# Dynamic Safety Constraints by Scenario Based Economic Model Predictive Control of Marine Electric Power Plants

Torstein I. Bø, *Member, IEEE,* and Tor Arne Johansen, *Senior Member, IEEE*

***Abstract*—This paper studies scenario based model predictive control (MPC) for dynamic safety constraints. For marine electric power plant with dc distribution and variable speed generator set, the speed of the generator sets should be as low as possible to increase the efficiency of the diesel engines. However, a safety margin towards under-speed is necessary. In this paper, a dynamical safety constraint is achieved by including a fault scenario in the model predictive control formulation. This is done by using a nominal trajectory of the predicted states for the fault free operation, and adding fault trajectories starting from the samples of the nominal trajectory. The fault trajectories simulate the fault scenario and dynamically constrain the nominal trajectory. The controller is shown to be effective using closed-loop simulations of a marine electric power plant.**

***Index Terms*—Power generation control, Marine vehicle power systems, Diesel driven generators, Fuel optimal control, Fault tolerance, Predictive control**

## I. Introduction

Diesel electric propulsion (DEP) has become the industry standard for vessels with varying power demand or high redundancy requirements. With DEP the power plant usually consists of multiple diesel generator sets. These produce electric power that is distributed to propulsion motors connected to the propellers, in addition to other electric loads of the vessel, such as drilling drives, heave compensators, cranes, and hotel loads. This gives a flexible system as generator sets can be connected and disconnected when the power demand or redundancy level changes.

DEP is commonly used for vessels with dynamic positioning (DP) systems. During DP operation the thrusters of the vessels are used to keep the position and heading of the vessel fixed. For vessels with DP classes 2 and 3, it is required that any single fault should not lead to loss of position [1]. One possible fault is a sudden disconnection of a generator set. The load of the disconnected generator set is immediately transferred to the remaining generator sets. The speed of the diesel engines will drop, as it takes time for diesel engines to increase their torque. For ac distribution systems this may result in under-frequency in the electric grid, which trips protection relays and will result in a blackout. The electric power demand can be reduced to avoid a too large drop in the speed of the diesel engine. Typically, fast load reduction (FLR) is used during such fault scenario. The power management system detects the fault and then commands the thruster drives and other variable speed drives to reduce their power consumption. This is done as the frequency converters are able to reduce the power demand quickly. [2] proposes that the variable speed drives measure the electric frequency of the ac grid and reduce the power demand when the electric frequency decreases below a threshold. A similar method can be used for dc distribution where the grid's voltage can be used as an indication of overload. Frequency dependent load shedding is typically implemented as one of the last measures to avoid an under-frequency, where some loads are disconnected if the frequency decreases below a threshold. This is undesired as it may take time to reconnect and start the disconnected equipments.

During the last decade, direct current (dc) distribution of electric power has entered the market for marine power plants [3], [4], [5], [6]. One of the benefit of dc distribution compared with conventional ac distribution is the possibility to run the diesel engines with varying speed, which essentially offers new free variables to be optimized. It is reported from the industry that diesel engines are often running with a power utilization of only 20% to 40%, which reduces the efficiency of the diesel engines. However, the efficiency can be increased by running the engines at low speed as this reduces the friction losses of the engine. The allowed range for the frequency is larger for vessels with dc distribution than using ac distribution, as the bus' electric frequency limits of the electrical distribution is removed and we are only left with the less restrictive speed limits of the diesel engines. In this article, a scenario based economic model predictive controller is used to minimize the fuel consumption by reducing the speed of the generator sets. However, the controller constrains the frequency to maintain a large enough frequency margin to avoid reduction of power consumption and diesel engine under-speed after a loss of a generator set. This is done by modifying the set-points of the diesel engines' governor.

Currently generator sets are controlled in speed droop or isochronous using PID or similar algorithms for speed governors [7]. Model predictive control and nonlinear control by feedback linearization are proposed as alternative control methods [8], [9], [10]. In [11], multiple methods for better control of engines are proposed, this includes observer design for noise-filtering, and inertia control to suppress frequency

T.I. Bø and T.A. Johansen are with Centre for Autonomous Marine Operations and Systems, Department of Engineering Cybernetics, Norwegian University of Science and Technology, NO–7491 Trondheim, Norway (e-mail: torstein.bo@ntnu.no).

The authors of this paper are funded by Design to verification of control systems for safe and energy efficient vessels with hybrid power plants (D2V), where the Research Council of Norway is the main sponsor. The second author is also funded by the Research Council of Norway, Statoil, and DNV through the Center of Excellence NTNU-AMOS. NFR: 210670/070, 223254/F50.

variations. A stochastic energy management system using particle swarm optimization is proposed in [12] for vessels with energy storage systems.

Model predictive control (MPC) with scenarios is used to establish a fault-tolerant controller, as scenarios are commonly used for robust MPC. An MPC for linear systems is presented in [13], where the system matrices can switch between a finite number of scenarios, with a given probability for each scenario. Other combinations of MPC and scenarios are presented in e.g., [14], [15]. These studies use scenarios to handle model uncertainties and disturbances. In the research field of robust MPC, it has been proposed to use approximate reachable sets to find the optimal control [16]. However, this gives sub-optimal solutions since a common control input is calculated for all possible sequences of uncertainties and disturbances. For linear systems, [17] suggest including feedback in the predicted trajectories, by using multiple different control inputs in the scenario tree. For non-linear systems, it is proposed to optimize a parametrization of the feedback law, see [18] and the references therein. Scenario-based model predictive control has also been suggested to be used in optimization of hedge options [19], for scheduling of batch processes [20], and scheduling of emergency vehicles [21].

There have been some studies on transients of the plant after reconfiguration of controllers due to faults. An investigation of responses due to reconfiguration of the controller is presented in [22], with different method for initializing the next controller. For faults which can be predicted, it has been suggests to use MPC to make a smooth accommodation of the fault [23]. It is suggested to use back calculation to set the initial states of the reconfigured controller and use a progressive accommodation scheme to achieve new LQR-gains [24].

Another approach to control a plant to a safe set is to use backward reachable set to calculate the fault-tolerant set [25]. The backward reachable set is a set containing all initial states, which can avoid an unsafe state set under a specified set of disturbances. A method for validating that a controller can avoid unsafe sets for linear hybrid systems using reachability analysis is presented in [26]. A similar study is done for nonlinear hybrid system using barrier certificates [27]. A method for selecting switching rules for a hybrid system, such that the state variables avoid an unsafe set, is presented in [28].

