Formal Analysis of Drum-Boiler Units to Maximize the Load-Following Capabilities of Power Plants

Ahmed El-Guindy, Dongkun Han, and Matthias Althoff

***Abstract*—The load-following capabilities of power plants became increasingly important in recent years as a means of ensuring a reliable operation of future power systems. In this work, we propose a generic approach, based on reachability analysis, to rigorously verify the safety of critical components that often pose limitations on the flexibility of conventional power plants to perform fast load changes. The proposed reachability algorithm makes it possible to compute the bounds of all possible trajectories for a range of operating conditions while simultaneously meeting the practical requirements of a real power plant. As an example, we consider the verification of the water level inside a drum unit. In contrast to previous work, our results are based on measurement data of a realistic configuration of a boiler system located within a 450 MW combined cycle plant in Germany. We use an abstract model which considers the modelling errors to ensure that all dynamic behaviors of the process are replicated by the abstraction. Through the implementation of our abstract model, we formally guarantee that the water level inside the drum always remains within safe limits for load changes equivalent to 40 MW which, as a result, exploits the power plant's adaptability and load-following capabilities.**

***Keywords*—Reachability analysis, boiler control, formal analysis, drum water level, thermal power plant**

I. Introduction

THE ongoing demand for rapid changes in power generation results from deregulation in the energy sector, the introduction of competitive markets, and the transition towards decentralized generation with considerable share of renewable resources [1]–[3]. Particularly, the load-following capabilities of conventional power-producing units become increasingly important as progressively intermittent and variable generators, such as wind turbines and solar cells, are added to the grid. This change forces power plants to adapt their power output regularly to ensure a reliable operation of power systems.

Each Transmission System Operator (TSO) preserves the frequency in its control area using a centralized control scheme. It compensates the deviation of the power grid frequency caused by the mismatch between supply and demand of the active power. The control action includes generation units (or loads) that respond to Automatic Generation Control (AGC) signals, in the case of secondary frequency control, or to manual operator dispatch commands in the event of tertiary control [4]. In Germany, the generation units subjected to this control scheme are obliged to provide, without interruption, active power in both directions (increased/decreased generation), whose typical limits range between 5 MW and 60 MW within a short time-scale of 5 min to 15 min [5].

A. Motivation

The drum unit of the boiler system naturally degrades the load-following capabilities of thermal power plants and limits their flexibility to meet the stringent requirements imposed by the corresponding TSO. A reason for this is that the regulation of the water level inside the drum is a tedious control task due to the process nonlinearities and non-minimum phase behavior related to the shrink and swell physical phenomena [6]. If the water level exceeds the upper limit, the water will be carried over to the superheater leading to an outage of the boiler. Surpassing the lower limit will cause overheating of the water wall tube resulting in serious tube rupture and severe damage.

In this work, we consider the drum unit located within the 450 MW combined cycle power plant (*München Süd GuD*), owned by Munich City Utilities[1]. As reported by the plant operators, the boiler unit trips on multiple occasions as the water level inside the drum exceeds the safety limits (±300 mm). The outage of the boiler has serious technical and economical consequences: the power plant is subjected to drastic economical losses, and the TSO loses one of its generating units which can jeopardize stability in its balancing area. Initial examination reveals that the problem is concerned with the feedwater control loop which employs the conventional PID-controller to regulate the water level inside the drum (see [7, Sec. III]). This problem is recurrent; emergency shutdowns in thermal power plants are commonly trigged due to poor regulation of the water level [8]–[11].

In recent work by the authors [7] and [12], an optimization of the water level control performance was attained using a centralized multivariable feedback controller. This controller outperforms the existing PID-controller in many aspects: it improves the control performance significantly and yields much tighter reference value tracking during high-load changes (≤ 40 MW). Due to the fact that the control action is based on a mathematical model of the real process (observer-based controller), plant operators have voiced skepticism about the safety of the new control scheme. Thus, we propose an algorithm based on reachability analysis in order to verify the control action in real-time. Our work corresponds to the growing body of literature that considers the intersection of formal methods and control theory.

To the best of our knowledge, no work exists in the literature that formally analyzes the correctness of the low-level controllers prior to the commissioning stage within the high-level distributed control system (DCS) of the power plant; that is, to guarantee that the synthesized controller meets the performance specifications under all eventualities. Instead, in

The authors are with the Department of Informatics, Technical University of Munich, 85748 Garching, Germany (E-mail: ahmed.elguindy@tum.de, dongkun.han@tum.de, althoff@in.tum.de).

[1] SWM Services GmbH https://www.swm.de/

other work, the control action is examined within a simulation environment that does not provide any formal guarantees, i.e. one cannot certify whether the system specifications will always remain within safe limits. Numerical simulations provide satisfying results only when there are no parametric or input uncertainties. This is, however, not generally the case due to the unavoidable mismatch between actual physical phenomena and derived models [13].

In this work we propose a systematic approach, based on reachability analysis, that formally verifies realistic steam generator systems employing modern control concepts. A general literature review about reachability analysis is found in [14] and [15]. Recently, in addition to numerical simulations and Lyapunov direct method, reachability algorithms have emerged as an alternative technique for the analysis of power systems. In [16] the effects of wind variability are investigated for the 39-bus New England system. The same authors suggest a set-theoretic method applied to capture the effect of uncertain generation on the power flow [17]. Similar studies on the impact of uncertain energy production on frequency deviation are reported for a reduced-order model of the U.S. power system [18]. Transient stability analysis is performed on the IEEE 30-Bus benchmark power system network in [19].

B. Contributions

In contrast to any previous work on reachability analysis, we construct an abstract model of the real process taking the modelling errors into account. The modelling errors are obtained in a systemic procedure based on measurement data, and considered as additional uncertain inputs when computing the reachable set. This procedure ensures that all behaviors of the system are included within the abstraction.

This is the first work to consider formal analysis of a real process in the power industry. The reachability algorithm we propose is computationally feasible and meets the practical requirements of a real power plant when subjected to the time constraints of secondary frequency control (5 min). Our algorithm offers the plant operator an opportunity to potentially avoid an unnecessary shutdown of the facility since reachability analysis establishes in advance whether a requested load dispatch by the TSO will trigger the safe limits of the water level when considering all eventualities.

II. Problem Formulation and Overview

The drum-boiler system falls under the class of systems modelled as a set of nonlinear, ordinary differential equations

$$\begin{aligned} \dot{x}(t) &= f(x(t), u(t)), \\ y(t) &= Cx(t), \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^{n_x}$, $u \in \mathbb{R}^{n_u}$ and $y \in \mathbb{R}^{n_y}$ are the state, input and output vectors, respectively, and $C \in \mathbb{R}^{n_y \times n_x}$ is the output matrix. It is assumed that the system is controllable and observable. Furthermore, the function $f(\cdot)$ is locally Lipschitz continuous thus differentiable in $x(t)$ and $u(t)$. This is a fairly general assumption that holds for many practical problems. The time dependency is often omitted for simplicity of notation.

The objective of this paper is to compute the reachable set of (1) over a user-defined time horizon $t \in [0, t_f]$ starting from a set of consistent initial states $\mathcal{R}(0)$ and a set of possible inputs/disturbances $\mathcal{U}$

$$\mathcal{R}^e([0,t_f]) := \left\{ x(t) \in \mathbb{R}^{n_x} \,\middle|\, x(t) = \int_0^t f(x(\tau), u(\tau)) d\tau, \right. \\ \left. x(0) \in \mathcal{R}(0),\, u(t) \in \mathcal{U},\, t \in [0, t_f] \right\}. \tag{2}$$

The exact reachable set $\mathcal{R}^e([0,t_f])$ can only be computed in special cases [20]. Thus, an over-approximation of the reachable set $\mathcal{R}([0,t_f]) \supseteq \mathcal{R}^e([0,t_f])$ is performed as tightly as possible. Clearly, if the over-approximative reachable set does not intersect with an unsafe set, then the original system is also safe.

We propose a generic approach using an abstract model described by a polynomial differential inclusion. The concept of model abstraction is frequently applied in the field of computer science within the context of model checking and software verification. An abstraction basically reduces the complexity associated with a mathematical model, such that the resulting approximated model preserves certain user-defined properties of the original system [21]. The polynomial abstraction considered in this work takes the modelling errors into account, thus ensuring that all behaviors of the system are confined within the inclusion

$$\dot{\hat{x}}(t) \in P(\hat{x}(t), u(t)) \oplus (L \cdot \mathcal{E}). \tag{3}$$

Here $P(\cdot)$ is a polynomial function, $\mathcal{E} \subset \mathbb{R}^{n_y}$ is the set of the modelling errors, $\hat{x} \in \mathbb{R}^{n_x}$ is the vector of the abstract model state variables, and $L \in \mathbb{R}^{n_x \times n_y}$ is a correction feedback matrix. The abstraction includes set-based addition (*Minkowski sum*) and linear transformation, defined as

$$\begin{aligned} \mathcal{X} \oplus \mathcal{Y} &:= \{x + y \,|\, x \in \mathcal{X},\, y \in \mathcal{Y}\}, \\ M \cdot \mathcal{X} &:= \{M \cdot x \,|\, M \in \mathbb{R}^{n_b \times n_a},\, x \in \mathcal{X}\}. \end{aligned} \tag{4}$$

Our approach, illustrated in Fig. 1, consists of four main steps: (1) modelling from first-principles, (2) polynomial approximation, (3) abstraction, and (4) computation of the over-approximative reachable set. In the following sections we describe the modelling of the drum unit (Sec. III) and the proposed polynomial abstraction (Sec. IV). We then describe the basic procedure to compute the reachable set (Sec. V). The proposed approach can be applied for different systems in many areas, including power systems, robotics, and autonomous cars, as long as the system is modelled as in (1).

