Switching Control Synthesis in the Presence of Uncertainty for an Aircraft Electric Power System Testbed

Linnea Persson

Mentor: Richard M. Murray *Co-mentor:* Scott C. Livingston

***Abstract*—With the recent trend towards more electric aircraft follows a larger number of electrical components and an increased architectural complexity of the aircraft electric power systems. We are looking at the case when only partial observability of the system is possible due to restricted sensing capabilities. Even with a limited observation it is possible to rule out some states from the from the set of all possible states as incompatible with this observation. By reconfiguring power and observing this modified system it is possible to better estimate the current state. In this report we describe the implementation of a state detection method that estimates the state by gradually removing impossible ones as knowledge of the system is gained on an aircraft electric power system testbed and on a model of the testbed made in Ptolemy II .**

I. Background

Aircraft power systems have traditionally had power distributed in 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 electrical system [1]. This makes the fulfillment of reliability and safety requirements more demanding.

The evolution towards more electric aircraft is driven by benefits such as the electrical components being lighter than their traditional counterparts, and that the electrical system is more adaptable. This makes them easier to handle and also means that the fuel usage will be lower per flight.

The aircraft electric power system (EPS) is a network of electrical components such as generators, interconnections, contactors and different types of loads and buses. The safety of the flight strongly depends on the ability of the system to power essential loads at all times, even in the case of failure in certain components. Consequently, this means that the more electric aircraft is highly dependent on having a good control system that is able to reroute power by switching contactors after sensing the environment.

Fulfilling the requirements on safety and reliability depends in part on the systems ability to detect critical faults that lead to loads becoming unpowered, and in part on its ability to identify alternative routings of power when one or more components have failed. When we have full observability the exact state is known, and so any faults are found directly. However, complete observability might not always be provided. Observation in the EPS is provided through different types of sensors, e.g., voltage or current sensors, and full observability would require monitoring all components through sensors at all times. One case when this is not possible is when one or more sensors have failed. Another case is when we want to limit the number of sensors for economical reasons or for practical reasons when implementing the physical electric power system.

II. Introduction

We consider the case when we want to limit the number of sensors in the system. To compensate for the smaller number of sensors estimation techniques can be used to evaluate the state. Where the sensors are placed in the system is important since the state detection efficiency will depend on having well placed sensors. This is something that is important to consider when placing sensors in a system.

Taking measurements at only a limited number of sensors will most often not return the exact state, but it will be possible to rule out

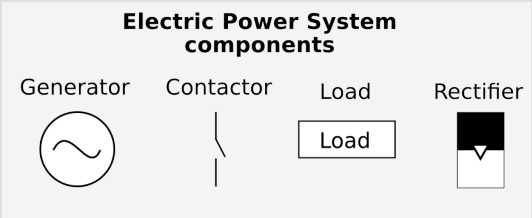

Fig. 1: How different components are graphically represented.

states that are not compatible with this particular measurement. The state detection is performed by repeatedly changing the paths that the power takes from sources to sensors, and thereafter observing the sensor values. Since loads cannot remain unpowered for more than a certain amount of time, the number of steps that we take in the state detection will be limited. If assuming that the state of the system will remain fixed throughout one state detection, the set of possible states will be reduced in each iteration by simply removing incompatible states from the set of all possible states.

Finding actions that rule out as many states as possible is of interest to render a more effective estimation algorithm that requires as few iterations as possible. One way of deciding how to reconfigure the contactors is described in Maillet et al. [2], where an aircraft EPS with four controllable contactors and two sensors has been considered. The proposed greedy algorithm performs as well as a brute force tactic where all possible configurations are tested.

III. Aircraft EPS

A possible setup for an aircraft EPS is depicted in Figure 2. There is an AC side and a DC side, and they are connected by rectifier units. The power sources are generators on the DC side, and on both sides there will be different types of loads and buses connected to the system. Contactors are electrically controlled relays, and they can be used to reroute power through the system or to cut of power coming from a faulty source.