The present paper applies a method for establishing dynamic safety constraints based on fault scenario. A power plant with three generator sets and dc distribution is used as the case plant. The typical fault scenario considered is a sudden disconnection of one of the generator sets. The MPC optimizes the fuel consumption of the plant and controls the frequency such that if a generator is suddenly disconnected the diesel engines have sufficiently high speed to avoid under-speed during the recovery. The idea of the controller was first presented in [29], for a marine electric power plant with ac distribution. It was later formalized in [30], including a linear case plant. This paper is an extension of [29]: the controller is formalized by methods presented in [30] and a diesel-electric power plant with a dc distribution system is used in the case plant. A linear model was used in [30] to demonstrate the controller. A more realistic plant is used in this article, with some modifications on the controller to avoid numerical problems. The performance of the plant is also compared with a plant with fixed speed generator sets. Note that scenario-based MPC is often used to establish a robust controller, with respect to model uncertainties, noise, and disturbances. However, the proposed controller uses scenario-based MPC to handle a worst case fault event where the model is known. The proposed controller must be combined with other control techniques to handle model uncertainties, noise, and disturbances.

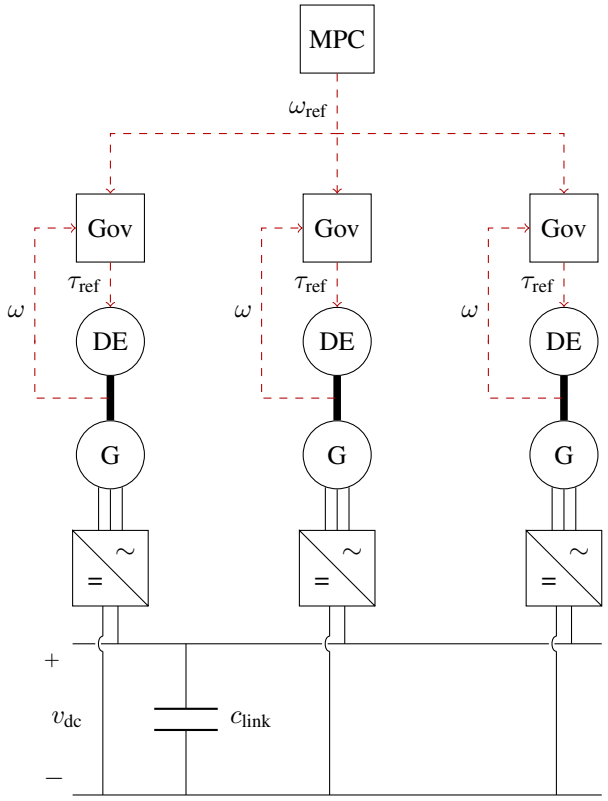


Fig. 1. Overview of the marine electric power plant without loads. The red dashed lines are signals, the thick lines are mechanical shafts, and the remaining lines represents electrical lines. Gov, DE, and G represents governor, diesel engine and generator. Loads are connected to the DC-link.

The paper is organized as follows: Section II introduces the models of the power plant including a process plant model used for simulation and a control plant model used internally in the controller. The controller is presented in Section III. Results from simulations are shown in Section IV, the fuel consumption of the plant running with the proposed controller is compared with operating the plant with fixed speed generator sets. Conclusions are drawn in Section V.

## II. Model

### A. Process Plant Model

A marine electric power plant is controlled in this article. Figure 1 gives an overview of a typical plant that will be used as a case study. The plant consists of three generator sets connected to a DC-link with a constant resistance as the load. The generator sets are rated to 9.1 MW. The model is expressed in per-unit notation [31]. A dc distribution system is used in this article as a case plant. However, the controller

TABLE I
NOMENCLATURE

| | |
|---|---|
| AVR | Automatic voltage regulator. |
| $D$ | Mechanical damping in generator in per-unit. |
| Droop | Droop of AVR. |
| $FC$ | Fuel consumption. |
| $H$ | Inertia constant of generator set. |
| $i_{dc}$ | Current through dc side of rectifier/load in per-unit. |
| $\mathbf{i}_{qd0}$ | Three-phase current through generator set in qd0-frame and per-unit. |
| $p$ | Active power of generator in per-unit. |
| $p_{\text{bus}}$ | Active power of loads connected to DC-link in per-unit. |
| $v_{dc}$ | Terminal voltage at DC-link in per-unit. |
| $v_{\text{no-load}}$ | No-load voltage of AVR in per-unit. |
| $\mathbf{v}_{qd0}$ | Three-phase terminal voltage of generator set in qd0-frame and per-unit. |
| $\tau_e$ | Electric torque in per-unit. |
| $\tau_{\text{ref}}$ | Reference torque of diesel engine in per-unit. |
| $\omega$ | Mechanical rotational speed in per-unit. |
| $\omega_{\text{ref}}$ | Reference mechanical rotational speed in per-unit. |

can be applied on ac distribution system as well, although the smaller frequency range gives less room for optimization. Equal generator sets are used in the case plant, as commonly used for marine power plant. The number of running generator sets is assumed to be given by the PMS' auto start/stop algorithm. A common reference speed of the generator set is assumed in this paper. This was chosen to simplify the explanation of the controller and to increase the computational performance. However, the method can easily be extended to include different sized generator sets and individually reference speed for the generator set.

It is hard to verify that it is optimal to run the generator set at a common speed, due to the dynamics of the fault scenarios. However, generators' rotating inertia acts as an energy reserve due to the kinetic energy. Hence, if the speed of one of the generator sets is reduced, the two other must increase their speed. The worst case after a fault is that one fast generator is disconnected. This means that if one generator decrease its speed, both of the remaining two must increase their kinetic energy just as much as the slow generator set decreased its kinetic energy. This gives an increased fuel consumption compared with running all the generators at the same speed, due to the friction losses. It should be noted that the safety constraint is not only affected by the kinetic energy, but also by the fuel injection dynamics.

Running the engines at the same load is optimal when the generator sets are running at the same speed, as the fuel consumption as a function of the torque is convex. Therefore, the generator sets uses symmetric load sharing (same load on each generator set). This also reduces the computational complexity, as only one control input is needed (instead of one speed setting and one load setting per generator set) and only one fault scenario per time step is needed (instead of one fault scenario per generator set).

