2015 American Control Conference
Palmer House Hilton
July 1-3, 2015. Chicago, IL, USA

Stochastic Model Predictive Control Design for Load Management System of Aircraft Electrical Power Distribution

Behrooz Shahsavari, Mehdi Maasoumy, Alberto Sangiovanni-Vincentelli, Roberto Horowitz

Abstract— **Aircraft Electric Power Systems (EPS) route power from generators to vital avionics loads by configuring a set of electronic control switches denoted as contactors. The external loads applied to an EPS, power requirement of the system, electrical component failure events, and the dynamics of the system are inherently uncertain. In this paper, we address the problem of designing a stochastic optimal control strategy for the EPS contactors. We first represent mathematical models of different components of an EPS, and formalize the performance metrics of the system as well as the constraints that should be satisfied in a stochastic modeling framework. We then formulate the optimization of the system performance as a stochastic model predictive control (SMPC) problem, and present two special cases of the proposed SMPC analysis to approximate the problem with linear mixed-integer optimization problems. Finally, we report simulation results to confirm the effectiveness of the proposed approach.**

I. Introduction

Advances in systems technology, high performance and reliable power electronics, together with powerful digital computing platforms have enabled an unprecedented amount of "electrification" of aircrafts in recent years [7]. Electrical and electronic components replace the mechanical systems such as hydraulics, and pneumatics to provide increased overall system efficiency [9]. However, the increased use of electrical components poses reliability concerns in aircraft electrical power generation and distribution.

In an aircraft electric power system (EPS), a set of electromechanical switches are actuated by supervisory control units to dynamically route electric power from generators to loads, while satisfying safety, reliability, and real-time performance requirements, as in Fig 1.

In our previous work [5], we addressed the problem of control design for aircraft EPS within a Platform-Based Design (PBD) methodology [10]. We developed an optimal load management system based on the formalization of the connectivity, safety and performance requirements of an EPS. We proposed a two-level hierarchical scheme where a high-level load management system (HL-LMS) 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 an "advice" for the low-level load management system (LL-LMS), which handles system faults by directly actuating the EPS contactors, and decides to implement such advice only if it is safe.

B. Shahsavari and R.Horowitz are with the Department of Mechanical Engineering, M. Maasoumy and A. Sangiovanni-vincentelli are with the Department of Electrical Engineering and Computer Sciences, all in University of California, Berkeley, CA 94720, USA {behrooz, mehdi_maasoumy, alberto, horowitz}@berkeley.edu

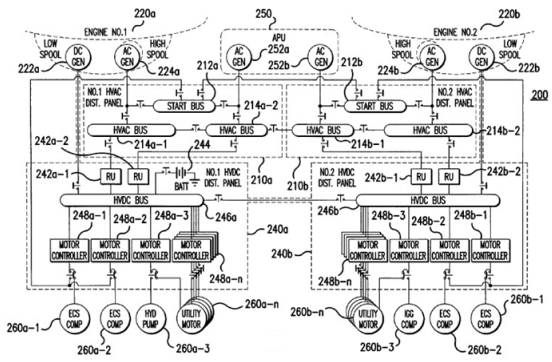

Fig. 1. Single line diagram of an EPS from a Honeywell, Inc. patent [6].

However, various quantities and phenomena in an EPS such as load forecast, power generation, and contactors and generators failure events are *stochastic* in nature. Furthermore, performance criteria such as succeeding in supplying power to buses and keeping the state of charge of battery above a certain threshold are often defined as probabilistic constraints (e.g. failure with probability less than 10^{-6}). To properly model uncertain behavior of various EPS components and system performance criteria, in this paper we improve upon the deterministic HL-LMS introduced in [5], with a novel stochastic model predictive control (SMPC) framework. The LL-LMS and its functionality are kept intact.

Our approach builds on a number of results that opened the way for a more formal EPS design methodology. An automated procedure for correct-by-construction design of the EPS control protocol is discussed in [11]. System specifications are first converted using linear temporal logic [8], and then automatically synthesized by leveraging formal methods to guarantee safety constraints. While the correctness of the final solution is guaranteed, its optimality with respect to a number of performance metrics is not addressed.

This paper is organized as follows: in Section II general system components, requirements and control architecture are described. In Section III the stochastic optimization problem for controlling the contactors is presented. We introduce two relaxations of the general problem in Section IV and provide solutions to them. Simulation results in Section V confirm the effectiveness of the proposed approach. Conclusions are drawn in Section VI.

978-1-4799-8684-2/$31.00 ©2015 AACC

II. System Description

A. Electric Power System

An aircraft EPS, as shown in Fig. 1, typically consists of a combination of generators, contactors, buses and loads. The connections among different components are specified by a Single Line Diagram (SLD), a simplified notation for representing three-phase power systems [7]. AC and DC *generators* deliver power to a number of AC and DC *loads* or power conversion equipments, such as *Transformers* and *Rectifier Units* (TRU). 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.

