52nd IEEE Conference on Decision and Control
December 10-13, 2013. Florence, Italy

Optimal Load Management System for Aircraft Electric Power Distribution

Mehdi Maasoumy[†], Pierluigi Nuzzo[*], Forrest Iandola[*], Maryam Kamgarpour[◇],
Alberto Sangiovanni-Vincentelli[*] and Claire Tomlin[*]

Abstract— **Aircraft Electric Power Systems (EPS) route power from generators to vital avionic loads by configuring a set of electronic control switches denoted as contactors. In this paper, we address the problem of designing a hierarchical optimal control strategy for the EPS contactors in the presence of system faults. We first formalize the system connectivity, safety and performance requirements in terms of mathematical constraints. We then show that the EPS control problem can be formulated as a Mixed-Integer Linear Program (MILP) and efficiently solved to yield load shedding, source allocation, contactor switching and battery charging policies, while optimizing a number of performance metrics, such as the number of used generators and shed loads. This solution is then integrated into a hierarchical control scheme consisting of two layers of controllers. The high-level controller provides control optimality by solving the MILP within a receding horizon approach. The low-level controller handles system faults, by directly actuating the EPS contactors, and implements the solution from the high-level controller only if it is safe. Simulation results confirm the effectiveness of the proposed approach.**

I. Introduction

Aircraft electric power systems (EPS) are safety-critical systems, which provide power to vital loads such as the landing gear or the flight control actuators. As several hydraulic, pneumatic and mechanical components get replaced by electrical components, modern aircraft EPS become increasingly more complex, because of the larger number of hardware subsystems as well as their interactions with the embedded control software [1]. Electrification of the power system allows implementing smart control techniques that can achieve higher performance and overall efficiency via optimal management of power resources. However, EPS design is performed today mostly following a sequential derivative design process with limited capability of estimating the effects of earlier design decisions on the final implementation (a variation of the V diagram originally developed for defense applications by the German DoD[1]). To reduce risks in the development process, newly developed designs have often been a reincarnation of older aircraft EPS, a practice destined to be soon discontinued as a substantial amount of new functionalities is required in today's aircraft.

We address the problem of correct-by-construction control design for aircraft EPS within a Platform-Based Design (PBD) methodology [2], successfully adopted in the automotive and consumer electronics [3] domains to overcome similar challenges and avoid expensive re-design steps. Our goal is to develop an optimal load management system based on the formalization of the connectivity, safety and performance requirements of an EPS. In PBD, the design is regarded as a platform instance, i.e. a valid composition of library elements that are pre-characterized by their cost and performance metrics. The objective is therefore to select a platform instance that correctly implements a given specification. The mapping of such a specification onto an architecture can be formalized by an optimization problem. In our flow, an *optimal control* problem is formulated following a receding horizon approach, by solving, at each time step, a Mixed-Integer Linear Program (MILP) to determine load shedding, source allocation, contactor switching and battery charging policies that are correct and optimize performance metrics, such as the number of used generators and shed loads. Since safety is of paramount importance for the application, the control scheme has to quickly react in the event of unexpected changes in loads or component failures. To do so, we propose a two-level hierarchical scheme where a high-level load management system receives as inputs the required-power prediction for each bus over a time horizon of interest, the health status (operational or faulty) of power sources and contactors, the whole set of system requirements, and solves the optimal control problem. The output is a piece of "advice" for the low-level load management system, which handles system faults by directly actuating the EPS contactors, and decides to implement such advice only if it is safe.

Our approach builds on a number of results that opened the way for a more formal EPS design methodology. In [4], the authors present a platform for modeling and architectural exploration of aircraft subsystems by simulations. Similarly, in [5], the authors leverage simulation using a flight dynamics model of the aircraft coupled to a model of the actuation system. While several optimization techniques have been reported for the power electronics, switches and converters, the problem of optimizing the overall power distribution system has received scant attention in the literature. In [6], the optimum voltage and power levels at various points of the network are determined to minimize the total weight, installation costs and fuel consumption. An optimization oriented EPS design methodology following the PBD paradigm was instead proposed in [7]. However, the main focus of both [6] and [7] was on the selection of the generators and the design of the topology, i.e. the interconnection among different EPS components, rather than optimal design of the switching logic for the EPS contactors and load management. An automated procedure for correct-by-construction design of the EPS control protocol is discussed in [8]. System specifications are first converted using linear temporal logic [9], and then automatically synthesized by leveraging formal methods to guarantee safety constraints. However, while the correctness of the final solution is guaranteed, its optimality with respect to a number of performance metrics, such as the number of used generators and shed loads, is not addressed.

This paper is organized as follows. After a brief description of a sample EPS system and its requirements in Section II, Section III illustrates our hierarchical optimal load management approach, including the formalization of the problem, while Section IV summarizes the simulation results. Finally, in Section V, conclusions are drawn.

II. System Description and Requirements

An aircraft EPS, as shown in Fig. 1, typically consists of a combination of generators, contactors, buses and loads. The

[†]Department of Mechanical Engineering, University of California, Berkeley, CA 94720-1740, USA. Corresponding author. Email: mehdi@me.berkeley.edu

[*]Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720-1740, USA.

[◇]Automatic Control Laboratory, ETH Zurich, Switzerland.

