EPiC Series in Computing

Volume 90, 2022, Pages 26–43

Proceedings of 9th International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH22)

Benchmarks for the Formal Verification of Power Systems

Matthias Althoff

Technical University of Munich,
Department of Informatics,
Munich, Germany
althoff@tum.de

Abstract

Benchmark proposal: Safe renewable energy systems are becoming increasingly important to combat climate change. Electric utility companies often use conservative approaches to feed in renewable energy to ensure a safe operation due to a lack of advanced analysis techniques. So far, mostly simulations are used in practice to safeguard the system against certain contingencies, which cannot provide guaranties. While so-called direct methods based on Lyapunov functions potentially provide formal guarantees, they are not really used in practice due to the difficulty of finding Lyapunov functions of larger models. However, we believe that reachability analysis can be conveniently used to ensure correctness, because it can be performed automatically without expert knowledge. To analyze the state of the art in this important application area, we provide a tool that automatically generates benchmark problems from a given system description. We also provide problems of different difficulty and for different types of analysis, namely transient stability analysis, verifying regions of attraction, and verifying robustness against uncertain power demand and production. Exemplary solutions of benchmark problems are shown as well.

1 Introduction

The scientific community has long agreed that the transition to a greener future must be accelerated. One possibility to accelerate this transformation is to make better use of the existing production of renewable energies. Besides better storage capabilities, a further possibility is a less conservative control of power systems—this, however, is often prevented due to conservative proven-in-use approaches. To establish modern control methods, one could convince decision makers by providing formal methods to prove that modern approaches ensure all necessary specifications, such as relevant grid codes. To the best knowledge of the author, we provide the first benchmarks for the formal verification of power systems to assess the state of the art in this area. Since power systems are very diverse, we also provide a tool for creating new benchmarks from standard system descriptions. Unlike existing tools for power systems, we will provide the explicit model described as differential algebraic equations. The lack of such a possibility to further improve formal methods becomes evident in the subsequent review of the state of the art.

1.1 State of the Art

Non-Formal Methods Even today, most power systems are only analyzed via numerical simulations [37,47]. Obviously, numerical simulations do not provide any guarantees for power systems with inherent uncertainties, because they only analyze one possible behavior for an assumed initial state, an assumed future system input, and under the assumption that the underlying models are exact. However, in reality, a) the initial state is often not exactly known since not all state variables can be measured or because measurements are scarce and the state has shifted in the meantime (see, e.g., [36]), b) inputs are uncertain due to various fluctuations, such as solar radiation, wind, and consumer behavior, and c) parameters are uncertain due to, e.g., unmodeled power electronics and aging effects. Even when only considering the smallest and largest values of n state variables at the initial point in time, m inputs, and o parameters, we already require 2^{n+m+o} simulations—and these do not even bound all solutions since power systems have no monotone dynamics in general [9]. Another issue is that it is unclear for how long a simulation has to be run until the system has been analyzed long enough. The aforementioned issues are only mitigated by faster simulation using parallelization [11,14,18, 27,44] and by Monte Carlo simulation [7,50,51] to address uncertain predictions.

Formal Methods - Direct methods Traditionally, the predominantly-researched formal methods for the analysis of power systems are so-called direct methods. Instead of explicitly simulating the behavior for stability analysis, direct methods compute regions in the state space from which the system state returns to the original operating point [17,41]. A major drawback of direct methods is that they require Lyapunov functions, which can only be found for simplified system dynamics [10,17,23,26,41]. The inability of analyzing realistic models unfortunately defeats the purpose of formal methods—if a formally verified model does not resemble the real system, the verification result cannot be transferred to the real system and thus becomes meaningless. Only when the used models are conformant, properties, such as safety, can be transferred to the real system [42]. Another disadvantage of direct methods developed so far for power systems is that they cannot check if phase, voltage, and frequency constraints are met since they only analyze if a steady state of a disturbed system is eventually reached. Especially the verification of bus voltage limits is important since violations can trigger protection devices to disconnect power lines and possibly cause cascading effects leading to a blackout [8].

Formal Methods - Reachability Analysis Reachability analysis can be seen as a set-based simulation of a system containing all states reachable by all of its possible simulation runs. Because all reachable states are included, one can prove various system properties, such as avoiding a set of unsafe states and/or reaching a set of goal states. One can even include temporal logic specifications by computing the product automaton of the system with a monitor automaton for the temporal logic specification, resulting in a verification problem with hybrid (i.e., mixed discrete and continuous) dynamics [4]. Since formal analysis of the nonlinear dynamics of power systems is undecidable [39], one cannot compute exact reachable sets for this system class—thus, one aims to compute as tight as possible over-approximations. Early work for reachability analysis in power systems was only able to analyze small systems [28,29], because the used approach has an exponential complexity with respect to the system dimension. The work in [15,16] has a polynomial complexity with respect to the system dimension; however, the approach requires to linearize the system dynamics so that the results cannot be directly transferred to the real system. Reachable sets of linear power systems with uncertain system matrices are presented in [49]. The first work with polynomial complexity with respect to the system dimension that can handle power systems modeled as differential-algebraic equations

is [3]; this work was later extended to a compositional approach [1]. Reachability analysis for a conformant model of a drum-boiler unit of a power plant has been performed in [21] to certify it for faster changes in power generation. Most other applications of reachability analysis in power systems use non-conformant models, such as the analysis of microgrids [32], the verification of voltage ride-through capabilities [48], the verification of grid frequency controllers [35], fault diagnosis [45], and the joint synthesis and verification of power system controllers [22].

Open-Source Tools for the Analysis of Power Systems Several open-source analysis tools for power systems exist [34, 38], such as MATPOWER [52], PYPOWER [33], and pandapower [46]. However, none of these tools provide the differential algebraic equations required for formally analyzing power systems. To the best knowledge of the author, only a few tools exist that create the differential algebraic equations symbolically, but these files cannot be directly accessed by formal verification tools. The MATLAB tool VST [12] uses symbolic computations, but its last update was more than 20 years ago and it does not run on all current operating systems due to the use of DLL files. A more recent tool using symbolic computations is [19]; however, in its current version, one cannot directly obtain the differential algebraic equations of the overall system.

1.2 Contributions

While there is an increasing effort to formally verify power systems, there exist no benchmarks to accelerate the development in this area. Since power systems are complex, one requires tool support to automatically create models of them. Unlike the simulation of power systems, which is typically performed by solving power system components locally, formal methods usually require a state space model of the entire system. To address these issues, we provide the following contributions:

- We provide the first benchmark suite for the formal verification of power systems.
- For the first time, we convert power system descriptions to models used for formal verification, such as SpaceEx [20]. As a byproduct, we generate files of the state space model consisting of differential and algebraic equations that can be used for further analyses.
- The benchmarks can be composed from given modules, consisting of a case file and a specification file.
- We provide solutions for selected benchmarks using CORA [2].

1.3 Organization

We first recall the essentials of power system dynamics in Sec. 2. This serves mainly two purposes: a) Researchers and practitioners from the formal verification community get a concise introduction into power systems and b) the provided equations will be used to explain the generation of the state space models. In Sec. 3 we show how to create different benchmarks from power system cases and specifications. Solutions of selected benchmark problems are presented in Sec. 4 and we draw conclusions in Sec. 5.