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.

B. System Requirements

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.* No bus can be powered by multiple AC generators at the same time.

R2) *Bus priorities.* Each bus has a prioritized list of preferred generators. If the first priority generator is unavailable, the second generator is used.

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.

C. Hierarchical Load Management System

In this paper we use the hierarchical architecture proposed in [5], that controls power source utilization, load shedding, contactor status and battery charge. 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 the 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 time horizon H, only the initial samples of the solution (up to time T) are sent to the LL-LMS as *advice*.

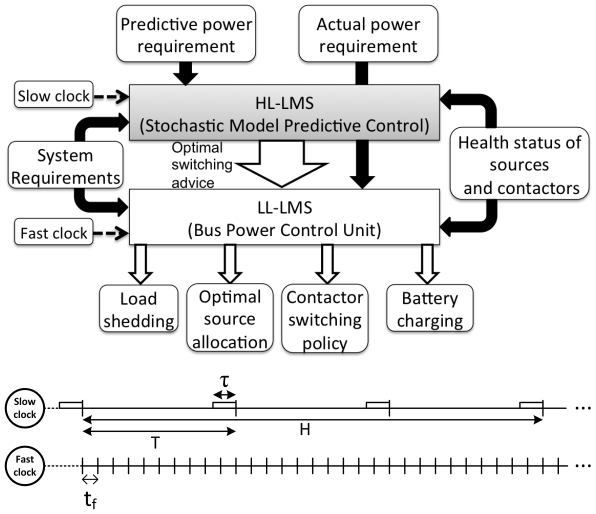

Fig. 2. Block diagram of the proposed hierarchical control architecture (top) and timing diagram for its operation (bottom). In the top figure, white arrows show control signals, black solid arrows show flow of information and dashed black arrows represent timers.

As discussed in detail in [5], The maximum computation time of the optimal control problem is assumed to be $\tau \leq T$. In fact, as discussed in Section V, 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 a component or an unpredicted change in load forecast is 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.

III. System Modeling

This section presents a refinement of the deterministic optimization problem given in [5] to capture the inherent

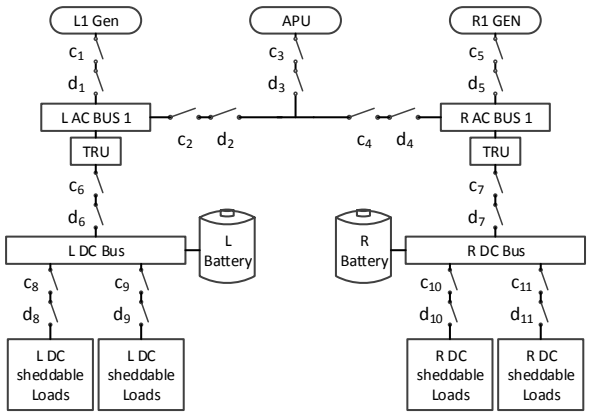

Fig. 3. Single line diagram of an electric power system.

randomness in the status of contactors, generators and external loads. We use the SLD in Fig. 3 as a running example.

For loads and generated power, it is possible to use prior statistical information, and current measured data attained by sensors, to obtain a prediction of these quantities. However, the health status of contactors and generators are inherently unpredictable. In the following subsection, we present a statistical model for each of these components.

1) ***Contactor Modeling****:* Health status of each contactor can be captured by a Boolean variable, which is zero when the contactor is failed and one when it is healthy. Notice that the "health status" of a contactor differs from the contactor "status" that is used in [5]. Indeed, the health status is a random variable, while the contactor status is a control parameter that is determined by the controller. Therefor, a contactor can transmit power only when it is healthy and closed. In Fig. 3 random variables associated to the contactors are shown by d_i's and control variables are shown by c_i's, where $i \in \{1, 2, \cdots, 11\}$.

We assume that when a contactor fails, it will remain inoperative forever. Hence, we model the health status of each contactor at time k as a Bernoulli random variable by conditioning on its health status at the previous time step

$$\left[d_i(k)|d_i(k-1)\right] =_D \mathcal{B}(h_i d_i(k-1)) \tag{1}$$

where $\mathcal{B}(h)$ denotes a Bernoulli distribution with h being the probability of outcome 1.

We categorize the contactors into two sets according to their placement in the SLD: 1) the contactors that transmit power from sources to buses which are called *source contactors*, and 2) *load contactors* that connect buses to loads. An important point to make is that although both types are inherently subject to failure, we can neglect the stochastic behavior of the latter case in the synthesis of HL-LMS controller. This assumption can be justified by considering two cases, namely when a source is disconnected and when a load is detached unwontedly. The HL-LMS controller can take the possibility of the former situation into account and disconnect some of the sheddable loads accordingly. However, there is nothing that the HL-LMS controller can do in the latter situation and from the standpoint of HL-LMS this type of failure – if not compensated by the LL-LMS – means less demand for power, which is not destructive.