III. Process Modelling

The simplified diagram of the steam generation process is shown in Fig. 2. Cold water inside the feedwater tank is pumped and heated at the economizer stage before going through the drum inlet. Due to the gravitational force, feedwater flows through the naturally circulated downcomer riser loop, where it is converted into steam at the evaporator stage. Different riser tubes collect the steam and supply it

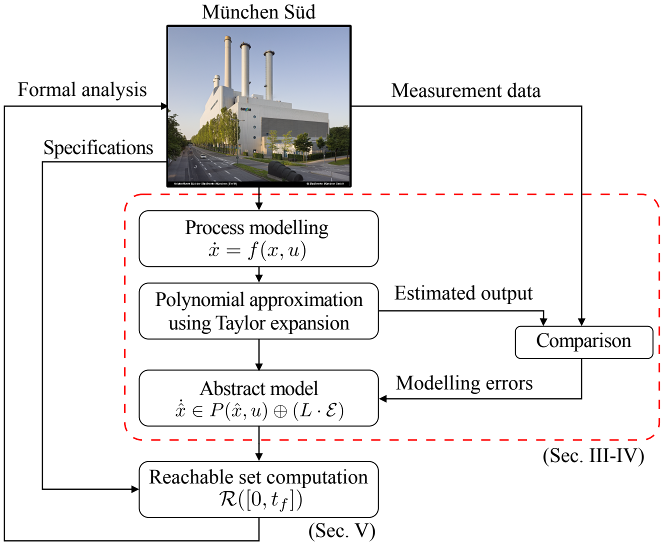


Fig. 1. Overview of our generic approach.

back into the drum. In the final stage, the saturated steam is taken from the drum outlet to the superheater. The system consists of four components: the drum unit, the regulating valves, the exhaust heat, and the controller. In this section, we briefly present the mathematical model of each component. For further details, with regards to the modelling assumptions and controller design, we refer the reader to previous work by the authors [7] and [12].

A. Drum-Boiler Model

We consider the well-developed Åström - Bell model [6]. The vector of the drum state variables $x_d \in \mathbb{R}^{n_d}$ consists of the pressure P_e [Pascal], the water volume V_{wt} [m^3], the steam-mass quality α_r [%] in the riser tubes, and the steam bubbles volume V_{sd} [m^3] under the water level. The inputs are the heat flow rate Q [J/s], the feedwater q_f [kg/s], and steam q_s flow rates. The nonlinear drum model is expressed by

$$\begin{aligned}\dot{P}_e &= \frac{e_{11}Q + q_f(e_{11}h_f - e_{21}) - q_s(e_{21} - e_{11}h_s)}{e_{11}e_{22} - e_{12}e_{21}},\\ \dot{V}_{wt} &= \frac{Q + q_f h_f - q_s h_s - e_{22}\dot{P}_e}{e_{21}},\\ \dot{\alpha}_r &= \frac{Q - \alpha_r q_{dc}(h_s - h_w) - e_{31}\dot{P}_e}{e_{33}},\\ \dot{V}_{sd} &= \frac{1}{T}(V_\circ - V_{sd}) - q_f\frac{h_f - h_w}{e_{44}(h_s - h_w)} - \frac{e_{41}\dot{P}_e + e_{43}\dot{\alpha}_r}{e_{44}},\end{aligned} \tag{5}$$

where the specific enthalpy h_f [J/kg], h_s, and h_w are computed using quadratic functions based on approximation of the steam tables. The expressions of the downcomer flow rate q_{dc}, and the nonlinear variables e_{nm} are found in the Appendix.

B. Controller Model

Fig. 3 illustrates the human machine interface (HMI) of the controller which comprises of a state observer (bottom, left-side) and a state-feedback controller with an Integral-controller (top, left-side). The I-controller ensures that the drum pressure and water level l [mm] track their corresponding reference signals w_p and w_l. Hence, the integrated errors $h := [\eta,\, \psi]^T$ are treated as artificial state variables

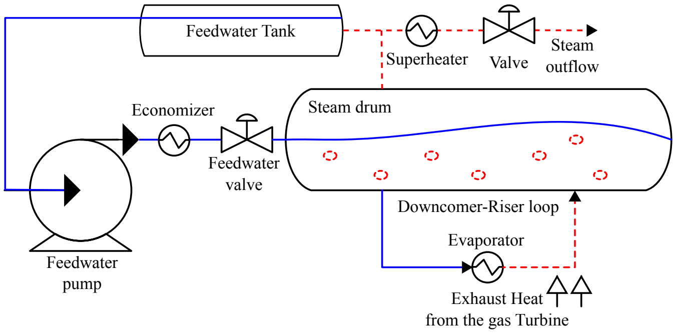


Fig. 2. Simplified description of the steam generation process. Red line (dotted) indicates hot steam and the blue line (solid) indicates cold water.

$$\begin{aligned}\dot{\eta} &= w_P - P_e,\\ \dot{\psi} &= w_l - l.\end{aligned} \tag{6}$$

Let $\hat{q}_f$ [kg/s], $\hat{r}_s$[%], and $\hat{r}_f$ denote the state-feedback controller output (control action) of the feedwater flow rate, the steam valve, and the feedwater valve opening percentages, respectively. These signals are generated by the controller to preserve the water level and pressure at the desired reference values according to

$$\begin{bmatrix}\hat{q}_f\\ \hat{r}_s\end{bmatrix} = K \cdot \begin{bmatrix}x_d\\ h\end{bmatrix}, \tag{7}$$

where $K \in \mathbb{R}^{(n_u-1)\times(n_d+n_y)}$ is the state feedback matrix. The control action of the feedwater flow rate $\hat{q}_f$ is compared to the actual flow rate, and the deviation between both generates the controller output of the feedwater valve opening percentage $\hat{r}_f$ using a feedback loop employing a PI-controller

$$\hat{r}_f = v_{pf}\left(1 + v_{if}\int_0^t (\hat{q}_f(\tau) - q_f(\tau))d\tau\right), \tag{8}$$

where v_{pf}, v_{if} are the proportional and integrator scalar gains of the PI-controller.

C. Model Extension

The heat flow rate Q is regarded as an additional state and not treated as an input variable due to the combined-cycle nature of the process. The heat is directly associated with the gas turbine exhaust temperature which corresponds to the electrical power demand P_D established by the TSO.

To easily represent the remaining equations, let κ [kg/h] denote the valve sizing coefficient, r [%] is the valve opening percentage, ν and τ are the gain and time constant for a first-order lag element, and the subscripts s, f, and D refer to steam, feedwater, and current demand, respectively. The heat flow rate is modeled as

