AALBORG UNIVERSITY

Safe Operation and Emergency Shutdown of Wind Turbines

Andreas Søndergaard Pedersen
Christian Sigge Steiniche

Intelligent Autonomous Systems, Master's Thesis

May 2012

Department of Electronic Systems
Aalborg University

AALBORG UNIVERSITY

Department of Electronic Systems
Section for Automation and Control
Fredrik Bajers Vej 7 C
9220 Aalborg
Denmark

Title:
Safe Operation and Emergency Shutdown of Wind Turbines

Field:
Intelligent Autonomous Systems (IAS)

Project periode:
September 2nd 2011 - May 31st 2012

Project group:
11gr939 / 12gr1039

Group members:
Andreas Søndergaard Pedersen
Christian Sigge Steiniche

Supervisors:
Post Doc Mikael Svenstrup (AAU)
Professor Rafael Wisniewski (AAU)

Number of pages:
Main report: 125
Total: 148

Abstract:
As the control systems and mechanical structures of wind turbines have become increasingly complex, it has simultaneously become more difficult to guarantee that a wind turbine structure is not damaged in any given situation. To avoid damage to the wind turbine a safety supervisor system, which can initialise an emergency shutdown, should be implemented. The purpose of a safety supervisor is to keep the components of the wind turbine from being damaged.
This project considers the design of a safety supervisor system which is able to guarantee the safety of complex wind turbine systems. In particular, multivariate safety supervisor systems are considered. This is done using the concept of safety envelopes, in which the system can be shut down without structural damage.
To construct safety envelopes, a model-based framework of barrier certificates, Positivstellensatz and sum of squares polynomial decomposition are considered. The framework enables an inclusion of a bounded stochastic wind disturbance and the emergency shutdown procedure in the safety envelope construction. To utilise this framework, a polynomial wind turbine model is developed. The model is developed such that structural safety critical components of the wind turbine are included. The resulting model is able to produce emergency shutdown trajectories of a typical 5-MW wind turbine.
The construction of safety envelopes is formulated as sum of squares programs (SOSP), with optimisation criteria related to the safety envelope size. The SOSP of the complete wind turbine system turns out to be computational complex. To reduce the complexity of the calculations, two different approaches are tested; safety envelope construction of separate subsystems and a compositional technique which includes the subsystem interconnections in the envelope construction. Both methods are implemented and tested on the fictitious NREL 5-MW wind turbine in the simulator `FAST`. The results indicate that multivariate safety supervisors, that guarantee the safety of complex wind turbines, can successfully be designed using this method.

Preface

This Master's thesis is written by two students at the Section for Automation and Control at Aalborg University (AAU), in the period from September 2nd 2011 to May 31st 2012. The thesis is documentation of the work conducted by the authors during the period of the project.

The authors would like to thank Mikael Svenstrup (AAU), Rafael Wisniewski (AAU) and Keld Hammerum (VESTAS) for their practical as well as theoretical supervision throughout the project. Additionally the authors would like to thank Christoffer Sloth (AAU) for his assistance with practical implementation of the compositional barrier certificate method [SPW12].

References

References used throughout the thesis are listed below:

- References to external material are given in square brackets with an abbreviation of the author(s) and the year of publication, i.e. [Par03].
- Internal references to parts of the thesis are given by numbers, as in Chapter 9.
- Figures and tables are referred to by numbers, with the first number referring to the chapter where the figure/table is located, followed by a sequential number, i.e. Figure 2.1.
- Equations are given as numbers in parentheses, with the first number referring to the chapter where the equation is located, followed by a sequential number, i.e. Equation (8.4)
- Software references are given in a monospaced font, i.e. `MATLAB`.

A complete list of symbols and acronyms can be found in the nomenclature on Page vi.

A DVD containing `MATLAB` scripts, `SIMULINK` models and the thesis in PDF-format is attached on Page 148.

The thesis is formatted in LaTeX using the *Computer Modern* font. Diagrams and figures are produced in `TikZ` and `MATLAB`.

Andreas Søndergaard Pedersen

Christian Sigge Steiniche

Nomenclature

Acronyms	
BMI	Bilinear Matrix Inequality
IEC	International Electrotechnical Commission
LMI	Linear Matrix Inequality
NREL	National Renewable Energy Laboratory
SDP	Semidefinite Program
SOS	Sum of Squares
SOSP	Sum of Squares Program
WECS	Wind Energy Conversion System
Symbols and notation	
$\boldsymbol{\Gamma}$	Interconnection polynomial Gram matrix
$\boldsymbol{\lambda}$	Lagrangian dual variables
$\boldsymbol{\mathcal{B}}$	Blade coordinate system
$\boldsymbol{\mathcal{H}}$	Hub coordinate system
$\boldsymbol{\mathcal{N}}$	Nacelle coordinate system
$\boldsymbol{\mathcal{T}}$	Tower coordinate system
Λ	Lagrangian
$\mathbb{Z}$	Set of integers
$\mathbb{R}$	Set of real numbers
$\mathbb{S}$	Set of symmetric matrices
$\mathbf{B}$	Covariance matrix from normal operation
$\mathbf{c}$	Normal operation mean
$\mathbf{E}$	Symmetric decision matrix for hyperellipsoid scaling
$\mathbf{g}_0$	Safety envelope polynomials
$\mathbf{g}_\mathrm{D}$	Disturbance polynomials
$\mathbf{g}_\mathrm{u}$	Unsafe set polynomials
$\mathbf{g}_\mathrm{X}$	State space polynomials
$\mathbf{Q}$	Polynomial representation Gram matrix
$\mathbf{z}$	Monomial vector
$\mathcal{D}$	Disturbance set
$\mathcal{I}(F)$	Ideal generated by F
$\mathcal{M}(F)$	Multiplicative monoid generated by F
$\mathcal{P}(F)$	Preordering cone generated by F
$\mathcal{Q}(F)$	Quadratic module generated by F
$\mathcal{R}_\mathbf{x}^\mathrm{d}$	Set of all polynomials in variables $\mathbf{x}$ with degree d
$\mathcal{S}$	Binary safety condition
$\mathcal{U}$	Input set
$\mathcal{X}$	State space
$\mathcal{X}_0$	Initial set/safety envelope
$\mathcal{X}_{0,\mathrm{comp}}$	Composed safety envelope
$\mathcal{X}_{0,\mathrm{opt}}$	Optimal safety envelope
$\mathcal{X}_\mathrm{n}$	Normal operation set
$\mathcal{X}_\mathrm{s}$	Safe set

