Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Optimizing Safety Supervisors for Wind Turbines using Barrier Certificates

M. Laurijsse * **R. Wisniewski** ** **S. Weiland** ***

* *Department of Electrical Engineering, Eindhoven University of Technology, Eindhoven, The Netherlands (e-mail: h.d.j.laurijsse@student.tue.nl).*
** *Section for Automation & Control, Aalborg University, 9220 Aalborg East, Denmark (e-mail: raf@es.aau.dk)*
*** *Control Systems Group, Eindhoven University of Technology, Eindhoven, The Netherlands (e-mail: s.weiland@tue.nl)*

Abstract: To avoid structural damage, a wind turbine is equipped with a safety supervisor that triggers an emergency shutdown procedure in case of internal faults or large wind gusts. This paper leverages the (compositional) barrier certificate framework for the design and optimization of such a supervisor. The problem is formulated as a sum of squares problem and is solved using semi-definite programming. Both a direct and compositional approach are successfully implemented and verified for the NREL 5MW reference turbine. In conclusion, the methods derived in this paper are indeed viable for the syntheses and optimization of safety systems for future wind turbines.

Keywords: Safety analysis, fault detection, barrier certificates, compositional, safety supervisor, wind turbines, sum of squares

1. INTRODUCTION

As fossil fuels are becoming increasingly scarce, sustainable energy sources grow in popularity, including wind energy conversion systems. In recent years, a lot of research effort has gone into reducing the costs of wind turbine energy. A trend is observed towards larger mechanical structures and more complex control systems for turbines.

To avoid damage to the wind turbine's mechanical and electrical components, the physical limits of the turbine should never be exceeded. When safety critical situations occur, due to internal faults such as malfunctioning hardware or due to external influences such as wind gusts, a safety supervisor system should trigger an emergency shutdown procedure for the wind turbine.

A commonly used method in industry is to monitor the rotational speed and shut down the turbine if some predefined threshold is exceeded. However, it is found in Johnson and Fleming [2011] that some structural elements are difficult (if not impossible) to protect using this type of supervisor, especially for larger and more complex structures. Furthermore, if such an univariate supervisor is used, it is often conservative yielding undesired shutdowns and economic losses.

As an alternative, this work will focus on the design of a safety system that uses measurements of multiple state variables. To this extend the barrier certificate framework is utilized, see Prajna and Jadbabaie [2004]. It is extended to allow for a reduction of the number of undesired shutdowns whilst maintaining its properties of guaranteeing that physical limits will never be violated. This leads to a reduction in the economic losses that may be caused by mechanical breakdown as well as unnecessary losses of production due to false shutdowns.

This work is a continuation and extension of the results presented in Wisniewski et al. [2013]. New optimization techniques are proposed and the computational complexity is reduced. Specifically, barrier certificates for different wind spans are computed independently and then combined to cover the full operating conditions. This approach significantly reduces the computational complexity allowing for direct optimization approaches and/or more complex and accurate models, resulting in less conservative safety supervisors.

The outline of this paper is as follows. First, some mathematical notations will be presented. Then the problem is formally addressed in Section 3. In Section 4, a mathematical framework for computing safety supervisors is derived. Two approaches are implemented and their results are given in Section 5. Finally, after discussing some improvements in Section 6, the conclusions are presented in Section 7.

2. NOMENCLATURE

The following notations are used throughout this paper. Vectors are displayed in lowercase bold, e.g., $\mathbf{a}$, matrices in uppercase bold, e.g., $\mathbf{A}$. A positive-semidefinite matrix $\mathbf{A}$ is denoted as $\mathbf{A} \succeq 0$, positive-definite matrices as $\mathbf{A} \succ 0$. The trace of a square matrix $\mathbf{A}$ is given by $\mathrm{Tr}\,\mathbf{A}$, a vector of the elements on its diagonal is given by $\mathrm{diag}\,\mathbf{A}$. The symbol $\dot{a}$ denotes the (partial) time derivative $\frac{da}{dt}$ or $\frac{\partial a}{\partial t}$, depending on the context. For a scalar function $f : \mathbb{R}^n \to \mathbb{R}$ the gradient is given as $\boldsymbol{\nabla} f(\mathbf{x}) = \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)$.

Sets are presented in calligraphic font, e.g., $\mathcal{A}$. The set of non-negative reals is denoted as $\mathbb{R}_{0+}$, positive reals as $\mathbb{R}_{+}$. The notation $\{a_i\}_{\mathcal{I}}$ is short hand for $\{a_i | i \in \mathcal{I}\}$. For a subset $\mathcal{B} \subseteq \mathcal{A}$, define $\mathcal{B}^{\mathrm{c}} = \mathcal{A} \backslash \mathcal{B} = \{a \in \mathcal{A} | a \notin \mathcal{B}\}$. Let $\prod$ denote the Cartesian product operator, e.g., $\prod_{i \in \{1,\ldots,k\}} \mathcal{A}_i = \mathcal{A}_1 \times \ldots \times \mathcal{A}_k$.

For a function $g : \mathcal{X} \to \mathbb{R}$, we denote by $\langle g \rangle_a$ the sublevel set

$$\langle g \rangle_a = \{\mathbf{x} \in \mathcal{X} | g(\mathbf{x}) \leq a\} \tag{1}$$

For convenience, let $\langle g \rangle$ denote $\langle g \rangle_0$. Furthermore, the volume of $\langle g \rangle_a$ is given by

$$\operatorname{vol} \langle g \rangle_a = \int_{\langle g \rangle_a} d\mathbf{x} \tag{2}$$

The set of all real-valued polynomials in n real indeterminates is denoted by $\mathcal{P}_n$. $\mathcal{P}_n^k$ denotes the set of all k-sized vectors of such polynomials. A polynomial $p \in \mathcal{P}_n$ is sum of squares (SOS) if there exist $p_1, \ldots, p_k \in \mathcal{P}_n$ such that $p = \sum_{i=1}^{k} p_i^2$. The set of sum of squares polynomials in n indeterminates is denoted by Σ_n.

The degree of a polynomial, denoted $\deg(p)$, is equal to the highest degree of its monomials. The degree of a monomial is equal to the sum of the exponents of its indeterminates. The set of all polynomials in n indeterminates with a degree of at most d is $\mathcal{P}_{n,d} = \{p \in \mathcal{P}_n | \deg(p) \leq d\}$. Similarly $\Sigma_{n,d} = \{s \in \Sigma_n | \deg(s) \leq d\}$.

3. PROBLEM FORMULATION

The task of the safety supervisor system is to timely initiate an emergency shutdown procedure when safety critical situations occur. It is important to note that since the emergency shutdown procedure itself poses stress on the wind turbine, its behavior should be anticipated in the design of a safety supervisor. It will be inadequate to simply check for absolute limits being violated.

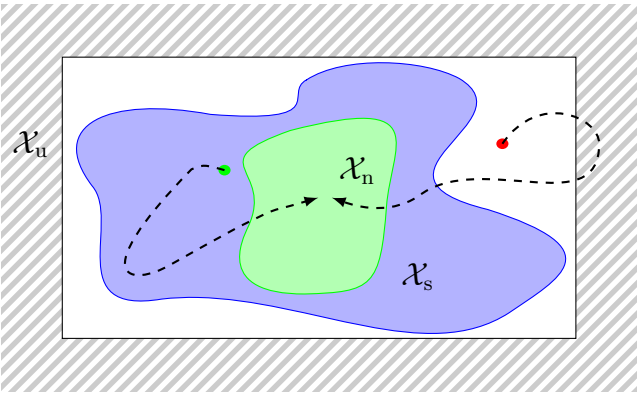

Fig. 1. Shutdown trajectories, with safe (green) and unsafe (red) start point. Unsafe region $\mathcal{X}_{\mathrm{u}}$ (striped), normal operation $\mathcal{X}_{\mathrm{n}}$ (green) and safe set $\mathcal{X}_{\mathrm{s}}$ (purple).

Throughout this paper we will use the following sets: $\mathcal{X}_{\mathrm{u}}$ contains the unsafe states where physical limits are violated, $\mathcal{X}_{\mathrm{n}}$ represents the normal modes of operation and $\mathcal{X}_{\mathrm{s}}$ represents the safe modes of operation of the wind turbine. Shutdown trajectories starting in $\mathcal{X}_{\mathrm{s}}$ will never enter $\mathcal{X}_u$. These sets are illustrated in Figure 1.