Often it is convenient to describe the EPS in terms of a graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$. We then let the nodes $\mathcal{N}$ of the graph represent generators, rectifiers and loads. The edges $\mathcal{E}$ of the graph can contain contactors, denoted $\mathcal{C}$. There is possibly a subset of the contactors which we cannot control. These are referred to as the *uncontrollable*

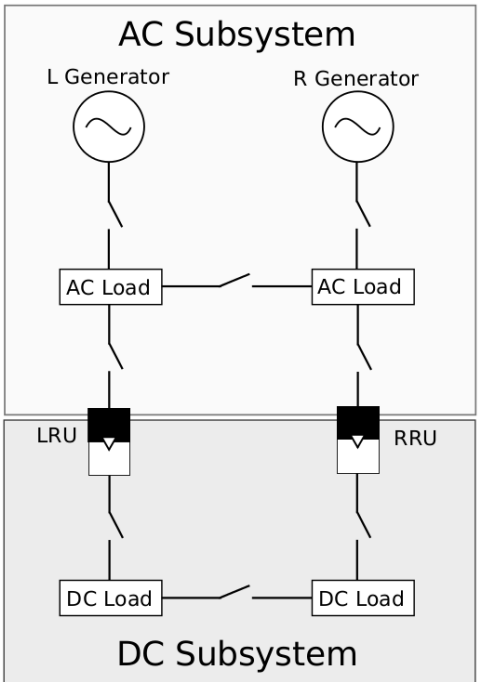

Fig. 2: An outline of the typical setup for Aircraft electric power systems. The EPS is divided into right and left following the two engines.

contactors $\mathcal{U} \subseteq \mathcal{C}$. The rest of the contactors are called *controllable contactors*.

IV. State Detection

A. State Definition

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. The uncontrollable contactors states are unknown and fixed throughout an estimation.

An *action* is a function on the controllable contactors

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

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

B. Sensing

The system is observed with the use of sensors. By defining a span of admissible voltage levels, each voltage measurement is translated to either (1), indicating an admissible voltage level, or (0) indicating that the voltage level is not correct.

$$m : \mathcal{S} \to \{0, 1\}, \tag{3}$$

where $\mathcal{S}$ is the set of sensors.

When in a certain state, the system can return only one possible set of measurements from the sensors. This set of measurements will most often not be unique, but shared between several different states. An observation of the sensors thus relates a configuration to a set of possible system states.

$$f : (m, c) \mapsto \hat{X} \subseteq X \tag{4}$$

where m is the measurement and c is the contactor configuration that the measurement was performed under. $\hat{X}$ is the current set of possible states.

C. Safety Requirements

For safety, there are certain requirements which must be fulfilled. One is that two AC sources never can be paralleled. This can be fulfilled by always controlling an action against the set of possible states. If there is any possibility that two or more generators might be paralleled with a certain action, this action is not taken.

Another requirement is a time constraint specifying the maximum allowed time for leaving loads unpowered. For safety, we cannot allow loads to be unpowered for more than a time T_{load}. This means that we must be able to determine the state sufficiently for reconfiguring the contactors so that all loads are powered in a finite number of steps. Whether or not it is possible to fulfill this requirement depends on the number of and the placement of the sensors in the system.

To be able to find a suitable way to reroute power, it is not always necessary to know the exact state of the system. Finding one path that with certainty powers all loads while not breaking any safety requirements in time is sufficient for fulfilling the timing requirement.

D. State Detection

The sensing is repeatedly performed while changing the configuration of the controllable contactors in between each sensing. Algorithm 1 captures the key elements of the state detection implemented with the testbed.

k := maximum number of steps;
m := sensor measurement;
c := contactor configuration;
$\hat{X} := X$;
step := 0;
while *step* $< k$ **do**
  $\hat{X}_{step} = f(m, c)$;
  $\hat{X} = X_{step} \cap \hat{X}$;
  if $|X| = 1$ **then**
    step = k;
  else
    $step = step + 1$;
    $u =$ next action;
    for $c \in \mathcal{C} \setminus \mathcal{U}$ **do**
      x(c) = u(c);
    end
  end
end
return $\hat{X}$;

Algorithm 1: Description of the state detection process

V. Testbed

A. Testbed Characteristics

The work in this project has been done on an existing aircraft EPS testbed [3] that has been modified to work with state estimation. A schematic of the current setup of the testbed is given in Figure 3, and an image of it is shown in Figure 4.

The power supplies for the testbed are represented by transformers transforming 120 VAC down to 24 VAC. The rectifiers that separates the AC and DC side is in the testbed represented by DC Power supplies that generates a voltage that can be set to values between 1.5 V and 27 VDC.