2) ***Power Source and Load Modeling****:* The output power source j, can be modeled as a Gaussian random variable $P_j^{max} =_D \mathcal{N}(\mu_{P_j}, \sigma_{P_j})$ where $\mathcal{N}(\mu, \sigma)$ denotes a μ-mean Gaussian distribution with variance of σ^2. We denote the i-th non-sheddable and sheddable load connected to bus j at time step k as $L_{ji}^{ns}(k)$ and $L_{ji}^{s}(k)$ respectively. Similar to the power sources, both of these load types are modeled as Gaussian random variables:

$$\begin{aligned} L_{ji}^{s}(k) &=_D \mathcal{N}\left(\mu_{L_{ji}^{s}(k)}, \sigma_{L_{ji}^{s}(k)}\right) \\ L_{ji}^{ns}(k) &=_D \mathcal{N}\left(\mu_{L_{ji}^{ns}(k)}, \sigma_{L_{ji}^{ns}(k)}\right). \end{aligned} \tag{2}$$

However, unlike the output power, the loads are not wide-sense stationary (WSS) and the mean and variance values are changing over time.

We model the required power at time step k as the summation of contributions from different power sinks (loads). Hence, for bus j

$$\begin{aligned} P_{req_j}(k) = &\sum_{i \in I_{j,h}^{s} \cup I_{j,f}^{s}} d_{ji}(k) c_{ji}(k) L_{ji}^{s}(k) \\ &+ \sum_{i \in I_{j,h}^{ns} \cup I_{j,f}^{ns}} d_{ji}(k) c_{ji}(k) L_{ji}^{ns}(k) \end{aligned} \tag{3}$$

where $I_{j,f}^{s}(k)$ and $I_{j,h}^{s}(k)$ denote the sets of sheddable loads connected to bus j by failed and healthy contactors respectively. Similarly, $I_{j,f}^{ns}(k)$ and $I_{j,h}^{ns}(k)$ respectively denote the set of non-sheddable loads connected to bus j by failed and healthy contactors at time step k. $P_{req_j}(k)$ is the total required power by electrical loads connected to bus j.

Let $d_{ji}(k)$ be a Bernoulli random variable that models the possibility of failure in the connection between bus j and load i when $t \in [kT, (k+1)T)$, i.e.

$$d_{ji}(k) =_D \mathcal{B}\left(h_{d_{ji}}(k)\right) \tag{4}$$

where $h_{d_{ji}(k)}$ is the probability that the connection is healthy – i.e. $d_{ji}(k) = 1$.

Each coefficient $c_{ji}(k)$ for bus j and load i at time k is a binary decision variable. If a contactor is healthy, it specifies whether power $L_{ji}(k)$ must be supplied or it can temporarily be interrupted for sheddable loads; and when that contactor fails, its value is constrained to zero, i.e. for $j = 1, \cdots, N^b$, where N^b is the number of buses, we have

$$c_{ji}(k) = \begin{cases} 1 & \forall\ i \in I_{j,h}^{ns}(k) \\ 0 & \forall\ i \in I_{j,f}^{ns}(k) \cup I_{j,f}^{s}(k) \\ \{0,1\} & \forall\ i \in I_{j,h}^{s}(k) \end{cases} \tag{5}$$

Finally, we capture shedding priorities $\forall m, n \in I_{j,h}^{s}(k)$

$$c_{jm}(k) \leq c_{jn}(k) \qquad \text{if } m \leq n, \;\; j = 1, ..., N^b \tag{6}$$

so that loads get ranked based on their priority if they are connected to healthy contactors.

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

$$P_{req_j}(k) = P_{sup_j}(k) - \beta_j(k) \quad j = 1, ..., N^b \quad \forall\, k \geq 0 \quad (7)$$

where the required power P_{req_j} from the loads, defined in (3), is equal to the amount of power supplied to bus j, $P_{sup_j}(k)$, minus the power used for charging battery set j, denoted as $\beta_j(k)$. Therefore, when $\beta_j(k) > \beta_{min}$ for some $\beta_{min} > 0$, the battery set j is in a *charging* state, while $\beta_j(k) \leq 0$ implies that the battery set j is used to provide the power deficit. When no battery is present (as in AC buses), $\beta_j(k) = 0$ is enforced at all times.