[1]See e.g. http://www.v-model-xt.de

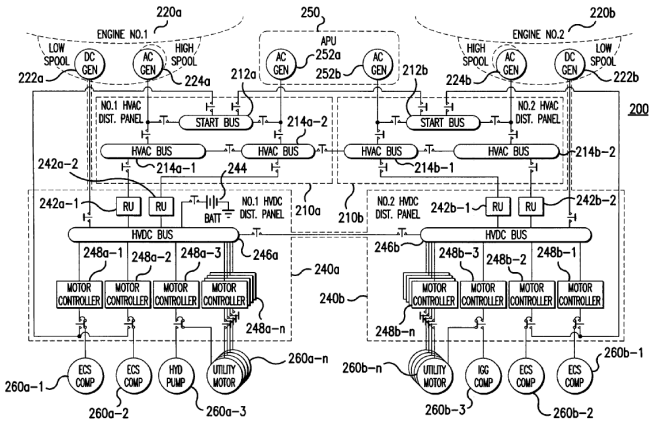

Fig. 1. Single line diagram of an electric power system from a Honeywell, Inc. patent [10].

connections among different components are specified by a Single Line Diagram (SLD), a simplified notation for representing three-phase power systems [1]. AC and DC *generators* deliver power to a number of AC and DC *loads* or power conversion equipment, such as *Transformers* and *Rectifier Units*. In addition to the generators connected to the aircraft engines, power-generation elements also include *Auxiliary Power Units* (APU) and *batteries*. Power is distributed via one or more *buses*, and connections of generators to loads are routed by a series of electromechanical switches, denoted as *contactors*. A subset of loads are critical and cannot be shed, while others can be taken off-line in case of emergency. Finally, current, voltage and contactor *sensors* are used to monitor the status of the system and to identify possible faults.

The role of the EPS distribution system is to guarantee that loads are powered with the required power levels. Therefore, in addition to sensors, the EPS control system consists of *Generator Control Units* (GCUs) and *Bus Power Control Units* (BPCUs). Each GCU regulates the output voltage of a generator to meet the desired power level for a range of expected loads. Conversely, the BPCU ensures robust operation of the system for a number of failures in its components, by opening or closing the contactors to adequately reroute power to critical loads.

The EPS system requirements are generally expressed in terms of safety and reliability properties. We list here some of the requirements that are relevant to the derivation of the optimal control problem in this paper:

- R1) *AC source parallelization.* Preserving the integrity of different AC sources requires that no bus can be powered by multiple AC generators at the same time.
- R2) *Bus priorities.* Each bus has a priority list that specifies which generator should be used to provide power. If the first generator in the priority list is unavailable, then a bus should be powered from the second generator, and so on. An example of a bus priority table for the SLD in Fig. 3 is shown in Table I.
- R3) *Load Shedding.* Sheddable loads are allowed to be shed if power supplies are insufficient, while non-sheddable loads must remain powered at all times. An electric Load Management System (LMS) is responsible for protection and shedding of loads, by respecting a load priority list as the one shown in Table II for the SLD in Fig. 3. A higher shedding priority suggests a load that should be shed first.

Designing an efficient EPS controller is certainly a challenge, the main drawback of current implementations being the lack of optimality in load shedding and power source allocation. In the next section, we propose a new architecture that addresses these issues.

TABLE I
BUS PRIORITY TABLE EXAMPLE

AC Bus 1	AC Bus 2	Priority
GEN 1	GEN 2	1 (most preferred)
GEN 2	GEN 1	2
APU	APU	3 (least preferred)

TABLE II
LOAD PRIORITY TABLE EXAMPLE

Non-sheddable loads (W)		Sheddable loads (W)		Shed priority
Bus 1	Bus 2	Bus 1	Bus 2	
5000	4000	1000	1000	1 (shed first)
1000	1000	5000	2000	2
1000	1000	2000	2000	3
2000	2000	2000	5000	4
1000	11000	1000	1000	5
1000	1500	5000	4000	6
45000	2000	1000	1000	7
5000	39000	2000	3000	8
8000	10000	2000	2000	9
500	500	2000	2000	10 (shed last)

III. THE OPTIMAL LOAD MANAGEMENT SYSTEM

A. Architecture

We propose a hierarchical architecture that controls power source utilization, load shedding, contactor status and battery charge via two layers of controllers. Fig. 2 shows a block diagram of the system (top), consisting of a *Low-Level LMS (LL-LMS)* and a *High-Level LMS (HL-LMS)*, and a timing diagram for its operation (bottom). The HL-LMS operates at a *slower clock* rate, with period T, and provides control optimality over a time horizon. The LL-LMS operates at a *faster clock* rate with period $t_f < T$, and guarantees system safety by quickly reacting in the event of unexpected changes in loads or component failures.

The HL-LMS solves an optimal control problem at each step, using a receding horizon approach. The inputs to the HL-LMS are the required-power prediction for each bus over a time horizon of interest (H, in Fig. 2), the health status (operational or faulty) of power sources and contactors, and the whole set of system requirements (e.g. including R1,R2, and R3). While each optimal control problem is solved for the larger time horizon H, only the initial samples of the solution (up to time T) are implemented and sent to the LL-LMS as *advice*.

The maximum computation time of the optimal control problem is assumed to be $\tau \leq T$. In fact, as discussed in Section IV, τ is usually much smaller than T in our application. However, to ensure more frequent updates to the HL-LMS, T can be chosen as $\max(\tau, t_f)$. Before the end of each slow clock cycle, by a time interval as long as τ, the optimal control problem is updated with the actual sensor readout on the status of sources, contactors and loads. A new solution is then computed and sent as advice.

The LL-LMS implements the BPCUs and, along with the GCUs, monitors the generator and contactor status more frequently (with a period t_f) to guarantee that each critical bus is powered at the desired voltage level (e.g. $T = 10t_f$ in Fig. 2). At each time step, the LL-LMS actuates the advice from the HL-LMS only if this is feasible, given the *actual* status of contactors, power sources and loads. If this is not feasible, e.g. when an unforeseen fault in

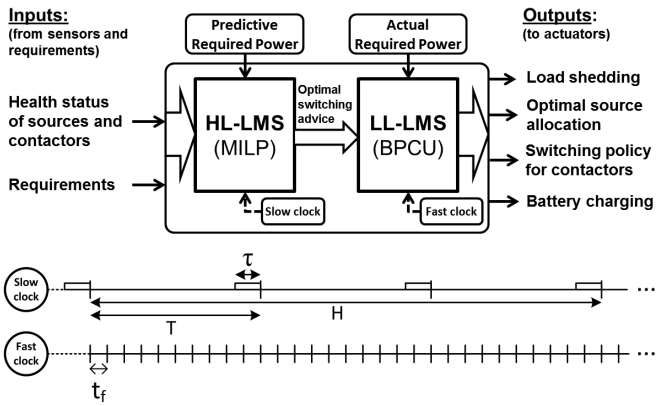

Fig. 2. Block diagram of the proposed hierarchical control architecture (top) and timing diagram for its operation (bottom).

