2013 American Control Conference (ACC)
Washington, DC, USA, June 17-19, 2013

Certificate for Safe Emergency Shutdown of Wind Turbines*

Rafael Wisniewski, Mikael Svenstrup, Andreas Søndergaard Pedersen, and Christian Sigge Steiniche

***Abstract*— To avoid damage to a wind turbine in the case of a fault or a large wind gust, a detection scheme for emergency shutdown is developed. Specifically, the concept of a safety envelope is introduced. Within the safety envelope, the system can be shutdown without risking structural damage to the turbine. To demarcate the boundary of the safety envelope, a protection certificate, is computed. To this end, a model-based framework of barrier certificates is used. As a result, the protection certificate problem is formulated as a sum-of-squares program with the optimisation criterion related to the volume of the safety envelope. The framework enables the inclusion of a bounded wind disturbance and the a priori known emergency shutdown procedure. For this purpose, the model of a wind turbine is developed that includes structural safety critical components.**

I. INTRODUCTION

By and large, this work aims at providing a protection mechanism, which ensures that the wind turbine avoids excessive structural loads by initiating a timely shutdown. Specifically, the protection system takes over and shuts down the turbine when the wind, a controller or an actuator behaves in a way that can damage the wind turbine.

In particular, the goal is to find out when to initiate a shutdown of the turbine in order not to break it down. This entails that specific states of the turbine must not exceed a specific maximal value during shutdown. This is illustrated by a two dimensional example in Fig. 1. The white area X_{A} is the set of admissible states. Accordingly, $X_{\mathrm{A}}^{\mathrm{c}}$, the complement of X_{A}, consists of states where a damage of a wind turbine can happen. The green area is the region of normal operation. The red curve exemplifies a shutdown trajectory; the shutdown is initiated at t_0, when the state trajectory exits the safety envelope X_D. Explicitly, the shutdown trajectory is a solution of the wind turbine equations of motion with the specific shutdown controller (not the nominal controller). The aim of the work is to find the safety envelope X_{D}, which is the set of all initial states of the shutdown trajectories that never exits X_{A}. Obviously, finding the set X_{D} might not be tangible. Nonetheless, a successful method relying on the computation of the invariance kernel has been developed for planar systems [1].

The problem studied in this paper is relaxed by the task of finding a subset X'_{D} of X_{D}, maximal with respect to a certain criterion discussed in Section IV. Since $X'_{\mathrm{D}} \subseteq X_{\mathrm{D}}$ the turbine will also be safe by using X'_{D} as a safety envelope. Specifically, the set X'_{D} is defined as a sub-level set of a function, dubbed a *protection function*. In conclusion, the protection function determines the time of shutdown that ensures that the shutdown trajectory stays within X_{A} during shutdown. To pronounce the resemblance between the above problem and the barrier certificate problem [2], we will call the task of finding a protection function - *a protection certificate problem*.

*This work was supported by Vestas Wind Systems A/S

The authors are with Department of Electronic Systems, Automation and Control, Aalborg University, Denmark; {raf, ms} at es.aau.dk, asped at elektro.dtu.dk, steiniche at gmail.com

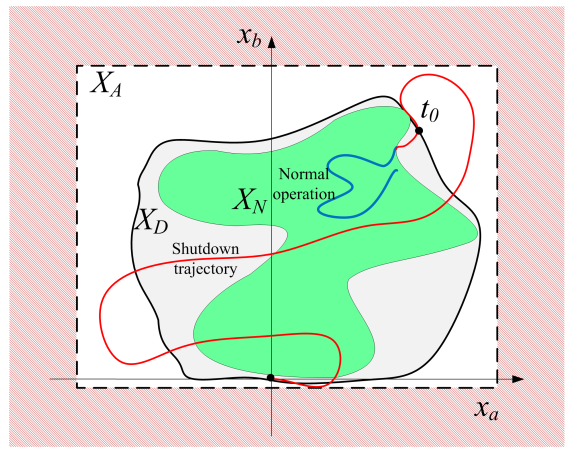

Fig. 1: A 2-D illustration of the protection certificate problem. The normal operation set X_N is shown as the green area. The white area, X_{A}, is the admissible set, i.e., the set of points where the turbine is not damaged. An appropriate multidimensional detection limit X_D will enable timely shutdown of the turbine, such that the trajectory is kept inside X_A. The states x_a, x_b are not meant to resemble any specific states. The examples of these states could be blade bending and rotor speed.

A popular solution to the protection certificate problem known in the wind industry is to monitor the rotational speed of the turbine and shutdown if some predefined threshold is exceeded. Nonetheless, for newer and larger turbines, it is anticipated that it will also be necessary to look at multiple states, which is the aim of this paper.

The results in this paper lean on the concept of a barrier certificate. It was formulated in [2] and extended in the context of safety verification with disturbances in [3]. A polynomial barrier certificate that separates the initial set X_{D} from the unsafe set $X_{\mathrm{A}}^{\mathrm{c}}$, should satisfy a range of conditions which can be stated as polynomial equalities and inequalities. These conditions can be transformed using the Positivstellensatz [4]. The Positivstellensatz states a relationship between a semi-algebraic set, and the existence of a certain polynomial [5]. The conditions of the barrier certificate can be satisfied if a solution to such a polynomial identity can be found.