Power supplied to bus j originates from one of the power sources. Assuming that there are N^b buses and N^s power sources, we enforce these constraints with

$$P_{sup_j}(k) = \sum_{m=1}^{N^s} \gamma_{mj}(k)\delta_{mj}(k)P_{mtoj}(k) \quad \forall j = 1, ..., N^b \quad (8)$$

where P_{mtoj} is the amount of power delivered by source m to bus j. $\gamma_{mj}(k)$ is a Bernoulli random variable that models the possibility of failure in the connection between source m and bus j when $t \in [kT, (k+1)T)$, i.e.

$$\gamma_{mj}(k) =_D \mathcal{B}\left(h_{\gamma_{mj}(k)}\right) \quad (9)$$

where $h_{\gamma_{mj}(k)}$ is the probability that the connection is healthy (i.e $\gamma_{mj}(k) = 1$) Binary variables δ_{mj} determine which source should power which bus, so that $\delta_{mj}(k) = 1$ enforces that source m powers bus j at time k. Also, since no AC sources can be connected in parallel, we need to enforce that each bus is powered by only one generator at every time

$$\sum_{m=1}^{N^s} \delta_{mj}(k) = 1 \quad j = 1, ..., N^b \quad \forall\, k \geq 0 \cdot \quad (10)$$

It is possible that at least one contactor placed in the connection from source m to bus j fails. We denote the set of buses that cannot be fed from source m, due to the failure in the connections, as $I^b_{m,f}$. Hence, we need to enforce the value of δ to be zero for those connections, i.e.

$$\delta_{mj}(k) = 0 \quad \forall j \in I^b_{m,f}(k) \quad i = 1, ..., N^s \quad (11)$$

Finally, 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 a power source m by the following equations $\forall\ k \geq 0$

$$\sum_{j=1}^{N^b} \delta_{mj}(k)P_{mtoj}(k) = \epsilon_m(k)\alpha_m(k)P^{max}_m(k), \quad m = 1, ..., N^s \quad (12)$$

where $P^{max}_m(k)$ is the maximum capacity of power source m at time $t = kT$. $\alpha_m(k)$ is a binary variable denoting the use of power source m, i.e. $\alpha_m(k) = 1$ if and only if source m is used to power a bus at time kT. Similar to (12) we can pose a constraint on the values of α_is connected to the failed generators. However, we assume that the output power of the failed generators is zero (i.e. $P^{max}(k) = 0$ for that generator). Hence, a constraint like (12) for α_is is redundant. $\epsilon_m(k)$ is a Bernoulli random variable that models the failure possibility of a contactor that connects the m-th source

$$\epsilon_m(k) =_D \mathcal{B}\left(h_{\epsilon_m(k)}\right). \quad (13)$$

*4) **Battery Dynamics**:* It is desirable to keep the battery charge level higher than a predefined minimum value. The reason for this limitation is that, completely discharging a battery will decrease its effective life. Also, a minimum battery charge can be used in unpredictable hazard cases. We model the battery charge level as in (14) where the battery charge level is the state and $\beta_j(k)$ as in (7) is the input, i.e.

$$E_j(k+1) = E_j(k) + \beta_j(k) \quad (14)$$

where $E_j(k)$ is the battery charge level at time k. Equation (7) shows that the value of $\beta_j(k)$ is a function of output powers and external loads. We know from the previous subsections that all these variables are random. Hence, $\beta_j(k)$ is also a random variable and its statistics depend on the statistics of powers, loads and contactors, as well as the status of contactors. Consequently, the battery charge level is also random. Since battery charge level is random, we cannot consider a deterministic constraint on it. Instead, we exploit chance constraints to guarantee that the battery charge level does not go lower than a given value with a given probability

$$Pr\left(E_j(k) \geq \phi_j\right) \geq (1 - \lambda_j), j = 1, \cdots, N^b, \forall k \geq 0 \quad (15)$$

where ϕ_j is the lower bound on the j-th battery charge level and λ_j is the maximum acceptable probability of violation.

*5) **Cost Function**:* We solve the optimal control problem at each time k over a horizon H and apply the first optimal control policy to the system. We aim to minimize the total number of load shedding as well as used generators. Hence, we consider a penalty for shedding each load as follows (16).

$$\sum_{k=n}^{n+H-1} \sum_{j=1}^{N^b} \Gamma_j^T[\mathbf{1} - C_j(k)] \quad (16)$$

where, $C_j(k) = [c_{j1}(k) \quad c_{j2}(k) \quad \cdots \quad c_{jn_j}(k)]^T$ 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 shedding for bus j. Components of Γ_j can be set to have same value, or be used to capture different priority associated with each load. For instance, if sheddable load i is more important than j for AC bus b, we choose $\gamma_{bi} \gg \gamma_{bj}$. In fact, satisfaction of load shedding priority tables is already enforced by (6).

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

$$\mu \sum_{k=n}^{n+H-1} \sum_{m=1}^{N^s} \alpha_m(k) \quad (17)$$

where μ is a constant weight parameter, that allows exploring the trade-offs in our multi-objective optimization.