At the top level is the MPC, which will be designed in this paper. It gives a common desired reference speed, $\omega_{\text{ref}}$, to the governors of the generator set. The output of the governor is the reference torque, $\tau_{\text{ref}}$, for the diesel engine, it is calculated by using a PID-controller with the speed error as input. The reference torque is rate limited by the engine manufactures to avoid thermal stress in the engine block and to some extent ensure complete combustion [32]. In addition, the diesel engines have a minimum and maximum speed and torque. We assume that internal control systems in the diesel engines are able to control the fuel injection such that the generated torque is kept at the reference torque.

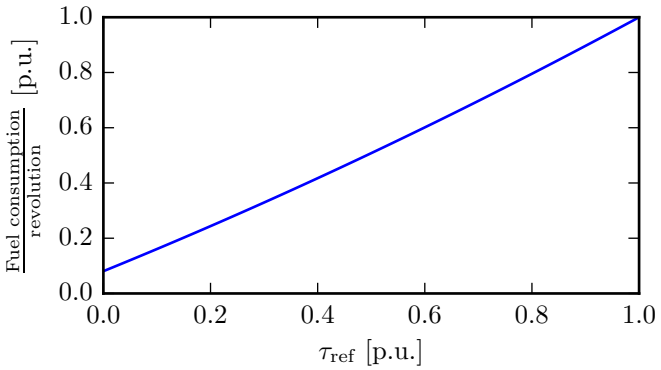


Fig. 2. Fuel consumption per revolution as a function of diesel engine's torque.

The per-unit speed of the generator set, $\omega$ is modeled by Newton's second law of rotation:

$$2H\dot{\omega} = \sum \tau = \tau_{\text{ref}} - \tau_e - D\omega \tag{1}$$

where $\tau_e$ is per unit electric torque from the generator, and $D$ is per unit damping coefficient. $H$ is the inertia constant of the generator set, defined as:

$$H = \frac{J\omega_b}{N_{\text{poles}}\tau_b},$$

where J is the moment of inertia of the generator set, $\omega_b$ is the base rotational speed, $\tau_b$ is the base torque, and $N_{\text{poles}}$ is the number of poles of the generator set. The fuel consumption is calculated by a second order Willans approximation [33] as shown in Fig. 2, which gives the following relationship between the mechanical torque of the diesel engine and fuel consumption:

$$FC = \omega\left(a_0 + a_1\tau_{\text{ref}} + a_2\tau_{\text{ref}}^2\right) \tag{2}$$

where $a_0$, $a_1$, and $a_2$ are constants and FC is the fuel consumption. Note that friction losses in the diesel engine are included in this model by setting $a_0 \neq 0$. To avoid double counting, $D$ should only include damping from the generator and not the diesel engine.

Parks equation is used to model the generator [31, Ch. 5.16], with parameters from [31, Tab. 5.10-1]. This is a model based on the flux-linkage in and between the stator and the rotor. The input to the model is the terminal voltage in the qd0-frame, $\mathbf{v}_{qd0}$, and the excitation voltage of the field windings in the rotor. The output is the stator current in qd0-frame, $\mathbf{i}_{qd0}$. The excitation voltage is set by the automatic voltage regulator (AVR). For dc distribution system, the AVR is used to control the active power sharing and the bus voltage. This is done with voltage droop, where the reference voltage of the dc side of the rectifier, $v_{\text{ref}}$, is given by:

$$v_{\text{ref}} = v_{\text{no-load}}\left(1 - p\text{Droop}\right) \tag{3}$$

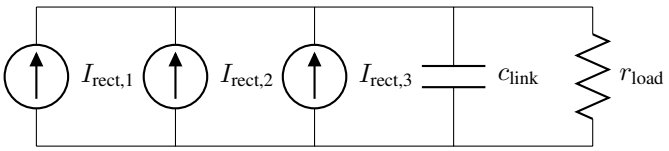


Fig. 3. Circuit diagram of the DC-link.

where $v_{\text{no-load}}$ is the reference voltage at zero active power, Droop is a constant, and $p$ is the active power of the generator set. The excitation voltage is then modified by a PID-controller in the AVR to achieve this reference voltage. The AVRs are equally configured in the case study, this gives symmetric load sharing.

The rectifiers are modeled as transformations, on rearranged form [34]:

$$i_{dc} = k_i \sqrt{i_q^2 + i_d^2} \tag{4}$$

$$\delta = \tan^{-1} \frac{i_d}{i_q} - \phi \tag{5}$$

$$\mathbf{v}_{qd0} = \begin{bmatrix} \cos\delta \\ \sin\delta \\ 0 \end{bmatrix} \frac{v_{dc}}{k_v} \tag{6}$$

where $k_i = 0.75$, $k_v = 1.29$, and $\phi = 0.24$ rad are constants from [34], $\delta$ is the load angle, $i_{dc}$ and $v_{dc}$ are the current and voltage on the dc side of the rectifier.

The DC-link is modeled as shown in Fig. 3. The rectifiers are modeled as variable current sources, the load is a constant resistor, and the capacitor bank is modeled as an equivalent capacitor.

### *B. Control Plant Model*

A simplified model, called the control plant model, is used internally in the MPC to increase the computational performance, while the previously presented process plant model is used for simulation. We assume that the load sharing is given by the droop curve. This means that the AVR is able to control the voltage of the generator perfectly to the reference voltage given by the droop curve. Using (3) and the power balance, we get:

$$\begin{bmatrix} 1 & \text{Droop}_1 & 0 & 0 \\ 1 & 0 & \text{Droop}_2 & 0 \\ 1 & 0 & 0 & \text{Droop}_3 \\ 0 & s_{b1} & s_{b2} & s_{b3} \end{bmatrix} \begin{bmatrix} v_{dc} \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} v_{\text{no-load},1} \\ v_{\text{no-load},2} \\ v_{\text{no-load},3} \\ p_{\text{bus}} \end{bmatrix} \tag{7}$$

where $s_{bi} = \dfrac{S_{bi}}{S_{b,\text{bus}}}$, $S_{bi}$ is the base power of generator set $i$, and $S_{b,bus}$ is the sum of the base power of the connected generator sets. The generators are assumed to be in steady state and the electric losses in the generator to be negligible. This gives the swing equation:

$$\tau_{e,i} = \frac{p_i}{\omega_i} \tag{8}$$

$$2H_i\dot{\omega}_i = \tau_{\text{ref},i} - \frac{p_i}{\omega_i} - D\omega_i \tag{9}$$

where $\tau_{\text{ref}}$ is controlled by the governor as described in the previous section.