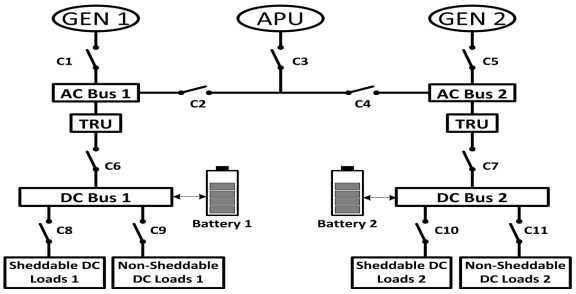

Fig. 3. Single line diagram of an electric power system. $C_i,\ \forall i = 1, ..., 11$ represent contactors.

TABLE III
NOMENCLATURE

Parameter	Definition
L^s_{ji}	Sheddable power sunk by load i of bus j
L^{ns}_{ji}	Non-sheddable power sunk by load i of bus j
n_j	Number of sheddable loads of bus j
N_j	Number of all loads of bus j
N^b	Number of buses
N^s	Number of power sources
$P^{\max}_j$	Maximum capacity of source j
$\overline{SoC}$	Maximum bound on battery state of charge
$\underline{SoC}$	Minimum bound on battery state of charge
T_s	Sampling time for HL-LMS optimization problem
T	Period of the slow clock
H	Prediction horizon of the optimal control problem
τ	Maximum computation time of the optimal control problem
t_f	Period of the fast clock
K	Parameter for battery charge dynamics
N^{as}	Number of allowed contactor switching events
γ_{ij}	Weight to penalize shedding of load j of bus i
λ_{ij}	Weight to capture source priority for source i to bus j
μ	Weight to penalize usage of an additional source
t_{chrg}	Time allowed for battery to reach $\underline{SoC}$
Variable	**Definition**
c_{ij}	Determines whether load i of bus j should be shed or not
P_{req_i}	Total required power of bus i
P_{sup_i}	Total power supplied to bus i
β_i	Power flow into/out of battery set i
$P_{i\text{to}j}$	Power delivered by source i to bus j
δ_{ij}	Determines connectivity of source i to bus j
α_i	Determines usage of source i
SoC_i	State of charge of battery set i
NoS_{ij}	Number of status transitions of contactor connecting source i to bus j

any component or an unpredicted change in power requirements are detected, the LL-LMS reroutes power based on its predefined, worst-case control policy. Then, the LL-LMS keeps implementing its control policy until the next HL-LMS cycle, when the information on the failure is communicated to the HL-LMS, which updates the optimization problem with additional constraints that account for the failure. The new constraints will remain in place until the failure is resolved. The above scheme is always at least as effective as the LL-LMS controller in guaranteeing system safety, while implementing at the same time more efficient source allocation, load shedding, and battery utilization strategies in the absence of faults.

In this paper, we assume that a BPCU is already available to implement the LL-LMS, by simply handling system faults without any concern on control optimality. Our main focus is then on the design of an optimal load management strategy for the HL-LMS and of its interface with the LL-LMS. Following the PBD methodology, the predictive information about the *required power* for each bus, the *load characteristics*, the *generation profiles* and the component *connectivity* from the SLD provide an abstraction of the EPS *architecture* in terms of optimization constraints. On the other hand, the *safety* and *performance* requirements listed above originate a set of constraints capturing the system *function*. The resulting control policy leads to optimal load shedding and generator utilization, while satisfying system requirements as well as constraints on the battery state of charge.

B. Problem Formulation

The first step of the methodology consists of capturing all the requirements and control goals as mathematical constraints. To detail this step we use the SLD shown in Fig. 3 as a running example. In Fig. 3, AC buses are connected to transformer-rectifier units (TRU) to convert AC power to DC power. Each DC bus has sheddable and non-sheddable loads, as well as a battery set. The underlying assumption is that TRU cause no power loss, i.e. the generated power available at each AC bus is equal to the power delivered to the corresponding DC bus. Therefore, in the simplified network topology of Fig. 3, each DC bus can be lumped together with the corresponding AC bus. A more complicate topology, e.g. including DC generators as in Fig. 1, would entail minor modifications in our formulation. To determine the load and source allocation policy, we leverage power balance equations based on a simplified steady-state power flow analysis. Extensions of our approach to support optimal AC power flow analysis, including reactive power allocation, are out of the scope of this paper. The reference bus priority table considered in this paper is shown in Table I, while the average power required by the loads in normal conditions, as well as the load shedding priority, is given in Table II. A list of all variables used in this section is available in Table III.

*1) **Load Modeling**:* Non-sheddable and sheddable loads are denoted by L^{ns} and L^s, respectively. We model the required power at time t as the summation of contributions from different power sinks (loads), some of which are sheddable. Hence, for bus j

$$P_{\text{req}_j}(t) = \sum_{i=1}^{n_j} c_{ji}(t) L^s_{ji}(t) + \sum_{i=n_j+1}^{N_j} c_{ji}(t) L^{ns}_{ji}(t) \qquad (1)$$

where, for $j = 1, 2, ..., N_j$, $P_{req_j}(t)$ is the total required power by all the electrical loads N_j connected to bus j. $L^s_{ji}(t)$ and $L^{ns}_{ji}(t)$ are the power sunk by load i connected to bus j at time t in the sheddable and non-sheddable case, respectively; n_j is the number of sheddable loads. Each coefficient $c_{ji}(t)$ for bus j and load i

at time t is a binary decision variable specifying whether power $L_{ji}(t)$ must be supplied or it can temporarily be interrupted for sheddable loads, i.e.