Loads were to begin with LEDs on both the AC and the DC side. Later we also added resistors

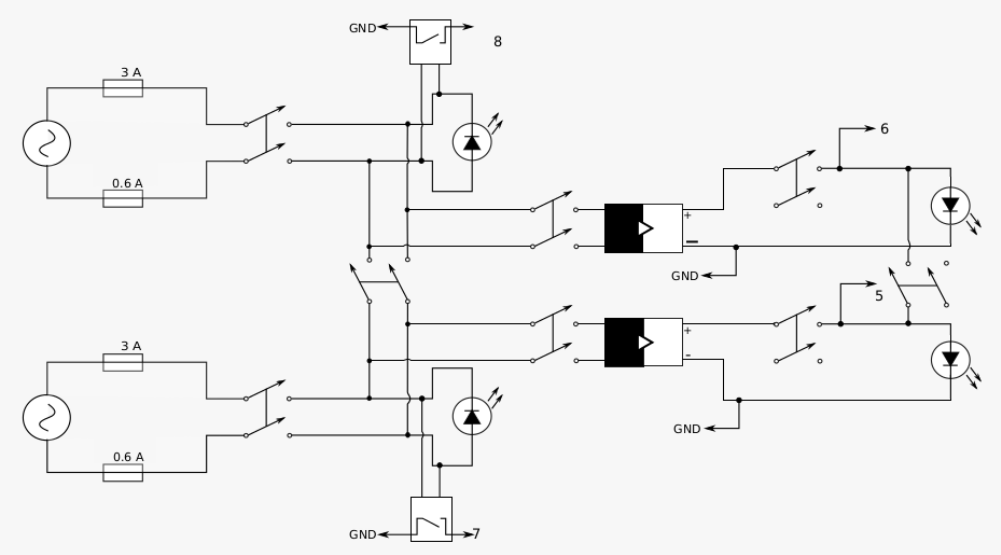

Fig. 3: A schematic showing the setup of the testbed. The numbers correspond to different ports that are used for sensing the voltage.

close to the LEDs of the DC side that each had resistance of $150\ \Omega$.

The testbed is equipped with four different sensors that senses the voltage level relative to ground. The admissible sensor levels for the DC side is 3.2-3.3 V when the DC voltage level is set to be 3.3 V. The sensors on the AC side does not sense a voltage level, but is instead managed by additional relays, that are closed when the voltage level is close to 24 V. Ports 7 and 8 in Figure 3 will sense 5.0 V when there is no closed circuit, and 0 when there is a closed circuit to ground. 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.

Instead of contactors, a relay board has been used in the testbed with a maximum capacity of 16 relays. There is one relay on each edge in the current setup, giving a total of 8 relays connected in the testbed. It is possible to set each relay to behave as a controllable contactor, uncontrollable contactor, or by setting it to always closed, as normal wire.

B. 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.

C. Implementation

The state detection algorithm described in algorithm 1 has been implemented to work with the testbed. The next action is decided by a greedy algorithm as described in [2], which gives the locally most effective action for all possible contactor-measurement combinations. The best action is based on the current state of the relays, the latest observation of the sensor measurements and what actions has previously been taken.

All combinations are calculated offline and saved into a database from which the next action is loaded during the actual state detection. Ending up in illegal states is avoided by forbidding certain actions that results in states that does not follow the rules as described in section IV-C. The illegal actions are found by counting the possible paths that can be taken between AC nodes and the generators. If there are two ways, the AC will be paralleled and so this action is marked as unsafe. This calculation is remade