2 Dynamics of Power Systems

Components of power systems, such as generators, loads, feeders, and transformers, are connected to so-called buses, which in turn are connected through power lines. Within a power system, the magnitudes of variables can vary significantly so that many values are normalized by the per unit system [p.u.] instead of using, e.g., the actual voltage. There are different ways to establish a per-unit system [31, Sec. 3.4]; however, the particular normalization is irrelevant for the formal verification of power systems, since also the specification is provided in the corresponding per-unit system. The variables associated with the i^{th} bus are the magnitude of the voltage V_i, the relative phase angle of the voltage Θ_i, active power P_i, and reactive power Q_i. Active power is actually consumed over a complete cycle of the alternating current waveform, while reactive power oscillates between the source and load in each cycle due to stored energy.

Generators are attached to generator buses and control the power as well as the voltage. The remaining buses are referred to as load buses, which may also include power generating elements that cannot control power and voltage, such as, e.g., wind turbines. A bus can be connected to a generator and a load. Because they share the same voltage and the overall power can be obtained by adding the negative load power and the positive generator power, those buses are treated as a generator bus. Since only the relative phase angles of the buses matter, one defines a generator bus as a reference—the so-called slack bus, which by definition has the relative phase angle $\Theta_i = 0$ and the given voltage controlled by the power generating element. By definition, the slack bus rotates with the designed angular velocity of the grid ω_s; e.g., the grid frequency in Europe is 50 Hz. The slack bus balances the slack between the active and reactive power generation and use. For convenience, the known variables of each bus type (the remaining two variables of each bus are unknown) are listed subsequently:

- Slack bus: V_i and $\Theta_i = 0$ are known.
- Generator bus: P_i and V_i are known.
- Load bus: P_i and Q_i are known.

We will use the following symbols to represent the number of different bus types:

- N_g: number of generators buses.
- N_l: number of load buses.
- N_c: number of cut transmission lines to obtain a user-specified subsystem.

The dynamics of power systems mainly originate from two sources: The dynamics of components and the power flow constraints, which will couple the dynamics of each component. In our benchmarks, the only dynamic components we consider are generators. We will first address the generator dynamics followed by the power flow constraints. Finally, we will present how faults in the power system are modeled and how the state space models are obtained.

2.1 Generator Dynamics

We use the generator dynamics from [15]. Please note that the phase angles of generators are denoted by δ to distinguish them from the phase angles of buses denoted by Θ. Generator models consist of the machine and a governor, where the latter is a device regulating the speed of the machine—in many cases by regulating the inflow of steam through a valve. The generator model has the subsequently listed state variables, input, and parameters for the i^{th} generator.

State variables:

- $\delta_i = \tilde{\delta}_i - \Theta_s$ [rad]: generator phase angles relative to the slack bus angle Θ_s (the generator phase angle is denoted by $\tilde{\delta}_i$).
- ω_i [rad/s]: angular velocity.
- $P_{m,i}$ [p.u.]: mechanical power.

Input:

- $P_{c,i}$ [p.u.]: commanded power production.
- $P_{g,i}$ [p.u.]: active power of the generator (see (2)).

Parameters:

- M_i [MJ/Hz^2]: rotational inertia.
- D_i [s/rad]: damping coefficient.
- $T_{SV,i}$ [s]: time constant of the governor.
- $\frac{1}{R_{D,i}}$ [-]: proportional gain of the governor.

The dynamic equations of the chosen generator model originate from a second-order machine model and a first-order governor model. This model is based on [15, eq. 19] and slightly modified by using power instead of torque as one of the state variables:

$$\begin{aligned} \dot{\delta}_i &= \omega_i - \omega_s, \\ \dot{\omega}_i &= -\frac{D_i}{M_i}(\omega_i - \omega_s) + \frac{1}{M_i}P_{m,i} - \frac{1}{M_i}P_{g,i}, \\ \dot{P}_{m,i} &= -\frac{1}{T_{SV,i}R_{D,i}}(\omega_i - \omega_s) - \frac{1}{T_{SV,i}}P_{m,i} + \frac{1}{T_{SV,i}}P_{c,i}. \end{aligned} \tag{1}$$

For simplicity, the same model is used for all generators and synchronous condensers, where the latter are generators that produce no active power. If no parameter values are specified, we use the values from [15] shown in Tab. 1 as default values, where $R_{D,i}$ is adjusted to account for the fact that power instead of torque is used as one of the state variables.

Table 1: Default parameter values of the generators.

$\forall i$:	M_i	D_i	$\lvert Y_{g,i}\rvert$	$\Psi_{g,i}$	$T_{SV,i}$	$R_{D,i}$	ω_s
	$\frac{1}{15\pi}$	0.04	5	$-\frac{\pi}{2}$	1	6π	120π

2.2 Power Flow Constraints

The power flow equations are obtained using standard methods, see e.g. [43, p.174]. The power flow equations have the following algebraic variables, inputs, and parameters for the i^{th} bus.

Algebraic variables:

- V_i [p.u]: absolute value of the bus voltage.
- $\Theta_i = \tilde{\Theta}_i - \Theta_s$ [rad]: bus phase angles relative to the slack bus angle Θ_s (the bus phase angle is denoted by $\tilde{\Theta}_i$).

- P_i [p.u.]: active power.
- Q_i [p.u.]: reactive power.
- E_i [p.u.]: generator voltage (applies only to generator buses).

Inputs:

- $P^d_{g,i}$: directly injected active power (e.g., from renewable energy sources).
- $Q^d_{g,i}$: directly injected reactive power (e.g., from renewable energy sources).

Parameters: The buses are connected via admittances $Y_{ij} = Y_{ji}$, where i and j are the indices of the connected buses. The admittance from the generator to the i^{th} generator bus is denoted by $Y_{g,i}$.

- $|Y_{ij}|$ [p.u.]: absolute value of the admittance.
- $\Psi_{ij} = \angle Y_{ij}$ [rad]: angle of the admittance.
- $|Y_{g,i}|$ [p.u.]: absolute values of the generator admittance.
- $\Psi_{g,i} = \angle Y_{g,i}$ [rad]: angle of the generator admittance.