$$c_{ji}(t) = \begin{cases} 1 & \forall\ i \in I_j^{ns}, \quad j = 1, 2, ..., N^b \\ \{0,1\} & \forall\ i \in I_j^{s}, \quad j = 1, 2, ..., N^b \end{cases} \tag{2}$$

where I_j^{ns} and I_j^s denote, respectively, the index set of non-sheddable and sheddable loads of bus j, and N^b is the total number of buses. Finally, we capture shedding priorities via the following constraints:

$$c_{j1}(t) \leq c_{j2}(t) \leq ... \leq c_{jN_j}(t) \quad \forall\ t \geq 0 \quad j = 1, 2, ..., N^b \tag{3}$$

so that loads get ranked based on their priority, e.g. for bus 1, since load 1 has the highest shedding priority, L_{11} must always be interrupted prior to L_{12} when the total supplied power is not sufficient.

*2) **Source Allocation and Switching Policy**:* For each DC bus i, a power balance equation can be written as follows:

$$P_{\text{req}_i}(t) = P_{\text{sup}_i}(t) - \beta_i(t) \quad i = 1, ..., N^b \quad \forall\ t \geq 0 \tag{4}$$

where the amount of required power P_{req_i} from the loads, defined as in (1), is constrained to be equal to the amount of power supplied to bus i, $P_{\text{sup}_i}(t)$, decreased by the power used for charging battery set i, denoted as $\beta_i(t)$. Therefore, when $\beta_i(t) > 0$, the battery set i is in a *charging* state, while $\beta_i(t) < 0$ implies that the battery set i is used to provide the power deficit. When no battery is present (as in AC buses), $\beta_i(t) = 0$ is enforced at all times.

The power supplied to bus i originates from one of the power sources, i.e. one of the engines or the APU. Assuming that there are N^b buses and N^s power sources, we enforce this constraint with the following equation:

$$\sum_{k=1}^{N^s} \delta_{ki}(t) P_{\text{ktoi}}(t) = P_{\text{sup}_i}(t) \quad i = 1, ..., N^b \quad \forall\ t \geq 0 \tag{5}$$

where P_{ktoi} is the amount of power delivered by source k to bus i. Binary variables δ_{ki} determine which source should power which bus, so that $\delta_{ki}(t) = 1$ enforces that bus i is powered by source k at time t. Also, since no AC sources can be connected in parallel (per requirement `R1`), we need to enforce that each bus is powered by only one AC generator at every time. Hence,

$$\sum_{k=1}^{N^s} \delta_{ki}(t) = 1 \quad i = 1, ..., N^b \quad \forall\ t \geq 0 \tag{6}$$

Furthermore, we need to guarantee that the power available at each generator equals the power flow from the generator to the supported buses. This constraint can be enforced for power source j by the following equation

$$\sum_{k=1}^{N^b} \delta_{jk}(t) P_{\text{jtok}}(t) = \alpha_j(t) P_j^{\max}(t) \quad j = 1, ..., N^s \tag{7}$$

where $P_j^{\max}$ is the maximum capacity of power source j at time t (a known value), and $\alpha_j(t)$ is a binary variable denoting the usage of power source j at time t, i.e. $\alpha_j(t) = 1$ iff at time t source j is connected and used to power a bus. Clearly, since the number of active sources should be less than or equal to the number of buses, $\sum_{j=1}^{N^s} \alpha_j(t) \leq N^b$ must hold for all $t \geq 0$. However, due to the presence of constraints (6) and the selected cost function term (13), discussed below, this constraint becomes redundant and can be removed.

*3) **Battery Dynamics**:* For each battery set i, the normalized *State of Charge* (SoC) dynamics is captured using a simple model[2], as follows:

$$SoC_i(t+1) = SoC_i(t) + T_s \cdot K \cdot \beta_i(t). \tag{8}$$

where T_s is the sampling time, $K > 0$ is a parameter constant for all battery sets, and $SoC \in [0, 1]$. $SoC = 1$ indicates a fully charged battery while $SoC = 0$ corresponds to a depleted battery. We would like to keep SoC within a safe interval, hence we enforce

$$\underline{SoC} \leq SoC_i(t) \leq \overline{SoC} \tag{9}$$

where $\underline{SoC}$ and $\overline{SoC}$, are the lower and upper limits on the SoC of batteries. If needed, constraint (9) can be enforced $\forall t \geq t_{\text{chrg}}$, where $t_{\text{chrg}} > 0$ is considered to allow time for battery charging up to the $\underline{SoC}$ bound (as done in the simulations of Section IV).

*4) **Contactor Wear**:* It is also important to keep contactor switching activity as low as possible, to avoid contactor wear. For this purpose, the total number of status transitions (from open to close and vice versa) for a contactor that connects power source i to bus j over a time horizon of H time steps can be computed as:

$$NoS_{ij}(t^*) = \sum_{t=t^*}^{t^*+H\cdot T_s} |\delta_{ij}(t) - \delta_{ij}(t+1)| \tag{10}$$

where $|.|$ is the absolute value function. We then require

$$NoS_{ij} \leq N^{as} \quad \forall\ i = 1, ..., N^b, \qquad \forall\ j = 1, ..., N^s \tag{11}$$

where N^{as} is a safety threshold for NoS_{ij}.

*5) **Cost Function**:* In our formulation, we aim to minimize the total number (and duration) of load shedding (see requirement `R3`), as well as used generators. To achieve the first goal, we minimize the following function

$$\sum_{j=1}^{N^b} \sum_{t=t^*}^{t^*+H\cdot T_s} \Gamma_j^T [1 - C_j(t)] \tag{12}$$

where, $C_j(t) = [c_{j1}(t) \quad c_{j2}(t) \quad ... \quad c_{jn_j}(t)]^T$ is the vector of load coefficients for each bus j and $\Gamma_j = [\gamma_{j1} \quad \gamma_{j2} \quad ... \quad \gamma_{jn_j}]^T$ is a vector of weights used to penalize the act of load shedding for bus j. The components of Γ_j can be set to have same value, or be used to capture the importance of each load. For instance, if sheddable load i is more important than j for AC bus k, we choose $\gamma_{ki} \gg \gamma_{kj}$. While the latter option provides more flexibility, it is not essential to our formulation. In fact, the satisfaction of the priority tables for load shedding is already enforced by (3).