As finding the set $\mathcal{X}_{\mathrm{s}}$ might not be tangible, we instead try to find a subset of $\mathcal{X}_{\mathrm{s}}$. More specifically, we try to find a function S such that $\langle S \rangle \subseteq \mathcal{X}_{\mathrm{s}}$. We will refer to $\langle S \rangle$ as the safety envelope and call S the protection function.

Once a protection function S is found, it is straightforward to implement a safety supervisor system. An emergency shutdown procedure should be triggered when S crosses 0. The design of a safety supervisor system hence boils down to finding an appropriate function S. To avoid unnecessary emergency shutdowns, we preferably have that $\operatorname{vol} \langle S \rangle$ is as large as possible. Moreover, a minimal requirement is that the turbine does not shut down during normal mode of operation, i.e., $\mathcal{X}_{\mathrm{n}} \subseteq \langle S \rangle \subseteq \mathcal{X}_{\mathrm{s}}$.

The remainder of this section is dedicated to formalizing the notions outlined above.

In an abstract way, the wind turbine during shutdown is described by $\Gamma = (\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_{\mathrm{n}}, \mathcal{X}_{\mathrm{u}})$. Where $f : \mathbb{R}^{n+m} \to \mathbb{R}^n$ is a well-defined state evolution map that is associated with differential equation

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{d}), \tag{3}$$

$\mathbf{x}(t) \in \mathcal{X} \subseteq \mathbb{R}^n$ the state, and $\mathbf{d}(t) \in \mathcal{D} \subseteq \mathbb{R}^m$ the disturbance input. $\mathcal{X}_{\mathrm{n}} \subseteq \mathcal{X}$ and $\mathcal{X}_{\mathrm{u}} \subseteq \mathcal{X}$ are as described above.

For some Lebesgue measurable and essentially bounded disturbance function $\bar{d} : \mathbb{R}_{0+} \to \mathcal{D}$, the solution of the differential equation (3) with $\phi(0) = x_0$ is denoted by $\phi_{x_0}^{\bar{d}}$, i.e.,

$$\frac{d\phi_{x_0}^{\bar{d}}(t)}{dt} = \mathbf{f}\left(\phi_{x_0}^{\bar{d}}(t), \bar{d}(t)\right) \tag{4}$$

Definition 1. (Safety). Let $\Gamma = (\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_{\mathrm{n}}, \mathcal{X}_{\mathrm{u}})$ be given. Then the set of safe initial states $\mathcal{X}_{\mathrm{s}} \subseteq \mathcal{X}$ is defined by

$$\mathcal{X}_{\mathrm{s}} = \{\mathbf{x} \in \mathcal{X} | \phi_{\mathbf{x}}^{\bar{d}}(t) \in \mathcal{X}_{\mathrm{u}}^{\mathrm{c}},\ \forall t \in \mathbb{R}_{0+},\ \forall \bar{d} \in \mathcal{L}_{\infty}(\mathbb{R}_{0+}, \mathcal{D})\} \tag{5}$$

System Γ is safe if $\mathcal{X}_{\mathrm{n}} \subseteq \mathcal{X}_{\mathrm{s}}$.

Definition 2. ((Exact) Safety Envelope). If there exists a scalar function $S : \mathbb{R}^n \to \mathbb{R}$ such that

$$\mathcal{X}_{\mathrm{n}} \subseteq \langle S \rangle \subseteq \mathcal{X}_{\mathrm{s}} \tag{6}$$

then S is a protection function with corresponding safety envelope $\langle S \rangle$. $\langle S \rangle$ is an exact safety envelope if it holds that

$$\langle S \rangle = \mathcal{X}_{\mathrm{s}}. \tag{7}$$

4. METHODOLOGY

4.1 Barrier Certificates

The barrier certificate framework was first proposed in Prajna and Jadbabaie [2004] and provides a way to verify the safety property as defined in Definition 1.

Theorem 3. (Weak Barrier Certificates). Given a system $\Gamma = (\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_{\mathrm{n}}, \mathcal{X}_{\mathrm{u}})$, let $B(\mathbf{x})$ be a differentiable scalar function satisfying

$$B(\mathbf{x}) \leq 0, \forall \mathbf{x} \in \mathcal{X}_{\mathrm{n}}, \tag{8a}$$

$$B(\mathbf{x}) > 0, \forall \mathbf{x} \in \mathcal{X}_{\mathrm{u}} \text{ and}, \tag{8b}$$

$$\nabla B(\mathbf{x}) \cdot \mathbf{f}(\mathbf{x}, \mathbf{d}) \leq 0, \forall (\mathbf{x}, \mathbf{d}) \in \mathcal{X} \times \mathcal{D}. \tag{8c}$$

If such a function exists the system is safe.

Proof. See, Prajna and Jadbabaie [2004] or Prajna et al. [2007]

A nice bonus result from this theorem is that it does not only prove the safety of a system, it can also be leveraged to construct a safety envelope.

Proposition 4. (Safety Envelope). Let $B(\mathbf{x})$ be a function as described in Theorem 3. Then, $\langle B \rangle$ is a safety envelope, i.e.,

$$\mathcal{X}_\mathrm{n} \subseteq \langle B \rangle \subseteq \mathcal{X}_\mathrm{s}. \tag{9}$$

Proof. Comparing (8a) with the definition of the $\langle \cdot \rangle$ operator in (1) it is immediately evident that $\mathcal{X}_\mathrm{n} \subseteq \langle B \rangle$. Furthermore for any $x_0 \in \langle B \rangle$ we have by definition that $B(x_0) \leq 0$. Then (8c) guarantees that $\forall t \in \mathbb{R}_{0+}$ and $\forall \bar{d} \in \mathcal{L}_\infty(\mathbb{R}_{0+}, \mathcal{D})$ it holds that $B(\phi^{\bar{d}}_{x_0}(t)) \leq B(x_0) \leq 0$. So by (8b) we have $\phi^{\bar{d}}_{x_0}(t) \notin \mathcal{X}_\mathrm{u}$, so that $x_0 \in \mathcal{X}_\mathrm{s}$. □

The protection function B in Theorem 3 can thus be used in a safety supervisor system. During normal mode of operation the supervisor will not intervene, at the same time it is guaranteed that the emergency shutdown procedure will be invoked before leaving $\mathcal{X}_\mathrm{s}$. However, the desired behavior during deviations from the normal operation that are not safety critical (i.e. $\mathbf{x} \notin \mathcal{X}_\mathrm{n}$ but $\mathbf{x} \in \mathcal{X}_\mathrm{s}$) is not specified by (8). Clearly we prefer the emergency shutdown procedures not to be invoked in these cases and hence want $\langle B \rangle$ to be as close to $\mathcal{X}_\mathrm{s}$ as possible.

Observe that (8c) ensures that the zero sub-level set $\langle B \rangle$ is positive invariant. In fact, any sub-level set $\langle B \rangle_a$ is invariant, as is illustrated in Figure 2. This notion is leveraged in Corollary 5.

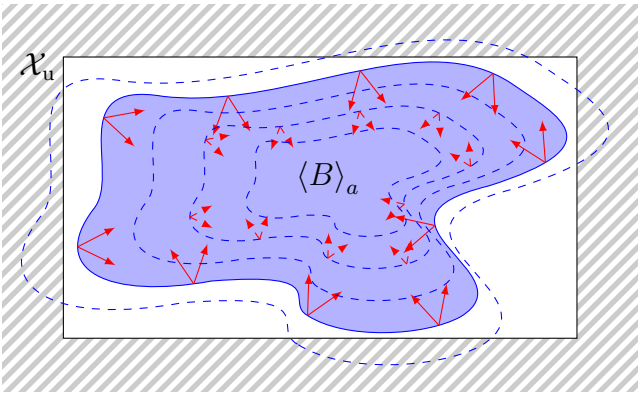

Fig. 2. Invariant level sets of $B(\mathbf{x})$

Corollary 5. (β Optimization). Given a function $B(\mathbf{x})$ satisfying Theorem 3, if there exists a $\beta \in \mathbb{R}_+$ such that

$$B(\mathbf{x}) - \beta > 0, \quad \forall \mathbf{x} \in \mathcal{X}_\mathrm{u}, \tag{10}$$

then

$$\mathcal{X}_\mathrm{n} \subseteq \langle B \rangle \subset \langle B \rangle_\beta \subseteq \mathcal{X}_\mathrm{s} \tag{11}$$

Proof. Note that $\langle B \rangle_\beta = \langle B - \beta \rangle$. Now, for positive β, (8a) still holds and (8c) is unaffected by this translation. It thus indeed suffices to validate (8b). Finally, since B is differentiable, the subset is strict, i.e. $\langle B \rangle \subset \langle B \rangle_\beta$. [1] □

[1] An exception exists for the trivial situation that $\mathcal{X}_\mathrm{u} = \emptyset$ or $\mathcal{X}_\mathrm{n} = \emptyset$.