The active and reactive power of a generator according to [43, eq. 5.10][1] are

$$\begin{aligned} P_{g,i} &= E_i V_i |Y_{g,i}| \cos(-\Psi_{g,i} - \delta_i + \Theta_i) - V_i^2 |Y_{g,i}| \cos(-\Psi_{g,i}), \\ Q_{g,i} &= E_i V_i |Y_{g,i}| \sin(-\Psi_{g,i} - \delta_i + \Theta_i) - V_i^2 |Y_{g,i}| \sin(-\Psi_{g,i}). \end{aligned}$$

Using $\cos(-\alpha) = \cos(\alpha)$ and $\sin(-\alpha) = -\sin(\alpha)$, we obtain

$$\begin{aligned} P_{g,i} &= E_i V_i |Y_{g,i}| \cos(\Psi_{g,i} + \delta_i - \Theta_i) - V_i^2 |Y_{g,i}| \cos(\Psi_{g,i}), \\ Q_{g,i} &= -E_i V_i |Y_{g,i}| \sin(\Psi_{g,i} + \delta_i - \Theta_i) + V_i^2 |Y_{g,i}| \sin(\Psi_{g,i}). \end{aligned} \tag{2}$$

In contrast to some other models, we use the most generalized form of power transfer between any two voltage sources through any connecting admittance. At each bus, the following active powers are added: The active power $P_{g,i}$ of the generators according to (2), the directly injected active power $P^d_{g,i}$, and the demanded active power $P_{d,i}$. Analogously, the reactive powers $Q_{g,i}$, $Q^d_{g,i}$, and $Q_{d,i}$ are added. Obviously, $P_{g,i} = Q_{g,i} = 0$ at load buses. The power flow equations as in [43, p.174] of each bus are

$$\begin{aligned} P_i = P_{g,i} + P^d_{g,i} + P_{d,i} &= \sum_{j=1}^{N_g+N_l} V_i V_j |Y_{ij}| \cos(\Psi_{ij} + \Theta_j - \Theta_i), \\ Q_i = Q_{g,i} + Q^d_{g,i} + Q_{d,i} &= -\sum_{j=1}^{N_g+N_l} V_i V_j |Y_{ij}| \sin(\Psi_{ij} + \Theta_j - \Theta_i). \end{aligned} \tag{3}$$

2.3 Power Dropout

For the transient stability analysis in Sec. 3.1.1, we model the power dropout of the i^{th} power plant by setting the active and reactive power in (3) and (1) to zero ($P_{g,i} = 0$, $Q_{g,i} = 0$). In addition, the variable E_i is no longer an unknown variable and is replaced by V_i during the power dropout, since the power plant can no longer control the voltage at the i^{th} bus. This bus then essentially becomes a load bus during power dropout.

[1] The reference uses impedance instead of admittance, so that the angle of the admittance $Y_{g,i}$ is negated compared to that of the impedance.

2.4 State Space Model

In order to make the power system dynamics amenable to formal verification tools, we rewrite the above power system model to a state space model. After introducing the vector of differential variables as $x \in \mathbb{R}^{n_d}$, the vector of algebraic variables as $y \in \mathbb{R}^{n_a}$, and the input vector as $u \in \mathbb{R}^m$, we obtain the following set of time-invariant, semi-explicit, index-1 differential equations:

$$\begin{aligned} \dot{x} &= f(x(t), y(t), u(t)), \\ 0 &= g(x(t), y(t), u(t)). \end{aligned} \tag{4}$$

Since we also want to provide simplified versions of the considered power systems, we make it possible to only consider a subset of buses behind cut transmission lines. The voltages $\hat{V}_k$ and phase angles $\hat{\Theta}_k$ at the cut transmission lines will become additional inputs. We introduce the function $k = h(i)$ returning the bus number k of the i^{th} cut transmission line ($i = 1 \dots N_c$).

The numbering of the power network buses is renumbered from the original benchmark problems as follows. In all benchmark problems, we declare the first bus ($i = 1$) to be the slack bus. The next buses ($i = 2 \dots N_g$) are the generator buses, which are in turn followed by the load buses ($i = N_g + 1 \dots N_g + N_l$). Due to this renumbering, we can assign the algebraic variables in a more systematic way as follows:

$$\begin{aligned} &i = 1 \dots N_g : && y_i = E_i \quad \text{(generator voltages)}, \\ &i = 1 \dots N_l : && y_{N_g+i} = V_{N_g+i} \quad \text{(voltages of load buses)}, \\ &i = 2 \dots (N_g + N_l) : && y_{N_g+N_l+i-1} = \Theta_i \quad \text{(phases of all buses, except the slack bus)}. \end{aligned} \tag{5}$$

The dynamic variables are

$$\begin{aligned} &i = 1 \dots N_g : && x_i = \delta_i \quad \text{(phase of generator)}, \\ &i = 1 \dots N_g : && x_{N_g+i} = \omega_i \quad \text{(angular velocity of generator)}, \\ &i = 1 \dots N_g : && x_{2N_g+i} = P_{m,i} \quad \text{(mechanical power of generator)}, \end{aligned} \tag{6}$$

and the inputs are assigned as follows:

$$\begin{aligned} &i = 1 \dots N_g : && u_i = P_{c,i} \quad \text{(commanded power)}, \\ &i = 1 \dots (N_g + N_l) : && u_{N_g+i} = P^d_{g,i} \quad \text{(directly injected active power)}, \\ &i = 1 \dots (N_g + N_l) : && u_{2N_g+N_l+i} = Q^d_{g,i} \quad \text{(directly injected reactive power)}, \\ &i = 1 \dots N_c, k = h(i) : && u_{3N_g+2N_l+i} = \hat{V}_k \quad \text{(voltage at cut transmission line)}, \\ &i = 1 \dots N_c, k = h(i) : && u_{3N_g+2N_l+N_c+i} = \hat{\Theta}_k \quad \text{(phase at cut transmission line)}. \end{aligned} \tag{7}$$

By symbolically replacing the variables of the model described in Sec. 2.1-2.3 using (5)-(7), we obtain the state space form in (4). The state-space models are used in the subsequently described benchmark problems.

3 Benchmark Creation

We compose benchmarks using the type of verification problem `type`, the case description `case`, and the specification `spec`. This modularity makes it possible to easily generate a large set of benchmarks from a smaller set of the above-mentioned components `type`, `case`, and `spec`. Furthermore, the modularity facilitates comparing the effects of various cases or specifications

by only changing these components. The benchmark ID is constructed by separating the IDs of each component by colons in the order

`type : case : spec.`

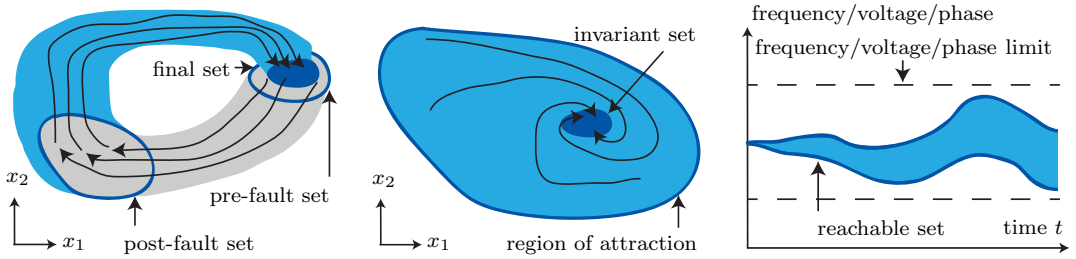
For instance, for `type`=`TSA`, `case`=`IEEE14-1`, `spec`=`MA2014-2`, the benchmark ID is

`TSA : IEEE14-1 : MA2014-2.`

Currently, the IDs of each component are specified within CORA. In the future, we might provide a separate website. In Sec. 3.1, we will introduce the current types of verification problems. The case format and the specification format is provided in Sec. 3.2 and Sec. 3.3, respectively.

3.1 Considered Verification Problems

As of now, we consider the three types of verification problems shown in Fig. 1: Transient stability analysis (TSA), verifying the region of attraction (RoA), and verifying robustness against uncertain power demand and production (Rob). We will specify each problem in more detail subsequently.