$\mathcal{X}_{\mathrm{u}}$	Unsafe set	
$\overline{\boldsymbol{\gamma}}$	Diagonal elements of interconnection polynomial Gram matrix	
$\Sigma_{\mathbf{x}}^{\mathrm{d}}$	Set of all sum of squares polynomials in variables $\mathbf{x}$ with degree d	
$\tau_{0,i}$	Safe set coupling variable of i^{th} subsystem	
$\tau_{\mathrm{u},i}$	Unsafe set coupling variable of i^{th} subsystem	
$\tau_{\mathrm{w},i}(\mathbf{u}_i, \mathbf{y}_i)$	Interconnection coupling variable of i^{th} subsystem	
φ	Lagrangian dual function	
$B(\mathbf{x})$	Barrier certificate	
$B_i(\mathbf{x}_i)$	Barrier certificate of i^{th} subsystem	
d	Locked parabola zero crossing	
$s.$	Sum of squares polynomial	
Model parameters and variables		
$\beta(t)$	Blade-pitch angle	[deg]
$\gamma_{\beta,\mathrm{max}}$	Maximum blade-pitch	[deg]
$\gamma_{\beta,\mathrm{min}}$	Minimum blade-pitch	[deg]
γ_{Δ}	Drive train torsion angle ultimate load limit	[rad]
$\gamma_{\beta,\mathrm{sr}}$	Blade-pitch rate limit	[deg/s]
γ_{fa}	Tower fore-aft angle ultimate load limit	[rad]
γ_{flap}	Flapwise blade tip displacement ultimate load limit	[m]
γ_{LL}	Lead-lag blade tip angle ultimate load limit	[rad]
γ_{r}	Rotor speed ultimate load limit	[rad/s]
$\gamma_{\mathrm{w,cut-in}}$	Cut-in wind speed	[m/s]
$\gamma_{\mathrm{w,cut-out}}$	Cut-out wind speed	[m/s]
$\lambda(t)$	Tip speed ratio	[-]
$\omega_{\beta}(t)$	Blade-pitch rate	[deg/s]
$\omega_{\mathrm{g}}(t)$	Generator angular velocity	[rad/s]
$\omega_{\mathrm{r}}(t)$	Rotor angular velocity	[rad/s]
$\overline{v}_{\mathrm{w}}$	Mean wind speed	[m/s]
ρ	Air density	[kg/m^3]
σ_{V}	Standard deviation of the turbulence	[-]
τ_{a_1}	Rotor axis torque	[Nm]
τ_{a_2}	Generator axis torque	[Nm]
$\tau_{\mathrm{aero}}(t)$	Aerodynamic torque generated by the wind-field	[Nm]
$\tau_{\mathrm{g}}(t)$	Generator load torque	[Nm]
$\tau_{\mathrm{r}}(t)$	Blade torque	[Nm]
$\theta_{\Delta}(t)$	Drive train torsional angle	[rad]
$\theta_{\beta}(t)$	Blade-pitch state	[deg]
$\theta_{\mathrm{g}}(t)$	Generator angle	[rad]
$\theta_{\mathrm{n}_1}(t)$	Internal gearbox angle	[rad]
$\theta_{\mathrm{n}_2}(t)$	Internal gearbox angle	[rad]
$\theta_{\mathrm{r}}(t)$	Rotor azimuth angle	[rad]
ξ_{flap}	Flapwise break point factor	[-]
ξ_{LL}	Lead-lag break point factor	[-]
B_{a_1}	Drive train torsional friction	[Nm/(rad/s)]
B_{a}	Drive train total torsional friction	[Nm/(rad/s)]
B_{g}	Generator friction	[Nm/(rad/s)]
B_{r}	Rotor friction	[Nm/(rad/s)]
B_{fa}	Tower fore-aft damping	[Nm/(rad/s)]
B_{flap}	Flapwise blade bending damping constant	[N/(m/s)]
B_{LL}	Lead-lag blade bending damping constant	[Nm/(rad/s)]
C_{p}	Power coefficient	[-]
C_{q}	Torque coefficient	[-]
C_{t}	Thrust coefficient	[-]
$F_{\mathrm{aero}}(t)$	Aerodynamic thrust generated by the wind-field	[N]