Corollary 5 allows us to turn the feasibility problem of Proposition 4 into an optimization problem. In doing so, the computational complexity barely increases. In fact, in some cases the optimal β is already known from the feasibility problem as will become apparent in the next section.

The approach in Corollary 5 only translates B, but does not alter the 'contour'. Whether the result is satisfactory will hence depend on the problem at hand. If not, Corollary 6 can be used to alter this 'contour' as well as increase the size of the set $\langle B \rangle$.

Corollary 6. (V Optimization). Let $B(\mathbf{x})$ be a function as described in Theorem 3. Let $V : \mathbb{R}^n \to \mathbb{R}$ be such that

$$B(\mathbf{x}) \leq V(\mathbf{x}), \quad \forall \mathbf{x} \in \mathcal{X}, \tag{12}$$

then

$$\mathcal{X}_\mathrm{n} \cup \langle V \rangle \subseteq \langle B \rangle \subseteq \mathcal{X}_\mathrm{s}. \tag{13}$$

Proof. Comparing (12) to the definition in (1) clearly yields $\langle V \rangle \subseteq \langle B \rangle$. The remainder of the proof is similar to that of Proposition 4. □

Now, inflating $\mathrm{vol}\,\langle V \rangle$ increases $\mathrm{vol}\,\langle B \rangle$ as well. A proper choice of V, with an optimizable volume, is essential in order to usefully apply Corollary 6. Remark 1 provides insights in using hyper-ellipsoids for this purpose. Note that in that case (12) can be relaxed to hold only for $\mathbf{x} \in \mathcal{X}_\mathrm{u}^\mathrm{c}$.

Remark 1. (Hyper-ellipsoids). Let $V(\mathbf{x})$ be an hyperellipsoid, i.e.,

$$V(\mathbf{x}) = (\mathbf{x} - \mathbf{b})^\mathrm{T} \mathbf{Q}^{-1} (\mathbf{x} - \mathbf{b}) - 1 \tag{14}$$

where $\mathbf{b} \in \mathcal{X}_\mathrm{s}$ and $\mathbf{Q} \succ 0$. Then its volume is given by

$$\mathrm{vol}\,\langle V \rangle = \frac{4}{3} \pi \sqrt{\det(\mathbf{Q})} \tag{15}$$

This volume could be maximized using the following optimization problem:

$$\begin{aligned} &\max \log\det \mathbf{Q} \\ &\text{s. t. (8) and (12)} \end{aligned} \tag{16}$$

If (8) and (12) are formulated as SOS constraints (Section 4.4), this program is convex, see Boyd and Vandenberghe [2004]. However, it is not linear in the optimization criterion. In order to ease the computation, it would be desirable to have a linear criterion. This could be achieved by instead maximizing the sum of the semi-principal axes. For real square matrices the sum of the eigenvalues is given by $\sum_{i=1}^n \lambda_i = \mathrm{Tr}\,\mathbf{Q}$. Now, to avoid a matrix inversion, we do not maximize $\mathrm{Tr}\,\mathbf{Q}$, but instead minimize its inverse. To this extend we substitute $\mathbf{E} = \mathbf{Q}^{-1}$ in (14) and obtain the following linear optimization problem:

$$\begin{aligned} &\min \mathrm{Tr}\,\mathbf{E} \\ &\text{s. t. (8) and (12)} \end{aligned} \tag{17}$$

Note that the program in (17) is not guaranteed to maximize (15), especially when the dimensions have different orders of magnitude. In some cases, results might improve by applying a weighting vector $\mathbf{w} \in \mathbb{R}^n_+$, i.e.,

$$\min \mathbf{w}^\mathrm{T} \,\mathrm{diag}\,\mathbf{E} \tag{18}$$

Whether these approaches are useful will depend on the problem at hand. When results are unsatisfactory, one can always switch back to the program in (16). ▷

Note that the observations in Remark 1 are particularly useful if a quadratic polynomial barrier certificate exists, i.e. there exists $B \in \mathcal{P}_{n,2}$, satisfying (8). In this case B could be of the form (14) and $\mathrm{vol}\,\langle B\rangle$ could be optimized directly.

Although Theorem 3 holds for a wide class of systems, in the remainder of this paper we will restrict ourselves to polynomial system descriptions and consider only polynomial barrier certificates $B \in \mathcal{P}_n$. In this case, finding a barrier certificate can be done using semi-definite programming (SDP), as will be shown in Section 4.4.

However, in that section it will also become apparent that the number of decision variables involved with such an SDP grows rapidly with the number of state variables n and polynomial degree d of the system description. Even for moderately sized n and d, the SDP might become computationally infeasible. Therefore, the next two subsections will first present methods that can be used to reduce the complexity of the SDP.

4.2 Compositional Barrier Certificates

The main idea in this section is to split the system into interconnected subsystems, each subsystem containing only a subset of the state variables. A barrier certificate can be computed per subsystem and then results can be combined to obtain a safety envelope for the complete system. This procedure was first introduced in Sloth et al. [2012b].

We consider a dynamical system which is given as an interconnection of k subsystems. Let $\mathcal{I} = \{1, \ldots, k\}$, then the system can be described as a set $\Gamma = \{\Gamma_i\}_\mathcal{I}$ with subsystems $\Gamma_i = (\mathbf{f}_i, \mathcal{X}_i, \mathcal{D}_i, \mathcal{X}_{\mathrm{n},i}, \mathcal{X}_{\mathrm{u},i}, \mathcal{U}_i, \mathbf{g}_i)$.

Given are the collections of continuous vector fields $f_i : \mathbb{R}^{n_i+m_i+q_i} \to \mathbb{R}^{n_i}$, state space $\mathcal{X}_i \subseteq \mathbb{R}^{n_i}$, external (disturbance) inputs $\mathcal{D}_i \subseteq \mathbb{R}^{q_i}$, normal modes of operation $\mathcal{X}_{\mathrm{n},i} \subseteq \mathcal{X}_i$, set of unsafe modes of operation $\mathcal{X}_{\mathrm{u},i} \subseteq \mathcal{X}_i$, interconnection inputs $\mathcal{U}_i \subseteq \mathbb{R}^{m_i}$, and interconnection output functions $g_i : \mathbb{R}^{n_i} \to \mathbb{R}^{r_i}$.

The sets $\mathcal{X}$, $\mathcal{X}_\mathrm{n}$, $\mathcal{X}_\mathrm{u}$, and $\mathcal{D}$ are constructed from the sets of the subsystems in the following fashion

$$\mathcal{X} = \prod_{i\in\mathcal{I}} \mathcal{X}_i, \qquad \mathcal{X}_\mathrm{n} = \prod_{i\in\mathcal{I}} \mathcal{X}_{\mathrm{n},i},$$
$$\mathcal{X}_\mathrm{u} = \prod_{i\in\mathcal{I}} \mathcal{X}_{\mathrm{u},i} \qquad \mathcal{D} = \prod_{i\in\mathcal{I}} \mathcal{D}_i,$$

Proposition 7. (Compositional Barrier Certificates). Given a set of subsystems $\Gamma = \{\Gamma_i\}_\mathcal{I}$, if there exist differentiable functions $B_i : \mathcal{X}_i \to \mathbb{R}$, constants $\alpha_i, \beta_i \in \mathbb{R}$ and functions $\gamma_i : \mathbb{R}^{m_i+r_i} \to \mathbb{R}$ for all $i \in \mathcal{I}$ such that

$$B_i(\mathbf{x}_i) + \alpha_i \leq 0, \qquad \forall \mathbf{x}_i \in \mathcal{X}_{\mathrm{n},i}, \tag{19a}$$
$$B_i(\mathbf{x}_i) - \beta_i > 0, \qquad \forall \mathbf{x}_i \in \mathcal{X}_{\mathrm{u},i}, \quad \text{and} \tag{19b}$$
$$\boldsymbol{\nabla} B_i(\mathbf{x}_i) \cdot \mathbf{f}_i(\mathbf{x}_i, \mathbf{u}_i, \mathbf{d}_i) \leq \gamma_i(\mathbf{u}_i, \mathbf{g}_i(\mathbf{x}_i)), \quad \forall (\mathbf{x}_i, \mathbf{u}_i, \mathbf{d}_i) \in \mathcal{X}_i \times \mathcal{U}_i \times \mathcal{D}_i \tag{19c}$$

with

$$\alpha = \sum_\mathcal{I} \alpha_i \geq 0, \quad \beta = \sum_\mathcal{I} \beta_i \geq 0, \quad \text{and}$$
$$\sum_\mathcal{I} \gamma_i(\mathbf{u}_i, \mathbf{g}(\mathbf{x}_i)) \leq 0, \quad \forall x_i \in \mathcal{X}_i, u_i \in \mathcal{U}_i \tag{20}$$

then the system is safe, with $B(\mathbf{x}) = \sum_\mathcal{I} B_i(\mathbf{x}_i)$ as protection function.