The generator sets in the case plant are identical and configured identically. The power is then shared equally and the generator set will run at the same speed, as the electric torque will be equal and the governors will respond similarly. This set-up is chosen as equally sized generator set and symmetric load sharing are commonly used for marine power plant. This also results in a smaller optimization problem. This gives the active power on each generator:

$$p = \frac{S_{b,\text{bus}} p_{\text{bus}}}{S_{bi} N_{\text{connected}}} = \frac{S_{bi} N_{\text{genset}} p_{\text{bus}}}{S_{bi} N_{\text{connected}}} = \frac{N_{\text{genset}} p_{\text{bus}}}{N_{\text{connected}}} \tag{10}$$

where $N_{\text{genset}}$ is the number of generator sets at the bus (connected or disconnected) and $N_{\text{connected}}$ is the number of generator sets connected to the bus. The speed of the generator sets are then given by:

$$2H\dot{\omega} = \tau_{\text{ref}} - \frac{N_{\text{genset}} p_{\text{bus}}}{N_{\text{connected}} \omega} - D\omega \tag{11}$$

where $p_{\text{bus}}$ is the per unit load of the loads connected to the DC-link.

## III. Fault-Tolerant MPC

After a sudden disconnection of a generator set, the power is transferred immediately to the remaining generators. The frequency will then decrease as the diesel engines' torque is constrained by the rate limitation. However, the engines are able to avoid under-speed if large enough frequency margin is chosen pre-fault. Therefore, the tasks of the plant controller is to:

- minimize the fuel consumption of the power plant by controlling the set-point speed of the diesel engines.
- set the generators' speed such that under-speed is avoided in the event of a sudden disconnection of a generator set.

The controller is based on the controller established in [30]. Multiple predicted trajectories are used in the MPC to achieve the control objectives. Fig. 4 shows a snapshot of predicted trajectories. The red dotted line shows the under-speed limit. The nominal trajectory (solid black) is the prediction for the nominal scenarios. This is the predicted speed of the generator sets if no fault occurs. The fault trajectories (dashed lines) are the prediction for the fault scenarios. These shows the generator sets' speed when a generator set is disconnected. These trajectories start from the points on the nominal trajectory, where the fault events may occur. A fault trajectory is started at each point in the nominal trajectory, except the initial point. The optimization problem is solved by finding the optimal trajectories for all the scenarios at once. Hence, the fault scenario's trajectories will constrain the optimal trajectory of the nominal scenario. All trajectories are constrained by the frequency limits of the generators and torque limits. Terminal constraints are also used to ensure recursive feasibility.

For variables used in the fault scenario the notation $x^f(t_0|t_f = t_l)$ is used, this denote the variable $x$ for the fault trajectory starting at time $t_l$. The notation is simplified for slack variables (e.g., $s_\omega^{+f}(t_i|t_f = t_l)$ is simplified to $s_\omega^+$) to increase the readability.

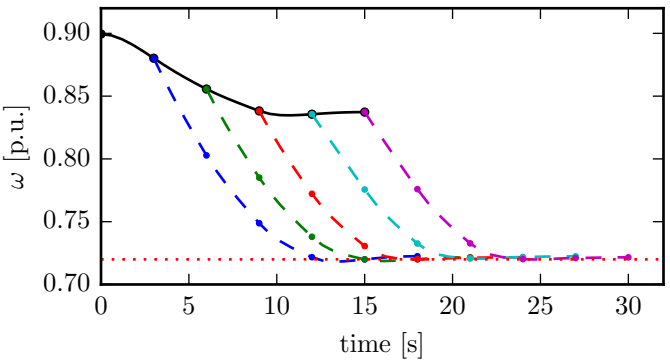


Fig. 4. Future trajectories for the generators' speed. The solid black line is the predicted trajectory of the nominal scenario. The dashed lines are the predicted fault scenarios, starting at $t_f = 3,\ 6,\ 9,\ 12,\ 15$ respectively. The dotted red line represents the under-speed limit which all trajectories should be above. An inter-sample violation of the constraints occurs as the constraints are only applied to the sample instants.

### A. State Constraints

For the nominal trajectory, the speed and torque of the engines are constrained to stay within the operational limits of the engines:

$$\underline{\omega} \leq \omega + s_\omega^+ - s_\omega^- \leq \overline{\omega} \tag{12}$$
$$0 \leq s_\omega^- \tag{13}$$
$$0 \leq s_\omega^+ \tag{14}$$
$$\underline{\tau}_{\text{ref}} \leq \tau_{\text{ref}} \leq \overline{\tau}_{\text{ref}} \tag{15}$$

where $\underline{\omega}$ and $\overline{\omega}$ are under- and over-speed limits, $\underline{\tau}_{\text{ref}}$ and $\overline{\tau}_{\text{ref}}$ are minimum and maximum torque. Two slack variables, $s_\omega^-$ and $s_\omega^+$, are used to make sure that the optimization problem is feasible. A linear term on the slack variables' cost can be used by using two slack variables instead of one.

The diesel engines torque is constrained by finite difference approximation of the rate constraint, for all $k = 1 \dots N$:

$$\underline{\dot{\tau}}_{\text{ref}} \leq \frac{\tau_{\text{ref}}(t_k) - \tau_{\text{ref}}(t_k - T_S)}{T_S} \leq \overline{\dot{\tau}}_{\text{ref}} \tag{16}$$

where $\underline{\dot{\tau}}_{\text{ref}}$ and $\overline{\dot{\tau}}_{\text{ref}}$ is the maximum negative and positive rate of change of the torque, $t_0$ is the initial time of the trajectory, $T_S$ is the sampling time of the MPC trajectory, and $N$ is length of the prediction horizon.

Similar constraints are used for the fault trajectories. However, to include a safety margin the constraints are narrowed by increasing the lower limits and decreasing the upper limits. E.g., the lower speed limit is 70% for the nominal scenario and 72% for the fault scenario. This margin is considered to be sufficiently large to include model errors and should be chosen by system knowledge.