Finally, we need to guarantee that the EPS obeys the bus priority table as much as possible. To this aim, we enforce that the following summation expression be also minimized

$$\sum_{k=n}^{n+H-1} \sum_{j=1}^{N^b} \Lambda_j^T \Delta_j(k) \quad (18)$$

where $\Delta_j(k) = [\delta_{1j}(k) \quad \delta_{2j}(k) \quad \cdots \quad \delta_{N^s j}(k)]^T$ 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 source allocation priorities, and penalizes the act of introducing new, unnecessary power sources. 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 APU to power bus 1, and $\lambda_{31} > \lambda_{21}$ (last priority) as a penalty for using R1 GEN. 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. 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 its 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 (3)-(18), the optimal load management problem at time step n and over horizon H can be formulated as follows:

SMPC formulation

$$\min_{S} \sum_{k=n}^{n+H-1} \left\{ \sum_{j=1}^{N^b} [\Gamma_j^T (1 - C_j(k)) + \Lambda_j^T \Delta_j(k)] + \mu \sum_{m=1}^{N^s} \alpha_m(k) \right\}$$

subject to:

$$\beta_j(k) = P_{sup_j}(k) - P_{req_j}(k) \tag{19a}$$

$$P_{req_j}(k) = \sum_{i \in I^s_{j,h} \cup I^s_{j,f}} d_{ji}(k) c_{ji}(k) L^s_{ji}(k) + \sum_{i \in I^{ns}_{j,h} \cup I^{ns}_{j,f}} d_{ji}(k) c_{ji}(k) L^{ns}_{ji}(k) \tag{19b}$$

$$P_{sup_j}(k) = \sum_{m=1}^{N^s} \gamma_{mj}(k) \delta_{mj}(k) P_{mtoj}(k) \tag{19c}$$

$$\sum_{j=1}^{N^b} \delta_{mj}(k) P_{mtoj}(k) = \epsilon_m(k) \alpha_m(k) P^{max}_m(k) \tag{19d}$$

$$c_{ji}(k) = \begin{cases} 1 & \forall\ j \in I^{ns}_{j,h}(k) \\ 0 & \forall\ j \in I^{ns}_{j,f}(k) \cup I^s_{j,f}(k) \\ \{0,1\} & \forall\ j \in I^s_{j,h}(k) \end{cases} \tag{19e}$$

$$c_{jl}(k) \leq c_{jo}(k) \quad \forall l, o \in I^s_{j,h}(k) \text{ and } l \leq o \tag{19f}$$

$$\delta_{mj} = \{0, 1\} \tag{19g}$$

$$\alpha_m = \{0, 1\} \tag{19h}$$

$$\sum_{m=1}^{N^s} \delta_{mj}(k) = 1 \tag{19i}$$

$$\delta_{ji}(k) = 0 \quad \forall i \in I^b_{j,f}(k) \tag{19j}$$

$$E_j(k+1) = E_j(k) + \beta_j(k) \tag{19k}$$

$$Pr\left(E_j(k) \geq \phi_j\right) \geq (1 - \lambda_j) \tag{19l}$$

where $j \in \{1, \cdots, N^b\}$, $m \in \{1, \cdots, N^s\}$ and $S = \{C_j(k), \Delta_j(k), \alpha_m(k), \beta_j(k), P_{sup_j}(k), P_{mtoj}(k)\}$ is the set of optimization variables. (19a) corresponds to the power balance for each bus, (19c) allocates power supplies to buses, (19e)-(19j) define the binary decision variables for the source selection and load shedding problems. Equations (19i) enforce that only one power supply powers each bus at all times, (19f) formulate the shedding priority relations, (19e) defines the sheddable and non-sheddable load coefficients. Constraints (19l) enforce that the probability of battery charge level being larger than a predefined value is greater than or equal to a specified amount.

IV. Solving Simplified Cases

SMPC formulation in (19) involves mixed integer nonlinear optimization. Many promising theoretical and methodological achievements for this type of problems have been reported by the researchers in recent years [3]. However, we will not discuss this approach here, as we prefer to focus on two special cases and show how they can be reformulated as mixed-integer linear programming problems that can be more effectively solved in real time applications.

We first discuss how the problem can be linearized when the contactors are assumed to be deterministic and then consider the case in which the loads are deterministic but the health status of contactors is stochastic.

A. Deterministic Contactors

We assume that health status of contactors is constant, i.e. d_{ji}, γ_{mj} and ϵ_m in (19) are all 1, and the failure of a contactor is modeled by constraint (19e). We replace (19l) with a linear inequality. Statistics of batteries charge level, $E_j(k)$, are functions of statistics of loads, powers, contactors and status of contactors. We first derive probability density function (PDF) for battery charge level and then change (19l) to an affine inequality between mean and standard deviation of battery charge level.