Proof. Sum (19a) over all subsystems

$$\sum_\mathcal{I} B_i(\mathbf{x}_i) + \sum_\mathcal{I} \alpha_i \leq 0, \qquad \forall \mathbf{x}_i \in \mathcal{X}_{\mathrm{n},i}$$
$$B(\mathbf{x}) + \alpha \leq 0, \qquad \forall \mathbf{x} \in \mathcal{X}_\mathrm{n} \tag{21}$$

By (20) we see that $\alpha \geq 0$ hence (19a) reduces to (8a). A similar reduction can be done for (19b) yielding (8b). The reduction of (19c)) to (8c)) is given in Section 4 of Sloth et al. [2012a]. Finally, differentiability of $B_i(\mathbf{x}_i)$ is conserved under addition, hence $B(\mathbf{x})$ is differentiable. Since $B(\mathbf{x})$ satisfies (8), the system is safe. Additionally, by Proposition 4, $\langle B\rangle$ is a safety envelope. □

The optimizations presented in Section 4.1 can be modified to be applicable to the compositional barrier certificate approach, which will be shown below.

Corollary 8. (Compositional β Optimization). Let $B(\mathbf{x}) = \sum_\mathcal{I} B_i(\mathbf{x}_i)$ be a given function satisfying Proposition 7 with β as defined in (20), then

$$\mathcal{X}_\mathrm{n} \subseteq \langle B\rangle \subseteq \langle B\rangle_\beta \subseteq \mathcal{X}_\mathrm{s} \tag{22}$$

Proof. By definition $\langle B\rangle \subseteq \langle B\rangle_\beta$. Furthermore from (19b) and (20) follows that $B(\mathbf{x}) - \beta > 0$, $\forall \mathbf{x} \in \mathcal{X}_\mathrm{u}$. □

Note that $\langle B\rangle = \langle B\rangle_\beta$ would only hold in trivial cases, typically we would find that $\langle B\rangle \subset \langle B\rangle_\beta$.

Corollary 9. (Compositional V Optimization). Let $\{B_i\}_\mathcal{I}$ be a collection of functions conforming to Proposition 7, additionally satisfying for some given collection $\{V_i : \mathbb{R}^{n_i} \to \mathbb{R}\}_\mathcal{I}$ that

$$B_i(\mathbf{x}_i) \leq V_i(\mathbf{x}_i), \quad \forall \mathbf{x}_i \in \mathcal{X}_i \tag{23}$$

then

$$\mathcal{X}_\mathrm{n} \cup \langle V\rangle \subseteq \langle B\rangle \subseteq \mathcal{X}_\mathrm{s} \tag{24}$$

where $V(\mathbf{x}) = \sum_\mathcal{I} V_i(\mathbf{x}_i)$

Proof. From (23) we have that $\sum_\mathcal{I} B_i(\mathbf{x}_i) \leq \sum_\mathcal{I} V_i(\mathbf{x}_i)$ so by definition $\langle V\rangle \subseteq \langle B\rangle$. □

By inspecting Proposition 7, we observe that (19) can be evaluated separately for every subsystem. Hence, the sub-certificates B_i can be generated independently. However, conditions (20) need to be satisfied globally and can only be verified after all sub-certificates are computed. If one or more conditions in (20) are violated, the certificates need to be recomputed using a different optimization criterion and (20) should be evaluated again until it is valid. This can be achieved using the sub-gradient algorithm presented in Algorithm 1.

4.3 Segmented Barrier Certificates

Aerodynamic properties introduce non-linearities in the wind turbine's behavior. To accurately model the turbine over the full operating conditions and wind span using polynomial approximations, a 12^{th} degree polynomial is required, see Pedersen and Steiniche [2012]. This section will present a method based on segmenting the disturbance input that will allow for low-degree approximations to still yield the desired accuracy.

Algorithm 1 Sub-gradient algorithm

Consider the definitions used in Proposition 7, let $\hat{\boldsymbol{\gamma}}_i$ be the tunable parameters in γ_i and define $\Delta_k = \frac{a}{b+k}$. Initiate $k = 0$ and set a, b, $\lambda_\alpha^{(0)}$, $\lambda_\beta^{(0)}$ and $\boldsymbol{\lambda}_\gamma^{(0)}$ to some appropriate values.

1. Compute B_i

Maximize $\lambda_\alpha^{(k)}\alpha_i + \lambda_\beta^{(k)}\beta_i - \boldsymbol{\lambda}_\gamma^{(k)}\hat{\boldsymbol{\gamma}}_i$ s.t. B_i satisfying (19).

2. Verify

Verify whether (20) holds. If so, terminate.

3. Update objective:

- $\lambda_\alpha^{(k+1)} = \lambda_\alpha^{(k)} - \Delta_k\alpha$
- $\lambda_\beta^{(k+1)} = \lambda_\beta^{(k)} - \Delta_k\beta$
- $\boldsymbol{\lambda}_\gamma^{(k+1)} = \boldsymbol{\lambda}_\gamma^{(k)} + \Delta_k\hat{\boldsymbol{\gamma}}$
- $k = k + 1$.

Return to step 1.

Proposition 10. (Segmented Barrier Certificates). Given a system $\Gamma = (\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_\mathrm{n}, \mathcal{X}_\mathrm{u})$, for $\mathcal{I} = \{1, ..., k\}$, cover $\mathcal{D}$ by open sets $\mathfrak{D} = \{\mathcal{D}_i\}_\mathcal{I}$ with a partition of unity $\Lambda = \{\lambda_i\}_\mathcal{I}$ subordinate to $\mathfrak{D}$. Let $\mathcal{B}$ be a family of a differentiable scalar functions $\mathcal{B} = \{B_i\}_\mathcal{I}$ satisfying for all $i \in \mathcal{I}$

$$B_i(\mathbf{x}) \leq 0, \forall \mathbf{x} \in \mathcal{X}_\mathrm{n}, \tag{25a}$$
$$B_i(\mathbf{x}) > 0, \forall \mathbf{x} \in \mathcal{X}_\mathrm{u} \text{ and}, \tag{25b}$$
$$\boldsymbol{\nabla} B_i(\mathbf{x}) \cdot \mathbf{f}(\mathbf{x}, \mathbf{d}) \leq 0, \forall (\mathbf{x}, \mathbf{d}) \in \mathcal{X} \times \mathcal{D}_i. \tag{25c}$$

If such a family $\mathcal{B}$ exists, the system is safe with protection function $B(\mathbf{x}, \mathbf{d}) = \sum_\mathcal{I} B_i(\mathbf{x})\lambda_i(\mathbf{d})$.

Proof. The following inequalities hold for all $\mathbf{d} \in \mathcal{D}$

$$B(\mathbf{x}, \mathbf{d}) = \sum_\mathcal{I} B_i(\mathbf{x})\lambda_i(\mathbf{d}) \leq \max_\mathcal{I} B_i(\mathbf{x}) \leq 0, \quad \forall \mathbf{x} \in \mathcal{X}_\mathrm{n},$$

$$B(\mathbf{x}, \mathbf{d}) = \sum_\mathcal{I} B_i(\mathbf{x})\lambda_i(\mathbf{d}) \geq \min_\mathcal{I} B_i(\mathbf{x}) > 0, \quad \forall \mathbf{x} \in \mathcal{X}_\mathrm{u},$$

$$\frac{\partial B}{\partial \mathbf{x}} f(\mathbf{x}, \mathbf{d}) = \sum_\mathcal{I} \frac{\partial B_i}{\partial \mathbf{x}} \lambda_i(\mathbf{d}) \mathbf{f}(\mathbf{x}, \mathbf{d})$$
$$\leq \max_\mathcal{I} \frac{\partial B_i}{\partial \mathbf{x}} \mathbf{f}(\mathbf{x}, \mathbf{d}) \leq 0, \qquad \forall \mathbf{x} \in \mathcal{X}.$$

Thus, $B(\mathbf{x}, \mathbf{d})$ conforms to (8) and by Proposition 4 is hence a protection function. □

Now, by choosing $\mathfrak{D}$ to consist of (partly) overlapping wind spans a subordinate partition of unity Λ can be easily defined. See for example the bump function in Tu [2008].