$$\dot{Q} = \frac{\nu_D P_D - Q}{\tau_D}, \tag{9}$$

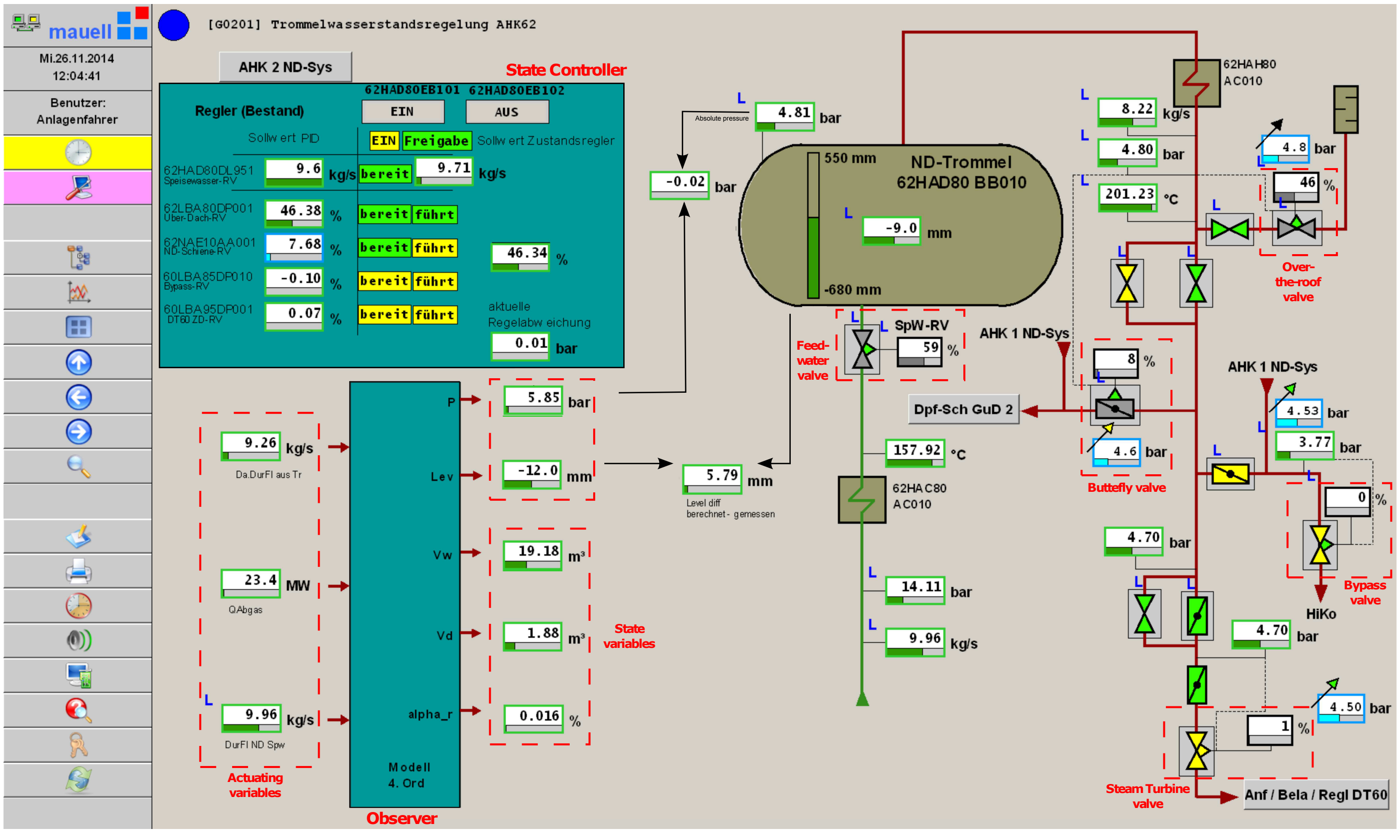


Fig. 3. Screenshot of the distributed control system (DCS) - Mauell ME-4012 illustrating the human machine interface (HMI) of the drum unit (right) alongside the observer-based state-feedback controller (left).

and the regulation through a control valve for feedwater and steam flow rates is

$$q_f = r_f \frac{\kappa_f \rho_f \sqrt{\Delta P_e \cdot 1\text{E-}5}}{3600}, \qquad \dot r_f = \frac{\nu_f \hat r_f - r_f}{\tau_f}, \tag{10}$$

$$q_s = r_s \frac{13.6\, \kappa_s \sqrt{\rho_s (P_e \cdot 1\text{E-}5)}}{3600}, \qquad \dot r_s = \frac{\nu_s \hat r_s - r_s}{\tau_s}, \tag{11}$$

where ΔP_e [Pascal] is the pressure drop across the feedwater valve, and $\rho\,[\mathrm{m}^3/\mathrm{kg}]$ denotes the density.

Combining the results (5)-(11), one obtains an 11-th order model with the input signals $u = [P_D,\, w_p,\, w_l]^T$, the state variables $x = [P_e,\, V_{wt},\, \alpha_r,\, V_{sd},\, \eta,\, \psi,\, Q,\, \hat r_f,\, r_f,\, r_s,\, \hat q_f]^T$, and the output vector $y = [P_e,\, l]^T$.

IV. Model Abstraction

In this section, we present how to obtain the polynomial model $P(\hat x(t), u(t))$ of the inclusion (3) using the Taylor expansion. We then illustrate the technique of linear output injection to guarantee asymptotic estimates of the state variables. Finally, we construct the set of modelling errors in an over-approximative manner so that the proposed abstraction includes all dynamic responses of the real system. Our approach is systematic but not formal: currently no formal way to translate reality into a mathematical representation exists.

A. Polynomial Approximation using Taylor Expansion

The motivation behind the choice of the polynomial approximation is its ability to represent complex mathematical expressions by a simplified form that substantially reduces the computational time required to compute the reachable set, without sacrificing the model accuracy and its fit to measurement data. For brevity, the state and input variables are combined into one vector $z := [x^T, u^T]^T \in \mathbb{R}^{n_z}$. This allows reformulation of the nonlinear system (1) into

$$\dot x = P(z) = \underbrace{\sum_{j=1}^{n_z} \frac{\partial f(z)}{\partial z_j}\bigg|_{z=z_{l*}} \Delta z_j}_{=:A\Delta x + B\Delta u} + \Phi(z), \tag{12}$$

with $\Delta x := x - x_{l*}$, $\Delta u := u - u_{l*}$, $\Delta z := z - z_{l*}$.

Here $A \in \mathbb{R}^{n_x \times n_x}$ and $B \in \mathbb{R}^{n_x \times n_u}$ are the system and input matrices evaluated at the point $z_{l*} := [{x_{l*}}^T, {u_{l*}}^T]^T$. The local Lipschitz continuous function $\Phi(\cdot)$ contains all higher order terms of the Taylor expansion

$$\Phi(z) = f(z_{l*}) + \frac{1}{2!} \sum_{j=1}^{n_z} \sum_{k=1}^{n_z} \frac{\partial^2 f(z)}{\partial z_j \partial z_k}\bigg|_{z=z_{l*}} \Delta z_j \Delta z_k$$

$$+\frac{1}{3!}\sum_{j=1}^{n_z}\sum_{k=1}^{n_z}\sum_{l=1}^{n_z}\frac{\partial^3 f(z)}{\partial z_j \partial z_k \partial z_l}\Bigg|_{z=z_{l*}}\Delta z_j \Delta z_k \Delta z_l + \dots \, . \tag{13}$$

B. Linear Output Injection

The vector $\hat{z} := [\hat{x}^T, u^T]^T$ and the variable $\Delta\hat{x} := \hat{x} - x_{l*}$ are introduced for further derivation. The concept of linear output injection was first proposed in [22] to construct the so-called *Luenberger observer*. The key idea is to use the discrepancy between the actual measurement value y and the observer output $\hat{y}$, i.e. to use the output error as a correction term applied to a feedback matrix L that decays the modelling errors over time. Hence the evolution of $\dot{\hat{x}}$ is expressed by a polynomial observer modeled as

$$\begin{aligned}\dot{\hat{x}} &= \phi(\hat{z}, e)\\ &= A\Delta\hat{x} + B\Delta u + \Phi(\hat{z}) + L\underbrace{C(\Delta x - \Delta\hat{x})}_{=:e}.\end{aligned} \tag{14}$$

Constructing a stable observer is not obvious due to the nonlinear dynamics of the modelling errors $\dot{e} := \dot{x} - \dot{\hat{x}}$. Furthermore, the matrix L is not unique, due to extra degrees of freedom arising in multivariable systems [23]. We assume that the matrix L is already chosen and focus on examining the asymptotic stability of the dynamics of the modelling errors. It can be seen from (12) and (14) that

$$\dot{e} = (A - LC)(\Delta x - \Delta\hat{x}) + [\Phi(z) - \Phi(\hat{z})] \, . \tag{15}$$

Theorem [24]. *If the feedback correction matrix L is chosen to hold*

$$\Omega < \frac{\lambda_{min}(Q)}{2\lambda_{max}(P)}, \tag{16}$$

then (15) *yields asymptotic stable estimates for* (12)*. Here Q and P are the symmetric matrices of the continuous Lyapunov equation $(A - LC)^T P + P(A - LC) = -Q$, $\lambda(\cdot)$ returns the eigenvalues of a matrix, and Ω is the constant of the local Lipschitz function $\Phi(\cdot)$ that satisfies:*

$$||\Phi(z) - \Phi(\hat{z})|| \le \Omega \, ||x - \hat{x}||. \tag{17}$$

The theorem presented above only serves as a means to check the observer stability. Due to its non-constructive nature, the theorem cannot be considered as a design approach. The task of designing the observer matrix L is outside the scope of this paper. We refer the reader to [25], in which the design procedure, in addition to the necessary and sufficient conditions for existence of the matrix L, are described in detail.

C. Constructing the Set of the Modelling Errors

We present a systematic approach to construct the set of the modelling errors $\mathcal{E}$ in an over-approximative manner. The proposed over-approximation guarantees that all possible trajectories of the errors $e(t)$, $\forall t \in [0, t_f]$ for n simulations are included within the constructed set. This is achieved by comparing the output $\hat{y}(t)$ within a simulation environment against validation data $y(t)$ with very rich excitation that covers the entire operational range of the process, thus including all possible values of the errors resulting from n scenarios.

The set of the modelling errors $\mathcal{E}_i$ is obtained by introducing a closed interval such that

$$\mathcal{E}_i := [-\gamma_i, \gamma_i] = \{a \in \mathbb{R} \,|\, -\gamma_i \le a \le \gamma_i\} \, , \tag{18}$$

$$\text{with} \begin{cases} \gamma_i := \max\limits_{k\,:1\dots n} \left(\delta_i^k\right), \\ \delta_i^k := \max\limits_{t\in[0,t_f]} \left\{ e_i^k(t) \in \mathbb{R}^+ \,\middle|\, e_i^k(t) = \left|y_i^k(t) - \hat{y}_i^k(t)\right| \right\}, \end{cases}$$

where the $\max(\cdot)$ operator is applied elementwise to return the maximum value, the subscript i and the superscript k denote the i-th measurable output and the k-th experiment, respectively, δ is the maximum of the absolute value of the error in the k-th experiment, while γ is the maximum error resulting from n simulations.