To examine if such a polynomial identity exists, the sum of squares (SOS) framework can be used [6]. Indeed, [6] shows how a sum of squares decomposition can be computed using semidefinite programming (SDP). Consequently, the search of a sum of squares decomposition becomes numerically tractable. In [7], the safety verification with barrier certificates is divided into subproblems with interconnections, which can be solved independently. Using this approach, the computational requirements are reduced [7].

The rest of the paper is organised as follows. Section II lists the nomenclature used in this paper. The problem of finding protection certificates is formulated in Section III. A method for computing protection certificates is developed in Section IV. Protection certificates are used to determine the safety envelope of a wind turbine in Section V.

II. Nomenclature

We use the following notations. For $k \in \mathbb{N}$, $\mathbf{k} = \{1, \ldots, k\}$. The set of nonnegative reals is denoted by $\mathbb{R}_+$, the set of nonnegative integers by $\mathbb{Z}_+$, and the set of natural numbers by $\mathbb{N}$. For a subset $B \subseteq A$, B^c denotes the complement of B in A. For open subsets $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^m$, and a nonnegative integer r, $C^r(U,V)$ denotes the set of C^r smooth maps from U to V.

The polynomials with real valued variables are denoted by $\mathcal{P}_n$ and $\mathcal{P}_n^m$ is a vector of m polynomials. A polynomial $p \in \mathcal{P}_n$ is a 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 of polynomials in n variables is denoted by Σ_n, with Σ_n^m a vector of m Σ_n-polynomials. We shall also use the set of polynomials in $\mathcal{P}_n$ of degree k,

$$\mathcal{P}_n(k) = \{p \in \mathcal{P}_n | \ \deg(p) = k\}.$$

The set of quadratic forms in n variables (homogeneous polynomials in $\mathcal{P}_n$ of degree 2) is denoted by $\mathcal{Q}_n$.

III. Problem Formulation

In this study, we have used the NREL 5MW reference wind turbine [8]. We will not present the model of a wind turbine in full [9]. Nonetheless, the model of the drive train and blade pitching is expounded in Subsection V-C for experimental study. The full analytical model used has been verified against FAST simulations of the NREL 5MW turbine. Furthermore, in Table I, we have listed the states in the description of the wind turbine used in this work, and in Table II the load limits of the system states.

In an abstract way, we define a wind turbine model during the shutdown,

$$\dot{x} = f(x, w), \ x(t_0) = x_0, \tag{1}$$

where $f : \mathbb{R}^n \times W \to \mathbb{R}^n$ with $W \subseteq \mathbb{R}^m$. The subset W is the set of credible disturbances, i.e., $w(t) \in W$ for all $t \in \mathbb{R}_+$. We suppose that f is well-defined. Note that this is the model describing turbine shutdown. Therefore the input, like e.g. blade pitch, is not regulated by a controller but predetermined and built into the model. We denote the

States	Symbol	Unit
Drive train		
Rotor angular velocity	ω_{r}	rad/s
Generator angular velocity	ω_{g}	rad/s
Drive train torsion angle	θ_{Δ}	rad
Flapwise blade bending		
Flapwise blade tip velocity	${}^{\mathrm{h}}v_{\mathrm{flap,x}}$	m/s
Flapwise blade tip displacement	${}^{\mathrm{h}}x_{\mathrm{flap}}$	m
Lead-lag blade bending (edgewise)		
Lead-lag blade tip angular velocity	${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}$	rad/s
Lead-lag blade tip angle	${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}$	rad
Tower		
Tower fore-aft angular velocity	${}^{\mathrm{t}}\omega_{\mathrm{fa,y}}$	rad/s
Tower fore-aft angle	${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$	rad
Blade-pitch actuator system		
Blade-pitch angular velocity	ω_{β}	rad/s
Blade-pitch angle	θ_{β}	rad
Wind model		
Wind turbulence component 1	$v_{\mathrm{w,t1}}$	m/s
Wind turbulence component 2	$v_{\mathrm{w,t2}}$	m/s

TABLE I: States of the wind turbine model.

State	Limit	Value
ω_{r}	$\gamma_{\mathrm{r}} = 2.025$ rad/s	$(-\infty\ ;\ \gamma_{\mathrm{r}}]$
θ_{Δ}	$\gamma_{\Delta} = 441.42 \cdot 10^{-3}$ rad	$[-\gamma_{\Delta}\ ;\ \gamma_{\Delta}]$
${}^{\mathrm{h}}x_{\mathrm{flap}}$	$\gamma_{\mathrm{flap}} = 11.57$ m	$[-\gamma_{\mathrm{flap}}\ ;\ \gamma_{\mathrm{flap}}]$
${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}$	$\gamma_{\mathrm{LL}} = 26.00 \cdot 10^{-3}$ rad	$[-\gamma_{\mathrm{LL}}\ ;\ \gamma_{\mathrm{LL}}]$
${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$	$\gamma_{\mathrm{fa}} = 9.54 \cdot 10^{-3}$ rad	$[-\gamma_{\mathrm{fa}}\ ;\ \gamma_{\mathrm{fa}}]$

TABLE II: Load limits of the system states

solution of the Cauchy problem (1) for a disturbance $w : \mathbb{R}_+ \to W$ by $\phi^w(x_0, t)$. As explained in Introduction, the set X_A is the admissible state space. We suppose that the state-constraints are of the type $g(x) \geq 0$ for $g : \mathbb{R}^n \to \mathbb{R}$ (as a minimum g shall be a continuous function). In other words, each system solution $\phi^w(x_0, t)$ with $x_0 \in X_D$ should belong to the set $X_A \equiv \bigcap_{i=1}^p V_i$ with $V_i = \{x \in \mathbb{R}^n | \ g_i(x) \geq 0\}$. Specifically in our case study, the set X_{A} is defined by the load limits in Table II.