Inequality (25c) still depends on the state evolution map $\mathbf{f}(\mathbf{x}, \mathbf{d})$. However, for the computation of each $B_i(\mathbf{x})$ this function only needs to be evaluated for $\mathcal{D}_i$. Hence in (25c) $\mathbf{f}(\mathbf{x}, \mathbf{d})$ could be substituted with $\mathbf{f}_i(\mathbf{x}, \mathbf{d})$, provided that for all $\mathbf{d} \in \mathcal{D}_i$ it holds that $\mathbf{f}_i(\mathbf{x}, \mathbf{d}) = \mathbf{f}(\mathbf{x}, \mathbf{d})$. Alternatively, a set of functions $\mathcal{F}_i(\mathbf{x}, \mathbf{d}) = \{\mathbf{f}_i(\mathbf{x}, \mathbf{d}, e) | e \in \mathcal{E}\}$ could be substituted in (25c) provided that $\mathbf{f}(\mathbf{x}, \mathbf{d}) \in \mathcal{F}_i(\mathbf{x}, \mathbf{d})$ for all $(\mathbf{x}, \mathbf{d}) \in \mathcal{X} \times \mathcal{D}_i$. Using this approach a conservative approximation of the aerodynamics model can be made by using only low degree polynomials.

Note that if in Theorem 3 we define $\mathcal{D}$ to be $\mathcal{D}_i$, inequalities (8) and (25) become the same. All results derived for the barrier certificate approach, such as the optimizations and compositional barrier certificates, are hence applicable to the segmented barrier certificates as well.

4.4 Sum of Squares

In order to compute the barrier certificate, inequalities (8) are formulated as a sum of squares (SOS) problem, which can be solved using semi-definite programming (SDP). This section will outline the main steps, the interested reader is referred to Parrilo [2003] or chapter 2 of Jarvis-Wloszek [2003] for more background on this topic.

The system is assumed to have a polynomial vector field $\mathbf{f}(\mathbf{x}, \mathbf{d})$ and all relevant sets are assumed to be described as semi-algebraic sets. Let $\mathbf{g}_\mathrm{x} \in \mathcal{P}_n^{k_\mathrm{x}}$, $\mathbf{g}_\mathrm{n} \in \mathcal{P}_n^{k_\mathrm{n}}$, $\mathbf{g}_\mathrm{u} \in \mathcal{P}_n^{k_\mathrm{u}}$, and $\mathbf{g}_\mathrm{d} \in \mathcal{P}_q^{k_\mathrm{d}}$, such that

$$\mathcal{X} = \{\mathbf{x} \in \mathbb{R}^n | \mathbf{g}_\mathrm{x}(\mathbf{x}) \geq 0\}, \tag{26a}$$
$$\mathcal{X}_\mathrm{n} = \{\mathbf{x} \in \mathbb{R}^n | \mathbf{g}_\mathrm{n}(\mathbf{x}) \geq 0\}, \tag{26b}$$
$$\mathcal{X}_\mathrm{u} = \{\mathbf{x} \in \mathbb{R}^n | \mathbf{g}_\mathrm{u}(\mathbf{x}) \geq 0\}, \tag{26c}$$
$$\mathcal{D} = \{\mathbf{d} \in \mathbb{R}^q | \mathbf{g}_\mathrm{d}(\mathbf{d}) \geq 0\} \tag{26d}$$

where the inequalities in (26) are satisfied coordinate-wise.

Lemma 11. (S-procedure). Let $\mathcal{X}_\mathrm{g} \subseteq \mathbb{R}^n$, $f \in \mathcal{P}_n$, and $\mathbf{g} \in \mathcal{P}_n^k$ so that $\mathbf{g}(\mathbf{x}) \geq 0$ (coordinate-wise) for any $\mathbf{x} \in \mathcal{X}_\mathrm{g}$. Now, if

$$\mathbf{s}(\mathbf{x}) \in \Sigma_n^k \text{ and} \tag{27}$$
$$f(\mathbf{x}) - \mathbf{s}^\mathrm{T}(\mathbf{x})\mathbf{g}(\mathbf{x}) \in \Sigma_n \tag{28}$$

then $f(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathcal{X}_\mathrm{g}$.

Using Lemma 11, Theorem 3 can be reformulated as an SOS problem.

Proposition 12. (Barrier Certificate SOS problem). Let $\Gamma = (\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_\mathrm{n}, \mathcal{X}_\mathrm{u})$ be given with $\mathcal{X}, \mathcal{D}, \mathcal{X}_\mathrm{n}$, and $\mathcal{X}_\mathrm{u}$ as defined in (26). If there exist $\epsilon \in \mathbb{R}_+$, $\mathbf{s}_\mathrm{x} \in \Sigma_n^{k_\mathrm{x}}$, $\mathbf{s}_\mathrm{n} \in \Sigma_n^{k_\mathrm{n}}$, $\mathbf{s}_\mathrm{u} \in \Sigma_n^{k_\mathrm{u}}$, $\mathbf{s}_\mathrm{d} \in \Sigma_q^{k_\mathrm{d}}$ and $B \in \mathcal{P}_n$ such that

$$-B - \mathbf{s}_\mathrm{n}^\mathrm{T}\mathbf{g}_\mathrm{n}, \tag{29a}$$
$$B - \epsilon - \mathbf{s}_\mathrm{u}^\mathrm{T}\mathbf{g}_\mathrm{u}, \text{ and} \tag{29b}$$
$$-\boldsymbol{\nabla} B \cdot \mathbf{f} - \mathbf{s}_\mathrm{x}^\mathrm{T}\mathbf{g}_\mathrm{x} - \mathbf{s}_\mathrm{d}^\mathrm{T}\mathbf{g}_\mathrm{d} \tag{29c}$$

are sum of squares, then $B(\mathbf{x})$ is a protection function.

Proposition 12 is a feasibility problem, but using the results in Corollary 5, Corollary 6 and/or Remark 1, an additional optimization criterion can be supplied in order to increase $\mathrm{vol}\,\langle B \rangle$.

A similar approach can be used to compute compositional barrier certificates as is demonstrated below. Let the following semi-algebraic subsets be defined for each subsystem $i \in \mathcal{I}$

$$\mathcal{X}_i = \{\mathbf{x}_i \in \mathbb{R}^{n_i} | \mathbf{g}_{\mathrm{x},i}(\mathbf{x}) \geq 0\}, \tag{30a}$$
$$\mathcal{X}_{\mathrm{n},i} = \{\mathbf{x}_i \in \mathbb{R}^{n_i} | \mathbf{g}_{\mathrm{n},i}(\mathbf{x}) \geq 0\}, \tag{30b}$$
$$\mathcal{X}_{\mathrm{u},i} = \{\mathbf{x}_i \in \mathbb{R}^{n_i} | \mathbf{g}_{\mathrm{u},i}(\mathbf{x}) \geq 0\}, \tag{30c}$$
$$\mathcal{U}_i = \{\mathbf{u}_i \in \mathbb{R}^{m_i} | \mathbf{g}_{\mathrm{c},i}(\mathbf{u}) \geq 0\}, \tag{30d}$$
$$\mathcal{D}_i = \{\mathbf{d}_i \in \mathbb{R}^{q_i} | \mathbf{g}_{\mathrm{d},i}(\mathbf{d}) \geq 0\} \tag{30e}$$

with all functions $\mathbf{g}_*$ of the appropriate size k_*.