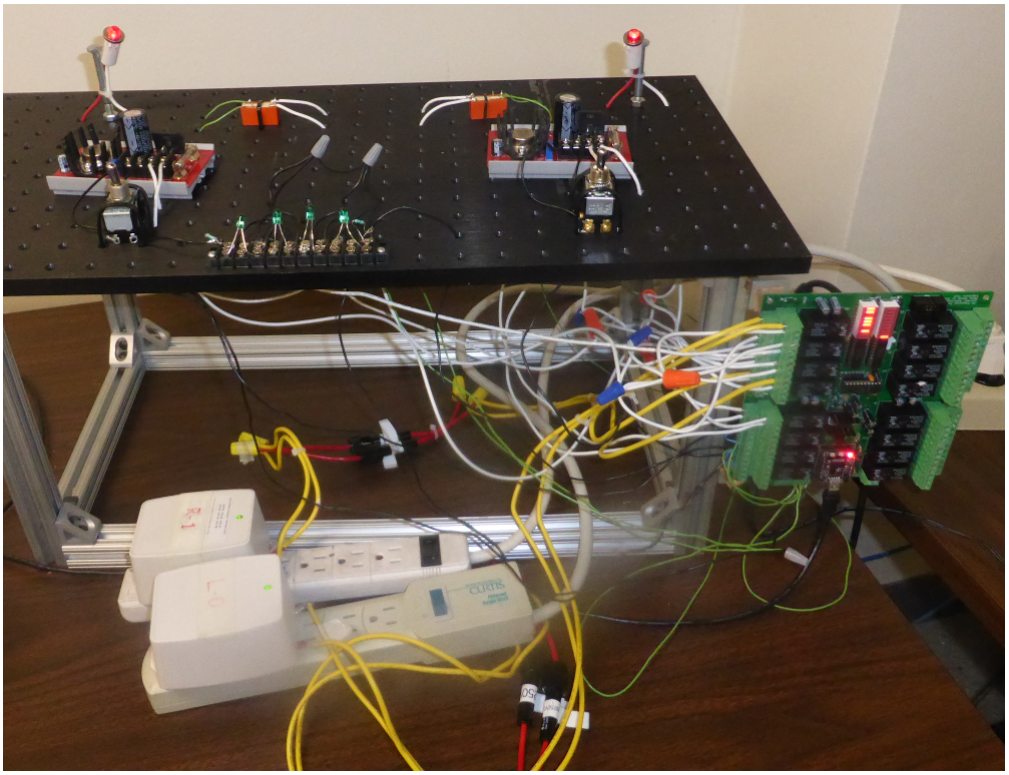

Fig. 4: The physical testbed. The LEDs in the back represent AC loads, and the LEDs in the front represents DC loads. Pictured is also the relay board (to the right), the two transformers functioning as generators (bottom), and rectifiers (between the AC and DC loads).

between each estimation since the unsafe actions will be different depending on what the state of the system is.

D. Ptolemy II Model

As a complement to the physical testbed, a model representing it has been made in Ptolemy II[1]. Having this model makes it possible to test scripts that are to be implemented to work with the testbed, and possibly find faults before they are tested on the testbed with the risk of causing permanent harm. It also facilitates testing more advanced EPS architectures than what is possible with the physical testbed without extensive work.

The estimation for the Ptolemy model works in the exact same way as described for the testbed above. The model used the same scripts and communicate with them using a HTTP server.

[1] http://ptolemy.eecs.berkeley.edu/ptolemyII/

E. Time delay

The capacitors of the rectifier units provides the DC side with a time relay T_{RU} under which the rectifiers can remain unpowered without causing any changes in the output power from it. The time delay is among other things dependent on the resistance on the DC side. When there is only a very low resistance, as in the case when only LEDs were connected to the DC side, the time delay will be barely noticeable.

Assuming that there is a time delay, if a component on the AC side fails, and this is discovered and an alternative power route is found in a time $T < T_{RU}$, then the error is never perceived by sensors on the DC side .

This result implies that if T_{RU} is large then it is not practical to use sensors on the DC side to estimate the state of components on the AC side, since the time delay will vary and the sensor measurements would therefore be either meaningless (when $T < T_{RU}$) or ambiguous

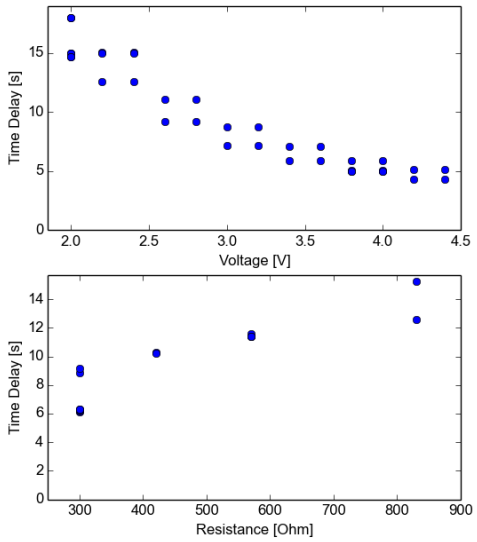

Fig. 5: Timing properties of the TTestbed. The time delay is taken as the time it takes for the voltage to drop to 95% of the starting value.

(when $T \approx T_{RU}$).

This also implies that we can look at the AC and the DC systems as being 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.

The presented arguments for the distributed view of the system only holds as long as $T_{RU} \gg T_{estim} + T_{control}$. If on the other hand T_{RU} is small it would be possible to add a delay 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 do have some control over the input voltage, the resistance and the capacitance, it will not be feasible to give them arbitrarily values to make the time delay small, since we still need to power the loads. From measurements made on

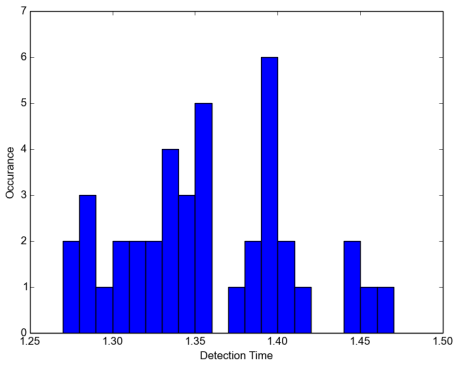

Fig. 6: Distribution of time it takes to estimate the state of the AC side with 3 steps for 40 tests.