### B. Terminal Constraints

To make sure that the optimization problem is recursively feasible, the states of the trajectories are constrained to terminate in equilibrium,

$$\dot{\omega}(t_N) = 0 \tag{17}$$
$$\omega_{\text{ref}}(t_N) - \omega(t_N) = 0 \tag{18}$$

Moreover, slack variables are added to the terminal constraints of the fault scenario, to make sure that the optimization problem is feasible, and to avoid numerical problem during optimization. For each fault trajectory starting at $t_l$:

$$\dot{\omega}^f(t_{l+N}) = s_{\omega T}^+ - s_{\omega T}^- \tag{19}$$
$$\omega_{\text{ref}}^f(t_{l+N}) - \omega^f(t_{l+N}) = s_{\omega_{\text{ref}} T}^+ - s_{\omega_{\text{ref}} T}^- \tag{20}$$

where individual slack variables are used for each trajectory.

### C. Optimization Problem

The reference speed of the generator set is changed in ramps to get smooth transitions by optimizing $\dot{\omega}_{\text{ref}}$. The differential equation of the integrator of the governor's PID controller is:

$$\dot{\xi} = \omega_{\text{ref}} - \omega \tag{21}$$

The initial values of the nominal trajectory are given by measurements,

$$\omega(t_0) = \omega_0 \tag{22}$$
$$\omega_{\text{ref}}(t_0) = \omega_{\text{ref},0} \tag{23}$$
$$\xi(t_0) = \xi_0 \tag{24}$$

where $\omega_0$, $\omega_{\text{ref},0}$, and $\xi_0$ are the currently measured values. The initial values of the fault trajectory starting at $t_l$ are:

$$\omega^f(t_l | t_f = t_l) = \omega(t_l) \tag{25}$$
$$\omega_{\text{ref}}^f(t_l | t_f = t_l) = \omega_{\text{ref}}(t_l) \tag{26}$$
$$\tau_{\text{ref}}^f(t_l | t_f = t_l) = \tau_{\text{ref}}(t_l) \tag{27}$$

Note that the reference torque is used as initial condition, which implicitly sets $\xi^f(t_0)$. This initial condition is used to get a continuous transition of $\tau_{\text{ref}}$ at the time instant one generator disconnect.

The following cost function is used in the optimization problem for the nominal scenario:

$$\begin{aligned}\Phi^n = \sum_{k=0}^{N-1} \Big[ & w_{\text{FC}} \text{FC}(t_k) + w_{s_\omega^-}(s_\omega^-(t_k) - s_{\omega,\text{ref}}^-)^2 \\ & + w_{s_\omega^+}(s_\omega^+(t_k) - s_{\omega,\text{ref}}^+)^2 \Big]\end{aligned} \tag{28}$$

where $w_i$ is the constant weight of cost $i$ and $i_{\text{ref}}$ is the constant reference values for slack variable $i$. The first term in the sum is the fuel consumption, while the remaining terms are penalties on the slack variables. The cost function for the fault scenario starting at time $t_f$ from the nominal scenario:

$$\begin{aligned}&\Phi^f(t_f = t_l) = \\ &\sum_{k=l}^{l+N-1} \Big[ w_{s_\omega^-}(s_\omega^-(t_k) - s_{\omega,\text{ref}}^-)^2 + w_{s_\omega^+}(s_\omega^+(t_k) - s_{\omega,\text{ref}}^+)^2 \Big] \\ &+ w_{s_{\omega T}^+}(s_{\omega T}^+ - s_{\omega T,\text{ref}}^+)^2 + w_{s_{\omega T}^-}(s_{\omega T}^- - s_{\omega T,\text{ref}}^-)^2 \\ &+ w_{s_{\omega_{\text{ref}} T}^+}(s_{\omega_{\text{ref}} T}^+ - s_{\omega_{\text{ref}} T,\text{ref}}^+)^2 + w_{s_{\omega_{\text{ref}} T}^-}(s_{\omega_{\text{ref}} T}^- - s_{\omega_{\text{ref}} T,\text{ref}}^-)^2\end{aligned} \tag{29}$$

The terms in the summation are penalties on the slack variables for the trajectory, while the remaining terms penalize the terminal constraints' slack variables. Note that the cost function

only penalize the slack variables. This is done as the fault trajectories should only constrain the nominal trajectory.

The optimization problem is:

$$\begin{aligned}\mathbf{U}^* = \arg\min_{\mathbf{U}} \left( \Phi^n + \sum_{l=1}^{N} \Phi^f(t_f = t_l) \right) \\ \text{subjected to } (11) - (27)\end{aligned} \tag{30}$$

where $\mathbf{U}$ contains all optimization variables, i.e., $\dot{\omega}_{\text{ref}}$ and slack variables, $s$, for all trajectories and $\mathbf{U}^*$ is the optimal control sequence. The cost function is sum of the nominal scenario's cost, $\Phi^n$, and each of the fault scenarios' cost $\sum_{l=1}^{N} \Phi^f(t_f = t_l)$. The first $\dot{\omega}_{\text{ref}}$ from the optimized control sequence is applied, at the next time instant the optimization is re-optimized with the new initial conditions. Note that $N_{\text{connected}} = N_{\text{genset}} = 3$ in (11) for the nominal scenario and $N_{\text{connected}} = 2$ and $N_{\text{genset}} = 3$ for the fault scenarios.

### D. Fault recovery controller

The controller is reconfigured after disconnection of a generator. The objective of the controller is to recover the plant after the fault. This can be done by following the trajectory found in the controller pre-fault. The speed of the generator set is controlled to a predefined speed, $\omega_{rc}$. The nominal speed is insufficient at high loads, due to the torque constraints of the diesel engine. Therefore, $\omega_{rc}$ is set to the highest value of

1) the nominal speed and
2) 5 % above the minimum required frequency, which is found by (11), setting $\dot{\omega} = 0$.

where the nominal speed is chosen in 1) as it gives large margin towards under- and over-speed of the diesel engine, and 5% safety margin in 2) is chosen to give some speed margin towards lack of power.