$F_{\mathrm{D}}(t)$	Aerodynamic drag	[N]
$F_{\mathrm{L}}(t)$	Aerodynamic lift	[N]
$F_{\mathrm{r}}(t)$	Blade thrust	[N]
g	Gravitational acceleration	[m/s^2]
$H_{\mathrm{turb}}(s)$	Turbulence filter	[-]
I_{ref}	IEC expected hub-height turbulence intensity	[-]
J_{g}	Generator inertia	[kg m^2]
J_{LL}	Lead-lag blade inertia beyond the break point	[kg m^2]
J_{r}	Rotor inertia	[kg m^2]
K_{a_1}	Rotor shaft spring constant	[Nm/rad]
K_{a_2}	Generator shaft spring constant	[Nm/rad]
K_{a}	Drive train total spring constant	[Nm/rad]
K_{V}	Turbulence power	[-]
K_{fa}	Tower fore-aft stiffness	[Nm/rad]
K_{flap}	Flapwise blade bending spring constant	[N/m]
K_{LL}	Lead-lag blade bending spring constant	[Nm/rad]
M_{flap}	Fictitious mass of the blade beyond the break point	[kg]
M_{n}	Tower fictitious mass	[kg]
N	Gear ratio	[-]
n_1	Rotor gear teeth number	[-]
n_2	Generator gear teeth number	[-]
R	Rotor radius	[m]
T_{V}	Turbulence frequency bandwidth	[-]
V_{e50}	IEC expected wind speed (3 sec avg.) with 50 years recurrence interval	[m/s]
$v_{\mathrm{eff}}(t)$	Rotor effective wind speed	[m/s]
V_{ref}	IEC reference mean wind speed	[m/s]
$v_{\mathrm{w,t1}}(t)$	Wind turbulence component 1	[m/s]
$v_{\mathrm{w,t2}}(t)$	Wind turbulence component 2	[m/s]
$v_{\mathrm{w}}(t)$	Horizontal hub height wind speed	[m/s]
$w(t)$	Driving turbulence noise	[-]
z	IEC height (vertical distance)	[m]
z_{hub}	IEC definition of hub height	[m]
${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}(t)$	Lead-lag blade tip angular velocity	[rad/s]
${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}(t)$	Lead-lag blade tip angle	[rad]
${}^{\mathrm{h}}v_{\mathrm{flap,x}}(t)$	Flapwise blade tip velocity	[m/s]
${}^{\mathrm{h}}x_{\mathrm{flap}}(t)$	Flapwise blade tip displacement	[m]
${}^{\mathrm{t}}\omega_{\mathrm{fa,y}}(t)$	Tower fore-aft angular velocity	[rad/s]
${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}(t)$	Tower fore-aft angle	[rad]

Contents

1 Introduction

1.1 Background

In recent years, wind power has become a popular source in energy conversion systems. As dependence on fossil fuels and concerns about the environment are increasing, so is the attention towards sustainable energy sources, giving Wind Energy Conversion Systems (WECS) increased attention. Today approximately 2.5% of the world's electrical usage is supplied by wind turbines. In Denmark alone, wind power contributes to 21% of the electrical production. Wind power showed in 2010 a global annual capacity growth rate of 23.6% [WWE10].

For wind turbines to be an attractive electrical power source, the wind turbine energy must be cheap and reliable. In recent years much research effort has been done to reduce the cost of the wind turbine energy. To reduce the cost of energy, the trend in wind turbine design has been leading towards increasingly larger wind turbines. Along with the increase in size, the complexity of the designs has also increased. The wind turbines implement a range of different sensors and the ability to control electrical converters, individual pitching of the blades and yaw of the rotor. The control of a wind turbine aims to achieve a maximum amount of power production while at the same time reducing structural loads and acoustical noise.

As the control systems and mechanical structures have become increasingly complex, it has simultaneously become difficult to guarantee that the wind turbine structure is not damaged in any given situation. Faults in the control system could lead to inappropriate behaviour of the wind turbine, which could potentially lead to a structural breakdown. Additionally, external events such as wind gusts could also cause the system to get damaged.

To avoid damage to the wind turbine, a safety supervisor system should be implemented. The purpose of a safety supervisor is to keep the mechanical and electrical components of the wind turbine from being damaged. When a critical situation arises, the safety supervisor should take action such that the wind turbine is not damaged. Safety critical situations can arise given some internal or external event. The objective of the safety supervisor is not to identify the source of a given event or malfunction, but simply to ensure that the wind turbine is not damaged. This is typically done by bypassing the control system and initialising an emergency shutdown procedure which takes the wind turbine to a complete stop. The safety supervisor has a higher priority level than the operational wind turbine control. Consequently, the safety supervisor can at any time take the control of the system.

Today, the design of the safety supervisors and the resulting trigger of an emergency shutdown are often very simple. Such a simple safety supervisor system might be an inadequate implementation given a large wind turbine with a complex control system. Additionally, the emergency shutdown procedure itself exposes the wind turbine structure to stress, why the design of a safety supervisor system, which guarantees the safety of the wind turbine system in every situation, becomes nontrivial.

A detailed safety analysis could possibly offer several positive results in relation to safety and reliability of large and complex wind turbines. This will in turn lead to lower cost of energy. In the following section a brief introduction to the terminology related to safety systems will be given. Once the terminology has been introduced the scope of the project can be defined.

1.2 Terminology

The terminology will be defined in general terms and later be defined more specifically towards a wind turbine system.

Safety The safety of a system is a binary condition, being either *safe* or *unsafe*.

Safe system A system is considered *safe* if the current state is not violating any of the *ultimate load limits* of the system and will not possibly lead to violation in the future given a bounded external disturbance.

Unsafe system A system is considered *unsafe* if it is not *safe*. If the system is in an *unsafe* state, it is assumed that the *ultimate load limits* of the system are violated or that there is a risk that they will be violated in the future.

Safety supervisor The purpose of a safety supervisor is to prevent the system from being *unsafe*. The safety supervisor may have access to certain actuators, which can be used to prevent the system from being *unsafe*. Two classes of safety supervisors are considered: the univariate safety supervisor and the multivariate safety supervisor. The univariate safety supervisor maps a single state into the safety condition (Supervisor: $\mathbb{R} \rightarrow \{\text{Safe, Unsafe}\}$). The class of multivariate safety supervisor maps multiple states into the safety condition (Supervisor: $\mathbb{R}^{\mathrm{n}} \rightarrow \{\text{Safe, Unsafe}\}$). A system can implement several univariate or multivariate safety supervisors.

Safe set The safe set is in the state space defined as the region in which the system is within the *ultimate load limits*. If the system state is in the safe set, it is not violating any of the *ultimate load limits* of the system. However, the *ultimate load limits* might possibly be violated in the future (notice the difference between *safe set* and *safe system*). The safe set will be denoted $\mathcal{X}_{\mathrm{s}}$.

Unsafe set The unsafe set is in the state space defined as the region in which the system violates the *ultimate load limits*. The unsafe set will be denoted $\mathcal{X}_{\mathrm{u}}$ and is the complement of the *safe set*.