In (18), there is a tradeoff between the size of n and the accuracy of the resulting set, which can be measured by computing the volume of $\mathcal{E}$

$$\text{vol}(\mathcal{E}) = 2^{n_y} \cdot \prod_{i=1}^{n_y} \gamma_i. \tag{19}$$

Clearly, the volume approaches the true value as n goes to infinity. However, it is not possible to simulate infinitely many possible scenarios. Thus, we heuristically choose n to hold

$$\frac{\text{vol}(\overline{\mathcal{E}}) - \text{vol}(\underline{\mathcal{E}})}{\text{vol}(\overline{\mathcal{E}})} \le \epsilon, \tag{20}$$

where the set $\overline{\mathcal{E}}$ is obtained by setting the number of simulations to be twice as large as the size of n required to construct $\underline{\mathcal{E}}$, such that the value of ϵ becomes small (e.g. 1E-3). The underlying idea behind (20) is that the double effort to conduct further simulations is not justified because the percentage of the improvement is negligible. Therefore, the size of n reliably ensures that

$$\lim_{n\to\infty} \text{vol}(\mathcal{E}_\infty) \approx \text{vol}(\overline{\mathcal{E}}). \tag{21}$$

Here $\mathcal{E}_\infty$ is the set of modelling errors constructed by running infinitely many simulations. After introducing a safety factor ξ, one may choose $\mathcal{E} := \xi \cdot \overline{\mathcal{E}}$. With the construction of the set of the modelling errors according to (18)-(20), we still need to compute the reachable set of the abstract model, as illustrated in the next section.

V. Reachability Analysis

This section describes the basics for the computation of reachable sets of (1). Our reachability algorithm is based on abstracting the polynomial observer (14) into linear differential inclusions for each consecutive time interval $\tau_k := [t_{k-1}, t_k]$. By using the model (14) for reachability analysis, we guarantee that all dynamic behaviors of the original system (1) are enclosed by computed reachable sets, since the polynomial observer takes into account the modelling errors which are obtained according to the procedure described in Sec. IV-C.

Since the linearization of (14) causes additional errors, these errors are determined in an over-approximative manner and considered as additional uncertain inputs. By recomputing the linearization for each τ_k, the over-approximation remains small and accurate results are acquired. We only consider constant-size time intervals $t_k = k \cdot r$, where $k \in \mathbb{N}$, $r \in \mathbb{R}^+$ are the time step and the time increment, respectively. An extension covering variable-size time steps is found in [26].

We introduce the vector $v := [\hat{x}^T,\, u^T,\, e^T]^T \in \mathbb{R}^{n_v}$, the linearization point $v_k^* := [x_k^{*T},\, u_k^{*T},\, e_k^{*T}]^T$, and $\Delta\hat{x}_k := \hat{x} - x_k^*$. The nonlinear model (14) is abstracted by a first-order Taylor expansion with the Lagrangian remainder $\mathcal{L}$ (see [27])

$$\dot{\hat{x}} \in \hat{A}_k \Delta\hat{x}_k \oplus \underbrace{\phi(v_k^*) \oplus \hat{B}_k \cdot \mathcal{U} \oplus L \cdot \mathcal{E} \oplus \mathcal{L}}_{=:\hat{\mathcal{U}}}, \tag{22}$$

where $\hat{A}_k$ and $\hat{B}_k$ are the system and input matrices at the time interval τ_k, respectively[2], and $\hat{\mathcal{U}} \subset \mathbb{R}^{n_x}$ is the set of uncertain inputs.

A. Reachable Set Computation of Linear Systems

The state-space equation of the linear system is described by the affine dynamics

$$\dot{\hat{x}} = \hat{A}_k \Delta\hat{x}_k + \hat{u}_c, \tag{23}$$

where $\hat{u}_c$ as the center of the set $\hat{\mathcal{U}}$. For $r = t_k - t_{k-1}$, the general solution of (23) is well-known to be

$$\hat{x}(t_k) = \underbrace{e^{\hat{A}_k r} \Delta\hat{x}_k(t_{k-1})}_{=:\hat{x}_h(t_k)} + \underbrace{\int_0^r e^{\hat{A}_k (r-\tau)} d\tau\, \hat{u}_c}_{=:\hat{x}_p(r)}, \tag{24}$$

where $\hat{x}_p(r)$ is the particular solution and $\hat{x}_h(t_k)$ is the homogeneous solution, which considers the initial condition $\Delta\hat{x}_k$ without external inputs.

The basic procedure to compute the reachable set of a linear system without inputs is illustrated in Fig. 4 and consists of:

1) Compute the homogeneous reachable set $\mathcal{H}(t_k)$ based on the initial set $\mathcal{H}(t_{k-1})$.
2) Enclose the set $\mathcal{H}(t_k)$ and $\mathcal{H}(t_{k-1})$ by a convex hull.
3) Enlarge the convex hull to account for curvature of the trajectories over the time interval τ_k.

B. Representation of Reachable Sets

The reachable set computation we present is in principle applicable for all kinds of set representation, e.g. polytopes, zonotopes, ellipsoids and support functions [14]. In this work, we use zonotopes as set representation. Zonotopes are centrally-symmetric convex polytopes, and often considered as the Minkowski sum of a finite set of segments [15], [28]. A zonotope in a subset $\mathbb{R}^{n_\mathcal{Z}}$ is expressed as

$$\mathcal{Z} = \left\{ x \in \mathbb{R}^{n_\mathcal{Z}} \,\middle|\, x = c + \sum_{i=1}^{p} \beta_i g^{(i)}, \beta_i \in [-1, 1] \right\}, \tag{25}$$

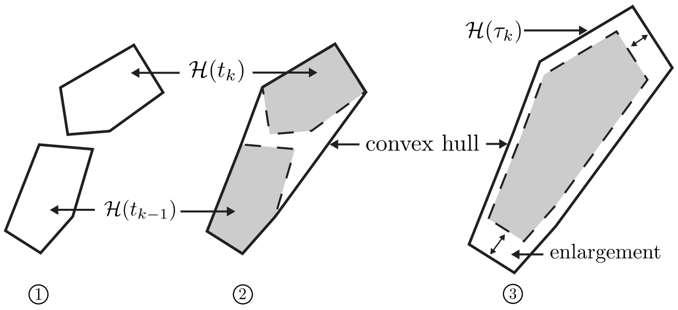


Fig. 4. Computation of reachable sets of a linear system without inputs.

where $c \in \mathbb{R}^{n_\mathcal{Z}}$ is the center of the zonotope and $g^{(i)} \in \mathbb{R}^{n_\mathcal{Z}}$ denotes the generators of $\mathcal{Z}$. The order of a zonotope is defined as $\mu := \frac{p}{n_\mathcal{Z}}$, where p is the number of generators.

Using zonotopes, the Minkowski sum and linear transformation (4) can be efficiently computed. In addition, the axis-aligned bounding box, or so-called interval hull of zonotopes can be efficiently computed which is advantageous for the computation of the Lagrangian remainder.

C. Over-approximation of Reachable Set

The over-approximation procedure of the reachable set of the general solution (24) is the same as the procedure in [15], [28], and [29]. The homogenous reachable set $\mathcal{H}(t_k)$ is computed by substituting the initial value $\Delta\hat{x}_k$ by $\mathcal{H}(t_{k-1})$ in the homogenous solution $\hat{x}_h(t_k)$, thus

$$\mathcal{H}(t_k) = e^{\hat{A}_k r} \cdot \mathcal{H}(t_{k-1}). \tag{26}$$

The neglected terms resulting from the Taylor expansion of the exponential matrix $e^{\hat{A}_k r} = \sum_{i=0}^{\sigma} \frac{r^i \hat{A}_k^i}{i!}$ are over-approximated by the remainder $\mathcal{E}(r)$ using an interval symmetrical matrix, i.e. a matrix with symmetric lower and upper bound on each element

$$\mathcal{E}(r) := [-W(r), W(r)], \tag{27}$$

$$W(r) := e^{|\hat{A}_k| r} - \sum_{i=0}^{\sigma} \frac{(|\hat{A}_k| r)^i}{i!}, \tag{28}$$

where σ is the number of terms of the Taylor expansion of the exponential matrix $e^{\hat{A}_k r}$. The absolute value $|\hat{A}_k|$ is defined element wise such that $|\hat{A}_k|_{ij} := \sup\{\hat{a}_{ij} | \hat{a} \in \hat{A}_k\}$.

The enlargement of the convex hull enclosing $\mathcal{H}(t_{k-1})$ and $\mathcal{H}(t_k)$ (see Fig. 4) is performed by computing the interval matrix $\mathcal{F}$ to account for all solutions starting from $\mathcal{H}(t_{k-1})$, such that

$$\mathcal{F} := \left(\bigoplus_{i=2}^{\sigma} \left[\left(i^{\frac{-i}{i-1}} - i^{\frac{-1}{i-1}} \right) r^i, 0 \right] \frac{\hat{A}_k^i}{i!} \right) \oplus \mathcal{E}(r). \tag{29}$$

Assuming the uncertain input set $\hat{\mathcal{U}}$ is convex and contains the origin, one can over-approximate the particular solution $\hat{x}_p(r)$ according to (see [15, Ch. 3])

$$\mathcal{P}(r) = \left(\bigoplus_{i=0}^{\sigma} \frac{|\hat{A}_k|^i \, r^{i+1}}{(i+1)!} \cdot \hat{\mathcal{U}} \right) \oplus \left(\mathcal{E} \cdot r \cdot |\hat{\mathcal{U}}| \right). \tag{30}$$

[2] The linearization of (14) is performed at each time interval τ_k, whereas the linearization of (1), as expressed by (12), is performed once to obtain the polynomial model as proposed by our generic approach in Fig. 1.