(a) Transient stability analysis.

(b) Verifying the region of attraction.

(c) Verifying robustness against uncertain power demand and production.

Figure 1: Supported verification problems.

In order to formally define the considered verification problems, we will require the following definitions. The initial state of a power system as modeled in (4) is consistent when $g(x(0), y(0), u(0)) = 0$. We assume that (4) has a unique solution $\gamma(t, x(0), y(0), u(\cdot))$ for all consistent initial states $x(0)$, $y(0)$ and all piecewise continuous input trajectories $u(\cdot)$, where $u(t)$ refers to their value at a specific point in time t. The set of consistent initial states is denoted by $[x^T(0), y^T(0)]^T \in \mathcal{R}(0)$ and the set of possible input trajectories is $\mathcal{U}(\cdot) = \{u(\cdot) | \forall t : u(t) \in \mathcal{U}(t)\}$, where $\mathcal{U}(t)$ is the set of possible inputs for a given point in time. Please note that depending on the benchmark, some inputs can be controlled, such as a demanded power production, while others are uncontrolled, such as disturbances. The exact reachable set for a time t_i is

$$\mathcal{R}^e(t_i) = \left\{ \gamma(t_i, x(0), y(0), u(\cdot)) \middle| [x^T(0), y^T(0)]^T \in \mathcal{R}(0), u(\cdot) \in \mathcal{U}(\cdot) \right\}.$$

Because one cannot compute the exact reachable set for nonlinear DAE systems [39], one resorts to algorithms solving the proposed benchmarks using some form of over-approximation. An over-approximative reachable set is denoted by $\mathcal{R}(t_i) \supseteq \mathcal{R}^e(t_i)$. For simplification, we will not distinguish between exact and over-approximative reachable sets from now on. The reachable set of a time interval $[t_i, t_{i+1}]$ is denoted by $\mathcal{R}([t_i, t_{i+1}]) = \bigcup_{t \in [t_i, t_{i+1}]} \mathcal{R}(t)$.

3.1.1 Transient Stability Analysis (TSA)

Informally, transient stability of a power system is referred to its capability of reaching an acceptable operating condition in which the generators are synchronized after a contingency. The set of possible contingencies that a system has to be resilient to is typically not formally fixed and is often at the discretion of the responsible engineer or operator; see, e.g., [27].

In our benchmarks, one specifies a power dropout as well as the time when the fault occurs $t_o > 0$ (fault occured) and when it is cleared $t_c > t_o$ (fault cleared). During the fault, the system dynamics is changed as described in Sec. 2.3. In our benchmarks, we use a stricter interpretation of transient stability, where we require that the reachable set returns to the set of initial states after the fault is cleared. To ensure that this is at least possible when no uncertainties are acting on the system, we require that the reachable set at time t_o is a subset of the initial reachable set:

$$\mathcal{R}(0) \supseteq \mathcal{R}(t_o).$$

Under this condition, one can show transient stability for the given contingency if

$$\exists t > t_c : \mathcal{R}(t) \subseteq \mathcal{R}(0).$$

3.1.2 Verifying the Region of Attraction (RoA)

The region of attraction (aka the basin of attraction or the domain of attraction) is a set of states from which the system always reaches a desired operating condition. For instance, if the reachable set is within the region of attraction after a fault is cleared, one can directly show transient stability for the considered fault. While a verified region of attraction simplifies many other verification problems, it is harder to verify since typically a larger set of states has to be considered compared to analyzing a more specific scenario.

Before we formalize the verification of a region of attraction, we first define an invariant set $\mathcal{S}$ [13, Def 2.2.]:

$$\forall t > 0, \forall u(\cdot) \in \mathcal{U}(\cdot), \forall [x^T(0), y^T(0)]^T \in \mathcal{S} : \gamma(t, x(0), y(0), u(\cdot)) \in \mathcal{S}.$$

To distinguish the above invariant set from those without uncertain inputs, one often refers to them as robust positively invariant sets [13, Def 2.2.]. We now define the region of attraction as the set

$$\mathcal{D} = \left\{ [x^T(0), y^T(0)]^T \,\middle|\, \forall u(\cdot) \in \mathcal{U}(\cdot) : \lim_{t \to \infty} \gamma(t, x(0), y(0), u(\cdot)) \in \mathcal{S} \right\}.$$

Most previous works consider the special case where the invariant set is the steady state [30, p. 314]. This, however, excludes relevant aspects, such as uncertain inputs and limit cycles. If, in addition, state and input constraints are always fulfilled before reaching the invariant set, one often calls such a region of attraction a safe set [25]. To verify the region of attraction, we have to show that for $\mathcal{R}(0) = \mathcal{D}$, it holds that

$$\exists t > 0 : \mathcal{R}(t) \subseteq \mathcal{S}.$$

3.1.3 Verifying Robustness against Uncertain Power Demand and Production (Rob)

Another verification problem is to check whether state constraints are met despite uncertain power demand and production. For instance, one would like to check whether the frequency, voltage, and phase limits are met despite uncertain power production from renewable sources. We denote the set of acceptable states as $\mathcal{X}$ so that robustness against uncertain power demand

and production for a user-specified time horizon t_f can be formulated as

$$\mathcal{R}([0, t_f]) \subset \mathcal{X}.$$

In contrast to verifying transient stability and the region of attraction, the considered time horizon is typically longer. Thus, this is a good benchmark to evaluate the amount of over-approximation that accumulates over time.

3.2 Case Format

Each case is a data structure shown in Fig. 2 specifying each component of the power system and how they are related through the bus system. The data structure contains 1) the specification of the buses, 2) parameters of the generators, and 3) system-wide specifications (name, demanded active and reactive power, voltage magnitudes, and the admittance matrix). Input and output buses are those with cut transmission lines. If the bus is within the considered subsystem, it is an output bus and an input bus, otherwise. As an example, let us consider the bottom left subsystem in Fig. 4: Input buses are 5, 6, 14, 15, 16 and output buses are 2, 4, 12.

- /
  - `bus` (specification of the buses)
    - `fault` $\in \mathbb{N}^{N_g}$ (vector of bus number with fault)
    - `generator` $\in \mathbb{N}^{N_g}$ (vector of bus numbers with generators)
    - `input` $\in \mathbb{N}^{N_g+N_l}$ (vector of bus numbers with cut transmission lines outside the system)
    - `load` $\in \mathbb{N}^{N_l}$ (vector of bus numbers with loads)
    - `output` $\in \mathbb{N}^{N_g+N_l}$ (vector of bus numbers with cut transmission lines inside the system)
    - `slack` $\in \mathbb{N}$ (bus number of the slack bus)
  - `genParam` (specification of the generator parameters)
    - `omega_s` $\in \mathbb{R}$ (angular velocity of the grid)
    - `D` $\in \mathbb{R}^{N_g}$ (vector of damping coefficients for each generator in bus.generator)
    - `M` $\in \mathbb{R}^{N_g}$ (vector of rotational inertias for each generator in bus.generator)
    - `Psi_g` $\in \mathbb{R}^{N_g}$ (vector of generator admittance angles for each generator in bus.generator)
    - `R_d` $\in \mathbb{R}^{N_g}$ (vector of inverse gains of the governor for each generator in bus.generator)
    - `T_sv` $\in \mathbb{R}^{N_g}$ (vector of time constants for each generator in bus.generator)
    - `Y_g` $\in \mathbb{R}^{N_g}$ (vector of absolute generator admittances for each generator in bus.generator)
  - `name` (name of the case)
  - `Pd` $\in \mathbb{R}^{N_g+N_l}$ (vector of demanded active power for each bus)
  - `Qd` $\in \mathbb{R}^{N_g+N_l}$ (vector of demanded reactive power for each bus)
  - `VM` $\in \mathbb{R}^{N_g+N_l}$ (vector of voltage magnitudes for each bus)
  - `Y` $\in \mathbb{C}^{N_g+N_l \times N_g+N_l}$ (admittance matrix)

Figure 2: Data structure of a case.