Proposition 13. Let $\Gamma = \{\Gamma_i\}_\mathcal{I}$ be given as in Section 4.2 with $\mathcal{X}_i$, $\mathcal{X}_{\mathrm{n},i}$, $\mathcal{X}_{\mathrm{u},i}$, $\mathcal{U}_i$, and $\mathcal{D}_i$, as defined in (30). If there exist $B_i \in \mathcal{P}_{n_i}$, $\alpha_i, \beta_i \in \mathbb{R}$, $\gamma_i \in \mathcal{P}_{m_i+r_i}$, $\epsilon \in \mathbb{R}_+$, $\mathbf{s}_{\mathrm{x},i} \in \Sigma_{n_i}^{k_{\mathrm{x}_i}}$, $\mathbf{s}_{\mathrm{n},i} \in \Sigma_{n_i}^{k_{\mathrm{n}_i}}$, $\mathbf{s}_{\mathrm{u},i} \in \Sigma_{n_i}^{k_{\mathrm{u}_i}}$, $\mathbf{s}_{\mathrm{c},i} \in \Sigma_{m_i}^{k_{\mathrm{c}_i}}$, and $\mathbf{s}_{\mathrm{d},i} \in \Sigma_{q_i}^{k_{\mathrm{d}_i}}$ for all $i \in \mathcal{I}$, such that

$$-B_i - \mathbf{s}_{\mathrm{n},i}^{\mathrm{T}}\mathbf{g}_{\mathrm{n},i} - \alpha_i, \tag{31a}$$

$$B_i - \epsilon - \mathbf{s}_{\mathrm{u},i}^{\mathrm{T}}\mathbf{g}_{\mathrm{u},i} - \beta_i, \text{ and} \tag{31b}$$

$$-\boldsymbol{\nabla}B_i \cdot \mathbf{f}_i - \mathbf{s}_{\mathrm{x},i}^{\mathrm{T}}\mathbf{g}_{\mathrm{x},i} - \mathbf{s}_{\mathrm{d},i}^{\mathrm{T}}\mathbf{g}_{\mathrm{d},i} - \mathbf{s}_{\mathrm{c},i}^{\mathrm{T}}\mathbf{g}_{\mathrm{c},i} + \gamma_i, \tag{31c}$$

are sum of squares and

$$\sum_{\mathcal{I}} \alpha_i, \ \sum_{\mathcal{I}} \beta_i, \text{ and } -\sum_{\mathcal{I}} \gamma_i, \tag{32}$$

are sum of squares, then $B(\mathbf{x}) = \sum_{\mathcal{I}} B_i(\mathbf{x}_i)$ is a protection function.

The s-procedures used in these SOS problems can drastically increase the number of decision variables. The number of monomials in each s-function is given by $\binom{n+d}{d}$, where n is the number of independent variables and d is the maximum degree. Depending on the system $\mathbf{f}$ and the semi-algebraic set descriptions $\mathbf{g}$ at hand, one can usually reduce these numbers. When a certain set function g does not depend on certain state variables, those can be excluded from the corresponding s-procedure s as well. It is easily verified that for $s \in \Sigma_{n'}$ with $n' < n$ Lemma 11 still holds (take the extreme case where $s \in \mathbb{R}_+$). Excluding those variables could in some cases also be non-conservative, depending on the problem structure.

Solving the SOS problem is computationally the most time-intense part of these methods. However, these computations are performed offline. The online calculations consist of the evaluation of the $B(\mathbf{x})$ polynomial, which is typically a low-degree polynomial in only a few state variables. This is not an issues with modern day computer systems, an FPGA has plenty of recourses to do so in real-time.

5. RESULTS

5.1 Turbine Model

Evidently, a safety supervisor should be designed for a specific wind turbine. The NREL 5-MW wind turbine model by Jonkman et al. [2009] will be used to provide a proof of concept. A simplified model was derived including the safety critical states. The model equations are given in (33), a description (and value) of state variables and parameters is given in Table 1. The derived model was verified against the FAST simulator configured for the same turbine, see Jonkman [2012].

$$\dot{\omega}_{\mathrm{r}} = \frac{1-\xi}{J_{\mathrm{r}}}\tau_{\mathrm{a}}(w, \omega_r, \beta) + \frac{k_{\mathrm{ll}}}{J_{\mathrm{r}}}\theta_{\mathrm{ll}} - \frac{B_{\mathrm{r}}}{J_{\mathrm{r}}}\omega_{\mathrm{r}} - \frac{N}{J_{\mathrm{r}}}\tau_{\mathrm{g}} \tag{33a}$$

$$\dot{\beta} = 8 \tag{33b}$$

$$\dot{\omega}_{\mathrm{t}} = \frac{L}{J_{\mathrm{t}}}F_{\mathrm{a}}(w, \omega_r, \beta) + \frac{mgL - k_{\mathrm{t}}}{J_{\mathrm{t}}}\theta_{\mathrm{t}} - \frac{B_{\mathrm{t}}}{J_{\mathrm{t}}}\omega_{\mathrm{t}} \tag{33c}$$

$$\dot{\theta}_{\mathrm{t}} = \omega_{\mathrm{t}} \tag{33d}$$

$$\dot{\omega}_{\mathrm{ll}} = \frac{\xi}{J_{\mathrm{ll}}}\tau_{\mathrm{a}}(w, \omega_r, \beta) - \frac{B_{\mathrm{ll}}}{J_{\mathrm{ll}}}\omega_{\mathrm{ll}} - \frac{k_{\mathrm{ll}}}{J_{\mathrm{ll}}}\theta_{\mathrm{ll}} \tag{33e}$$

$$\dot{\theta}_{\mathrm{ll}} = \omega_{\mathrm{ll}} \tag{33f}$$

For convenience the states (the variables on the left side of (33)) will collectively be referred to as $\mathbf{x}$ and the state functions (right side of (33)) will be referred to as $\mathbf{f}$.

Table 1. Turbine Model Description

States, parameters, functions and disturbances of the model			
Description		**Value**	**Unit**
Rotor & Drive train			
Rotor angular velocity	ω_{r}	-	rad/s
Blade-pitch angle	β	-	deg
Generator torque input	τ_{g}	-	Nm
Equivalent rotor-side damping	B_{r}	1.5e5	Nm/(rad/s)
Equivalent rotor-side inertia	J_{r}	4.05e7	$\mathrm{kg \cdot m^2}$
Gearing Ratio	N	97	-
Tower			
Tower fore-aft angular velocity	ω_{t}	-	rad/s
Tower fore-aft angle	θ_{t}	-	rad
Tower damping	B_{t}	7.22e8	Nm/(rad/s)
Tower stiffness	k_{t}	1.47e10	Nm/rad
Equivalent tower mass	m	5.01e5	kg
Tower length	L	87.6	m
Tower inertia	J_{t}	3.54e9	$\mathrm{kg \cdot m^2}$
Gravitational acceleration	g	9.81	$\mathrm{m/s^2}$
Lead-lag blade bending (edgewise)			
Blade tip angular velocity	ω_{ll}	-	rad/s
Blade tip angle	θ_{ll}	-	rad
Blade damping	B_{ll}	3.00e8	Nm/(rad/s)
Blade stiffness	k_{ll}	6.75e7	Nm/rad
Blade inertia	J_{ll}	1.24e7	$\mathrm{kg \cdot m^2}$
Aerodynamics			
Aerodynamic torque function	τ_{a}	-	Nm
Aerodynamic thrust function	F_{a}	-	N
Wind disturbance input	w	-	m/s
Torque ratio	ξ	0.5	-

Lookup tables for the aerodynamic rotor torque $\tau_{\mathrm{a}}(w, \omega_{\mathrm{r}}, \beta)$ and aerodynamic thrust $F_{\mathrm{a}}(w, \omega_{\mathrm{r}}, \beta)$ can be found using turbine simulations. However, the wind acts as an unknown (bounded) disturbance. For a given windspan $\mathcal{W}$, we therefore like an expression of the aerodynamic functions in the form

$$\mathcal{F}_{\mathrm{a}}(\omega_{\mathrm{r}}, \beta) = \{F_{\mathrm{a}}(w, \omega_{\mathrm{r}}, \beta) | w \in \mathcal{W}\}, \tag{34}$$

$$\mathcal{T}_{\mathrm{a}}(\omega_{\mathrm{r}}, \beta) = \{\tau_{\mathrm{a}}(w, \omega_{\mathrm{r}}, \beta) | w \in \mathcal{W}\}. \tag{35}$$

By fitting a polynomial on both $\min \mathcal{F}_{\mathrm{a}}(\omega_{\mathrm{r}}, \beta)$ and $\max \mathcal{F}_{\mathrm{a}}(\omega_{\mathrm{r}}, \beta)$, an analytical expression describing (34) can be derived. Evidently, the same approach holds for the aerodynamic torque $\mathcal{T}_{\mathrm{a}}$.