Safety envelope A safety envelope defines a region in the state space in which the system is *safe*. The region of the safety envelope is a subset of the *safe set*. The safety envelope set will be denoted $\mathcal{X}_0$. If an emergency shutdown is initialised inside the safety envelope, the system trajectory will not evolve to some state in the unsafe set $\mathcal{X}_{\mathrm{u}}$.

Ultimate load limits The ultimate load limits of a system are defined to be a set of constraints which the system must not violate. The ultimate load limits define the boundary between the *safe set* and the *unsafe set*. The constraints could be defined by mechanical or electrical limits of the system.

Normal operation The normal operation is defined as the region in state space where a functional system is observed during typical operation given typical external conditions.

Emergency shutdown When an emergency shutdown is triggered, the wind turbine is brought to a stop as fast as possible. Several different methods can be used in the emergency shutdown procedure. Often the emergency shutdown procedure is based on a combination of aerodynamic and mechanic braking principles.

Safe life Certain components of a wind turbine are labelled *safe life*. These components are designed to be very reliable. Systems using safe life components can assume that these are always functional. As a result, safe life components can be used in critical systems.

1.3 Safety Supervisor

In the following, the general concept and purpose of safety supervisors are introduced.

The mechanical structure and the electrical components of a wind turbine are designed to be able to handle the loads expected during normal operation. However, several situations can cause a wind turbine to diverge from normal operation. In the case of wind turbines an external event, such as an extreme wind gust, could cause the system to leave the normal operation. To make sure that the wind turbine is not damaged during operation, a safety supervisor should trigger an emergency shutdown prior to any component being damaged. Throughout this thesis the limits of the system components which must not be exceeded are denoted *ultimate load limits*. A simple example could be the bending of the wind turbine blades. If the wind speed suddenly increases or the control system is faulty, this could lead to extreme bending of the blades. The objective of the safety supervisor would in this case be to shut down the wind turbine prior to the blades being damaged. An obvious safety constraint of the blade bending is the distance to the wind turbine tower.

In the design of a safety supervisor it is assumed that the components of the system are functional. This assumption separates the safety supervisor from a fault detection system. In the wind turbine case, it is assumed that the mechanical and electrical systems used in the emergency shutdown are working. In particular, it is assumed that the sensors used by the safety supervisor provide valid measurements and that the actuators used by the safety supervisor are functional. The sensors which can be used in critical systems such as the safety supervisor are labelled *safe life*. It is, however, not assumed that the control systems of the wind turbine are working correctly. The safety supervisor will be able to guarantee the safety of the wind turbine even if the control systems are faulty.

The fact that the safety supervisor should be able to guarantee safety of the system regardless of the condition of the controller has an important practical advantage. When new control algorithms are introduced, the new controller must be certified. However, if a safety supervisor is implemented, only the supervisor needs to be certified. As the safety supervisor has a higher priority than the controller, a change in the control algorithm does not require a recertification of the system. As a result, control algorithms can easily and cheaply be changed.

According to [IEC06] automatic or remote restart of the wind turbine is not allowed if an emergency shutdown has been initiated. Consequently, power production is not only lost during the shutdown, but also until the wind turbine has been examined by appropriate personnel. Designing a too conservative shutdown strategy may lead to frequent emergency shutdowns, which in turn lead to loss of power production and unnecessary mechanical stress.

1.4 Project Scope

The scope of this project is to find a method which can be used in the design of a wind turbine safety supervisor and use the method in the design of a safety supervisor. The safety supervisor should be able to guarantee the safety of the mechanical and electrical components of a wind turbine during operation, given a set of bounded external conditions, such as bounded wind speeds.

In the design of a safety system, the concept of safety envelopes will be considered. The safety envelope defines a subset of the state space in which the system is safe. A safety envelope of the system should be designed such that an emergency shutdown can safely be executed as long as the system is in the safety envelope. If such a safety envelope can be constructed, then the boundary of the envelope can be used as shutdown criterion. The safety envelope should be designed according to the normal operation of the wind turbine, such that the resulting safety system becomes useful in practice.

The objective of this project is to find a method which can be used to construct a practical useable safety envelope which guarantees the safety of the wind turbine system. This safety envelope can in turn be used as an emergency shutdown criterion in a safety supervisor implementation.

1.5 Outline

The thesis is divided into chapters. Below an outline of the chapters is given in order to provide an overview of the thesis.

Chapter 2: System Description
In this chapter an overview of a typical wind turbine is given. Additionally a specific wind turbine model and type are chosen and the general operation of this wind turbine introduced. This includes specification of the specific wind turbine and its control system.

Chapter 3: IEC Wind Turbine Standards
In this chapter, the safety regulations during operation of a wind turbine according to the IEC-61400 standards are examined. In particular the requirements and recommendations to the safety system and emergency shutdown procedure of the wind turbine are discussed.

Chapter 4: Safety Critical Situations
In this chapter some safety critical situations, in relation to the wind turbine operation, are examined. In particular three different situations are simulated. This is done in order to identify the effects which should be considered in the design of a wind turbine safety system.

Chapter 5: Safety Verification Methods
In this chapter, methods which can be used to construct a safety system are examined. The requirements to the methods are listed and the method which fit the requirements the best is chosen.

Chapter 6: Wind Turbine Dynamic Model
In this chapter a dynamical model of a wind turbine is developed. First the components which should be included in the model are identified. The wind turbine model is divided into parts, which are modelled separately. Finally the model parts are assembled into one complete model, which is compared to a reference wind turbine model.

Chapter 7: Operation Analysis
In this chapter the normal operation of the NREL 5-MW wind turbine is examined. This is done such that the safety supervisor system can be designed according to the normal operation. By including the normal operation of the wind turbine in the safety supervisor design, the amount of emergency shutdowns can be reduced. Additionally the ultimate load limits of the wind turbine are defined from the normal operation measurements.