3.3 Specification Format

The data structure for each specification is shown in Fig. 3. All types of verification problems require the set of initial dynamic states $\mathcal{R}(0)$ and the set of inputs $\mathcal{U}$. In case the set of inputs varies over time, one has to specify its change over time. Further values required for different verification problems are listed in Fig. 3.

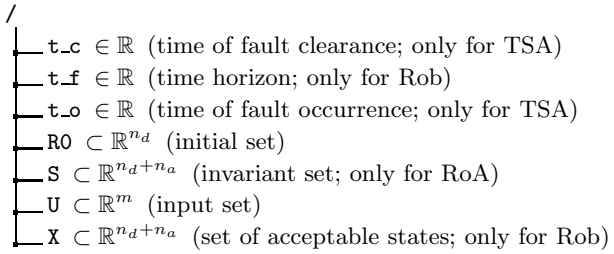


Figure 3: Data structure of a specification.

4 Numerical Experiments

At this point, we already provide 35 cases and 51 specifications, which can be combined to various benchmarks. Obviously, cases and benchmarks cannot be combined arbitrarily, but for different parameterizations of generators, one could reuse the same specification and for the same case, specifications of varying difficulty can be combined. As an example, we will show results of one benchmark for each verification type. All computations have been performed on an Intel Core i7-8565U CPU with 1.80 GHz and 24 GB of memory.

4.1 Automatic Creation of Case Descriptions

In order to conveniently create new benchmarks, case descriptions in well-established formats can be loaded. So far, we provide the conversion of the PSS/E RAW format [40] and the MATPOWER format [52] into our data structure shown in Fig. 2. The data structures are created in CORA [2] by calling

```
loadPowerSystemCase(casefilename, filename, 'MATPOWER')
loadPowerSystemCase(casefilename, filename, 'PSSE'),
```

where `casefilename` is the filename of the case to be loaded and `filename` is the filename of the generated case. Please note that the conversions can only be obtained when MATPOWER [52] is installed. Unspecified parameters from other formats are handled by providing default values. For instance, the default values for generator parameters are listed in Tab. 1.

4.2 Automatic Creation of Models

The case specifications according to Fig. 2 cannot be directly used by any current formal verification tool. Most tools require state space models so that we provide a method to automatically create the time-invariant, semi-explicit, index-1 differential equation system in (4) by calling

```
powerSystem2cora(filename)
```

in CORA. All equations are automatically generated by symbolic computations to exclude errors that could be caused by manual implementations. Abstractions to linear ordinary differential equations and linear differential equations can be performed using the methods provided in CORA. The mathematical background of these abstractions is provided in [5]. The obtained models can be exported using the SpaceEx format through

```
cora2spaceex(obj,filename),
```

where `obj` is the CORA object to be converted and `filename` specifies the name of the SpaceEx model. The SpaceEx format is predominantly used by other formal verification tools and in the ARCH competition [6,24]—the largest competition for the formal verification of continuous and hybrid systems.

4.3 Transient Stability Analysis

Verifying transient stability is demonstrated for the benchmark `TSA:IEEE30-1:MA2014-30-1`. As the case ID suggests, it is the IEEE 30-bus benchmark shown in Fig. 4, where each generator is parameterized by the values listed in Tab. 1. Bus 1 is declared as the bus where the power dropout will occur. Next, let us introduce $\mathbf{0}$ as a vector of zeros of appropriate size and $[-1,1]^p$ as the p-ary Cartesian product of intervals [-1,1], i.e., a p-dimensional unit box. The values of the specification are as follows:

- $\texttt{t\_c} = 0.13$ s
- $\texttt{t\_o} = 0.1$ s
- $\texttt{R0} = x_0 + \left[0.005[-1,1]^6 \times 0.1[-1,1]^6 \times 0.001[-1,1]^6\right], \quad x_0 = [0.6199,\ 0.0087,\ -0.1236,\ -0.1756,\ -0.2219,\ -0.2512,\ 120\pi,\ 120\pi,\ 120\pi,\ 120\pi,\ 120\pi,\ 120\pi,\ 2.6,\ 0.4,\ 0,\ 0,\ 0,\ 0]$.
- $\texttt{U} = \mathbf{0}$

The reachable sets of this problem are computed by abstracting the system dynamics to linear differential inclusions on-the-fly. Because the computation of the abstraction error consumes most of the time and the main coupling of the dynamics is already considered by the linear abstraction, the abstraction error is computed compositionally as presented in [1]. The regions for the compositional computation of the abstraction error are shown in Fig. 4.

The transient stability of this benchmark could be verified in 405 s using the machine specified above. Selected projections of the reachable set are shown in Fig. 5.

4.4 Verifying the Region of Attraction

One of the standard examples in the literature for verifying the region of attraction of power systems is the single-machine-infinite-bus (SMIB) system. The identifier of this benchmark is `RoA:SMIB-1:MA2022-1-1`. In contrast to the demonstration of larger benchmarks, the dynamics follows directly from neglecting the torque dynamics in (1) and inserting $\Theta_i = 0$ as well as $\Psi_{g,i} = -\pi/2$ in (2):

$$\begin{aligned}\dot{x}_1 &= x_2,\\ \dot{x}_2 &= \frac{1}{M}(P_m - E\,V\,|Y_g|\sin(x_1) - Dx_2).\end{aligned}$$

The parameter values are taken from Tab. 1 and the differential and algebraic variables that became constants due to the above simplifications are chosen as $P_m = E = V = 1$ [p.u.]. Thus, the equilibrium point becomes $x_0 = [\arcsin(1/|Y_g|), 0]^T$. Using the CORA notation for an ellipsoid, the values of the specification are as follows:

- $\texttt{R0} = x_0 + 0.7[-1,1]^2, \quad x_0 = [\arcsin(1/|Y_g|), 0]^T$.
- $\texttt{S} = \texttt{ellipsoid}(Q, x_0), \quad Q = \begin{bmatrix} 0.0201 & -0.0249 \\ -0.0249 & 4.9999 \end{bmatrix}$.
- $\texttt{U} = \mathbf{0}$.