Definition 1 (Maximal Safety)**.** *Let $f : \mathbb{R}^n \times W \to \mathbb{R}^n$ with $W \subseteq \mathbb{R}^m$ be Lipschitz continuous. Let X_{A} be a subset of the state space $\mathbb{R}^n$. We say that $X_{\mathrm{D}} \subseteq \mathbb{R}^n$ is safe (for the pair (X_{A}, f)) if for all $x_0 \in X_{\mathrm{D}}$ and $w : \mathbb{R}_+ \to W$ (Lebesgue) measurable, $\phi^w(x_0, t) \in X_{\mathrm{A}}$ for all $t \in \mathbb{R}_+$.*
We say that X_{D} is maximal safe set (for the pair (X_{A}, f)) if it is safe and whenever there is a safe set X'_{D}, then $X'_{\mathrm{D}} \subseteq X_{\mathrm{D}}$.

Let $\mathcal{G}$ be a family of functions on $\mathbb{R}^n$. We denote by $\langle \mathcal{G} \rangle$ the intersection of 0-sublevel sets of the functions in $\mathcal{G}$,

$$\langle \mathcal{G} \rangle = \{x \in \mathbb{R} | \ g(x) \leq 0 \text{ for all } g \in \mathcal{G}\}.$$

The volume of $\langle \mathcal{G} \rangle$ is denoted by $\mathrm{vol}\,\langle \mathcal{G} \rangle$,

$$\mathrm{vol}\,\langle \mathcal{G} \rangle = \int_{\langle \mathcal{G} \rangle} dx.$$

Definition 2 (Relaxed Maximal Safety)**.** *Let $f : \mathbb{R}^n \times W \to \mathbb{R}^n$, and let X_{A} be a subset of the state space $\mathbb{R}^n$. Suppose that $\mathcal{G}$ is a family of functions. We say that $\{g_1, \ldots, g_k\} \subseteq \mathcal{G}$ is k-maximal safe in $\mathcal{G}$ if*

1) *$\langle g_1, ..., g_k \rangle \equiv \langle \{g_1, ..., g_k\} \rangle$ is safe, and*

2) *if there is* $\{g'_1, ..., g'_k\} \subseteq \mathcal{G}$ *such that* $\langle g'_1, ..., g'_k \rangle$ *is safe then* $\mathrm{vol}\,\langle g'_1, ..., g'_k \rangle \leq \mathrm{vol}\,\langle g_1, ..., g_k \rangle$.

In the following, we will study 1-maximal safety in the family of quadratic functions or polynomials of degree up to d.

To this end, we recall the concept of a barrier certificate from [2]. For the subsets X_N and X_A of $\mathbb{R}^n$, a continuously differentiable function B that satisfies the conditions:

$$B(x) \leq 0 \quad \forall x \in X_\mathrm{N} \tag{2a}$$

$$B(x) > 0 \quad \forall x \in X_\mathrm{A}^c \tag{2b}$$

$$\tfrac{\partial B}{\partial x}(x) f(x,w) \leq 0 \quad \forall (x,w) \in B^{-1}(0) \times W \tag{2c}$$

is called a *barrier certificate* (for the triple $(X_\mathrm{N}, X_\mathrm{A}^c, f)$). If there exists a barrier certificate then the set X_N (in fact also $\langle B \rangle$) is safe for the pair (X_A, f). In essence, the barrier certificate is a function that is negative over the safe set and positive over the unsafe set (by (2a) and (2b)). Furthermore, by (2c), the derivative along the flow of the system, where $B(x) = 0$, is negative or zero. This means that the system can never cross this "barrier" where $B(x) = 0$ and thus $B(x(t)) \leq 0\ \forall t$, which means that the system will never be unsafe.

If the set $B^{-1}(0) \times W$ in the universal quantifier of (2c) is replaced by the set $X \times W$, where X is the state space, the function B will be called a *weak barrier certificate*.

Let $\mathcal{B}$ be the set of all barrier certificates. For a subset $\mathcal{G} \subseteq C^1(\mathbb{R}^n, \mathbb{R})$, we define $\mathcal{B}_\mathcal{G} = \mathcal{B} \cap \mathcal{G}$.

We are in place to formulate the problem studied in this paper. For a $b \in \mathbb{R}^n$, let $\mathcal{Q}_n(b)$ denote the set of the functions of the form

$$g := g_Q : \ \mathbb{R}^n \to \mathbb{R};\ x \mapsto (x-b)^\mathrm{T} Q^{-1} (x-b) - 1 \tag{3}$$

with a positive definite matrix Q.