Chapter 8: Safe Operation Envelope
In this chapter the concept of safety envelopes and barrier certificates are formulated. A simple example using the Lyapunov equation in the design of a safety envelope is given in order to clarify the concept. Additionally the shape of the safety envelopes is chosen and a range of suitable optimisation criteria are discussed.

Chapter 9: Envelope Construction
In this chapter the theory which is used in the search of safety envelopes is introduced. This includes two different barrier certificate formulations, introduction to sum of squares decomposition of polynomials and introduction to the usage of the Positivstellensatz' by Stengle and Putinar. Additionally it is demonstrated how this theory will be used in the search of a wind turbine safety envelope.

Chapter 10: Computation of Safety Envelope
In this chapter the search of the wind turbine safety envelope is formulated and the problem is discussed. In order to solve the problem, a range of assumptions are introduced. Subsequently, safety envelopes which are valid given the assumptions are found. From the safety envelopes, the safety supervisor system is constructed and the resulting safety supervisor system implemented on the reference wind turbine. A range of safety critical situations are simulated in order to verify the developed safety supervisor system.

Chapter 11: Compositional Safety Envelope Construction
In this chapter a compositional safety envelope method is utilised. Using this method, the problem of constructing safety envelopes can be split up into smaller problems, which are connected through a few shared variables. By considering a range of small connected problems, the computational requirements are lowered. A range of safety critical situations are simulated in order to verify the developed safety supervisor system.

Chapter 12: Conclusion
In this chapter conclusions to the results obtained throughout the thesis are given, as well as a conclusion of the final results.

Chapter 13: Future Work
In this chapter some suggestions to further work are given.

In this chapter a motivation has been given to consider a design of wind turbine safety systems targeted large and complex wind turbines. Possible advantages of a safety system designed specifically towards large and complex wind turbines have been discussed. Additionally the scope of the project has been formulated. Finally an outline of the chapters of the thesis was given. In the following chapter an overview of the considered wind turbine system is given.

System Description 2

As no physical wind turbine is available, a wind turbine simulator will be used as replacement. In the following, the selected simulator and a wind turbine reference model are introduced.

2.1 Wind Turbine Overview

In this section an overview of the general wind turbine system will be presented. Many different wind turbine design concepts exist. In general the concepts can be divided into vertical axis and horizontal axis rotor designs, with the latter being the most popular. Additionally, the horizontal axis rotor wind turbines can be divided by up-wind and down-wind designs and by the number of blades of the rotor [JFM09].

In this project the class of horizontal axis wind turbines is considered. The wind turbine is assumed to be of the up-wind design with three blades.

In Figure 2.1 the general components of a wind turbine are illustrated.

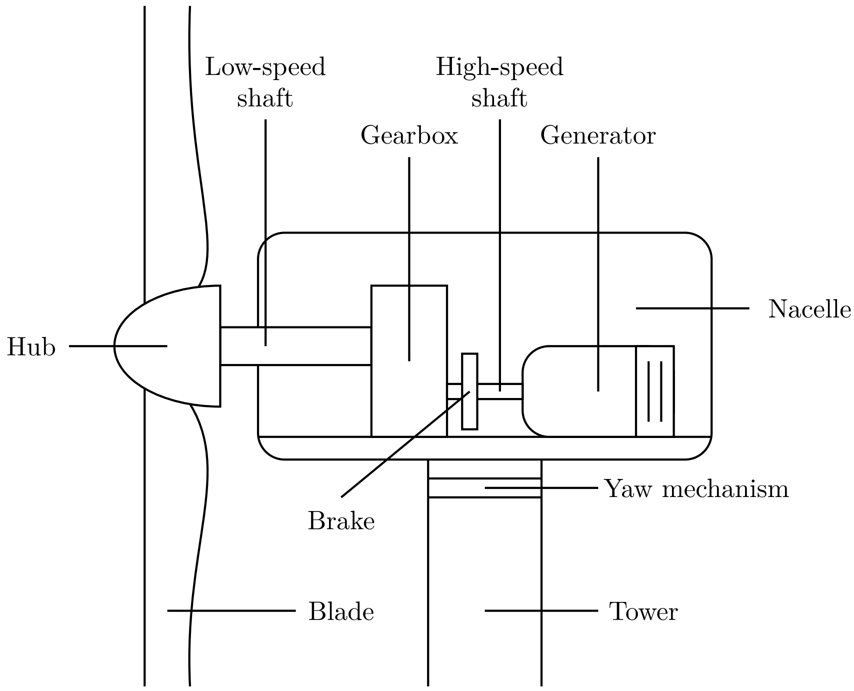


Figure 2.1: *Wind turbine structural overview*

In the following the functionality of the main components of the wind turbine will be described [JFM09].

Rotor - The rotor comprises the blades of the wind turbine. The blades convert the kinetic energy of the wind into rotational mechanical energy. In variable-blade-pitch wind turbines, the blade-pitch angle can be changed to change the torque delivered by the rotor.

Hub - The hub connects the rotor to the low speed shaft. The blade-pitch actuator system is located inside the hub.

Nacelle - The nacelle contains components such as the shafts, gearbox, brakes and generator. Additionally the nacelle provides the structural connection between the tower and the rotor.

Transmission system - In most wind turbine designs the rotor is connected to the generator through a transmission system. The system consists of the two shafts. The low-speed shaft connects the rotor to the gearbox and the high-speed shaft connects the gearbox to the generator. In this way the transmission system transmits the mechanical power of the rotor to the electrical generator. The gearbox increases the rotational speed of the shaft, such that the speed is more suitable for driving the electrical generator. Some wind turbines are designed with gearless drive trains.

Brakes - Most wind turbines include a mechanical brake which can be used to stop the rotor, and keep it stopped. The brake can be applied during an emergency shutdown of the wind turbine. Some wind turbine brakes are only designed to be used for parking.

Generator - The generator converts the mechanical energy into electricity. In variable-speed wind turbines a converter is used to interface the generator to the AC grid.