the testbed, we can see that the time delay for the testbed vary from 5 to 15 seconds for some used values of the input voltage and the resistance. This is pictured in Figure 5. Compared to the time it takes to complete the state detection on the testbed seen in Figure 6, which varies between approximately 1.27 and 1.47 seconds, the time delay for the rectifier is considerably higher. This speaks in favor of using the distributed version of the system, 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.

Using the mean values calculated from the same data as pictured in Figure 6 and Figure 5, the following lower bound is found

$$\begin{aligned} T_{RU} &= 9.4 \text{ s} \\ T_{step} &= 0.5 \text{ s} \\ \Rightarrow T_{estim} &= 9.9 \cdot 2 + 1.5 = 19.8 \text{ s}. \end{aligned} \tag{5}$$

It is clear that with these times, adding a time delay is not a practical solution. Instead, since $T_{RU} \gg T_{control}$, using a distributed system is a reasonable choice.

The distributed model can be realized by completely deattaching the AC side from the DC side. Figure 7 displays the distributed version of the EPS in Figure 2. The rectifiers on the DC side can now be regarded as sources of the DC system, while the rectifiers can be regarded as a special type of load for which the requirement is to power at least one. Almost the exact same state detection method as described previously can be used here, one difference being that paralleling of the DC

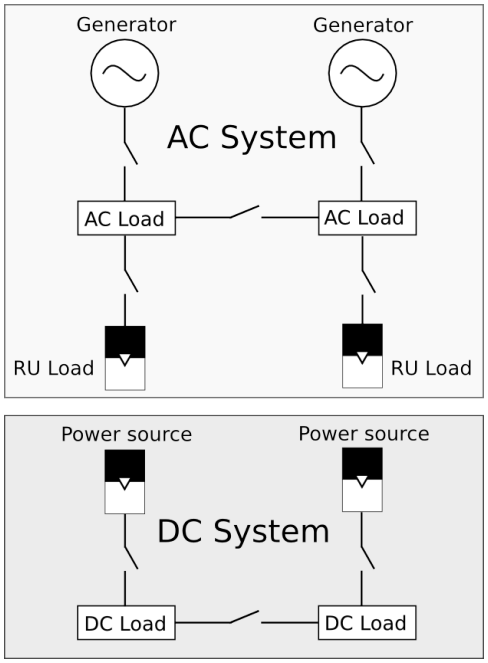

Fig. 7: If the time delay from the rectifiers is large enough, it is possible to use a distributed system instead of a centralized, as argumented for in section V-E

"sources" is allowed.

VI. Conclusion

It was possible to implement the state detection algorithm on the testbed, but the lack of resistance on the DC side that was used initially caused the time delay of the rectifier units to be insignificant. After adding resistance and measuring the time constants discussed in section V-E, it is clear that a distributed system is preferable to the centralized view that we started out with. The distributed system will moreover require fewer steps in the state detection algorithm since the subsystems contains fewer components than the total system.

VII. Future Work

A first attempt to run the state detection on the testbed with a distributed setup has been made, however, for the state detection to be truly distributed would require that two or more threads are run in parallel. This remains to be implemented.

In the current version of the state estimation ' it is assumed that the set of controllable contactors is known and remains constant. A more realistic approach would allow this set to change between each state detection, especially if the interpretation of the uncontrollable contactors is that they are failed contactors that presumably started out as non-failed (controllable).

Another challenge related to this is to allow the set of reliable measurements to change in time, or equivalently the set of working sensors to change in time. Both sensor failure and contactor failure would require a changed version of equation (4), since we assume that we know what to measure and read when we look for the measurement m and the contactor configuration c. A way to find and evaluate these quantities when some of the values might be corrupted remains to be done.

References

[1] I. Moir and A. Seabridge, *Aircraft Systems: Mechanical, Electrical and Avionics Subsystems Integration*, ser. Aerospace Series. Wiley, 2011.

[2] Q. Maillet, H. Xu, N. Ozay, and R. M. Murray, "Dynamic state estimation in distributed aircraft electric control systems via adaptive submodularity," in *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, Dec 2013, pp. 5497–5503.

[3] 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 *Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control*, ser. HSCC '13. ACM, 2013, pp. 89–94.