D. Computing the Set of the Linearization Errors

As described in (22), the linearization errors are obtained by computing the Lagrangian remainder, expressed as

$$\mathcal{L}_j = \left\{ \frac{1}{2}(v - v_k^*)^T \frac{\partial^2 \phi_j(\zeta(v, v_k^*))}{\partial v^2}(v - v_k^*) \right. \\ \left. \middle| \zeta(v, v_k^*) \in \{v_k^* + \alpha(v - v_k^*) \,|\, \alpha \in [0, 1]\} \right\}, \quad (31)$$

where j denotes the system dimension of (14). In order to evaluate the set of the linearization errors $\mathcal{L}_j$ within a time interval τ_k, one has to consider the possible values of $v \in \mathcal{V}(\tau_k)$ resulting from the Cartesian product

$$\mathcal{V}(\tau_k) := \mathcal{R}(\tau_k) \times \mathcal{U} \times \mathcal{E}, \quad (32)$$

where $\mathcal{R}(\tau_k) \subset \mathbb{R}^{n_x}$ is the reachable set of the linear differential inclusion (22) in the time interval τ_k. In order to determine the maximum absolute value of $\mathcal{L}_j$ for $v \in \mathcal{V}(\tau_k)$ efficiently, the following over-approximation is proposed [30, Prop. 1]

$$\begin{aligned} &|\mathcal{L}_j| \subseteq [0,\, \ell_j]\,, \\ \text{with } &\ell_j = \lambda^T \max_{v \in \mathcal{V}(\tau_k)} \left\{ \left| \frac{\partial^2 \phi_j(\zeta(v, v_k^*))}{\partial v^2} \right| \right\} \lambda, \\ \text{and } &\lambda = |c_v - v_k^*| + \sum_{i=1}^{p} |g_v^{(i)}|, \end{aligned} \quad (33)$$

where c_v and $g_v^{(i)}$ are the center and generators of the zonotope $\mathcal{V}(\tau_k)$, respectively.

Our previous work has shown that the bounding vector ℓ of the absolute value of the Lagrangian remainder is minimized by choosing $v_k^* = c_v$ as the linearization point [30, Prop. 2], where c_v is the center of the reachable set $\mathcal{V}(\tau_k)$. Since the center c_v is not known in advance, it is approximated by a one-step Euler integration based on the center $\hat{c}$ of $\mathcal{V}(t_{k-1})$

$$v_k^* = \hat{c} + \frac{r}{2}\phi(\hat{c}) \approx c_v, \quad (34)$$

where the step size is $0.5r$ because the center of the reachable set $\mathcal{V}(t_{k-1})$ for the time interval τ_k is expected to be reached after half the interval duration of $r = t_k - t_{k-1}$.

VI. Simulation Results

First we present the validation of the polynomial model (12) against measurement data to show its ability to capture the dynamic behavior of the real process. The validation data covers almost the entirety of the gas turbine operational range, i.e. from 70 MW to 120 MW in both directions (increased/decreased generation). The data was collected over a period of one year while the main author worked at the power plant *München Süd*. We then illustrate the histogram distribution of the modelling errors when employing the technique of linear output injection, and investigate the safety of the water level against high-load transitions ($\leq$ 40 MW) by computing the over-approximative reachable set of the polynomial observer (14). Finally, we outline the special findings using reachability analysis. All computations are performed on a standard computer with an Intel Core i7-4810MQ CPU.

A. Validation of the Polynomial Model

The model is realized in MATLAB R2014b using the Symbolic toolbox, and is approximated by a polynomial function using the Taylor expansion at $P_D = 95\,\text{MW}$ (center of the gas turbine operational range). The validation procedure is carried out by simulating the models (1-st, 2-nd and 3-rd order polynomial functions) and comparing the simulation results to the experimental data. All simulations are performed using the `ODE45` solver.

As shown in Fig. 5 and Fig. 6, the polynomial models replicate the dynamic behavior of the real process, and most importantly, the shrink and swell physical phenomena. The model inaccuracy is acknowledged and identifiable and is caused by the nature of the proposed polynomial approximation, and by the simplification of certain components during the modelling procedure. Practically speaking, this inaccuracy can be deemed acceptable and is adequate for further analysis, i.e. design of the matrix L, model-based control design (see [7] and [12]), and computation of the reachable set.

B. Validation using Linear Output Injection

The observer (14) is compared to multiple trajectories with a duration ranging between 2 h and 5 h. The comparison covered all major possible excitation conditions; that is, either slow or fast transition with small, medium and high load change. We only present three conditions: (a) fast transitions with small load changes equivalent to 10 MW, (b) slow transitions with medium load changes equivalent to 20 MW, and (c) fast transitions with high load changes equivalent to 40 MW (worst-case scenario). Fig. 7 shows the histogram distribution of the modelling errors e_p and e_l for the aforementioned scenarios using the 3-rd order polynomial model with linear output injection. As depicted in Fig. 7, the modelling errors increase for high load changes.

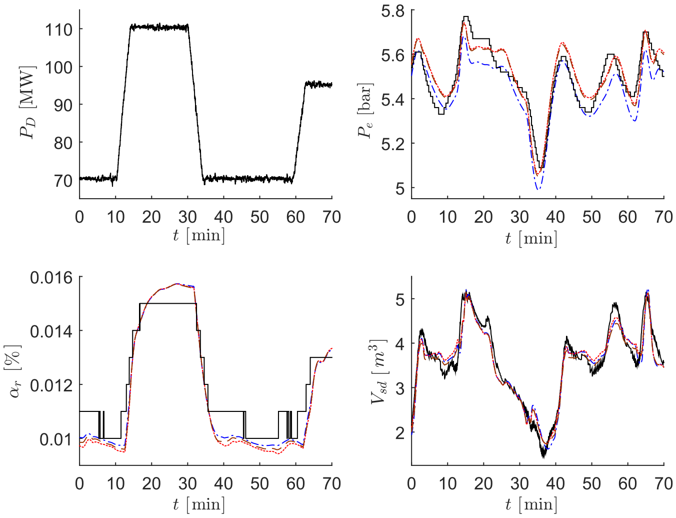


Fig. 5. Comparison between measurement data (black solid line), 1-st (blue dashed-dotted line), 2-nd (red dotted line) and 3-rd (brown dashed line) order polynomial model for perturbations of the gas turbine power.

TABLE I. INTERVAL OF THE MODELLING ERRORS FOR DIFFERENT MODELS USING LINEAR OUTPUT INJECTION

Model	$\mathcal{E}_P$ [bar]	$\mathcal{E}_l$ [mm]
1-st order	$[-0.1100, 0.1100]$	$[-21.8374, 21.8374]$
2-nd order	$[-0.0532, 0.0532]$	$[-14.3283, 14.3283]$
3-rd order	$[-0.0512, 0.0512]$	$[-14.1288, 14.1288]$
[6]	$[-0.0380, 0.0380]$	$[-10.6481, 10.6481]$

The interval of the modelling errors, which is obtained using (18) according to the procedure described in Sec. IV-C, is shown in Table I. It is clear that the 1-st order (linear model) does not fit the experimental data well. The 4-th and higher order models, however, are not considered since little improvement is achieved when comparing the error resulting from both the 2-nd and 3-rd order approximations: the complexity of using a higher polynomial approximation is not justified since it only results in a more complicated model which contradicts our goal of simplifying the complex nonlinear expressions found in (5) (see the Appendix). Although the original model (5) [6] has the minimum modelling errors, we illustrate in the following subsection the computational benefit of using a polynomial model. All subsequent results are over-approximated as we fully consider the modelling errors $\mathcal{E}$ from Table I.

C. Load-following Safety Verification

The reachable set is computed over a time-horizon t_f with a time increment $r = 1\,\mathrm{s}$ using the **Co**ntinuous **R**eachability **A**nalyser (CORA) toolbox [31]. CORA integrates various vector and matrix set representations and operations as well as reachability algorithms of various system classes.