Tower - The tower provides structural support to the nacelle and rotor. A tall tower allows long blades resulting in a large coverage area of the rotor. Additionally, a tall tower provides favourable aerodynamic conditions. The nacelle is mounted on the top of the tower. The mount allows a yaw mechanism to rotate the nacelle. By yaw-rotation, the rotor can be aligned with the wind. In upwind wind turbine designs an active yaw mechanism is essential as the orientation of the rotor does not self-align with the wind.

In the following section, the general operation of a wind turbine is discussed.

2.2 General Operation

The general operation of the wind turbine is controlled by a superior controller sometimes denoted the sequence controller. The objective of the sequence controller is to control the general operation of the wind turbine based on the wind conditions. The general operation can typically take the following set of states [Hau06]:

- Idle
- Start-up
- Power production
- Shutdown
- Emergency shutdown

The *idle* and *power production* states are stationary, while the remaining states are transitions between the stationary states. The changes between these general operation states are primarily based on wind speed measurements. The operational states and the transitions between the states are illustrated in Figure 2.2. The transition between the *power production* state and the *emergency shutdown* state, is the main focus of this thesis.

When the wind speed v_{w} is not sufficient for the wind turbine to produce power, the wind turbine is in an *idle* state. In the idle state, the blades are pitched out of the wind, and the mechanical brake is applied. When the wind speed exceeds the cut-in wind-speed $\gamma_{\mathrm{w,cut-in}}$, the sequence controller changes the operation to the *start-up* state. In this state, the rotor speeds up. If the wind speed is sufficient, the rotor reaches the cut-in rotor speed $\gamma_{\mathrm{r,cut-in}}$. When the cut-in rotor speed is reached, the generator is started and the wind turbine enters the *power production* state and starts producing power. If the cut-in rotor speed cannot be reached, the sequence controller initiates a *shutdown* of the rotor, bringing it back to the idle state. In the power production state the objective is to maximise the power production. A controller strategy used in the power production is briefly introduced in Section 2.5.

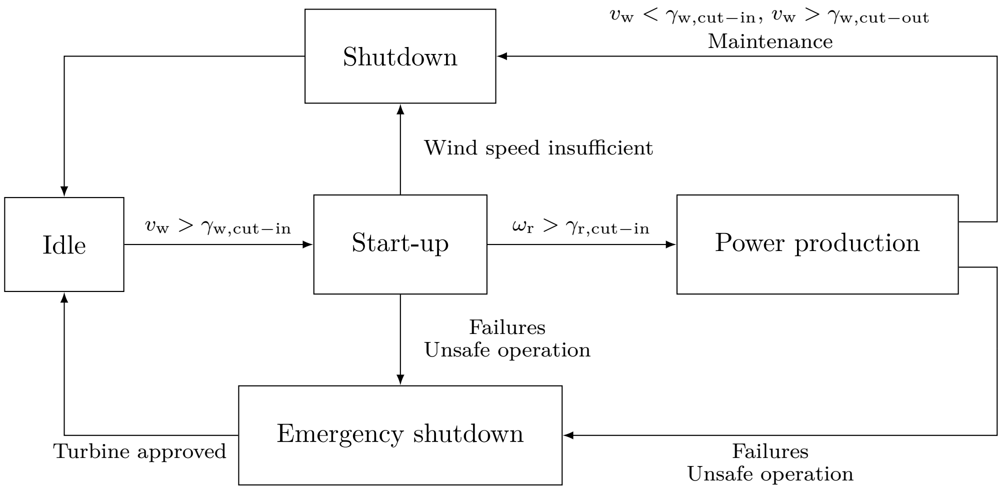


Figure 2.2: *General operation states of a typical wind turbine. The idle and power production states are stationary. The remaining states are transition states. The arrows indicate the possible transitions between the states.*

If the wind speed in the power production state exceeds the cut-out wind speed $\gamma_{w,cut-out}$ or goes below the cut-in wind speed $\gamma_{w,cut-in}$ the wind turbine is shut down, bringing it to the idle state.

If a failure occurs or the wind turbine enters an unsafe state (such as extensive tower bending) an emergency shutdown can be initialised. The emergency shutdown procedure and strategy of a wind turbine depends on the specific model. When the turbine has entered the emergency shutdown state it is required to stay in the state, until it has been approved by a certified technician. Consequently, the wind turbine cannot automatically be brought back to the idle state. The part of the sequence controller which monitors the safety of the wind turbine and initialises the emergency shutdown procedure if necessary, is throughout this thesis denoted the *safety supervisor*.

The safety supervisor uses safe life sensors to determine whether the wind turbine is safe or unsafe. When it is detected that the system is evolving towards the unsafe set, the supervisory system bypasses the operational control systems and initiates the emergency shutdown procedure. The bypassing of the operational control and initialisation of the emergency shutdown is illustrated in Figure 2.3.

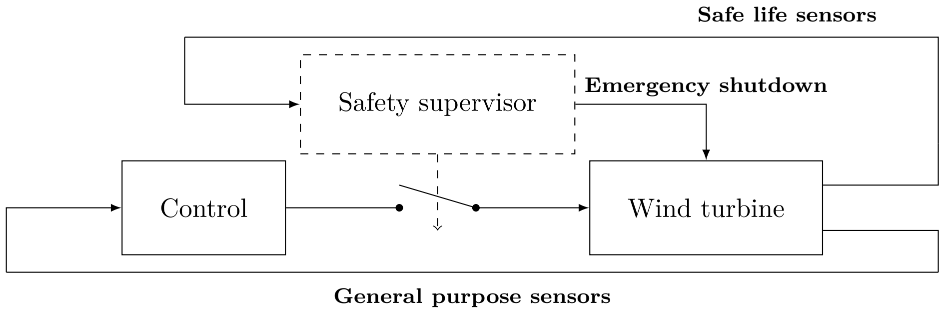


Figure 2.3: *When an unsafe situation is detected, the safety supervisor bypasses the operational control and initiates an emergency shutdown.*

In the following sections, a wind turbine simulator and a reference wind turbine model are introduced.