To achieve our second objective, i.e. minimize the number of generators utilized at all times, we augment the cost function with the following integral term

$$\mu \sum_{j=1}^{N^s} \sum_{t=t^*}^{t^*+H\cdot T_s} \alpha_j(t) \tag{13}$$

where μ is a constant weight parameter, which allows exploring the trade-offs involved in the multi-objective optimization problem.

Finally, we need to guarantee that the EPS obeys the bus priority table in Table I as far as possible (as per `R2`). To this aim, we enforce that the following integral expression be also minimized

$$\sum_{j=1}^{N^b} \sum_{t=t^*}^{t^*+H\cdot T_s} \Lambda_j^T \Delta_j(t) \tag{14}$$

[2]The ampere-hour (Ah) capacity of a battery depends on its temperature, rate of discharge, and age [11]. However, in this paper we do not consider this level of detail for the battery model.

where $\Delta_j(t) = [\delta_{1j}(t) \quad \delta_{2j}(t) \quad ... \quad \delta_{N^s j}(t)]^T$ is the source allocation variable vector for bus j and $\Lambda_j = [\lambda_{1j} \quad \lambda_{2j} \quad ... \quad \lambda_{N^s j}(t)]^T$ is a weighting vector that captures the source allocation priorities and penalizes the act of introducing new, unnecessary power sources in the first place. For instance, in the case of three power sources for bus 1, as in Fig. 3, we can set $\lambda_{11} = 0$ (highest priority or no penalty), $\lambda_{21} \neq 0$ (second priority in the list) as a penalty for using the GEN 2 to power bus 1, and $\lambda_{31} > \lambda_{21}$ (last priority) as a penalty for using the APU. In general, we have $\lambda_{jj} = 0$ and $\lambda_{ij} \neq 0, \quad \forall\, i \neq j$. We capture the bus priority requirements using a penalty function instead of a hard constraint, since the HL-LMS policy is deemed as a recommendation in our formulation. When the total required power is within the ratings of more than one generator, the optimizer will not violate the priority table as it minimizes the overall cost. Conversely, when a power source is not able to meet the power requirement at a bus, a decision needs to be taken on whether a load should be shed or a new supply should be introduced in the network. Our formulation is flexible enough to allow exploration of the trade-offs involved in such a choice by modifying the weighting vectors.

*6) **Putting it All Together**:* Using (1)-(14), the optimal load management problem can be formulated as follows:

Optimization problem for HL-LMS

$$\min_{S} \sum_{t=t^*}^{t^*+H\cdot T_s} \left\{ \sum_{j=1}^{N^b} [\Gamma_j^T (1 - C_j(t)) + \Lambda_j^T \Delta_j(t)] + \mu \sum_{j=1}^{N^s} \alpha_j(t) \right\}$$

subject to:

$$\sum_{k=1}^{n_i} c_{ik}(t) L_{ik}^s(t) + \sum_{k=n_i+1}^{N_i} c_{ik}(t) L_{ik}^{ns}(t) = P_{\mathrm{sup}_i}(t) - \beta_i(t)$$
$$\forall i = 1, ..., N^b \tag{15a}$$

$$\sum_{k=1}^{N^s} \delta_{ki}(t) P_{\mathrm{ktoi}}(t) = P_{\mathrm{sup}_i}(t) \quad \forall i = 1, ..., N^b \tag{15b}$$

$$\sum_{k=1}^{N^b} \delta_{jk}(t) P_{\mathrm{jtok}}(t) = \alpha_j(t) P_j^{\max}(t) \quad \forall j = 1, ..., N^s \tag{15c}$$

$$\sum_{k=1}^{N^s} \delta_{ki}(t) = 1 \qquad \forall i = 1, ..., N^b \tag{15d}$$

$$SoC_i(t+1) = SoC_i(t) + \beta_i(t) \qquad \forall i = 1, ..., N^b \tag{15e}$$

$$\underline{SoC} \leq SoC_i(t) \leq \overline{SoC} \quad \forall t \geq t_{\mathrm{chrg}}, \forall i = 1, ..., N^b \tag{15f}$$

$$\sum_{t=t^*}^{t^*+H\cdot T_s} |\delta_{ij}(t) - \delta_{ij}(t+1)| \leq N^{as} \quad \forall i = 1, ..., N^b$$
$$\forall j = 1, ..., N^s \tag{15g}$$

$$\delta_{ij}(t) = \{0, 1\} \quad \forall j = 1, ..., N^b \quad \forall i = 1, ..., N^s \tag{15h}$$

$$c_{j1}(t) \leq c_{j2}(t) \leq ... \leq c_{jN_j}(t) \quad \forall j = 1, ..., N^b \tag{15i}$$

$$c_{ji}(t) = 1 \qquad \forall j = 1, ..., N^b \quad \forall\, i \in I_j^{ns} \tag{15j}$$

$$c_{ji}(t) = \{0, 1\} \qquad \forall j = 1, ..., N^b \quad \forall i \in I_j^s \tag{15k}$$

$$\alpha_i(t) = \{0, 1\} \qquad \forall i = 1, ..., N^s \tag{15l}$$

where $S = \{C_j(t), \Delta_j(t), \alpha_j(t), \beta_i(t), P_{\mathrm{sup}_i}(t), P_{jtoi}(t)\}$ is the set of optimization variables, and constraints containing t should be evaluated at $t = \{t^*, t^* + T_s, ..., t^* + H \cdot T_s\}$.