*1) **Battery Charge Level Statistics**:* Mean and covariance dynamics of the battery charge level are given by:

$$\mu_{req_j}(k) = \sum_{i \in I^s_{j,h} \cup I^s_{j,f}} c_{ji}(k) \mu_{L^s_{ji}}(k) + \sum_{i \in I^{ns}_{j,h} \cup I^{ns}_{j,f}} c_{ji}(k) \mu_{L^{ns}_{ji}}(k) \tag{20a}$$

$$\sigma^2_{req_j}(k) = \sum_{i \in I^s_{j,h} \cup I^s_{j,f}} c_{ji}(k) \sigma^2_{L^s_{ji}}(k) + \sum_{i \in I^{ns}_{j,h} \cup I^{ns}_{j,f}} c_{ji}(k) \sigma^2_{L^{ns}_{ji}}(k) \tag{20b}$$

Similarly, the statistics of P_{sup_j} can be characterized by

$$\mu_{sup_j}(k) = \sum_{m=1}^{N^s} \delta_{mj}(k) \mu_{P_{mtoj}}(k) \tag{21a}$$

$$\sigma^2_{sup_j}(k) = \sum_{m=1}^{N^s} \delta_{mj}(k) \sigma^2_{P_{mtoj}}(k) \tag{21b}$$

where (19a) links $\beta_j(k)$ to $P_{sup_j}(k)$ and $P_{req_j}(k)$

$$\mu_{\beta_i}(k) = \mu_{sup_i} - \mu_{req_i} \tag{22a}$$

$$\sigma^2_{\beta_i}(k) = \sigma^2_{sup_i}(k) + \sigma^2_{req_i}(k) \tag{22b}$$

TABLE I

DESIGN PARAMETERS

Parameter	Value	Parameter	Value
ϕ_1	1.0×10^5	ϕ_2	1.1×10^5
λ_1	1.0×10^{-2}	λ_2	1.0×10^{-2}
$t_{min,1}$	$40s$	$t_{min,2}$	$20s$
$\sigma^2_{L^s_{ij}}/L^s_{ij}$	1.0×10^{-1}	$\sigma^2_{L^{sn}_{ij}}/L^{ns}_{ij}$	1.0×10^{-1}

The battery charge level can be found by integrating the current over the time, which after discretization can be presented by (19k). Equivalently, we can write $E_i(k)$ as

$$E_j(k) = \sum_{\tau=0}^{k-1} \beta_j(\tau) \quad j = 1, \cdots, N^b \tag{23}$$

where, without loss of generality, we have assumed that $E_i(0) = 0$. Finally, we derive the statistics of battery charge level by exploiting (22) and (23),

$$\mu_{E_j}(k) = \sum_{\tau=0}^{k} \mu_{\beta_j}(k), \qquad \sigma^2_{E_j}(k) = \sum_{\tau=0}^{k} \sigma^2_{\beta_j}(k) \tag{24}$$

*2) **Linearization**:* We use (24) and the method proposed by [1] to replace (19l) by a linear inequality between mean and standard deviation of battery charge level (24)

$$\begin{aligned} Pr\left(E_j(k) \le \phi_j\right) &\le \lambda_j \\ \frac{1}{2} + \frac{1}{2}\text{erf}\left(\frac{\phi_j - \mu_{E_j}(k)}{\sqrt{2\sigma^2_{E_j}(k)}}\right) &\le \lambda_j \\ \phi_j + \sigma_{E_j}(k)\left[\sqrt{2}\text{erf}^{-1}\left(1 - 2\lambda_j\right)\right] &\le \mu_{E_j}(k). \end{aligned} \tag{25}$$

B. Deterministic Loads

We now consider a case where loads and power sources are deterministic, but source contactors are subject to failure in a stochastic sense. Suppose that contactor health status data received just before starting each horizon is valid only for that time step k, and contactors may fail with some probabilities during the SMPC horizon. Here we assume:

A0) All the loads and power sources are deterministic.
A1) A contactor remains inoperative if it fails.
A2) Contactors that connect loads to DC buses never fail.
A3) Power sources never fail during one horizon of the optimization problem – i.e. $\epsilon_m(k) = 1$ with probability 1 for $1 \le m \le N^s$.

Let $\Psi_j(k)$ be a matrix that contains all the random variables corresponding to the past health statuses of source contactors

$$\Psi_j(k) := \begin{bmatrix} \gamma_{1j}(1) & \gamma_{2j}(1) & \cdots & \gamma_{N^s j}(1) \\ \gamma_{1j}(2) & \gamma_{2j}(2) & \cdots & \gamma_{N^s j}(2) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{1j}(k) & \gamma_{2j}(k) & \cdots & \gamma_{N^s j}(k) \end{bmatrix}.$$