We strive to find $g \in \mathcal{B}_{\mathcal{Q}_n(b)}$ such that the volume of its 0-sublevel set is maximal, i.e.,

$$g = \arg \max_{h \in \mathcal{B}_{\mathcal{Q}_n(b)}} \mathrm{vol}\,\langle h \rangle, \tag{4}$$

which means g is 1-maximal safe in $\mathcal{B}_{\mathcal{Q}_n(b)}$. We shall call the function g in (4) a *protection certificate* (for the triple $(X_\mathrm{N}, X_\mathrm{A}, f)$). The 0-level set of g can then be used as the detection limit X_D in Fig. 1.

IV. Computation of Protection Certificates

To find a protection certificate, we re-formulate the problem of computing the protection certificate (4) to an SOS program, which will be described briefly in this section.

A. SOS Programming

By [10], a polynomial p of degree $2d$ belongs to Σ_n if and only if there exist a positive semi-definite matrix P and a vector of monomials Z which contains all monomials of x of degree $\leq d$ such that $p(x) = Z^\mathrm{T}(x) P Z(x)$.

The existence of an SOS decomposition of a polynomial can be expressed as an SDP feasibility problem. Therefore, the formulation of a problem as an SOS makes the problem computationally tractable.

Proposition 1 ([11]). *Given a finite set* $\{p_i \in \mathcal{P}_n\}_{i \in \mathbf{m}}$, *the existence of a set of scalars* $\{a_i \in \mathbb{R}\}_{i \in \mathbf{m}}$ *such that*

$$p_0 + \sum_{i=1}^{m} a_i p_i \in \Sigma_n \tag{5}$$

is a Linear Matrix Inequality (LMI) feasibility problem.

In summary, we strive to formulate a protection certificate problem as an SOS program. In detail, let $k, l \in \mathbb{N}$, let $\alpha_{i,0}$ and $\alpha_{i,j} \in \mathcal{P}_n$ for $(i,j) \in \mathbf{l} \times \mathbf{k}$, and let $w_j \in \mathbb{R}$. An SOS program is the problem

$$\arg \min_{(c_1,\ldots,c_k) \in \mathbb{R}^k} \sum_{j=1}^{k} w_j c_j \quad \text{subject to}$$

$$\alpha_{i,0} + \sum_{j=1}^{k} \alpha_{i,j} c_j \in \Sigma_n,\ \forall i \in \mathbf{l}. \tag{6}$$

As explained above, such a problem can be effectively solved by means of SDP.

B. Certificates for Positiveness

The next task is to convert the problem of existence of a polynomial barrier certificate to SOS programming. The subsequent proposition formalizes the problem of constrained positivity of polynomials, which is a direct result of applying Positivstellensatz.

Proposition 2 ([12]). *Let* $\{a_i\}_{i \in \mathbf{k}}$ *and* $\{b_i\}_{i \in \mathbf{l}}$ *belong to* $\mathcal{P}_n$, *then*

$$p(x) \geq 0 \qquad \forall x \in \mathbb{R}^n : a_i(x) = 0,\ \forall i = 1,2,...,k \quad \textit{and} \quad b_j(x) \geq 0,\ \forall j = 1,2,...,l \tag{7}$$

is satisfied, if the following holds

$$\exists r_1, r_2, \ldots, r_k \in \mathcal{P}_n \quad \textit{and} \quad \exists s_0, s_1, \ldots, s_l \in \Sigma_n \quad \textit{such that}$$

$$p = \textstyle\sum_{i=1}^{k} r_i a_i + \sum_{i=1}^{l} s_i b_i + s_0. \tag{8}$$

The following observation will be instrumental. A polynomial $p \in \mathcal{P}_n$ is strictly positive ($p(x) > 0 \quad \forall x \in \mathbb{R}^n$), if there exists a $\epsilon > 0$ such that

$$\big(p(x) - \epsilon\big) \in \Sigma_n. \tag{9}$$

C. Polynomial Barrier Certificates $B_{\mathcal{P}_n}$

To compute barrier certificates using SOS programming, we restrict the vector fields to be polynomial. Furthermore, the admissible set and the normal operation set will be semialgebraic sets, i.e., they will be given by polynomial inequalities. Let $g_\mathrm{N} : \mathbb{R}^n \to \mathbb{R}^{k_\mathrm{N}}$, $g_\mathrm{A} : \mathbb{R}^n \to \mathbb{R}^{k_\mathrm{A}}$, $g_W : \mathbb{R}^m \to \mathbb{R}^{k_W}$, and $g_\mathrm{X} : \mathbb{R}^n \to \mathbb{R}^{k_\mathrm{X}}$, for some $k_{X_\mathrm{N}}, k_{X_\mathrm{A}}, k_X, k_W \in \mathbb{N}$, be vectors of polynomials with coordinate functions $g_i \in \mathcal{P}_n$; for example, $g_\mathrm{N} = (g_1, \ldots, g_{k_\mathrm{N}}) \in \mathcal{P}_n^{k_\mathrm{N}}$. Then

$$X_\mathrm{N} \equiv \{x \in \mathbb{R}^n | g_\mathrm{N}(x) \geq 0\}, \tag{10a}$$

$$X_\mathrm{A}^c \equiv \{x \in \mathbb{R}^n | g_\mathrm{A}(x) \geq 0\}, \tag{10b}$$

$$W \equiv \{w \in \mathbb{R}^m | g_W(w) \geq 0\}, \tag{10c}$$

$$X \equiv \{x \in \mathbb{R}^n | g_\mathrm{X}(x) \geq 0\}, \tag{10d}$$

where X is the considered domain of the state space and the inequalities in (10) are satisfied coordinate-wise.