The result is a mixed integer nonlinear program because of constraints (15b) and (15c). However, we observe that every product $\delta_{ji}(t)P_{jtoi}(t)$ in (15b)-(15c) includes a binary variable $\delta_{ji}(t)$ and a real variable $P_{\mathrm{jtoi}}(t)$ for which $0 \leq P_{\mathrm{jtoi}}(t) \leq U_j(t)$ holds, where $U_j(t) = P_j^{\max}$, the maximum power capacity of source j, is known. Therefore, by exploiting these facts, we can reformulate the above problem as follows. We first introduce a set of new variables $\pi_{ji}(t) = \delta_{ji}(t)P_{\mathrm{jtoi}}(t)$ to replace each product term in (15b)-(15c). Then, for each new variable $\pi_{ji}(t)$, we add the following constraints $\forall\ t \geq 0$:

$$0 \leq \pi_{ji}(t) \leq P_{\mathrm{jtoi}}(t) \tag{16a}$$

$$P_{\mathrm{jtoi}}(t) - U_j(t)(1 - \delta_{ji}(t)) \leq \pi_{ji}(t) \leq U_j(t)\delta_{ji}(t) \tag{16b}$$

Therefore, after these transformations, (15b) and (15c) can be replaced by the following constraints, enforced $\forall\ t \geq 0$

$$\sum_{k=1}^{N^s} \pi_{ki}(t) = P_{\mathrm{sup}_i}(t) \quad \forall i = 1, ..., N^b \tag{17a}$$

$$\sum_{k=1}^{N^b} \pi_{jk}(t) = \alpha_j(t) P_j^{\max}(t) \quad \forall j = 1, ..., N^s \tag{17b}$$

$$0 \leq \pi_{ji}(t) \leq P_{\mathrm{jtoi}}(t) \tag{17c}$$

$$P_{\mathrm{jtoi}}(t) - U_j(t)[1 - \delta_{ji}(t)] \leq \pi_{ji}(t) \leq U_j(t)\delta_{ji}(t) \tag{17d}$$

which turn the original problem into a MILP.

The above formulation can also support faulty scenarios with minor modifications. In fact, whenever a path between source j to bus i is not available, an extra constraint $\delta_{ji} = 0$ can be added to the problem, to account for either generator or contactor faults. This formulation provides the optimal solution while addressing the faulty event at the same time.

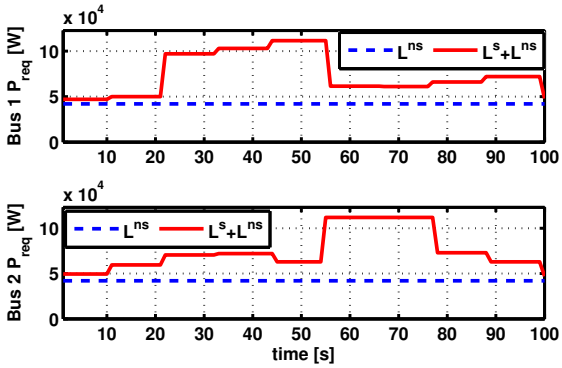

Fig. 4. Power requirement for AC Buses 1 and 2.

IV. Experimental Results

The MILP in Section III-B was formulated using YALMIP [12] and solved with CPLEX [13] for a time horizon of 100 s and a sampling time T_s=1 s. The maximum number of allowed switching events over the time horizon was set to N^{as}=2. By using t_f =0.5 s for the LL-LMS period, $T = 10T_s$ =10 s for the update rate of the receding horizon optimization, and H =30 for the prediction horizon, we obtained 960 binary and 660 real decision variables. On a 4-core 2.67-GHz Intel processor with 3.86 GB of memory, the average and maximum solver times were 0.20 s and 0.29 s, respectively. Based on our experiments, we selected τ =1 s, which is consistent with the timing diagram in Fig. 2. However, as we will show in Table IV, larger values for T and H can also be accommodated in our framework, as long as accurate predictions for

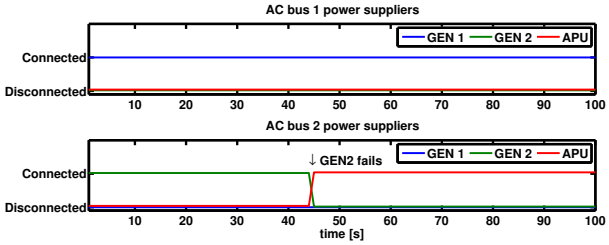

Fig. 5. Power allocation in the case of failure and only LL-LMS ($T_s = 1$ s, no battery utilization).

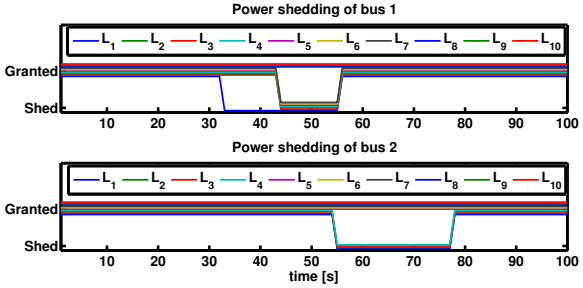

Fig. 6. Load shedding in the case failure and only LL-LMS ($T_s = 1$ s, no battery utilization). Sheddable loads are labeled $L_1, ..., L_{10}$.

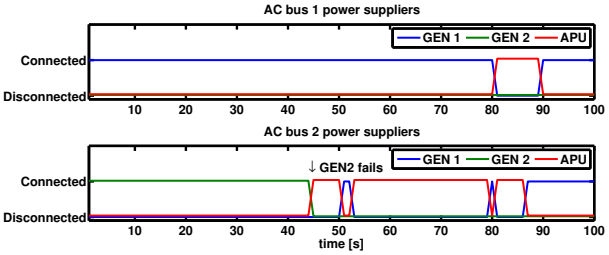

Fig. 7. Power allocation in the case of failure and hierarchical control.