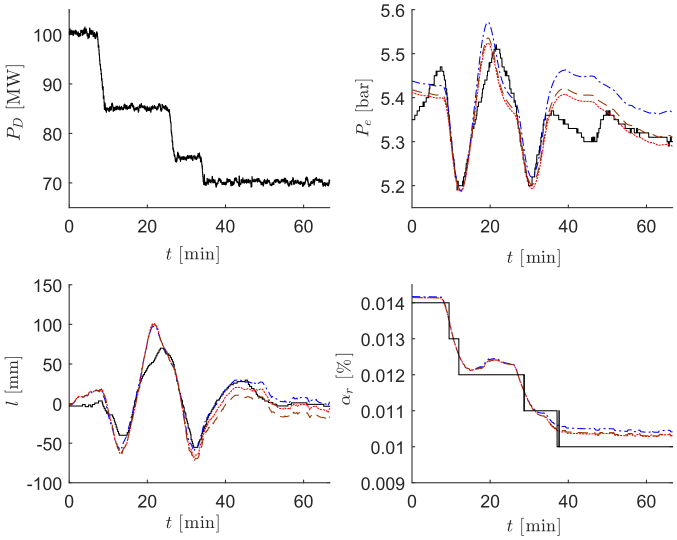
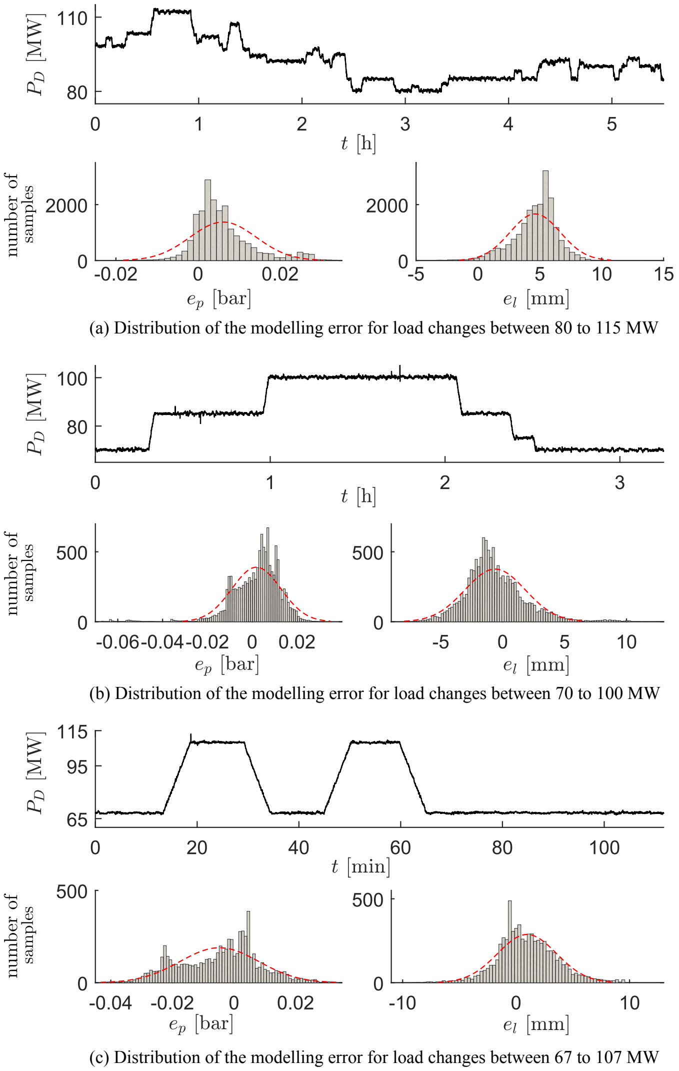


Fig. 6. Comparison between measurement data (black solid line), 1-st (blue dashed-dotted line), 2-nd (red dotted line) and 3-rd (brown dashed line) order polynomial model for decrease of the gas turbine power from 100 MW to 70 MW.

When *München Süd* is subjected to secondary frequency control, it is notified by the TSO 5 min earlier to meet a load change equivalent to 40 MW. The task is to guarantee that the water level l inside the drum does not surpass ±300 mm during the load transition. If the limits are triggered, the boiler is tripped as a safety precaution to protect critical components, e.g., the superheater and the steam-turbine. During this time, the power plant is no longer operational and is unable to meet load requirements of the TSO.

The power demand P_D has a fixed trajectory for a load change of 40 MW in both directions (increased/decreased generation) which is the maximum load transition that can be requested by the TSO. The input P_D follows the maximum allowable load gradient that can be imposed on the plant ($8\,\frac{\mathrm{MW}}{\mathrm{min}}$). We include uncertainty to the initial set of the drum state variables when computing the reachable set, since initial states



(a) Distribution of the modelling error for load changes between 80 to 115 MW

(b) Distribution of the modelling error for load changes between 70 to 100 MW

(c) Distribution of the modelling error for load changes between 67 to 107 MW

Fig. 7. Histogram distribution of the modelling errors e_p and e_l for different loading conditions. (a) Rapid transitions for small load-changes, (b) slow transition for medium load-changes, (c) rapid transitions for high-load changes.

are not exactly known due to increasingly varying operating conditions in current power systems. We define the interval $\boldsymbol{U} := [-1,\, 1]$, and assign the center of the initial set as the steady state solution of (14) denoted by the superscript zero. Therefore, the initial drum pressure is $P_e(0) \in P_e^0 \oplus 1\text{E}4 \cdot \boldsymbol{U}$, the initial volume of water is $V_{wt}(0) \in V_{wt}^0 \oplus 0.5 \cdot \boldsymbol{U}$, the initial steam quality is $\alpha_r(0) \in \alpha_r^0 \oplus 0.001 \cdot \boldsymbol{U}$, the initial steam volume under the water level is $V_{sd}(0) \in V_{sd}^0 \oplus 0.5 \cdot \boldsymbol{U}$, and the initial heat flow rate is $Q(0) \in Q^0 \oplus 1\text{E}5 \cdot \boldsymbol{U}$.

The time-domain bounds of the reachable set of the drum pressure and water level, and the reachable set projections of chosen state variables are illustrated in Fig. 8 and Fig. 9, respectively. The visualization of the 2-D projection is quite beneficial to the plant operators, since they are interested in the dynamic behavior of the water level and pressure against the loading condition of the gas turbine. The water level does not reach the safety limit, hence the safety of the drum-boiler unit is formally verified under maximum loading condition imposed by the TSO.

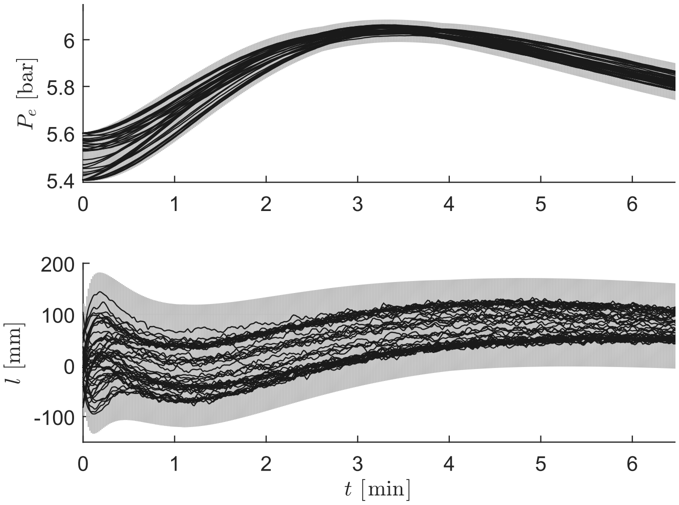


Fig. 8. The time-domain bounds of the reachable set for a load-change of the gas turbine from 70 MW to 110 MW. Black lines represents random simulation results ($n = 50$), the gray area shows the reachable set.

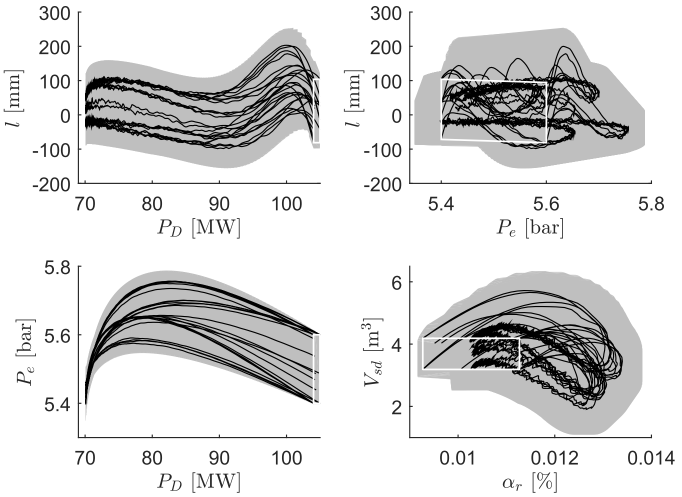


Fig. 9. Selected projections of the reachable set for a load-change of the gas turbine from 110 MW to 70 MW. Black lines represent random simulation results ($n = 25$), the gray area shows the reachable set, the white box is the initial set of state variables $\mathcal{R}(0)$.

Fig. 10 illustrates the quality of the over-approximation resulting from the set of the uncertain modelling errors. The zonotope order μ and the time increment r are chosen to reduce the resulting wrapping effect such that the computed reachable set is tight. It is worth mentioning that there exists no wrapping-free algorithms in the literature for the class of nonlinear systems. Our approach systemically constructs an abstract model strictly based on measurement data from the power plant, in contrast to any previous work on reachability analysis requiring more conservative assumptions on the modelling errors. We always have to account for the maximum error resulting over n simulations, otherwise we cannot formally guarantee that the specifications of our particular problem are always met under all eventualities. Finding simple but less conservative enclosures is being considered for future work.