By Proposition 2, we can characterise the set $B_{\mathcal{P}_n}$ using the sum of squares.

Proposition 3. *A polynomial $B \in \mathcal{P}_n$ is a barrier certificate for the triple $(X_\mathrm{N}, X_\mathrm{A}^c, f)$ if there exist $\epsilon_1, \epsilon_2 > 0$, $B \in \mathcal{P}_n$, $s_\mathrm{N} \in \Sigma_n^{k_\mathrm{N}}$, $s_\mathrm{A} \in \Sigma_n^{k_\mathrm{A}}$, $s_\mathrm{X} \in \Sigma_n^{k_\mathrm{X}}$, and $s_W \in \Sigma_m^{k_W}$ such that*

$$- B - s_\mathrm{N}^\mathrm{T} g_\mathrm{N}, \tag{11a}$$

$$B - \epsilon_1 - s_\mathrm{A}^\mathrm{T} g_\mathrm{A}, \text{ and} \tag{11b}$$

$$- \frac{\partial B}{\partial x} f - \epsilon_2 - s_W^\mathrm{T} g_W - s_X^\mathrm{T} g_X \tag{11c}$$

are sum of squares.

In conclusion, by Proposition 2, (11a)-(11c) satisfies each condition in (2a)-(2c). Whether a polynomial B satisfies the conditions (11) is a feasibility problem in SOS programming as specified by (6).

We shall denote the set of all polynomials satisfying (11) by $\bar{\mathcal{B}}_{\mathcal{P}_n}$. It follows from Proposition 3 that $\bar{\mathcal{B}}_{\mathcal{P}_n} \subseteq \mathcal{B}_{\mathcal{P}_n}$.

D. Maximum Volume of Ellipsoid

The last ingredient necessary to compute the protection certificate (4) is the calculation of the volume of an ellipsoid.

Let $g_Q \in \mathcal{Q}_n(b)$, then the volume of the ellipsoid $\langle g_Q \rangle$ is

$$\mathrm{vol}\,\langle g_Q \rangle = \frac{4}{3}\pi\sqrt{\det(Q)}.$$

Hence, the volume of an ellipsoid can be maximised by maximising $\det(Q)$. Nonetheless, this is a nonlinear optimisation problem. [13] shows that introducing $\log\det(Q)$ makes the maximum volume problem convex. The resulting optimisation problem becomes

$$\begin{aligned} &\max\ \log\det(Q) \\ &\text{s.t. } Q \succ 0,\ \langle g_Q \rangle \subseteq \langle B \rangle,\ B \in \bar{\mathcal{B}}_{\mathcal{P}_n}, \end{aligned} \tag{12}$$

where $Q \succ 0$ signifies that Q is positive definite. According to Proposition 2, if there is $s_Q \in \Sigma_n$ such that

$$-B(x) + s_Q\left((x-b)^\mathrm{T} Q^{-1}(x-b) - 1\right) \in \Sigma_n \tag{13}$$

then $\langle g_Q \rangle \subseteq \langle B \rangle$.

The volume maximisation (12) is not linear; although, it is convex. We strive to solve the above problem by means of SDP. Therefore, we will replace the volume of an ellipse by a linear substitute.

At the outset, observe that the volume of an ellipsoid is proportional to the product of magnitudes of its semi-principal axes. This is because the eigenvalues of Q are equal to the squares of the semi-principal axes. To relax the nonlinear problem of finding the maximum volume over ellipsoids, the linear problem of maximum sum of the semi-principal axes squared, i.e., the sum of the eigenvalues of Q, is considered.

Recall that for an ellipsoid g_Q, the sum of the eigenvalues of Q is equal to the trace of Q. By replacing the trace of Q with the trace of Q^{-1}, the maximisation of the semi-principal axes is stated as a minimisation problem:

$$\begin{aligned} &\min\ \mathrm{Tr}\ \mathrm{Q}^{-1} \\ &\text{s.t. } Q \succ 0,\ B \in \bar{\mathcal{B}}_{\mathcal{P}_n},\ \langle g_Q \rangle \subseteq \langle B \rangle. \end{aligned} \tag{14}$$

The above optimisation problem is linear in the objective, thus indeed corresponds to SDP.

In conclusion, the above objective of minimising the sum of magnitudes of the semi-principal axes is not identical to the objective of volume maximisation. However, the trace of Q^{-1} does provide a similar measure and can directly be used in SDP.

V. Implementation

In our terminology, the ellipsoid $\langle g_Q \rangle = \{x \in \mathbb{R}^n |\ x^\mathrm{T} Q^{-1} x - 1 \leq 0\} \subseteq X_\mathrm{A}$ with the positive definite matrix Q of maximal trace is called a *safety envelope*. A *protection certificate* is a function B that satisfies the optimisation problem (14).