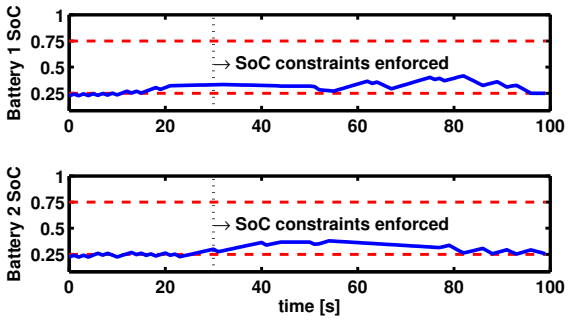

Fig. 8. Battery charge level in the case of failure and hierarchical control ($T_s = 1$ s, $\underline{SoC} = 0.25$, $\overline{SoC} = 0.75$, $t_{\text{chrg}} = 30$ s).

the required power are available. Choosing $H = 20$ s leads to 640 binary and 440 real variables, reducing the average and maximum solver times down to 0.177 s and 0.282 s. Finally, $H \leq 10$ s was observed to drastically deteriorate the quality of the results, as HL-LMS did not have sufficient information on predicted power requirements to take an adequate decision ahead of time.

We assume that AC Bus 1 and 2 in Fig. 3 have the power requirements shown in Fig. 4. These profiles are selected to mimic a typical scenario for the whole aircraft mission, even if they are scaled to a smaller time span to speed up simulation. The maximum power capacity is assumed to be 100 kW for GEN 1 and GEN 2, and 104 kW for the APU. To demonstrate the advantage of a hierarchical, optimization-based approach, we present simulation results in the occurrence of a failure when only the LL-LMS is active and when both the LL-LMS and HL-LMS operate together.

A. Occurrence of Failure (LL-LMS Only)

Fig. 5 shows the source allocation policy when only LL-LMS is active. A fault is introduced at $t = 45$ s for GEN 2, which keeps it in failure mode for the rest of the flight. Once LL-LMS detects the fault, it switches the power source for Bus 2 from GEN 2 to the APU. In fact, GEN 1, which has a higher priority in Table I, is not enough to cover by itself the power demands of all the non-sheddable loads. To minimize load shedding, a peak of 112 kW in the required power could only be handled by leveraging the extra power supplied by the batteries, in addition to inserting the APU. However, LL-LMS makes no attempts at optimizing the number of used power sources at each time and can connect batteries only in the case of emergency. As a result, the number of shed loads, shown in Fig. 6, is eventually higher than HL-LMS would propose.

B. Occurrence of a Failure (HL-LMS+LL-LMS)

To implement the HL-LMS, we set $\underline{SoC}$ and $\overline{SoC}$ to 0.25 and 0.75, and use the same values of γ for all the loads connected to each bus, since the satisfaction of their shedding priorities is already enforced via (15i) in the general problem formulation. Moreover, as a design choice, we set $\gamma_1 = \gamma_2 = 500$ and μ=10. As discussed in Section III-B, we also select $\lambda_1 = [0 \quad 1 \quad 2]$ and, by symmetry, $\lambda_2 = [1 \quad 0 \quad 2]$.

Fig. 7, 8 and 9 show source allocation, battery charge level and load shedding when GEN 2 fails at time $t = 45$ s. The HL-LMS is not able to predict such a fault while computing the optimal control input for the interval $[40, 50]$ s. However, at time $t = 45$ s, the LL-LMS detects that GEN 2 has failed, discards the control input from the HL-LMS and uses its predefined control strategy to connect Bus 2 to the APU up to time $t = 50$ s. Only when the HL-LMS collects the actual health status of generators and contactors for the interval $[50, 60]$ s, it gets notified that GEN 2 has failed and is able to accommodate such a fault by incorporating the extra constraints $(\delta_{i2} = 0, \quad i = 1, ..., N^b)$ to the MILP formulation. As a result, GEN 2 is no longer used during the mission.

Up to time $t = 44$ s, whenever DC Bus 1 requires more power than GEN 1 can provide, batteries are used as a backup supply. This is no longer the case after GEN 2 fails. Since no battery charge control is implemented at the LL-LMS level, the only possible solution is to shed the loads from Bus 1 to decrease its power requirements. Such loads are then powered back as soon as the advice from the HL-LMS is implemented again.

C. Discussion

Simulation results confirm the effectiveness of our algorithm, capable of providing an optimal policy that satisfies both EPS safety and performance requirements. To explore the impact of γ and μ parameters on the result, we performed a set of tests for different values of these parameters. As expected, the smaller the values of γ_1 and γ_2, the higher is the number of shed loads and the smaller is the number of used generators over time. On the other hand, smaller values for μ tend to encourage the use of more generators than the ones strictly needed because of power requirements.

To compare the performance of the hierarchical control architecture with the one of a conventional controller (LL-LMS only) in

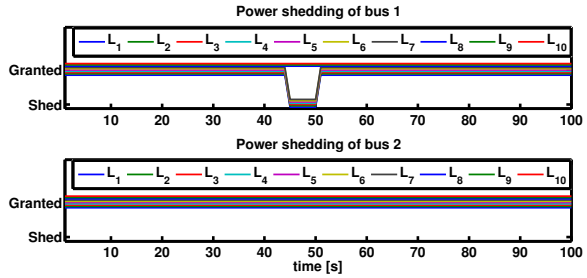

Fig. 9. Load shedding in the case of failure and hierarchical control. Sheddable loads are labeled $L_1, ..., L_{10}$.