A1 implies that $\gamma_{mj}(k_1) \ge \gamma_{mj}(k_2)$ if $1 \le k_1 \le k_2 \le k$, which will significantly decrease the number of possible values for $\Psi_j(k)$. For instance, if the power lines from sources to DC buses do not share any common contactors, columns of $\Psi_j(k)$ are independent and there are only $(k+1)^{N^s}$ possible values of $\Psi_j(k)$. We denote $\bar{\Psi}_j(k) := \{\bar{\Psi}^r_j(k) | 1 \le r \le N_{\Psi_j(k)}\}$ as the set of all outcomes of $\Psi_j(k)$, and $N_{\Psi_j(k)}$ as the cardinality of this set. Hence, the complementary CDF in (19l) can be decomposed

$$Pr\left(E_j(k) \ge \phi_j\right) = \sum_{r=1}^{N_{\Psi_j(k)}} t^{j,k}_r \pi^{j,k}_r \tag{26}$$

$$t^{j,k}_r := Pr\left(E_j(k) \ge \phi_j | \Psi_j(k) = \bar{\Psi}^r_j(k)\right) \tag{27}$$

$$\pi^{j,k}_r := Pr\left(\Psi_j(k) = \bar{\Psi}^r_j(k)\right). \tag{28}$$

For a given $\bar{\Psi}_{ij}(k)$, prior probability $Pr\left(\Psi_i(k) = \bar{\Psi}_{ij}(k)\right)$ can be found based on the failure probability of contactors and the power transmission architecture. The conditional probability, $t^{j,k}_r$, can be represented as a constraint

$$\begin{aligned} &Pr\left(E_j(k) \ge \phi_j | \Psi_j(k) = \bar{\Psi}^r_j(k)\right) \\ &= Pr\left(\sum_{\tau=0}^{k-1} \beta_j(\tau) \ge \phi_j | \Psi_j(k) = \bar{\Psi}^r_j(k)\right) \\ &= Pr\Bigg(\underbrace{\sum_{\tau=0}^{k-1}\left[\sum_{m=1}^{N^s} \bar{\gamma}_{mj}(k)\delta_{mj}(k)P_{mtoj}(k) - P_{req_j}(k)\right]}_{E_{\bar{\Psi}^r_j(k)}} \ge \phi_j\Bigg) \\ &= \begin{cases} 1 & \text{if } E_{\bar{\Psi}^r_j(k)} \ge \phi_j \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{29}$$

where $\bar{\gamma}_{mj}(k)$ is the element (m, j) in $\bar{\Psi}^r_j(k)$.

Finally we need to change the logical relations in (29) to a suitable form for the optimization problem. This can be done by introducing an auxiliary variable $\bar{t}^{j,k}_r$

$$\bar{t}^{j,k}_r = \max\left(0, E_{\bar{\Psi}^r_j(k)} - \phi_j\right) \tag{30}$$

$$t^{j,k}_r = \frac{1}{\xi_j}\min\left(\xi_j, \bar{t}^{j,k}_r\right) \tag{31}$$

Constant ξ_j should be chosen such that $0 < \xi_j < \phi_j$.

V. SIMULATION RESULTS

In this section, we show the effectiveness of the proposed control design methodology by a simulation study for a particular example of an EPS, which is shown in Fig. 3. The optimization problem is formulated in YALMIP [4] and CPLEX-IBM [2] is used as the solver. On a 3.40GHz Quad-core Intel CPU with 12.0 GB memory the average solver time was 0.52s. We assume that there are 10 sheddable DC loads connected to each of the DC buses. The profiles of the total sheddable and non-sheddable loads are presented in Fig. 4. The design parameters are listed in Table. I. Figures 7, 5, 6 and 8 respectively shows the load shedding for AC bus 1 and 2, batteries charging status, and batteries charge level.

As it is shown in Fig. 8 we require the battery charge level to raise above a lower bound after a given time. Here we assume that the battery charge level is zero at the beginning. Therefore, the controller has to shed some of the loads and instead use the power to charge the batteries. Both figures 7 and 5 show that the loads with low priority (i.e. with smaller subscript) are shed at the beginning to satisfy the

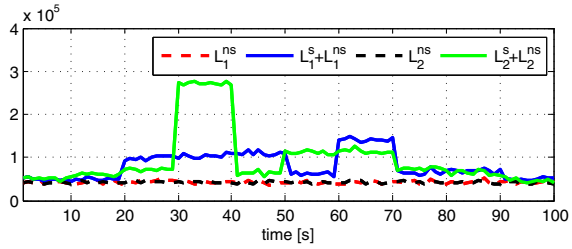

Fig. 4. Load profiles.

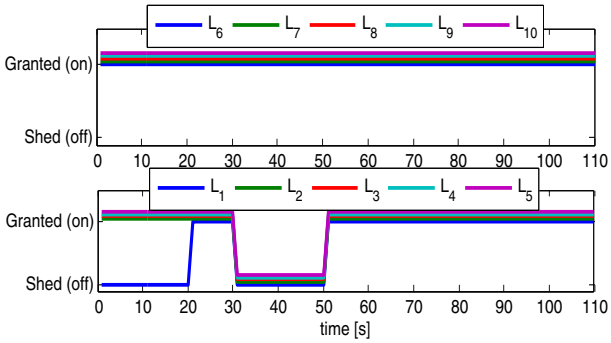

Fig. 5. Load shedding for AC bus 2.