TABLE II. Comparison between the computational time of reachability analysis using different models

Model	t_f	$\mathcal{R}([0, t_f])$	$\mathcal{L}([0, t_f])$
2-nd	5 min	41.41 s	34.06 s
3-rd	5 min	206.37 s	198.53 s
[6]	10 s	3420 s	3078 s

Table II shows a comparison between the computational time of reachability analysis using different models. Using the 3-rd order polynomial model, it takes 206.37 s to compute the reachable set, where the calculation of the Lagrangian remainder consumes 96 % of the time. The computational time

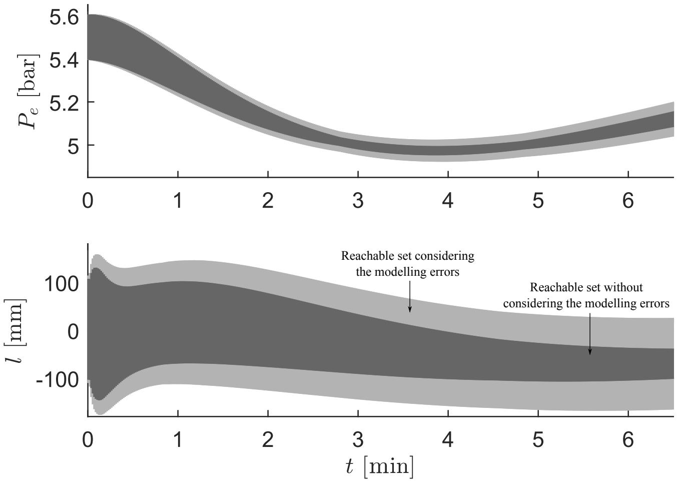


Fig. 10. Comparison between the time-domain bounds of the reachable set without considering uncertain inputs (dark gray), and considering uncertain inputs (light gray) for a load-change of the gas turbine from 110 MW to 70 MW.

meets practical requirements of the plant as it allows online verification of the process safety for high-load transitions in the requested time (t$\leq$ 5 min). Using the nonlinear model presented in Sec. III without a polynomial approximation, it takes 57.2 min to compute the reachable set for a time-horizon of 10 s. The huge difference in the computational time is due to the complicated expressions (see the Appendix), which were simplified with a polynomial function, thus in return substantially reduces the computational complexity making the algorithm feasible for practical problems.

D. Discussion of Results

The special findings using reachability analysis can be summarized as follows: we formally guarantee that the controller meets the performance specifications under all eventualities, because we have taken the modelling errors into account. Meeting performance specifications cannot be achieved using numerical simulations since they do not guarantee any formal properties. Furthermore, it is not possible to simulate infinitely many simulations corresponding to infinitely many possible uncertain input trajectories. Numerical simulations are indeed simple to implement, however, they are only useful to gain an initial idea about the system behavior (see Fig. 5 and Fig. 6).

The proposed reachability algorithm can be faster than sufficiently many numerical simulations. One simulation of our model takes approximately 0.49 s using the `ODE45` solver; however, the simulation of all corner cases requires 2^n simulations (exponential problem), where n is the number of states, consuming roughly 1012 s of computational time. On the contrary, using our approach, the computational time necessary to compute the reachable set is 41.41 s (see Table II).

The significant difference in computational time showcases the feasibility of our algorithm compared to deterministic simulations. Our approach meets the practical requirements of the power plants, when subjected to the time constraints of secondary frequency control (5 min) imposed by the TSO. Furthermore, the algorithm considers all eventualities and formally verifies the safety of the boiler in real-time.

VII. Conclusion

We present a generic approach to rigorously verify the safety of the critical process variables in power plants when subjected by the TSO to high-load changes which, as a result, exploits the power plant's flexibility and load-following capabilities. Our analysis is based on a real boiler system located at a 450 MW combined cycle plant (*München Süd*) in Munich, Germany. In order to demonstrate the effectiveness of the proposed technique, we compute the reachable set for the evolution of the state variables of the drum with load changes equivalent to 40 MW.

An abstraction to a polynomial differential inclusion based on measurement data is proposed. It is shown that the Åström - Bell model [6] can be approximated by a polynomial function without losing the fit to experimental data. The abstraction is systematically performed and returns the modelling errors, whereby all dynamic behaviors of the original system are captured by the abstraction. The proposed abstraction substantially reduces the computational time required to compute the reachable set in comparison with the original system.

According to our final results, it is computationally feasible to implement the proposed reachability algorithm while meeting the practical requirements of a real power plant. The reachability algorithm can be easily integrated into a distributed control system (DCS), in parallel to the existing control structure, and operates automatically without any interaction from the operator. Because reachability analysis establishes in advance whether or not a requested load dispatch by the TSO will trigger the water level safe limit considering all eventualities, the plant operator can potentially avoid an unnecessary shutdown of the facility.

Acknowledgment

Financial support from the German Research Foundation (DFG) is gratefully acknowledged (AL 1185/2-1). We would also like to express our sincere gratitude to Stadtwerke München (SWM Services GmbH) for their willingness to allow us to perform experiments at the power plant München Süd. We would also like to express our gratitude to the reviewers for constructive criticism.

References

[1] D. S. Kirschen, "Demand-side view of electricity markets," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 520–527, 2003.

[2] J. C. Smith, M. R. Milligan, E. A. DeMeo, and B. Parsons, "Utility wind integration and operating impact state of the art," *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 900–908, 2007.

[3] H. Banakar, C. Luo, and B. T. Ooi, "Impacts of wind power minute-to-minute variations on power system operation," *IEEE Transactions on Power Systems*, vol. 23, no. 1, pp. 150–160, 2008.

[4] Y. G. Rebours, D. S. Kirschen, M. Trotignon, and S. Rossignol, "A survey of frequency and voltage control ancillary services - Part I: Technical features," *IEEE Transactions on Power Systems*, vol. 22, no. 1, pp. 350–357, 2007.

[5] L. Hirth and I. Ziegenhagen, "Control power and variable renewables: A glimpse at German data," in *Proc. of the 10th International Conference on European Energy Market*, 2013.

[6] K. J. Åström and R. D. Bell, "Drum boiler dynamics," *Automatica*, vol. 36, pp. 363–378, 2000.

[7] A. El-Guindy, S. Runzi, and K. Michels, "Optimizing drum-boiler water level control performance: A practical approach," in *Proc. of the 2014 IEEE Multi-Conference on Systems and Control*, 2014, pp. 1675–1680.

[8] M. Nakamoto, K. Shimizu, and H. Fukuda, "Multivariable control for a combined cycle power plant," *Control Engineering Practice*, vol. 3, no. 4, pp. 465–470, 1995.

[9] M. G. Na, "Auto-tuned PID controller using a model predictive control method for the steam generator water level," *IEEE Transactions on Nuclear Science*, vol. 48, no. 5, pp. 1664–1671, 2001.

[10] F. Zhao, J. Ou, and W. Du, "Simulation modeling of nuclear steam generator water level process: A case study," *ISA transactions*, vol. 39, no. 2, pp. 143–151, 2000.

[11] M. V. Kothare, B. Mettler, M. Morari, P. Bendotti, and C.-M. Falinower, "Level control in the steam generator of a nuclear power plant," *IEEE Transactions on Control Systems Technology*, vol. 8, no. 1, pp. 55–69, 2000.

[12] A. El-Guindy, F. Nickel, and K. Michels, "Centralised multivariable feedback control of steam drums in combined cycle power plants," *VGB PowerTech*, vol. 95, no. 4, pp. 73–78, 2015.

[13] W. L. Oberkampf, S. M. DeLand, B. M. Rutherford, K. V. Diegert, and K. F. Alvin, "Error and uncertainty in modeling and simulation," *Reliability Engineering & System Safety*, vol. 75, no. 3, pp. 333–357, 2002.

[14] C. Le Guernic, "Reachability analysis of hybrid systems with linear continuous dynamics," Ph.D. dissertation, Université Joseph-Fourier-Grenoble I, 2009.

[15] M. Althoff, "Reachability analysis and its application to the safety assessment of autonomous cars," Ph.D. dissertation, Technische Universität München, 2010.

[16] Y. C. Chen and A. D. Domínguez-García, "A method to study the effect of renewable resource variability on power system dynamics," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 1978–1989, 2012.

[17] X. Jiang, Y. C. Chen, and A. D. Domínguez-García, "A set-theoretic framework to assess the impact of variable generation on the power flow," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 855–867, 2013.

[18] H. N. V. Pico, D. C. Aliprantis, and E. C. Hoff, "Reachability analysis of power system frequency dynamics with new high-capacity HVAC and HVDC transmission lines," in *Proc. of the IREP Bulk Power System Dynamics and Control Symposium*, 2013, pp. 1–9.

[19] M. Althoff, "Formal and compositional analysis of power systems using reachable sets," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2270–2280, 2014.

[20] G. Lafferriere, G. J. Pappas, and S. Yovine, "Symbolic reachability computation for families of linear vector fields," *Journal of Symbolic Computation*, vol. 32, no. 3, pp. 231 – 253, 2001.

[21] E. M. Clarke, O. Grumberg, and D. E. Long, "Model checking and abstraction," *ACM transactions on Programming Languages and Systems*, vol. 16, no. 5, pp. 1512–1542, 1994.

[22] D. G. Luenberger, "Observing the state of a linear system," *IEEE Transactions on Military Electronics*, vol. 8, pp. 74–80, 1964.

[23] J. Kautsky, N. K. Nichols, and P. Van Dooren, "Robust pole assignment in linear state feedback," *International Journal of Control*, vol. 41, no. 5, pp. 1129–1155, 1985.

[24] F. E. Thau, "Observing the state of non-linear dynamic systems," *International Journal of Control*, vol. 17, no. 3, pp. 471–479, 1973.

[25] R. Rajamani, "Observers for Lipschitz nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 43, no. 3, pp. 397–401, 1998.

[26] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler, "SpaceEx: Scalable verification of hybrid systems," in *Computer Aided Verification*. Springer, 2011, pp. 379–395.

[27] M. Berz and G. Hoffstätter, "Computation and application of taylor polynomials with interval remainder bounds," *Reliable Computing*, vol. 4, no. 1, pp. 83–97, 1998.