As an example a 3rd degree fit to the maximum torque $\max \mathcal{T}_{\mathrm{a}}(\omega_{\mathrm{r}}, \beta)$ is shown in Figure 3. The colored surface is the obtained from simulation data, the black mesh grid is the polynomial fit. For this example, as well as the remainder of this section, the wind span is chosen to be $\mathcal{W} = [17, 20.5]$ m/s.

The bounds on the wind turbine's states during normal mode of operation are given in Table 2. The table also contains the ultimate load limits that should never be violated. These bounds are also described as algebraic sets conform (26), which will prove to be useful in describing de SOS program in the next subsection.

Note that $\mathcal{X}_{\mathrm{u}} = \mathcal{X}_{\mathrm{u},\omega_{\mathrm{r}}} \cup \mathcal{X}_{\mathrm{u},\theta_{\mathrm{t}}} \cup \mathcal{X}_{\mathrm{u},\theta_{\mathrm{ll}}}$ and can hence not be written in the form of (26c). Instead, (29b) will need to be verified for each unsafe region separately.

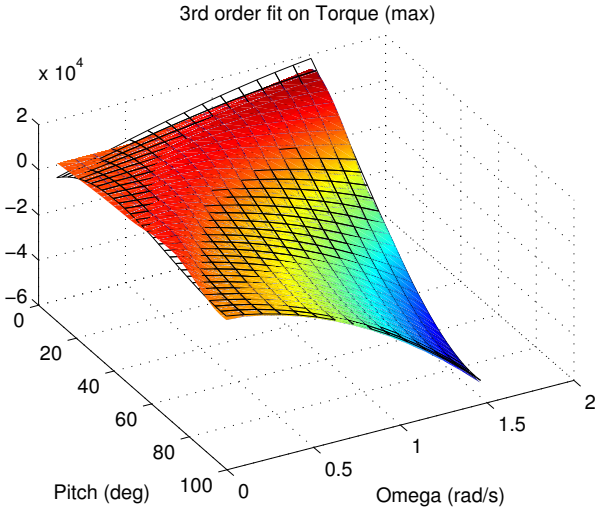

Fig. 3. Polynomial fit on aerodynamics

Table 2. Normal operation and physical limits

State	Bounds	Algebraic set
Normal operation		
ω_r	$[1.2, 1.35]$	$g_{\mathrm{n},\omega_\mathrm{r}} = (\omega_\mathrm{r} - 1.2)(1.35 - \omega_\mathrm{r})$
β	$[14, 18]$	$g_{\mathrm{n},\beta} = (\beta - 14)(18 - \beta)$
θ_t	$[0.5e^{-3}, 3e^{-3}]$	$g_{\mathrm{n},\theta_\mathrm{t}} = (\theta_\mathrm{t} - 0.5e^{-3})(3e^{-3} - \theta_\mathrm{t})$
ω_t	$[-2e^{-3}, 2e^{-3}]$	$g_{\mathrm{n},\omega_\mathrm{t}} = (\omega_\mathrm{t} + 2e^{-3})(2e^{-3} - \omega_\mathrm{t})$
θ_ll	$[-0.2e^{-2}, 2e^{-2}]$	$g_{\mathrm{n},\theta_\mathrm{ll}} = (\theta_\mathrm{ll} + 0.2e^{-2})(2e^{-2} - \theta_\mathrm{ll})$
ω_ll	$[-1.5e^{-2}, 1.5e^{-2}]$	$g_{\mathrm{n},\omega_\mathrm{ll}} = (\omega_\mathrm{ll} + 1.5e^{-2})(1.5e^{-2} - \omega_\mathrm{ll})$
Ultimate limits		
ω_r	$[-\infty, 1.6]$	$g_{\mathrm{u},\omega_\mathrm{r}} = \omega_\mathrm{r} - 1.6$
θ_t	$[-7e^{-3}, 7e^{-3}]$	$g_{\mathrm{u},\theta_\mathrm{t}} = -(\theta_\mathrm{t} + 7e^{-3})(7e^{-3} - \theta_\mathrm{t})$
θ_ll	$[-6e^{-2}, 6e^{-2}]$	$g_{\mathrm{u},\theta_\mathrm{ll}} = -(\theta_\mathrm{ll} + 6e^{-2})(6e^{-2} - \theta_\mathrm{ll})$

5.2 Ellipsoid Barrier Certificate

Given the model description in the previous section, formulations for finding a barrier certificate can now be presented. The certificate will be of the structure

$$B = (\mathbf{x} - \mathbf{b})^\mathrm{T}\mathbf{E}(\mathbf{x} - \mathbf{b}) - 1. \tag{36}$$

Since the states have different orders of magnitude a weighted optimization criterion is chosen, i.e., $\min \mathbf{w}^\mathrm{T}$ diag $\mathbf{E}$. The weighting vector is chosen to be proportional to the width of the bounds on the normal operation.

Using Proposition 12 and the optimization criterion presented above, it is now possible to reformulate the problem as is shown in SOS Problem 1.

SOS Problem 1 Complete wind turbine system

$$\begin{aligned}
\min\ & \mathbf{w}^\mathrm{T} \operatorname{diag} \mathbf{E} \text{ over } \mathbf{E} \in \mathbb{R}^{6\times 6} \succeq 0,\ s_1, s_2, s_3 \in \Sigma_{1,2}, \\
& \mathbf{s}_\mathrm{n} \in \Sigma^6_{1,2},\ \mathbf{s}_\mathrm{x} \in \Sigma^2_{1,4},\ \mathbf{s}_\mathrm{d} \in \Sigma^2_{3,4} \\
\text{s.t.}\ & -B - \mathbf{s}_\mathrm{n}^\mathrm{T}\mathbf{g}_\mathrm{n} \in \Sigma \\
& B - \epsilon - s_1 g_{\mathrm{u},\omega_\mathrm{r}} \in \Sigma \\
& B - \epsilon - s_2 g_{\mathrm{u},\theta_\mathrm{t}} \in \Sigma \\
& B - \epsilon - s_3 g_{\mathrm{u},\theta_\mathrm{ll}} \in \Sigma \\
& -\boldsymbol{\nabla} B\mathbf{f} - \mathbf{s}_\mathrm{x}^\mathrm{T}\mathbf{g}_\mathrm{x} - \mathbf{s}_\mathrm{d}^\mathrm{T}\mathbf{g}_\mathrm{d} \in \Sigma
\end{aligned}$$

The resulting protection function was implemented and verified using the FAST simulator. Three cases have been tested; 1) normal operation, during which the wind turbine should not shut down, 2) generator failure, during which the generator power suddenly drops to zero due to a grid failure, and 3) pitch failure, one of the pitch controllers fails and one of the blades is pitched in the wind (emergency shutdown controllers are assumed to function). The supervisor shows the desired behavior in all three cases. Figure 4 depicts some simulation results for case 2.

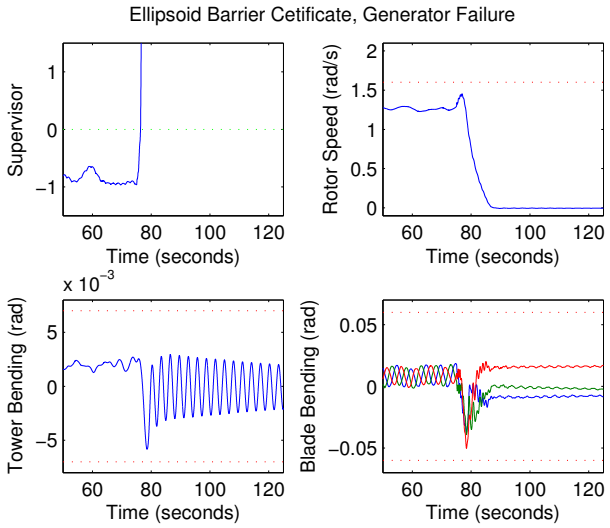

Fig. 4. State trajectories during generator failure

5.3 Compositional Barrier Certificate

Although the approach in the previous section is successful in finding a barrier certificate, during optimization of the code it was found that minor changes to the problem description might cause the solvers to run into numerical problems and no longer converge towards a proper solution. If additional safety properties need to be verified (requiring additional states), it is expected that this approach will no longer be computationally feasible. This section will demonstrate an alternative approach that will reduce the complexity of the SOS problem by dividing the system into subsystems. The model equations of (33) will be regrouped as follows:

Drive:

$$\dot{\omega}_\mathrm{r} = \frac{1-\xi}{J_\mathrm{r}}\tau_\mathrm{a}(w, \omega_r, \beta) + \frac{k_\mathrm{ll}}{J_\mathrm{r}}\theta_\mathrm{ll} - \frac{B_\mathrm{r}}{J_\mathrm{r}}\omega_\mathrm{r} - \frac{N}{J_\mathrm{r}}\tau_\mathrm{g} \tag{37a}$$

$$\dot{\beta} = 8 \tag{37b}$$

Tower:

$$\dot{\omega}_\mathrm{t} = \frac{L}{J_\mathrm{t}}F_\mathrm{a}(w, \omega_r, \beta) + \frac{mgL - k_\mathrm{t}}{J_\mathrm{t}}\theta_\mathrm{t} - \frac{B_\mathrm{t}}{J_\mathrm{t}}\omega_\mathrm{t} \tag{37c}$$

$$\dot{\theta}_\mathrm{t} = \omega_\mathrm{t} \tag{37d}$$

$$\dot{\beta} = 8 \tag{37e}$$

Blade:

$$\dot{\omega}_\mathrm{ll} = \frac{\xi}{J_\mathrm{ll}}\tau_\mathrm{a}(w, \omega_r, \beta) - \frac{B_\mathrm{ll}}{J_\mathrm{ll}}\omega_\mathrm{ll} - \frac{k_\mathrm{ll}}{J_\mathrm{ll}}\theta_\mathrm{ll} \tag{37f}$$

$$\dot{\theta}_\mathrm{ll} = \omega_\mathrm{ll} \tag{37g}$$

$$\dot{\beta} = 8 \tag{37h}$$

The blade pitch β is included in every subsystem, adding decision variables to the problem formulation. However, in this way less interconnections are required that would otherwise also introduce decision variables. Moreover, the chosen approach is less conservative.

In this case, an ellipsoid barrier certificate proofs to be too conservative and no such certificate could be found. Instead a third degree barrier certificate is synthesized. To increase $\operatorname{vol}\langle B\rangle$, the approach of Corollary 6 and Remark 1 is used, with

$$V_i = (\mathbf{x}_i - \mathbf{b}_i)^{\mathrm{T}}\mathbf{E}_i(\mathbf{x}_i - \mathbf{b}_i) \tag{38}$$

The resulting SOS formulation for the tower subsystem is presented in SOS Problem 2.

SOS Problem 2 Tower subsystem

$$\begin{aligned}
\min\ & -\lambda_\alpha\alpha_{\mathrm{t}} - \lambda_{\beta_{\mathrm{t}}}\beta_{\mathrm{t}} - (\lambda_{\beta_{\mathrm{d}}} + \lambda_{\beta_{\mathrm{ll}}})\beta_{\mathrm{R}} + \boldsymbol{\lambda}_\gamma^{\mathrm{T}}\mathbf{M}_{\mathrm{t}}\hat{\gamma}_{\mathrm{t}} \\
& + \lambda_{\mathrm{E}}\mathbf{w}_{\mathrm{t}}^{\mathrm{T}}\operatorname{diag}\mathbf{E}_{\mathrm{t}} \\
\text{over } & B_{\mathrm{t}} \in \mathcal{P}_{3,3},\ \mathbf{E}_{\mathrm{t}} \in \mathbb{R}^{3\times 3} \succeq 0,\ \alpha_{\mathrm{t}}, \beta_{\mathrm{t}}, \beta_{\mathrm{R}}, \hat{\gamma}_{\mathrm{t}} \in \mathbb{R} \\
& s_{\mathrm{u}}, s_{\mathrm{x}} \in \Sigma_{1,4},\ \mathbf{s}_{\mathrm{v}} \in \Sigma_{1,4}^2,\ \mathbf{s}_{\mathrm{n}} \in \Sigma_{1,2}^3,\ s_{\mathrm{d}} \in \Sigma_{3,4} \\
\text{s.t. } & -B_{\mathrm{t}} - \mathbf{s}_{\mathrm{n}}^{\mathrm{T}}\mathbf{g}_{\mathrm{n}} - \alpha_{\mathrm{t}} \in \Sigma \\
& V_{\mathrm{t}} - B_{\mathrm{t}} - \mathbf{s}_{\mathrm{v}}\mathbf{g}_{\mathrm{v}} \in \Sigma \\
& B_{\mathrm{t}} - \epsilon - s_{\mathrm{u}}g_{\mathrm{u},\theta_{\mathrm{t}}} - \beta_{\mathrm{t}} \in \Sigma \\
& B_{\mathrm{t}} - \epsilon - \beta_{\mathrm{R}} \in \Sigma \\
& -\boldsymbol{\nabla}B_{\mathrm{t}}\mathbf{f}_{\mathrm{t}} - s_{\mathrm{x}}g_\beta - s_{\mathrm{d}}g_{\mathrm{d}} + \hat{\gamma}_{\mathrm{t}}\omega_{\mathrm{r}}^2 \in \Sigma
\end{aligned}$$

The compositional SOS program is successful in computing a barrier certificate. Using the same test procedures as before, the safety supervisor is verified. The compositional safety supervisor succeeds in all three cases.

6. FURTHER WORK

By inspecting the turbine model and semi-algebraic set descriptions, we were able to decrease the number of variables and degree of the s-procedures. This led to a significant decrease in the number of decision variables so that the problem became computationally feasible. However, this reduction was done manually. It is desired to derive formal procedures and requirements so that the minimal degree of B and all s-procedures could be (automatically) determined for arbitrary model descriptions.

This work only focusses on the syntheses of a safety supervisor and assumes the shutdown procedures to be known and fixed. However, the methods presented could be used to compare alternatives or optimize parameters in the shutdown procedure itself. This could be done iteratively or directly during the computation of a safety envelope. Albeit, in the latter case (8c) is no longer linear in the optimization parameters and a different computational approach is required.

Finally, it should be noted that only very basic verification and testing was performed in this work. More elaborate testing and analysis is clearly required before such a safety supervisor would be implemented in real-life.

7. CONCLUSIONS

This work shows that a safety supervisor system can be synthesized and optimized using the barrier certificate framework. Successful implementations have been given for a NREL 5MW reference model using both an hyper-ellipsoid optimization as well as a compositional approach. It is expected that especially the last method could be applied to even more complex systems. This allows for more accurate models having advanced dynamics, the verification of additional safety criteria and/or the optimization of the emergency shutdown procedures. In conclusion, the methods derived in this paper are to be considered for implementation when designing safety systems for large-scale wind turbines.

REFERENCES

Boyd, S. and Vandenberghe, L. (2004). *Convex Optimization*. Cambridge University Press, New York, NY, USA.

Jarvis-Wloszek, Z.W. (2003). *Lyapunov Based Analysis and Controller Synthesis for Polynomial Systems Using Sum-of-squares Optimization*. Ph.D. thesis, University of California, Berkeley.

Johnson, K.E. and Fleming, P.A. (2011). Development, implementation, and testing of fault detection strategies on the national wind technology center's controls advanced research turbines. *Mechatronics*, 21(4), 728 – 736.

Jonkman, J., Butterfield, S., Musial, W., and Scott, G. (2009). Definition of a 5-mw reference wind turbine for offshore system development. Technical Report NREL/TP-500-38060, National Renewable Energy Laboratory.

Jonkman, J.M. (2012). Nwtc computer-aided engineering tools: Fast. URL `http://wind.nrel.gov/designcodes/simulators/fast/`.

Parrilo, P.A. (2003). Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming*, 96(2), 293–320.

Pedersen, A.S. and Steiniche, C.S. (2012). *Safe Operation and Emergency Shutdown of Wind Turbines*. Master's thesis, Aalborg University.

Prajna, S. and Jadbabaie, A. (2004). Safety verification of hybrid systems using barrier certificates. In *In Hybrid Systems: Computation and Control*, 477–492. Springer.

Prajna, S., Jadbabaie, A., and Pappas, G.J. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8), 1415–1429.

Sloth, C., Wisniewski, R., and Pappas, G. (2012a). On the existence of compositional barrier certificates. In *IEEE Conference on Decision and Control (CDC), 2012*, 4580–4585.

Sloth, C., Pappas, G.J., and Wisniewski, R. (2012b). Compositional safety analysis using barrier certificates. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, HSCC '12, 15–24. ACM, New York, NY, USA.

Tu, L. (2008). *An Introduction to Manifolds*, 127–133. Springer Science+Business Media, LLC.

Wisniewski, R., Svenstrup, M., Pedersen, A., and Steiniche, C. (2013). Certificate for safe emergency shutdown of wind turbines. In *American Control Conference (ACC), 2013*, 3667–3672.