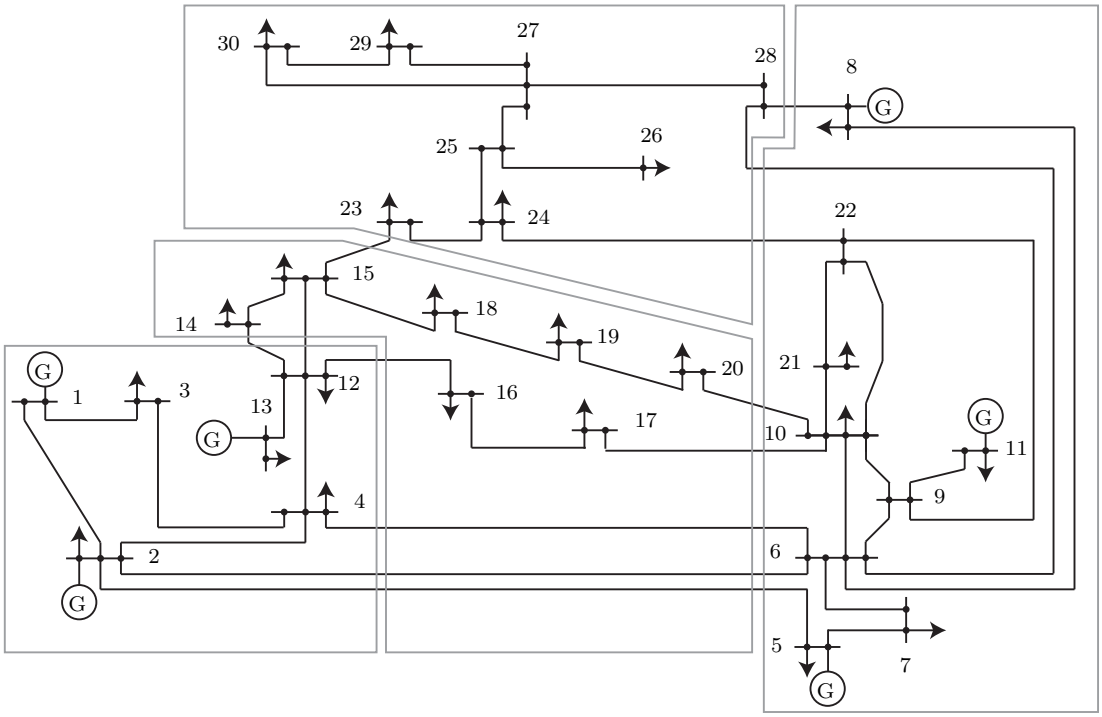


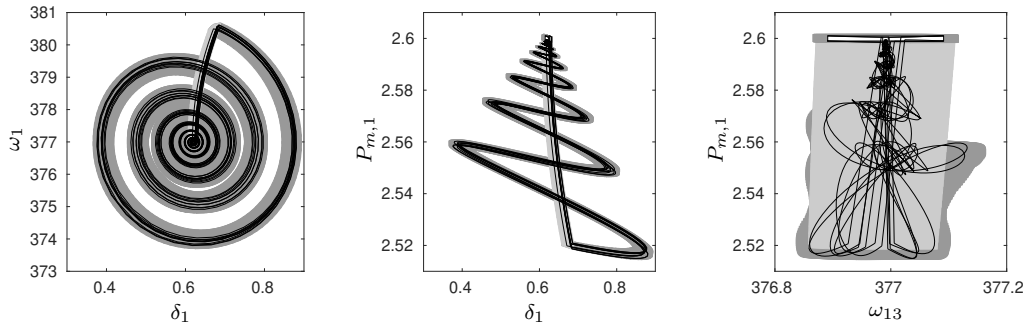
Figure 4: IEEE 30-bus benchmark system. Gray lines show subsystem borders and a circle around the letter G indicates a generator.

By using CORA, the provided region of attraction can be verified within 6.9 s. The reachable set as well as the initial set and the invariant set are shown in Fig. 6.

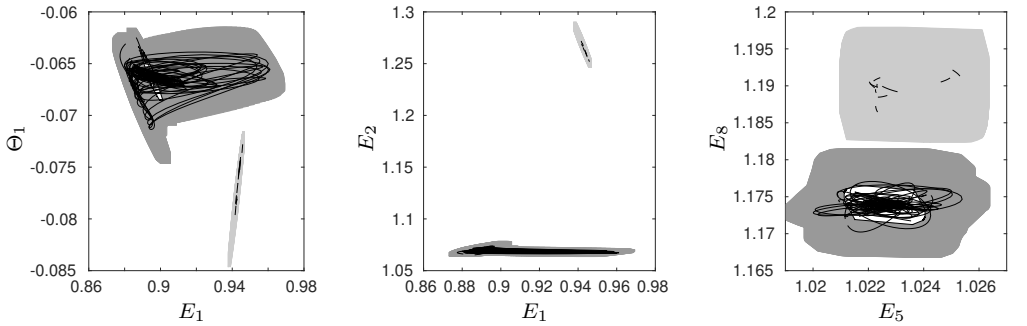
4.5 Verifying Robustness against Uncertain Power Demand and Production

As an example for verifying the robustness against uncertain power demand and production, we show results of the benchmark `Rob:IEEE14-2:MA2014-14-2`. As the case name suggests, we use the IEEE 14-bus benchmark depicted in Fig. 7. Renewable energy production is modeled by directly injecting active power at bus 13 and 14 (see [15]), where $\forall t \in [0,5]$ s : $P^d_{g,13}(t), P^d_{g,14}(t) \in \{\frac{t}{5}P^* | P^* \in [0.04, 0.06]$ [p.u.]$\}$ modeling that the production uncertainty grows linearly over time. The conventional power plants produce only active power at bus 1 and 2: $P_{c,1} = 2$ [p.u.] and $P_{c,2} = 0.4$ [p.u.]. The verification problem is specified as follows:

- `t_f` $= 5$ s
- `R0` $= x_0 + \left[0.005[-1,1]^5 \times 0.1[-1,1]^5 \times 0.001[-1,1]^5\right]$, $x_0 = [0.3333, -0.0192, -0.2221, -0.2482, -0.2332, 120\pi, 120\pi, 120\pi, 120\pi, 120\pi, 2.0, 0.4, 0, 0, 0]$.
- `U` is chosen according to (7) with $P^d_{g,13}(t), P^d_{g,14}(t) \in \frac{t}{5}P^*$, where $P^* \in [0.04, 0.06]$ [p.u.].
- `X` $= x_0 + \left[\pi[-1,1]^5 \times 0.5\pi[-1,1]^5 \times 0.03[-1,1]^5\right]$.



(a) Projections on differential variables of the 30-bus system.



(b) Projections on algebraic variables of the 30-bus system.

Figure 5: Selected projections of reachable sets for transient stability analysis. Black lines show random simulations, gray areas show reachable sets, and white boxes show initial sets. Dark gray represents pre-fault and post-fault sets, while light gray represents fault-on sets. Algebraic variables jump when switching to and from the faulty operation.

We could verify the specification in CORA using reachability analysis within 207 s. As for the 30-bus benchmark, we computed the abstraction errors compositionally using the two subsystems as indicated in Fig. 7. Selections on reachable sets over time for the time interval $[0, 5]$ s are presented in Fig. 8 together with random simulations for which a constant input is changed every 0.2 s, causing jumps of algebraic variables.