The cost function used in the reconfigured controller is:

$$\begin{aligned}\Phi^{rc} = {} & w_\omega(\omega - \omega_{rc})^2 + w_{\dot{\omega}}\dot{\omega}^2 \\ & + \sum_{k=0}^{N-1} \left[ w_{s_\omega^-}(s_\omega^-(t_k) - s_{\omega,\text{ref}}^-)^2 + w_{s_\omega^+}(s_\omega^+(t_k) - s_{\omega,\text{ref}}^+)^2 \right]\end{aligned} \tag{31}$$

The optimization problem is:

$$\begin{aligned}\mathbf{U}^* = \arg\min_{\mathbf{U}} \Phi^{rc} \\ \text{subjected to } (11) - (18) \text{ and } (21) - (24)\end{aligned} \tag{32}$$

Note that the constraints are similar to the constraints on the nominal trajectory in (30). Hence, the constraints on the trajectory is relaxed, compared with the fault scenario of (30). Therefore, the fault recovery controller is feasible if (30) was feasible at the previous step. In addition, if (30) was feasible with slack variables equal to zero at the previous step, then (32) is feasible with slack variables equal to zero. The cost on the slack variables are tuned such that the the slack variables are zero for the optimal solution if this is a feasible solution. This is done by setting $s_{\text{ref}}$ sufficiently small. Hence, the fault recovery controller recovers the plant without violating the constraints if (30) was feasible with slack variables equal to zero at the previous step. Fault trajectories are not included in the optimization problem; hence, the constraints for the fault trajectories are omitted.

The disconnection may occur during an inter-sample, this means that the controller is not reconfigured before the next update of the MPC. However, the governor will increase the diesel engine torque due to the decrease of the engines speed. The torque will then typically be constrained by the torque rate constraint, similarly as what occurs using the control sequence from the MPC.

## IV. Simulation Results

The performance of the controller is tested through simulation. The process plant model presented in Section II-A is used to simulate the system, while the control plant model is used for predictions in the MPC as described in Section II-B. A prediction horizon of 15 seconds is used with a sampling and update period of 3 seconds. The horizon length is chosen short enough to give real-time performance, while long enough to achieve sufficiently large region of feasibility. The update period is small enough to capture most of the fastest dynamics. Parameters for the controller and models are given in Tabs. II and III. The weights of all slack variables (e.g., $w_{s_\omega^+}$ and $w_{s_\omega^-}$) are set to 100, the reference value of the slack variables (e.g., $s_{\omega,\text{ref}}^+$ and $s_{\omega,\text{ref}}^-$) are set to $-100$, and $w_{\text{FC}} = w_\omega = w_{\dot{\omega}} = 1$. Note that the slack variables cannot reach the chosen reference value due to the constraints ($0 \leq s$). However, this is used to include a linear term in the cost on the slack variables. Hence, similar response as an exact penalty function can be achieved, where the slack variable is only utilized when the problem else would have been infeasible.

Figs. 5 and 6 show closed loop simulations of the power plant with 40% and 70% load. One of the three connected generator sets are disconnected after 51 seconds. The load is immediately transferred to the remaining generator sets and the controller is reconfigured to use the fault recovery controller. The fault recovery controller increases the diesel engines' torque as quickly as possible, but it is constrained by a rate constraint. Eventually the diesel engines reach the maximum torque. Afterwards the fault recovery controller regulates the generators' frequency to a fixed frequency close to or higher than the nominal frequency.

Pre-fault, the MPC regulates the engine speed as low as possible, while still high enough to avoid under-speed when the sudden disconnection occurs. A margin of 2% is added to the under-speed limit of the fault scenario. For the case with a load of 40%, the frequency drops below this under-speed limit (dotted line at 72%) while it is able to stay above the nominal under-speed limit (dashed line at 70%). The violation occurs due to the simplification of the rate constraint in the MPC's model. However, the frequency margin is sufficiently large to handle the model error.

For the case with a load of 70%, the limitation of the diesel engines' torque constrains the speed. The maximum power of the diesel engine is the product of the maximum torque and the engine's speed. Fig. 6 shows that at approximately the same time as the frequency is at its lowest, the diesel engine reaches its maximum torque. The diesel engines gets a high enough

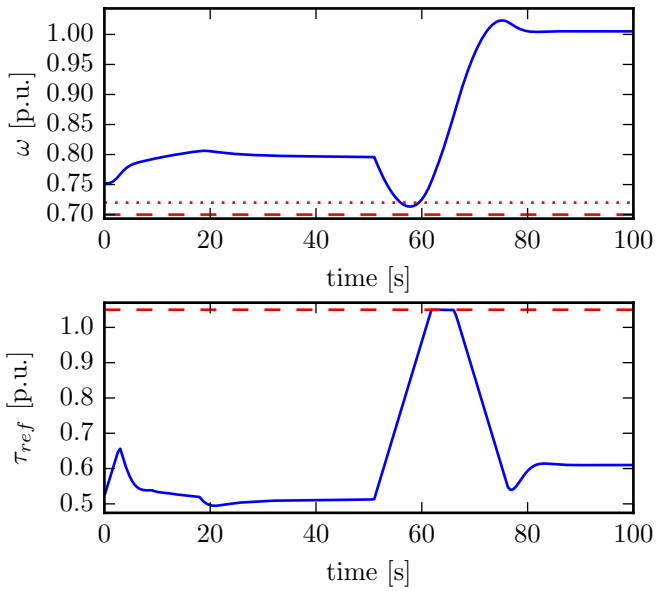


Fig. 5. Simulation of the power plant running with a load of 40%. One of the three connected generator sets is disconnected after 51 seconds. In the plot for frequency, the dotted red line shows the under-speed limit used in the fault scenarios, while the dashed red line show the under-speed limit used in the nominal scenario and the reconfigured controller. In the plot for $\tau_{\text{ref}}$, the dashed red line shows the maximum diesel engine torque.

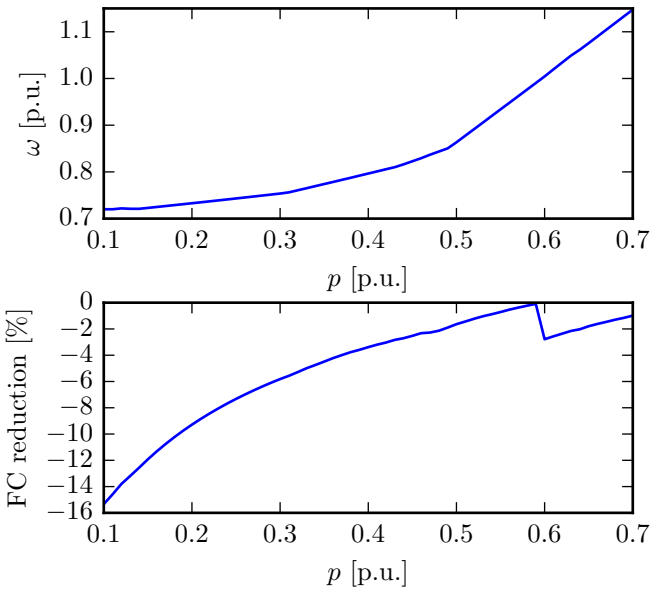


Fig. 7. The left plot shows the optimal steady state generator set speed as a function of the load. The right plot shows the reduction of fuel consumption with the proposed controller compared with running generator set at rated speed. Note that a new generator set must be started when the steady state speed is above the rated speed, this reduces the generators efficiency.