2.3 Wind Turbine Simulator

As no physical wind turbine is available real system testing is not possible. As replacement a wind turbine simulator will be used. The simulator will be considered equivalent to a real system. In particular the `FAST` (Fatigue, Aerodynamics, Structures, and Turbulence) wind turbine simulator from NREL will be used. The `FAST` simulator can be configured to simulate three-bladed, horizontal-axis wind turbines. The simulator models a wind turbine using a combination of rigid and flexible bodies. A `MATLAB SIMULINK` interface is available. The simulator has been evaluated by "Germanischer Lloyd WindEnergie" and found suitable for "the calculation of onshore wind turbine loads for design and certification" [Jon10].

The simulator supports control of blade-pitch, yaw, brake and generator torque and can be configured to resemble a range of different wind turbines.

To be able to use the `FAST` simulator as reference, the simulator should be configured according to a specific wind turbine model. In the following section the wind turbine reference model is chosen, and the overall specifications of the model given.

2.4 Wind Turbine Reference Model

In this project it is chosen to consider a specific wind turbine type and model. The chosen type is a three-bladed upwind variable-speed variable-blade-pitch wind turbine. The particular reference model is a NREL 5-MW baseline wind turbine [NRE11]. The NREL 5-MW wind turbine is a reference model inspired by an actual 5-MW wind turbine. This specific wind turbine is chosen as it is a representative model of a typical multi-megawatt turbine and detailed parameter data is available in [JBMN09]. Additionally the model has been included in the `FAST` wind turbine simulator [JJ05].

The general structural characteristics of the NREL 5-MW wind turbine components are given in the Table 2.1.

NREL 5-MW specifications		
Parameter	**Symbol**	**Value**
Power rating	-	5 MW
Blades	-	3
Rotor radius	R	63 m
Hub height	L	90 m
Hub diameter	-	3 m
Rotor mass	M_{r}	110000 kg
Nacelle mass	M_{n}	240000 kg
Tower mass	M_{t}	347460 kg
Cut-in wind speed	$\gamma_{\mathrm{w,cut-in}}$	3 m/s
Rated wind speed	-	11.4 m/s
Cut-out wind speed	$\gamma_{\mathrm{w,cut-out}}$	25 m/s
Rated rotor speed	-	1.27 rad/s (12.1 rpm)
Rated tip speed	-	80 m/s
Blade-pitch span	$[\gamma_{\beta,\mathrm{min}}, \gamma_{\beta,\mathrm{max}}]$	$0° - 90°$
Blade-pitch rate limit	$\gamma_{\beta,\mathrm{sr}}$	$8°$/sec

Table 2.1: *NREL 5-MW wind turbine specifications [JBMN09]*

To be able to simulate the typical operation of the NREL 5-MW turbine, a control system should be implemented. In the following section a variable-speed variable-blade-pitch controller is described.

2.5 Wind Turbine Reference Control System

In [JBMN09] a conventional variable-speed, variable-blade-pitch controller matching the NREL 5-MW wind turbine is designed. The control system does not include control actions such as nacelle yaw, start-up, shutdown or protection functions. This control system will be used throughout this project.

The control system comprises the control of the generator-torque and the control of the collective blade-pitch. The objective of the generator-torque controller is to maximise the power capture, when the wind turbine is operating below the rated operation point (below the power production for which it is designed / rated). When the wind turbine operates above the rated operation point, the blade-pitch controller will regulate the generator speed.

The control scheme is divided into three regions. The regions and the corresponding operation of the controllers are listed in Table 2.2.

Control scheme			
Region	**Description**	**Torque control**	**Pitch control**
1	Below cut-in wind speed	Zero torque	Zero pitch
2	Above cut-in wind speed	Maximise power	Zero pitch
3	Above rated	Constant power	Constant generator speed

Table 2.2: *The three operation regions define the objective controllers*

The control scheme has been implemented in `MATALB SIMULINK`, where the control system can be expanded to include a safety supervisor system.

2.6 Wind Turbine Emergency Shutdown Procedure

As mentioned, no emergency shutdown procedure is specified for the NREL 5-MW wind turbine in [JBMN09]. As no emergency shutdown procedure is given, it is chosen to consider a typical implementation. Variable blade-pitch wind turbines can according to [Hau06] typically only stop the rotor by pitching of the blades. The mechanical brake is in this case only applied when the rotor has stopped. As the blade-pitch procedure is critical in order to avoid unsafe situations such as rotor runaway, reliable operation of the emergency shutdown blade-pitch procedure is essential. As a consequence, the blade-pitch procedure used in the emergency shutdown is typically designed in a simple manner.

It is chosen to consider an emergency shutdown procedure using blade-pitch only. Additionally, this blade-pitch procedure is considered static. It is assumed that the blade-pitch is designed as a feed-forward procedure. The blade-pitch system of the NREL 5-MW wind turbine has a maximum pitch rate of 8°/s. The emergency shutdown blade-pitch procedure is accordingly assumed to be a static procedure taking the blade-pitch angle from a given angle to 90° with a maximum blade-pitch rate of 8°/s. When the emergency shutdown procedure is initialised, the generator torque will be set to zero.

In this chapter the general functionality of a wind turbine was discussed. Additionally, a wind turbine simulator, wind turbine reference model, reference controller and emergency shutdown procedure were chosen. In the following chapter the IEC wind turbine standards are examined in relation to wind turbine safety systems.

3 IEC Wind Turbine Standards

For the safety system to be applicable, it must comply with the given requirements. When the requirements are known, the safety system can be designed accordingly. The wind turbine requirements are defined in the IEC Wind Turbine Standards (IEC61400).

In [IEC06] the requirements to wind turbine safety are specified. The purpose of the standard is to protect the wind turbines against damage during planned lifetime. This includes control and protection systems. The requirements are defined according to wind turbine classes.

In the following section the wind turbine classes are described.