5 Conclusions

We presented the first benchmark suite for the formal verification of power systems. Because power systems have complicated dynamics, whose manual derivation is error-prone, we also provide a method to automatically generate the dynamics in the form of time-invariant, semi-explicit, index-1 differential equations. Our conversion supports the widely used formats PSS/E RAW and MATPOWER. Further details can be found in the CORA manual. This benchmark suite will hopefully facilitate research in the area of formal methods for power systems—an area, where formal methods can contribute to combating climate change.

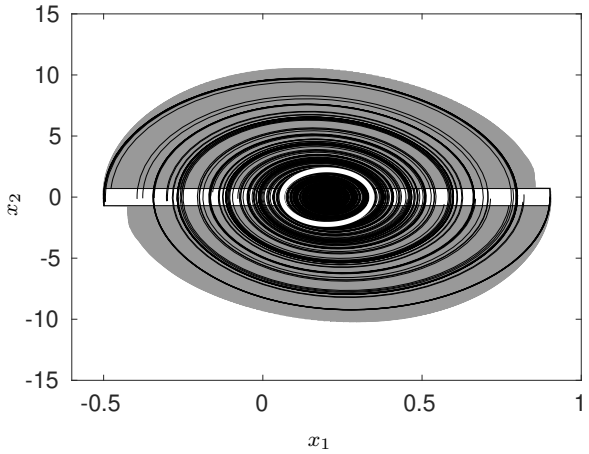


Figure 6: Verified region of attraction of the single-machine-infinite-bus (SMIB) system. The white box shows the initial set $\mathcal{R}(0)$ and the white ellipsoid the invariant set $\mathcal{S}$.

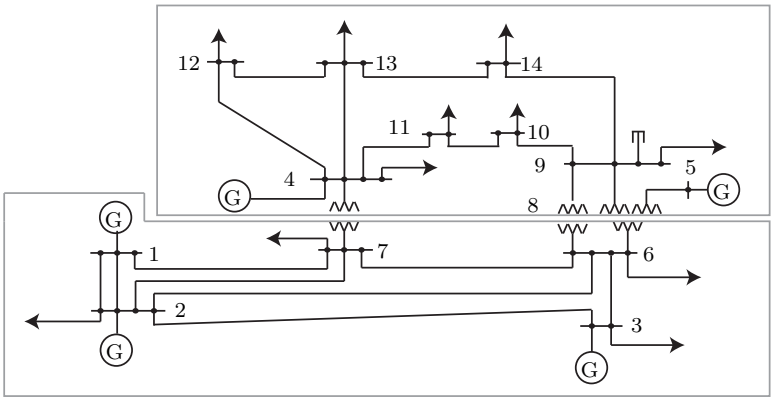


Figure 7: IEEE 14-bus benchmark system. Gray lines show subsystem borders.

Acknowledgment

The author gratefully acknowledges financial support by the European Commission project justITSELF under grant number 817629 and the Bavarian Research Foundation project STROM under grant number AZ-1473-20.

References

[1] M. Althoff. Formal and compositional analysis of power systems using reachable sets. *IEEE Transactions on Power Systems*, 29(5):2270–2280, 2014.

[2] M. Althoff. An introduction to CORA 2015. In *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*, page 120–151, 2015.

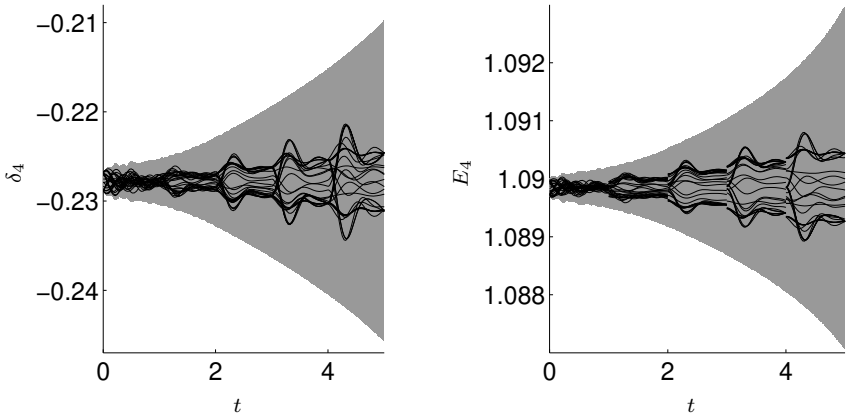


Figure 8: Selected variable bounds over time due to variations in renewable energy production. Black lines show random simulations, the gray area shows the reachable sets.

[3] M. Althoff, M. Cvetković, and M. Ilić. Transient stability analysis by reachable set computation. In *Proc. of the IEEE PES Conference on Innovative Smart Grid Technologies Europe*, page 1–8, 2012.

[4] M. Althoff, G. Frehse, and A. Girard. Set propagation techniques for reachability analysis. *Annual Review of Control, Robotics, and Autonomous Systems*, 4(1):369–395, 2021.

[5] M. Althoff and B. H. Krogh. Reachability analysis of nonlinear differential-algebraic systems. *IEEE Transactions on Automatic Control*, 59(2):371–383, 2014.

[6] M. Althoff, E. Ábrahám, M. Forets, G. Frehse, D. Freire, C. Schilling, S. Schupp, and M. Wetzlinger. ARCH-COMP21 category report: Continuous and hybrid systems with linear continuous dynamics. In *Proc. of the 8th International Workshop on Applied Verification of Continuous and Hybrid Systems*, volume 80, page 1–31, 2021.

[7] P. M. Anderson and A. Bose. A probabilistic approach to power system stability analysis. *IEEE Transactions on Power Apparatus and Systems*, 102(8):2430–2439, 1983.

[8] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20(4):1922–1928, 2005.

[9] D. Angeli and E. D. Sontag. Monotone control systems. *IEEE Transactions on Automatic Control*, 48(10):1684–1698, 2003.

[10] M. Anghel, F. Milano, and A. Papachristodoulou. Algorithmic construction of Lyapunov functions for power system stability analysis. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 60(9):2533–2546, 2013.

[11] P. Aristidou, D. Fabozzi, and T. Van Cutsem. Dynamic simulation of large-scale power systems using a parallel Schur-complement-based decomposition method. *IEEE Transactions on Parallel and Distributed Systems*, 25(10):2561–2570, 2014.

[12] S. Ayasun, C. O. Nwankpa, and H. G. Kwatny. Voltage stability toolbox for power system education and research. *IEEE Transactions on Education*, 49(4):432–442, 2006.

[13] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[14] J. S. Chai and A. Bose. Bottlenecks in parallel algorithms for power system stability analysis. *IEEE Transactions on Power Systems*, 8(1):9–15, 1993.

[15] Y. C. Chen and A. D. Domínguez-García. Assessing the impact of wind variability on power system small-signal reachability. In *Proc. of the International Conference on System Sciences*, page 1–8, 2011.

[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*, 27(4):1978–1989, 2012.

[17] H.-D. Chiang, C.-C. Chu, and G. Cauley. Direct stability analysis of electric power systems using energy functions: Theory, applications, and perspective. *Proceedings of the IEEE*, 83(11):1497–1529, 1995.