A. Safety Envelope for Complete Wind Turbine

The complete polynomial model of the examined wind turbine with emergency shutdown procedure as described in Section III includes 13 states with polynomial degree 12. Driving turbulence noise is regarded as a disturbance. The high polynomial degree of the model is due to the degree of the polynomials representing aerodynamic coefficients, C_p and C_t.

Using the formulation of a weak barrier certificate, the search for a wind turbine safety envelope is stated as demonstrated in Section IV. The SOS programming for the safety envelope, given the complete wind turbine system and the trace safety envelope optimisation criterion, is formulated in SOS Program 1.

SOS Program 1 Complete wind turbine system

$\min \mathrm{Tr}\, Q^{-1}$

over $B \in \mathcal{P}_{13},\ Q \in S_+(13)$,

$s_1, s_2, s_3, s_4, s_5, s_6 \in \Sigma_{\mathbf{13}},\ s_{\mathrm{X,D}} \in \Sigma_{14}^{14}$

s.t. $B - s_1(\omega_\mathrm{r} - \gamma_\mathrm{r}) \in \Sigma_{13}$

$B - s_2({\theta_\Delta}^2 - {\gamma_\Delta}^2) \in \Sigma_{13}$

$B - s_3({}^\mathrm{h}{x_\mathrm{flap}}^2 - {\gamma_\mathrm{flap}}^2) \in \Sigma_{13}$

$B - s_4({}^\mathrm{h}{\theta_\mathrm{LL,x}}^2 - {\gamma_\mathrm{LL}}^2) \in \Sigma_{13}$

$B - s_5({}^\mathrm{t}{\theta_\mathrm{fa,y}}^2 - {\gamma_\mathrm{fa}}^2) \in \Sigma_{13}$

$- B + s_6 g_Q \in \Sigma_{13}$

$- \dfrac{\partial B}{\partial x} f - s_\mathrm{X,D}^\mathrm{T} g_\mathrm{X,D} \in \Sigma_{14}$

where

$S_+(n)$ is the set of $n \times n$ positive definite matrices, and

$g_Q(x) = x^\mathrm{T} Q^{-1} x - 1$.

In SOS Program 1, f is the wind turbine system, B is the protection certificate, Q is the matrix defining the safety envelope, $\{\gamma_{\mathrm{r}},\ \gamma_{\Delta},\ \gamma_{\mathrm{flap}},\ \gamma_{\mathrm{LL}},\ \gamma_{\mathrm{fa}}\}$ are the load limits of the chosen states, and $g_{\mathrm{X,W}} = (g_{\mathrm{X}}, g_{\mathrm{W}}) \in \mathcal{P}_{14}^{13} \times \mathcal{P}_{14}$ is a vector of polynomials defining the state space and disturbance set

$$\{(x, w) \in \mathbb{R}^{13} \times \mathbb{R} |\ g_{\mathrm{X}}(x) \leq 0,\ g_{\mathrm{W}}(w) \leq 0\}. \tag{15}$$

The bounded wind disturbance and bounded state space are defined as elements in the set (15). Relating to the illustration in Fig. 1, the load limits are given by the admissible set X_A and either $\langle g_Q \rangle$ or $\langle B \rangle$ can be used as detection limit X_D since $\langle g_Q \rangle \subseteq \langle B \rangle$.

As the model f is of relative high dimension and the degrees of the polynomials are at the same time relatively high, the SOS program becomes very complex. A single constraint such as $s_1 \in \Sigma_{13}$ generates a matrix inequality $P_1 \succeq 0$; with 13 states and polynomial degree $2d = 12$, the size of P_1 becomes

$$\binom{n+d}{d} \times \binom{n+d}{d} = 27132 \times 27132. \tag{16}$$

With 64 bit double representation of the elements in MATLAB this requires 5.9 GB of memory. Furthermore, a decision matrix of this size has 5.2 million decision variables.

In the following, the problem is divided into subproblems, which are solved individually [7].

B. Safety Envelopes of Separate Subsystems

The model is divided into subsystems which are studied individually. As the subsystems are examined separately the interconnections between the subsystems are not directly included in the calculation of the safety envelopes. Interconnections which are considered essential are introduced as unknown bounded disturbances to a given subsystem.

The complete model is divided into the following subsystems: the drive train and blade-pitching, the tower top bending, the flapwise blade bending, and the lead-lag blade bending. The drive train and blade-pitching subsystem includes the drive train, blade-pitch model and the aerodynamic properties of the rotor.

The subsystems and their interconnections are illustrated in Fig. 2. The interconnections are indicated by arrows between the involved subsystems. The solid arrow is the real wind disturbance, the curly arrows - the fictitious disturbances (as replacements for the interconnections), and the dashed arrows - the interconnections, which are neglected.