[28] A. Girard, "Reachability of uncertain linear systems using zonotopes," in *Hybrid Systems: Computation and Control*. Springer, 2005, pp. 291–305.

[29] O. Stursberg and B. H. Krogh, "Efficient representation and computation of reachable sets for hybrid systems," in *Hybrid Systems: Computation and Control*. Springer, 2003, pp. 482–497.

[30] M. Althoff, O. Stursberg, and M. Buss, "Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization," in *Proc. of the 47th IEEE Conference on Decision and Control*, 2008, pp. 4042–4048.

[31] M. Althoff, "An Introduction to CORA 2015," in *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*, 2015.

Appendix

A. Nomenclature

Drum-Boiler Model Variables

α_r	Steam-mass quality in the riser tubes [%]
ΔP_e	Pressure drop across the feedwater valve [Pascal]
l	Water level inside the drum [mm]
P_D	Electrical power demand [MW]
P_e	Drum pressure [Pascal]
Q	Gas turbine heat flow rate [MW]
q_{dc}	Downcomer flow rate [kg/s]
q_f	Feedwater flow rate [kg/s]
q_s	Steam flow rate [kg/s]
r_f	Feedwater valve opening percentage [%]
r_s	Steam valve opening percentage [%]
V_{sd}	Steam volume under the water level [m^3]
V_{wt}	Water volume inside the drum [m^3]

Controller Model Variables

$\hat{q}_f$	Controller output of the feedwater flow rate [kg/s]
$\hat{r}_f$	Controller output of the feedwater valve opening percentage [%]
$\hat{r}_s$	Controller output of the steam valve opening percentage [%]
w_l	Set value of the drum water level [mm]
w_p	Set value of the drum pressure [Pascal]

Drum-Boiler Thermodynamics Properties

ρ_s	Steam density [m^3/kg]
ρ_w	Water density [m^3/kg]
h_f	Feedwater specific enthalpy [J/kg]
h_s	Steam specific enthalpy [J/kg]
h_w	Water specific enthalpy [J/kg]
t_{sat}	Saturation temperature [°C]

Drum-Boiler Parameters

β	Dimensionless coefficient [−]
A_d	Water level surface area [m^2]
A_{dc}	Downcomer cross-sectional area [m^2]
C_p	Specific heat capacity [J/kg K]
K_{dc}	Friction coefficient [−]
m_d	Drum mass [kg]
m_r	Riser mass [kg]
$V_\circ$	Volume in hypothetical situation [m^3]
V_d	Drum volume [m^3]
V_{dc}	Downcomer volume [m^3]
V_r	Riser tubes volume [m^3]
T	Steam residence time inside the drum [s]

B. Drum-Boiler Nonlinear Variables

The nonlinear variables e_{nm} appearing in the Åström - Bell model (5) are

$$
\begin{aligned}
e_{11} &= \rho_w - \rho_s, \\
e_{12} &= V_{wt}\frac{\partial \rho_w}{\partial P_e} + V_{st}\frac{\partial \rho_s}{\partial P_e},
\end{aligned}
$$

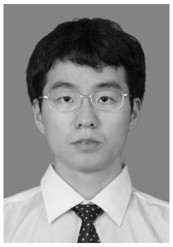
$$
\begin{aligned}
e_{21} &= \rho_w h_w - \rho_s h_s,\\
e_{22} &= V_{wt}\left(h_w \frac{\partial \rho_w}{\partial P_e} + \rho_w \frac{\partial h_w}{\partial P_e}\right) + \\
&\quad V_{st}\left(h_s \frac{\partial \rho_s}{\partial P_e} + \rho_s \frac{\partial h_s}{\partial P_e}\right) - V_t + m_t C_p \frac{\partial t_{\text{sat}}}{\partial P_e},\\
e_{31} &= \left(\rho_w \frac{\partial h_w}{\partial P_e} - \alpha_r h_c \frac{\partial \rho_w}{\partial P_e}\right)(1-\bar{\alpha}_v)V_r + \\
&\quad \left(\rho_s \frac{\partial h_s}{\partial P_e} + (1-\alpha_r) h_c \frac{\partial \rho_s}{\partial P_e}\right)\bar{\alpha}_v V_r + \\
&\quad (\rho_s + (\rho_w - \rho_s)\alpha_r))\, h_c V_r \frac{\partial \bar{\alpha}_v}{\partial P_e} - \\
&\quad V_r + m_r C_p \frac{\partial t_{\text{sat}}}{\partial P_e},\\
e_{33} &= ((1-\alpha_r)\rho_s + \alpha_r \rho_w)\, h_c V_r \frac{\partial \bar{\alpha}_v}{\partial P_e}\\
e_{41} &= V_{sd} \frac{\partial \rho_s}{\partial P_e} + \alpha_r (1+\beta) V_r \left((1-\bar{\alpha}_v)\frac{\partial \rho_w}{\partial P_e} + \right.\\
&\quad \left. \bar{\alpha}_v \frac{\partial \rho_s}{\partial P_e} + (\rho_s - \rho_w) + \frac{\partial \bar{\alpha}_v}{\partial P_e}\right) + \\
&\quad \frac{1}{h_c}\left(\rho_s V_{sd} \frac{\partial h_s}{\partial P_e} - \right.\\
&\quad \left. V_{sd} - V_{wd} + \rho_w V_{wd} \frac{\partial h_w}{\partial P_e} + m_d C_p \frac{\partial t_{\text{sat}}}{\partial P_e}\right),\\
e_{43} &= \alpha_r (1+\beta)(\rho_w + \rho_s) V r \frac{\partial \bar{\alpha}_v}{\partial P_e},
\end{aligned}
$$

with:

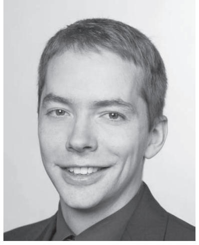
$$
\begin{aligned}
q_{dc} &= \sqrt{\frac{19.6 \rho_w A_{dc} (\rho_w - \rho_s)\bar{\alpha}_v V_r}{K_{dc}}},\\
h_c &= h_s - h_w,\\
m_t &= m_d + m_r,\\
V_t &= V_d + V_r + V_{dc} = V_{wt} + V_{st},\\
V_{wd} &= V_{wt} - V_{dc} - (1-\bar{\alpha}_v)V_r,\\
\bar{\alpha}_v &= \frac{\rho_w}{\rho_w - \rho_s}\left(\frac{\zeta - 1}{\zeta}\ln(1+\zeta)\right),\\
\zeta &= \alpha_r \frac{(\rho_w - \rho_s)}{\rho_s},\\
\frac{\partial \bar{\alpha}_v}{\partial P_e} &= \frac{1}{(\rho_w - \rho_s)^2}\left(\rho_w \frac{\partial \rho_s}{\partial P_e} - \rho_s \frac{\partial \rho_w}{\partial P_e}\right),\\
&\quad \left(1 + \frac{\rho_w}{\rho_s(1+\zeta)} - \frac{\rho_s + \rho_w}{\zeta \rho_s}\ln(1+\zeta)\right),\\
\frac{\partial \bar{\alpha}_v}{\partial \alpha_r} &= \frac{\rho_w}{\rho_s \zeta}\left(\frac{\ln(1+\zeta)}{\zeta} - \frac{1}{1+\zeta}\right).
\end{aligned}
$$

In addition steam tables are required to evaluate h_s, h_w, ρ_s, ρ_w, $\frac{\partial \rho_s}{\partial P_e}$, $\frac{\partial \rho_w}{\partial P_e}$, $\frac{\partial h_s}{\partial P_e}$, t_{sat}, and $\frac{\partial t_{\text{sat}}}{\partial P_e}$ at the saturation pressure of the drum.

Ahmed El-Guindy is currently a Ph.D. candidate at Technische Universität München, Germany. He received his B.Sc. degree in Electrical Engineering in 2011 from Ain Shams University, Egypt, and his M.Sc. degree in Information and Automation Engineering in 2013 from Universität Bremen, Germany. He joined the Department of Informatics at Technische Universität München in 2015. His research interests include power systems, energy conversion systems, formal methods in control, and reachability analysis.



Dongkun Han is currently a research associate at Technische Universität München. He received his Ph.D. degree in Electrical and Electronic Engineering from the University of Hong Kong in 2014. From 2013 to 2014 he was an exchange research student at Information Systems Laboratory, Stanford University. From 2009 to 2010, he was a research assistant at Power System Modelling Laboratory, China Southern Power Grid Co. Ltd. He joined the Department of Computer Science at Technische Universität München in 2014. His research interests include the formal verification of power systems, robust consensus of multi-agent systems, synchronization of complex network, polynomial systems, semidefinite programming and sums of squares technique.



Matthias Althoff is assistant professor in Computer Science at Technische Universität München, Germany. He received the Diploma Engineering degree in Mechanical Engineering in 2005, and his Ph.D. degree in Electrical Engineering in 2010, both from Technische Universität München, Germany. From 2010 to 2012 he was a postdoctoral researcher at Carnegie Mellon University, Pittsburgh, USA, and from 2012 to 2013 an assistant professor at Technische Universität Ilmenau, Germany. His research interests include formal verification of continuous and hybrid systems, reachability analysis, planning algorithms, nonlinear control, automated vehicles, and power systems.