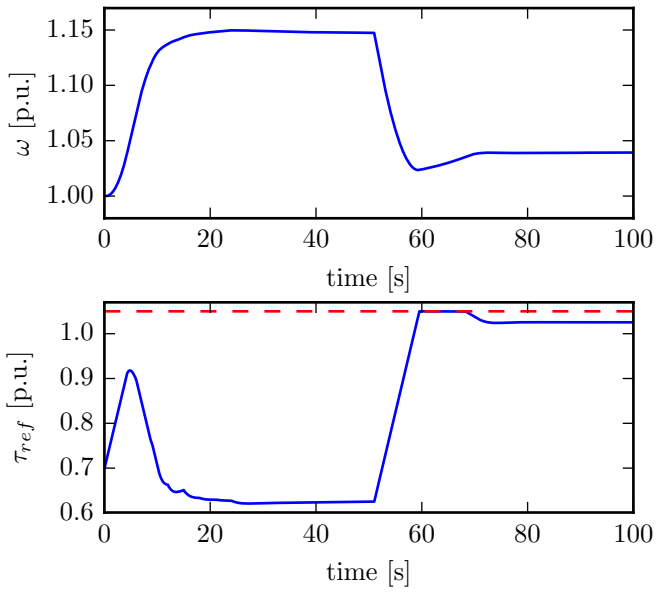


Fig. 6. Simulation of the power plant running with a load of 70%. One of the three connected generator sets is disconnected after 51 seconds. In the plot for $\tau_{\text{ref}}$, the dashed red line shows the maximum diesel engine torque.

speed during post-fault recovery to achieve enough power to be able to both generate the extra electric power and accelerate the generator set post-fault. This is done by increasing the engine speed pre-fault.

The left plot in Fig. 7 shows the optimal steady state speed of the generator set as a function of the load. The frequency is dynamically increased as the load increases. The controller is not able to run at higher load than 70% with this configuration, as the post fault load on each generator set will be too high if the load increases above this level. In the right plot, the fuel savings of using this algorithm are shown. The fuel savings are calculated by comparing the fuel consumption of the present plant with the fuel consumption of the same plant with generator sets running at their rated speed. Additional generator sets must be connected when the load is higher than 60 % and fixed speed is used to make sure that the plant can recover if a generator set is suddenly disconnected. This reduces the efficiency of the generator sets.

The optimization problem consists of 206 optimization variables and 179 constraints. The computational time is between 0.2 and 1.3 seconds per update period, when using ACADO's C++ interface and a 3.5 GHz Intel® Xeon™ E3 processor. Note that ACADO's C++ interface is not designed for constraints that combine constraints at different time instances, such as the initial constraint of a fault trajectory $\big(\text{e.g., } \omega^f(t_l|t_f = t_l) = \omega(t_l)\big)$. This is by-passed by adding auxiliary optimization variables. Therefore, the implemented optimization problem can be substantially condensed. It is also the authors experience that using ACADOs c-code export function will give a significant performance improvement (typically 10 to 100 times faster). Hence the MPC can be implemented in real time.

## V. Conclusion

This paper proposes a method to control a marine power plant that includes safety constraints based on fault scenarios. The controller uses the fault scenarios internally in the MPC to make sure that it controls the generator sets' speed such

TABLE II
PARAMETERS FOR CONSTRAINTS USED IN THE MPC. THE RECONFIGURED CONTROLLER USES THE PARAMETERS FOR THE NOMINAL SCENARIO.

| | Nominal scenario | Fault scenario |
|---|---|---|
| $\underline{\omega}$ | 0.70 | 0.72 |
| $\overline{\omega}$ | 1.20 | 1.18 |
| $\underline{\tau}_{\text{ref}}$ | 0 | 0 |
| $\overline{\tau}_{\text{ref}}$ | 1.05 | 1.03 |
| $\underline{\dot{\tau}}_{\text{ref}}$ | -1/20 seconds | -1/22 seconds |
| $\overline{\dot{\tau}}_{\text{ref}}$ | 1/20 seconds | 1/22 seconds |

TABLE III
PARAMETERS FOR THE MODEL.

| | |
|---|---|
| Droop | 0.001 |
| D | 0.01 |
| H | 5.6 seconds |

that a sufficiently large safety margin towards under-speed is achieved. Hence, a sudden disconnection of a generator set can occur without risk of blackout and the need for load reduction. The advantages of the controller are less conservative safety constraints, which gives a fuel consumption reduction of up to 15 %. The disadvantage is a larger and more computational expensive optimization problem, in addition to the need to identify and model the worst case fault scenarios. The simulations show that the controller fulfills the control objectives as long as a safety margin is used. Future work would involve an implementation of the algorithm in a lab or full-scale experiment.

## REFERENCES


[1] "Guidelines for vessels with dynamic positioning systems," International Maritime Organization (IMO), Tech. Rep. Maritime Safety Committee (MSC) Circular 645, 1994.

[2] J. J. May, "Improving engine utilization on DP drilling vessels," in *Dynamic Positioning Conference*, 2003.

[3] J. F. Hansen, J. O. Lindtjørn, and K. Vanska, "Onboard DC Grid for enhanced DP operation in ships," in *Dynamic Positioning Conference*, 2011.

[4] L. Briant, "Demand for greener, more efficient propulsion systems," *Marine Log*, vol. 117, no. 3, pp. 22–23, 2012.

[5] "IEEE recommended practice for 1 kV to 35 kV medium-voltage dc power systems on ships," *IEEE Std 1709-2010*, pp. 1–54, Nov 2010.

[6] E. Skjong, R. Volden, E. Rodskar, M. Molinas, T. Johansen, and J. Cunningham, "Past, Present and Future Challenges of the Marine Vessel's Electrical Power System," *IEEE Transactions on Transportation Electrification*, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7451276/

[7] A. K. Ådnanes, *Maritime Electrical Installations and Diesel Electric Propulsion*, Oslo, Norway, 2003.