C. Illustration - Drive Train and Blade Pitching

In the following, the drive train and blade-pitching subsystem will be called the *drive train* for short. The states of the drive train are $x_{\mathrm{r}} = (\omega_{\mathrm{r}},\ \omega_{\mathrm{g}},\ \theta_{\Delta},\ \theta_{\beta},\ \omega_{\beta})$. This subsystem incorporates the emergency shutdown procedure through the blade-pitch model and the aerodynamic functions and is thus the most complex of the subsystems. The drive train is in the complete wind turbine in Fig. 2 connected to the lead-lag bending of the blades and tower top velocity. The lead-lag bending of the blades affects the rotor torque; whereas, the tower top velocity influences the wind speed experienced by the rotor. These interconnections after the separation of subsystems are not included in the following drive train model. The drive train subsystem $\dot{x}_{\mathrm{r}} = f^{\mathrm{r}}(x_{\mathrm{r}}, w)$ is

$$\begin{aligned}
\dot{\omega}_{\mathrm{r}} &= J_{\mathrm{r}}^{-1} \left[\tau_{\mathrm{aero}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - K_{\mathrm{a}}\theta_{\Delta} - B_{\mathrm{a}}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})\right] \\
\dot{\omega}_{\mathrm{g}} &= J_{\mathrm{g}}^{-1} \left[K_{\mathrm{a}}N\theta_{\Delta} + B_{\mathrm{a}}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}) - B_{\mathrm{g}}\omega_{\mathrm{g}}\right] \\
\dot{\theta}_{\Delta} &= \omega_{\mathrm{r}} - N\omega_{\mathrm{g}} \\
\dot{\theta}_{\beta} &= \omega_{\beta} \\
\dot{\omega}_{\beta} &= -0.6\omega_{\beta} - 0.0894\theta_{\beta}
\end{aligned} \tag{17}$$

with $\tau_{\mathrm{aero}} = \frac{1}{2}\rho A R {v_{\mathrm{w}}}^2 C_{\mathrm{q}}(v_{\mathrm{w}}, \omega_{\mathrm{r}}, \beta)$ and $\beta = -\theta_{\beta} + 90$. $J_{r,g}$ is rotor and generator inertia respectively, $B_{r,a,g}$ are friction constants, N is the gear ratio and K_a is the drive train torsional stiffness. The state space X, unsafe set X_{A}^{c} and disturbance set W of the drive train subsystem are

$$\begin{aligned}
X &= \left\{ x_{\mathrm{r}} \in \mathbb{R}^5 \;\middle|\; \begin{array}{c} 0.5 \text{ rad/s} \leq \omega_{\mathrm{r}} \leq 3 \text{ rad/s}, \\ 0.5 \cdot 97 \text{ rad/s} \leq \omega_{\mathrm{g}} \leq 3 \cdot 97 \text{ rad/s}, \\ -0.5 \text{ rad} \leq \theta_{\Delta} \leq 0.5 \text{ rad}, \\ 0^\circ \leq \theta_{\beta} \leq 90^\circ, \\ -20^\circ/\text{s} \leq \omega_{\beta} \leq 20^\circ/\text{s} \end{array} \right\} \\
X_{\mathrm{A}}^{\mathrm{c}} &= \{x_{\mathrm{r}} \in X |\ \omega_{\mathrm{r}} - \gamma_{\mathrm{r}} \geq 0\} \cup \left\{x_{\mathrm{r}} \in X |\ {\theta_{\Delta}}^2 - {\gamma_{\Delta}}^2 \geq 0\right\} \\
W &= \{v_{\mathrm{w}} \in \mathbb{R} |\ 15 \text{ m/s} \leq v_{\mathrm{w}} \leq 25 \text{ m/s}\},
\end{aligned} \tag{18}$$

where γ_{r} is the load limit of the rotor velocity and γ_{Δ} the load limit of the drive train torsion.

The state space in the analysis has been limited such that the rotational speed of the rotor is considered in the interval [0.5 rad/s, 3 rad/s]; and because of the gearing, the rotational speed of the generator is examined in the interval [$0.5 \cdot 97$ rad/s, $3 \cdot 97$ rad/s]. Consequently, it is assumed that the wind turbine cannot become unsafe when the rotor angular velocity is below 0.5 rad/s. Additionally, it is assumed that the blade-pitch angle θ_{β} is limited to the interval $[0^\circ, 90^\circ]$. The wind disturbance is bounded such that it can only take values in the range 15 m/s to 25 m/s. To find a safety envelope of the drive train, the technique developed in Section IV is used to transform the safety envelope optimisation into an SOS Program 2.

Likewise, the procedure demonstrated above has been used for the three remaining subsystems in Fig. 2.

SOS Program 2 Drive train subsystem

$$\begin{aligned}
&\min \operatorname{Tr} Q^{-1} \\
&\qquad \text{over } B \in \mathcal{P}_5,\ Q \in S_+(5),\ s_1, s_3 \in \Sigma_5,\ s_{\mathrm{X,D}} \in \Sigma_6^6 \\
&\text{s.t. } B - s_1(\omega_{\mathrm{r}} - \gamma_{\mathrm{r}}) \in \Sigma_5 \\
&\qquad B - s_3({\theta_{\Delta}}^2 - {\gamma_{\Delta}}^2) \in \Sigma_5 \\
&\qquad - B + s_6 g_Q \in \Sigma_5 \\
&\qquad - \frac{\partial B}{\partial x_{\mathrm{r}}} f^{\mathrm{r}} - s_{\mathrm{X,D}}^{\mathrm{T}} g_{\mathrm{X,D}}^{\mathrm{r}} \in \Sigma_6.
\end{aligned}$$