TABLE IV

NUMBER OF OPTIMIZATION VARIABLES AND SOLVER TIME FOR A 2-BUS 3-GENERATOR EPS, WHEN THE TIME HORIZON INCREASES

Prediction horizon (H)	10	20	50	100
Number of opt. var.	430	860	2150	4300
Solver time (s)	0.3	0.19	1.25	25

terms of load shedding, we define a normalized shedding index, which quantifies the percentage of shed loads over the duration of a mission, and is based on the cost term in (12):

$$I_{\text{shed}} = \frac{\sum_{j=1}^{2}\sum_{t=0}^{100}\Gamma_j^T[1 - C_j(t)]}{\sum_{j=1}^{2}\sum_{t=0}^{100}\Gamma_j^T\mathbf{1}} \cdot 100\%, \qquad (18)$$

where $\mathbf{1} \in \mathbb{R}^{N_j}$ is a vector of ones. In our simulations, I_{shed} decreases from 9.2% for LL-LMS to 1.7% for the hierarchical controller, which means a 5-fold improvement in the latter case.

Similarly, a source utilization index can be defined based on (14):

$$I_{\text{source}} = \sum_{j=1}^{2}\sum_{t=0}^{100}\Lambda_j^T\Delta_j(t), \qquad (19)$$

which quantifies the cost associated to the usage of power sources over the duration of a mission. In our simulation, I_{source} decreases from 110 (LL-LMS only) to 76 (LL-LMS + HL-LMS), which is a 31%-reduction in the hierarchical control case.

To test the *scalability* of the proposed framework, we performed optimizations with different time horizons. No substantial improvement in the quality of the solution was observed for $H > 30$ in our experiments, in spite of the larger computation time. However, as evident from Table IV, even problems with thousands of variables can be solved in a few seconds using the proposed formulation. Finally, we also implemented controllers for EPS topologies with a larger number of generators and loads, in which the number of buses and contactors is also increased proportionally. The results in Table V show that, for a realistic number of generators (normally less than 10), computation times stay largely compatible with the timing assumptions needed for the correct operation of the proposed hierarchical scheme.

V. CONCLUSIONS

We developed a hierarchical optimal load management system for aircraft electric power distribution. In our approach, a high-level load management system (HL-LMS) coordinates load shedding, source allocation and battery utilization, by solving an efficient mixed integer-linear program within a receding horizon approach. The result of the optimal control problem is offered as advice to a low-level load management system (LL-LMS) that can directly actuate the EPS contactors. Every time a failure occurs, the advice from the HL-LMS is disregarded and the LL-LMS applies a predefined, worst-case control policy, until the high-level optimization problem formulation is updated with the actual system status to accommodate the fault.

TABLE V

NUMBER OF OPTIMIZATION VARIABLES AND SOLVER TIME FOR H=30 (B AND G STAND FOR BUS AND GENERATOR, RESPECTIVELY)

Number of nodes	Number of opt. var.	Solver time (s)
B=4, G=3	binary: 960, real: 660	ave: 0.20, max: 0.29
B=10, G=5	binary: 2300, real:1650	ave: 2.10, max: 2.22
B=20, G=10	binary: 6100, real: 6300	ave: 6.87, max: 7.0

In addition to guaranteeing system safety, our hierarchical architecture shows substantial performance improvements with respect to a conventional one, based on just an LL-LMS, in terms of percentage of shed loads and number of utilized sources. Finally, simulation results show that the optimal control problem scales reasonably in the context of the selected application.

VI. ACKNOWLEDGMENTS

The authors wish to acknowledge Richard Poisson (UTC), Mohammad Mozumdar (CSULB), Huy Vo (UCB) for helpful discussions. This work was supported in part by IBM and United Technology Corporation through the iCyPhy consortium and by TerraSwarm, one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA. The second and third authors were also supported, respectively, by an IBM Ph.D. Fellowship, and the US DoD through the NDSEG Fellowship program.

REFERENCES

[1] I. Moir and A. Seabridge, *Aircraft Systems: Mechanical, electrical, and avionics subsystems integration*. Chichester, England: John Wiley & Sons Inc, 2008.

[2] A. Sangiovanni-Vincentelli, "Quo vadis, SLD? Reasoning about the trends and challenges of system level design," *Proc. IEEE*, no. 3, pp. 467–506, 2007.

[3] P. Nuzzo, F. De Bernardinis, and A. Sangiovanni Vincentelli, "Platform-based mixed signal design: Optimizing a high-performance pipelined ADC," *Analog Integr. Circuits Signal Process.*, vol. 49, no. 3, pp. 343–358, 2006.

[4] J. Bals, G. Hofer, A. Pfeiffer, and C. Schallert, "Virtual iron bird – A multidisciplinary modelling and simulation platform for new aircraft system architectures," *DGLR Luft-und Raumfahrtkongress*, 2005.

[5] P. Krus and J. Nyman, "Complete aircraft system simulation for aircraft design – Paradigms for modelling of complex system," in *Int. Congress Aeronautical Sciences*, 2000.

[6] S. Chandrasekaran, S. Ragon, D. Lindner, Z. Gurdal, and D. Boroyevich, "Optimization of an aircraft power distribution subsystem," *Journal of aircraft*, vol. 40, no. 1, pp. 16–26, 2003.

[7] A. Pinto, S. Becz, and H. M. Reeve, "Correct-by-construction design of aircraft electric power systems," in *2010 AIAA ATIO/ISSMO Conference*, September 2010.

[8] H. Xu, U. Topcu, and R. M. Murray, "A case study on reactive protocols for aircraft electric power distribution," in *Int. Conf. Decision and Control*, 2012.

[9] A. Pnueli, "The temporal logic of programs," in *Proc. Symp. on Foundations of Computer Science*, Nov. 1977, pp. 46–57.

[10] R. Michalko, "Electrical starting, generation, conversion and distribution system architecture for a more electric vehicle," Oct. 21 2008, US Patent 7,439,634.

[11] C. R. Spitzer, *The avionics handbook*. CRC Press LLC, 2001.

[12] J. Lofberg, "Yalmip: A toolbox for modeling and optimization in matlab," in *Int. Symp. Computer Aided Control Systems Design*, 2004, pp. 284–289.

[13] (2012, Feb.) IBM ILOG CPLEX Optimizer. [Online]. Available: www.ibm.com/software/integration/optimization/cplex-optimizer/