[8] J. F. Hansen, A. K. Ådnanes, and T. I. Fossen, "Modelling, simulation and multivariable modelbased predictive control of marine power generation system," in *Proceedings of IFAC Conference: Control Applications in Marine Systems, CAMS'98*, Fukuoka, Japan, 1998, pp. 45–50.

[9] A. Veksler, T. A. Johansen, E. Mathiesen, and R. Skjetne, "Governor principles for increased safety on vessels with diesel-electric propulsion," in *European Control Conference*, Zurich, Switzerland, 2013, pp. 2579–2584.

[10] J. F. Hansen and T. I. Fossen, "Nonlinear control of marine power generation systems," in *Proc. of 13th Power Systems Computation Conference*, Trondheim, Norway, 1999, pp. 539–544.

[11] D. Radan, "Integrated control of marine electrical power systems," Doctoral thesis, monograph, Norwegian University of Science and Technology, 2008.

[12] E. A. Sciberras, B. Zahawi, D. J. Atkinson, A. Breijs, and H. van Vugt, "Managing shipboard energy – a stochastic approach," *IEEE Transactions on Transportation Electrification*, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7505991/

[13] D. Bernardini and A. Bemporad, "Scenario-based model predictive control of stochastic constrained linear systems," in *Proc. 48h IEEE Conf. Decis. Control*, Dec. 2009, pp. 6333–6338.

[14] G. C. Calafiore and L. Fagiano, "Robust Model Predictive Control via Scenario Optimization," *IEEE Trans. Automat. Contr.*, vol. 58, no. 1, pp. 219–224, 2013.

[15] G. Schildbach, L. Fagiano, C. Frei, and M. Morari, "The scenario approach for stochastic model predictive control with bounds on closed-loop constraint violations," *Automatica*, vol. 50, no. 12, pp. 3009–3018, 2014.

[16] J. M. Bravo, T. Alamo, and E. F. Camacho, "Robust MPC of constrained discrete-time nonlinear systems based on approximated reachable sets," *Automatica*, vol. 42, no. 10, pp. 1745–1751, Oct. 2006.

[17] P. O. M. Scokaert and D. Q. Mayne, "Min-max feedback model predictive control for constrained linear systems," *IEEE Trans. Automat. Contr.*, vol. 43, no. 8, pp. 1136–1142, 1998.

[18] D. Limon, T. Alamo, D. M. Raimondo, D. M. n. Peña, J. M. Bravo, A. Ferramosca, and E. F. Camacho, "Input-to-state stability: a unifying framework for robust model predictive control," in *Nonlinear Model Predict. Control*, L. Magni, D. M. Raimondo, and F. Allgöwer, Eds. Springer Berlin Heidelberg, 2009, vol. 384, pp. 1–26.

[19] A. Bemporad, L. Bellucci, and T. Gabbriellini, "Dynamic option hedging via stochastic model predictive control based on scenario simulation," *Quant. Financ.*, pp. 1739–1751, Feb. 2014.

[20] A. Bonfill, A. Espuña, and L. Puigjaner, "Proactive approach to address the uncertainty in short-term scheduling," *Comput. Chem. Eng.*, vol. 32, no. 8, pp. 1689–1706, Aug. 2008.

[21] G. C. Goodwin and A. M. Medioli, "Scenario-based, closed-loop model predictive control with application to emergency vehicle scheduling," *Int. J. Control*, vol. 86, no. 8, pp. 1338–1348, Aug. 2013.

[22] T. Kovâcshâzy, G. Péceli, and G. Simon, "Transient reduction in reconfigurable control systems utilizing structure dependence," in *Instrum. Meas. Technol. Conf. 2001. IMTC 2001. Proc. 18th IEEE*, 2001, pp. 1143–1147.

[23] L. Lao, M. Ellis, and P. D. Christofides, "Proactive Fault-Tolerant Model Predictive Control," *AIChE J.*, vol. 59, no. 8, pp. 2810–2820, 2013.

[24] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, "Diagnosis and Fault-Tolerant Control," in *Diagnosis Fault-Tolerant Control*, 2nd ed. Springer Berlin Heidelberg, 2006, pp. 10–23.

[25] J. H. Gillula, G. M. Hoffmann, M. P. Vitus, and C. J. Tomlin, "Applications of hybrid reachability analysis to robotic aerial vehicles," *Int. J. Rob. Res.*, vol. 30, no. 3, pp. 335–354, Jan. 2011.

[26] F. D. Torrisi and A. Bemporad, "Discrete-time hybrid modeling and verification," in *IEEE Conf. Decis. Control*, 2001, pp. 2899–2904.

[27] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A Framework for Worst-Case and Stochastic Safety Verification Using Barrier Certificates," *IEEE Trans. Automat. Contr.*, vol. 52, no. 8, pp. 1415–1428, 2007.

[28] S. Coogan and M. Arcak, "Guard synthesis for safety of hybrid systems using sum of squares programming," in *51st IEEE Conf. Decis. Control*, Dec. 2012, pp. 6138–6143.

[29] T. I. Bø and T. A. Johansen, "Scenario-based fault-tolerant model predictive control for diesel-electric marine power plant," in *MTS/IEEE Ocean. Bergen*, Jun. 2013, pp. 1–5.

[30] T. I. Bø and T. A. Johansen, "Dynamic safety constraints by scenario based economic model predictive control," in *Proc. IFAC World Congress, Cape Town, South Africa*, 2014, pp. 9412–9418.

[31] P. C. Krause, *Analysis of Electric Machinery (McGraw-Hill series in electrical engineering)*, 2nd ed. McGraw Hill Higher Education, Feb. 2002.

[32] T. I. Bø, A. R. Dahl, T. A. Johansen, E. Mathiesen, M. R. Miyazaki, E. Pedersen, R. Skjetne, A. J. Sørensen, L. Thorat, and K. K. Yum, "Marine vessel and power plant system simulator," *IEEE Access*, vol. 3, pp. 2065–2079, 2015.

[33] L. Guzzella and C. H. Onder, *Introduction to Modeling and Control of Internal Combustion Engine Systems*, 2nd ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[34] I. Jadric, D. Borojevic, and M. Jadric, "Modeling and control of a synchronous generator with an active dc load," *IEEE Transactions on Power Electronics*, vol. 15, no. 2, pp. 303–311, Mar 2000.