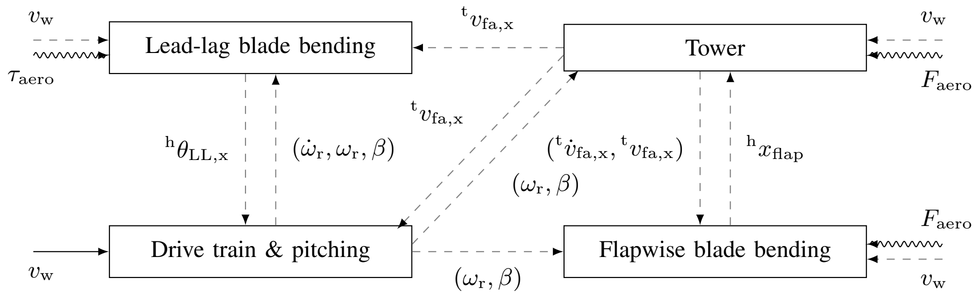

Fig. 2: The four separate subsystems are illustrated by boxes. The solid arrow is the real wind disturbance, the curly arrows the fictitious disturbances and the dashed arrows the interconnections which are neglected. ${}^{t}v_{fa,x}$ is the forward velocity of the tower, which can be calculated from the tower angular velocity state and the length of the tower: ${}^{t}v_{fa,x} = L\,{}^{t}\omega_{fa,y}$.

VI. Discussion

To use this method on a real wind turbine, there are some additional considerations to be made. For example, the safety envelope in the illustrational example above, is calculated using a limited wind range and rotor speed. For a real turbine, the full range of possible wind velocities and rotor speed would have to be included. It would be straightforward to include this. However, a larger disturbance range will inevitably lead to a smaller safety envelope.

The operational control of the wind turbine in power production mode is divided into regions determined by the wind speed. In order to cover normal operation, it is beneficial or even necessary to design a safety envelope specifically to each region of the operational controller. In the end it will be an "engineering tradeoff" to choose the disturbance range and number of operational regions. It is not the aim of this paper to evaluate further on implementation of specific tradeoff's.

Another assumption in the above example, is that all states are available, either measured or estimated. This might not always be the case. A smaller number of sensors will also lead to less certainty about the turbine state, and thereby a smaller safety envelope. Selection of the number of states for the use in the safety certificate is also an "engineering tradeoff", and the developed method provides the optimised safety envelope with the given sensors.

The computational complexity of the developed method is relatively high as described in Section V-A. However, it should be noted that it is essential to separate offline and online computational complexity. Online complexity should be very low, since it is necessary for the turbine to check the safety at each time step. This complies well with the developed method, since checking safety only requires evaluating if g_Q in (3) is negative. The complexity for finding the protection certificate is allowed to be much higher, since the analysis can be done offline.

VII. Conclusions

The paper showed that a multivariate model-based safety supervisor system can improve the safety guarantee and increase the uptime of large wind turbines, compared to simple univariate safety supervisors often used today. The implemented safety supervisor demonstrated the ability to commence emergency shutdowns prior to unsafe situations and to stay passive during normal operation of the wind turbine. Using the concept of barrier certificates, the search for safety envelopes can be formulated as a computationally tractable optimisation algorithm.

References

[1] M. Maggiore, B. Rawn, and P. Lehn, "Invariance kernels of single-input planar nonlinear systems," in *American Control Conference (ACC), 2011*, 29 2011-july 1 2011, pp. 1420 –1425.

[2] S. Prajna, "Barrier Certificates for Nonlinear Model Validation," *Automatica*, vol. 42, no. 1, pp. 117–126, Jan. 2006.

[3] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A Framework for Worst-Case and Stochastic Safety Verification Using Barrier Certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, Aug. 2007.

[4] J. Bochnak, M. Coste, and M.-F. Roy, *Real algebraic geometry*, ser. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Berlin: Springer-Verlag, 1998, vol. 36, translated from the 1987 French original, Revised by the authors.

[5] J. B. Lasserre, *Moments, Positive Polynomials and Their Applications*. Imperial College Press, 2010.

[6] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical Programming*, vol. 96, no. 2, pp. 293–320, May 2003.

[7] C. Sloth, G. J. Pappas, and R. Wisniewski, "Compositional safety analysis using barrier certificates," in *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, ser. HSCC '12. New York, NY, USA: ACM, 2012, pp. 15–24.

[8] J. Jonkman, S. Butterfield, W. Musial, and G. Scott, "Definition of a 5-mw reference wind turbine for offshore system development," National Renewable Energy Laboratory, Tech. Rep., 2009.

[9] R. J. M. Fernando D. Bianchi, Hernan De Battista, *Wind Turbine Control Systems*. Springer, 2007.

[10] M. Choi, T. Lam, and B. Reznick, "Sums of squares of real polynomials," in *Symposia in Pure Mathematics*, vol. 58, no. 2, 1995, pp. 103–126.

[11] P. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical Programming*, vol. 96, no. 2, pp. 293–320, 2003.

[12] G. Chesi, "LMI techniques for optimization over polynomials in control: A survey," *IEEE Trans. Automatic Control*, vol. 55, no. 11, pp. 2500–2510, 2010.

[13] S. Boyd and L. Vandenberghe, *Convex Optimisation*, 1st ed. Cambridge University Press, 2004.