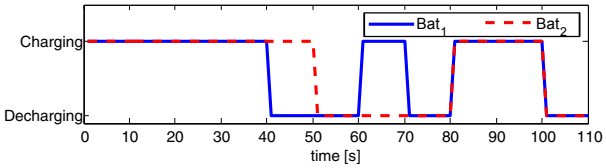

Fig. 6. Batteries charging status.

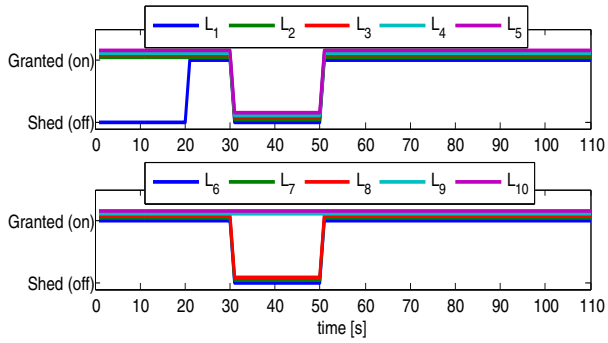

Fig. 7. Load shedding for AC bus 1.

aforementioned requirements. The other factor that can cause load shedding is very large amount of required power, such that the total power supplied by the batteries and generators is not enough to feed all the external loads. This is shown in bus 2 load profile in Fig. 4, where a huge load spike is considered from $30s$ to $40s$. The effect of this large required load can be seen in both the battery charge level and the load shedding graphs. Since the battery charge level should be higher that a lower bound with 99% probability, the controller tries to keep the actual battery charge level always higher than the lower bound. Note that in Fig. 8 the battery charge level has never decreased to the lower bound even in those time intervals that the required power has a large value.

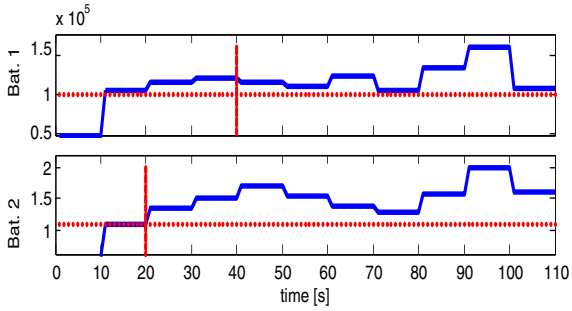

Fig. 8. Normalized battery charge levels.

VI. Conclusions and Future Work

In this paper, we presented a stochastic control design methodology for aircraft power systems. We introduced uncertainty in the inputs and dynamics of the system, and formulated the optimization of system performance as a stochastic optimal control problem. We derived a linearized version under a set of assumptions that can be accurate when the probability of failure in contactors is considerably small in comparison with the healthiness probability. In future work we plan to exploit thesparsity of the Jacobian and Hessian matrices to solve the original nonlinear problem efficiently with a primal-dual interior point method.

Acknowledgement

We thank Pierluigi Nuzzo, Forrest Iandola and Richard Poisson for fruitful discussions in an earlier version of this work. This work was supported in part by the iCyPhy Research Center (Industrial Cyber-Physical Systems, supported by IBM and United Technologies).

References

[1] L. Blackmore, H. Li, and B. Williams. A probabilistic approach to optimal robust path planning with obstacles. In *in Proceedings of the American Control Conference*, 2006.

[2] IBM ILOG CPLEX Optimizer. Available on: http://www.ibm.com/software/integration/optimization/cplex-optimizer/, 2014.

[3] D. Li and X. Sun. *Nonlinear integer programming*, volume 84. Springer Science & Business Media, 2006.

[4] J. Lofberg. Yalmip: A toolbox for modeling and optimization in matlab. In *Computer Aided Control Systems Design, 2004 IEEE International Symposium on*, pages 284–289. IEEE, 2004.

[5] M. Maasoumy, P. Nuzzo, F. Iandola, M. Kamgarpour, A. Sangiovanni-Vincentelli, and C. Tomlin. Optimal load management system for aircraft electric power distribution. In *Conference on Decision and Control*, June 2013.

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

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

[8] A. Pnueli. The temporal logic of programs. In *Proc. Symp. on Foundations of Computer Science*, pages 46–57, Nov. 1977.

[9] K. Sampigethaya and R. Poovendran. Aviation cyber x2013;physical systems: Foundations for future aircraft and air transport. *Proceedings of the IEEE*, 101(8):1834–1855, Aug 2013.

[10] A. Sangiovanni-Vincentelli. Quo vadis, SLD? Reasoning about the trends and challenges of system level design. *Proc. IEEE*, (3):467–506, 2007.

[11] 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.