[18] M. L. Crow and M. Ilić. The parallel implementation of the waveform relaxation method for transient stability simulations. *IEEE Transactions on Power Systems*, 5(3):922–932, 1990.

[19] Hantao Cui, Fangxing Li, and Kevin Tomsovic. Hybrid symbolic-numeric framework for power system modeling and analysis. *IEEE Transactions on Power Systems*, 36(2):1373–1384, 2021.

[20] A. Donzé and G. Frehse. Modular, hierarchical models of control systems in SpaceEx. In *Proc. of the European Control Conference*, page 4244–4251, 2013.

[21] A. El-Guindy, D. Han, and M. Althoff. Formal analysis of drum-boiler units to maximize the load-following capabilities of power plants. *IEEE Transactions on Power Systems*, 31(6):4691–4702, 2016.

[22] A. El-Guindy, K. Schaab, B. Schürmann, D. Han, O. Stursberg, and M. Althoff. Formal LPV control for transient stability of power systems. In *Proc. of the IEEE PES General Meeting*, 2017.

[23] U. Gabrijel and R. Mihalic. Direct methods for transient stability assessment in power systems comprising controllable series devices. *IEEE Transactions on Power Systems*, 17(4):1116–1122, 2002.

[24] L. Geretti, J. A. dit Sandretto, M. Althoff, L. Benet, A. Chapoutot, P. Collins, P. S. Duggirala, M. Forets, E. Kim, U. Linares, D. P. Sanders, C. Schilling, and M. Wetzlinger. ARCH-COMP21 category report: Continuous and hybrid systems with nonlinear dynamics. In *Proc. of the 8th International Workshop on Applied Verification of Continuous and Hybrid Systems*, volume 80, page 32–54, 2021.

[25] F. Gruber and M. Althoff. Computing safe sets of linear sampled-data systems. *IEEE Control Systems Letters*, 5(2):385–390, 2021.

[26] I. A. Hiskens and D. J. Hill. Energy functions, transient stability and voltage behavior in power systems with nonlinear loads. *IEEE Transactions on Power Systems*, 4(4):1525–1533, 1989.

[27] V. Jalili-Marandi, Z. Zhou, and V. Dinavahi. Large-scale transient stability simulation of electrical power systems on parallel GPUs. *IEEE Transactions on Parallel and Distributed Systems*, 23(7):1255–1266, 2012.

[28] L. Jin, R. Kumar, and N. Elia. Reachability analysis based transient stability design in power systems. *Electrical Power and Energy Systems*, 32:782–787, 2010.

[29] L. Jin, H. Liu, R. Kumar, J. D. McCalley, N. Elia, and V. Ajjarapu. Power system transient stability design using reachability based stability-region computation. In *Proc. of the 37th Annual North American Power Symposium*, page 338–343, 2005.

[30] H. K. Khalil. *Nonlinear Systems*. Pearson, 3rd edition edition, 2014.

[31] P. Kundur. *Power System Stability and Control*. McGraw-Hill, 1994.

[32] Y. Li, P. Zhang, and M. Althoff. Distributed formal analysis for power networks with deep integration of distributed energy resources. *IEEE Transactions on Power Systems*, 34(6):5147–5156, 2018.

[33] R. W. Lincoln. *Learning to trade power*. PhD thesis, University of Strathclyde, Glasgow, U.K., 2011.

[34] F. Milano and L. Vanfretti. State of the art and future of OSS for power systems. page 1–7, 2009.

[35] A. Mohapatra, V. S. Perić, and T. Hamacher. Formal verification of grid frequency controllers. In *Proc. of IEEE PES Innovative Smart Grid Technologies Europe*, page 1–6, 2021.

[36] A. Monticelli. Electric power system state estimation. *Proceedings of the IEEE*, 88(2):262–282, 2000.

[37] M. D. Omar Faruque, T. Strasser, G. Lauss, V. Jalili-Marandi, P. Forsyth, C. Dufour, V. Dinavahi, A. Monti, P. Kotsampopoulos, J. A. Martinez, K. Strunz, M. Saeedifard, X. Wang, D. Shearer, and M. Paolone. Real-time simulation technologies for power systems design, testing, and analysis. *IEEE Power and Energy Technology Systems Journal*, 2(2):63–73, 2015.

[38] S. Pfenninger, L. Hirth, I. Schlecht, E. Schmid, F. Wiese, T. Brown, C. Davis, M. Gidden, H. Heinrichs, C. Heuberger, S. Hilpert, U. Krien, C. Matke, A. Nebel, R. Morrison, B. Müller, G. Pleßmann, M. Reeg, J. C. Richstein, A. Shivakumar, I. Staffell, T. Tröndle, and C. Wingenbach. Opening the black box of energy modelling: Strategies and lessons learned. *Energy Strategy Reviews*, 19:63–71, 2018.

[39] A. Platzer and E. M. Clarke. The image computation problem in hybrid systems model checking. In *Hybrid Systems: Computation and Control*, LNCS 4416, page 473–486. Springer, 2007.

[40] H. Ravindra, M. O. Faruque, M. Steurer, M. Andrus, and Md K. H. Pulok. Conversion of PSS®E models into RSCAD models: Lessons learned. In *Proc. of the 40th Annual Conference of the IEEE Industrial Electronics Society*, page 3743–3749, 2014.

[41] M. Ribbens-Pavella and F. J. Evans. Direct methods for studying dynamics of large-scale electric power systems – a survey. *Automatica*, 21(1):1–21, 1985.

[42] H. Roehm, J. Oehlerking, M. Woehrle, and M. Althoff. Model conformance for cyber-physical systems: A survey. *ACM Transactions on Cyber-Physical Systems*, 3(3):Article 30, 2019.

[43] P. Schavemaker and L. van der Sluis. *Electrical Power System Essentials*. Wiley, 2008.

[44] J. Shu, W. Xue, and W. Zheng. A parallel transient stability simulation for power systems. *IEEE Transactions on Power Systems*, 20(4):1709–1717, 2005.

[45] J. Su and W. Chen. Model-based fault diagnosis system verification using reachability analysis. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(4):742–751, 2019.

[46] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun. Pandapower—an open-source python tool for convenient modeling, analysis, and optimization of electric power systems. *IEEE Transactions on Power Systems*, 33(6):6510–6521, 2018.

[47] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang. Risk assessment of cascading outages: Methodologies and challenges. *IEEE Transactions on Power Systems*, 27(2):631–641, 2012.

[48] H. N. Villegas Pico and D. C. Aliprantis. Voltage ride-through capability verification of wind turbines with fully-rated converters using reachability analysis. *IEEE Transactions on Energy Conversion*, 29(2):392–405, 2014.

[49] H. N. Villegas 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.

[50] W. Wangdee and R. Billinton. Bulk electric system well-being analysis using sequential Monte Carlo simulation. *IEEE Transactions on Power Systems*, 21(1):188–193, 2006.

[51] X. Yu and C. Singh. A practical approach for integrated power system vulnerability analysis with protection failures. *IEEE Transactions on Power Systems*, 19(4):1811–1820, 2004.

[52] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on Power Systems*, 26(1):12–19, 2011.