.org, 2014. http://ptolemy.org/books/Systems.
5. R. Rogersten, H. Xu, N. Ozay, U. Topcu, and R. M. Murray. An aircraft electric power testbed for validating automatically synthesized reactive control protocols. In *Proc. of the Conf. on Hybrid Systems: Computation and Control (HSCC)*, pages 89–94, 2013. http://resolver.caltech.edu/CaltechAUTHORS:20130115-094546873.
6. H. Xu, U. Topcu, and R. M. Murray. A case study on reactive protocols for aircraft electric power distribution. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 1124–1129, Dec 2012.