3.1 IEC Wind Turbine Classes

In [IEC06] wind turbines are divided into classes. Each class defines a wind speed and turbulence intensity for which a wind turbine of the specific class should be able to stay safe and respect the design lifetime of at least 20 years. The classes are chosen to represent many different sites and to cover most applications. The three general classes are given in Table 3.1.

Wind turbine classes			
	I	**II**	**III**
V_{ref}	50 m/s	42.5 m/s	37.5 m/s
A - I_{ref}	0.16		
B - I_{ref}	0.14		
C - I_{ref}	0.12		

Table 3.1: *Mean wind (V_{ref}, 10 minutes average) and turbulence intensity (I_{ref}) parameters of wind turbine design classes*

The mean wind speed V_{ref} is an average measure during a time period of 10 minutes. The turbulence reference I_{ref} is given as the ratio of the wind speed standard deviation to a constant mean wind speed of 15 m/s. In [JB07] the NREL 5-MW wind turbine is assumed to be of class I_{B}. In this class the wind turbine should be able to stay safe in a mean wind of 50 m/s and with a turbulence intensity of 0.14. It should be noted that the standard does not state any design requirements to when the wind turbine should be operational.

From a safety perspective, primarily the turbulence intensity is of interest. As the fluctuations of the mean wind speed are of low frequency (refer to Section 6.6), the wind turbine can be shut down when the mean wind speed reaches the defined cut-out wind speed. If the mean wind speed exceeds the cut-out wind speed, it can be assumed that the wind turbine is in idle mode. When considering emergency shutdown it is assumed that the wind turbine is active. In this situation it is important to have knowledge about the maximum expected turbulence intensity, as the high frequencies of the turbulence could render the system unsafe during operation.

As the NREL 5-MW has a cut-out mean wind speed of 25 m/s, this is assumed to be the highest mean wind speed for which the emergency shutdown system should be designed. Assuming a mean wind speed of 25 m/s, the turbulence will result in wind speeds fluctuating around 25 m/s. According to [IEC06][Hau06] the highest wind speed averaged over three seconds with a recurrence period of 50 years can be calculated as

$$V_{\mathrm{e50}} = 1.4 V_{\mathrm{ref}} \left(\frac{z}{z_{\mathrm{hub}}} \right)^{0.11} = 1.4 \cdot 25 \text{ m/s} \cdot \left(\frac{90 \text{ m}}{90 \text{ m}} \right)^{0.11} = 35 \text{ m/s}, \tag{3.1}$$

with $z = 90$ m and $z_{\mathrm{hub}} = 90$ m being the reference height and the hub height. According to [IEC06] the wind turbine should be able to stay safe during the 50 years recurrence wind gust. Consequently the safety supervisor system should be able to handle wind gusts up to 35 m/s.

In the following section the IEC wind turbine protection system requirements are examined.

3.2 IEC Protection System

According to [IEC06] the wind turbine operation and safety must be governed by a *protection system*. Concerns regarding structural loads must be addressed in order to ensure that the wind turbine does not break down during its lifetime [Han08]. Concerns regarding fatigue loads are not considered in the design of the protection system.

A protection system is in [IEC06] defined as in Definition 1.

Definition 1 (IEC, Protection system): *The protection functions shall be activated as a result of failure of the control function or of the effects of an internal or external failure or dangerous event. The protection functions shall maintain the wind turbine in a safe condition. The activation levels of the protection functions shall be set in such a way that the design limits are not exceeded.*

Throughout this thesis, this *protection system* will be refer to as a *safety supervisor system* or simply a *safety system*. The safety system shall govern the operation of the wind turbine, but should be passive during normal operation. When the safety system detects a safety critical situation, the system should take action.

If the safety system detects a dangerous event, it can trigger the emergency shutdown procedure. An emergency shutdown is in [IEC06] defined as in Definition 2.

Definition 2 (IEC, Emergency shutdown): *Rapid shutdown of the wind turbine triggered by a protection function or by manual intervention.*

This emergency shutdown can according to IEC-61400 be implemented using different strategies. In [IEC06] it is recommended that both direct mechanical as well as aerodynamical braking are applied during shutdown. The emergency shutdown procedure should be able to bring the rotor to a complete stop from any operational condition within a defined limit [IEC06].

The safety system should according to IEC-61400 be able to trigger the emergency shutdown procedure such that the wind turbine is not damaged given either an extreme external event or internal failure. In both cases the emergency shutdown should be activated prior to any violations of critical constraints. Additionally it is in [IEC01] noted that it is essential to consider the loads arising from the emergency shutdown itself. Note that it should be possible to initialise an emergency shutdown at any time, without the wind turbine being damaged. It is not allowed that the wind turbine enters a state in which it is not possible to shut down the system without damaging it. Consequently, the effects of the emergency shutdown procedure itself must be included in the construction of the safety supervisor system.

In the following chapter, safety critical situations will be simulated using the `FAST` wind turbine simulator.

Safety Critical Situations 4

In this chapter, situations related to the safety of a wind turbine will be simulated using the `FAST` simulator, the NREL 5-MW wind turbine and the NREL 5-MW wind turbine controller. This is done to examine how unsafe situations can arise. Additionally, the simulations can help clarify what should be considered when designing a safety supervisor system. The simulations should be seen as a conceptual examination, rather than typical wind turbine situations.

4.1 Emergency Shutdown Trigger

To protect the wind turbine from unsafe situations, the safety system must be able to initialise the emergency shutdown procedure prior to any exceedance of ultimate load limits. The following example simulates a situation with a fictitious ramp-like increase in wind speed. A fictitious ultimate load limit on the tower top fore-aft displacement is assumed to be 0.7 m. The safety system should ensure that this limit is not reached.

Figure 4.1 illustrates the tower top fore-aft displacement and velocity, without any safety supervisor system. At time 10 s the wind speed increases, which results in an increase of the tower top fore-aft displacement. The dashed line represents the fictitious ultimate load limit of the tower top displacement. If the tower top displacement exceeds the ultimate load limit, the tower is damaged.

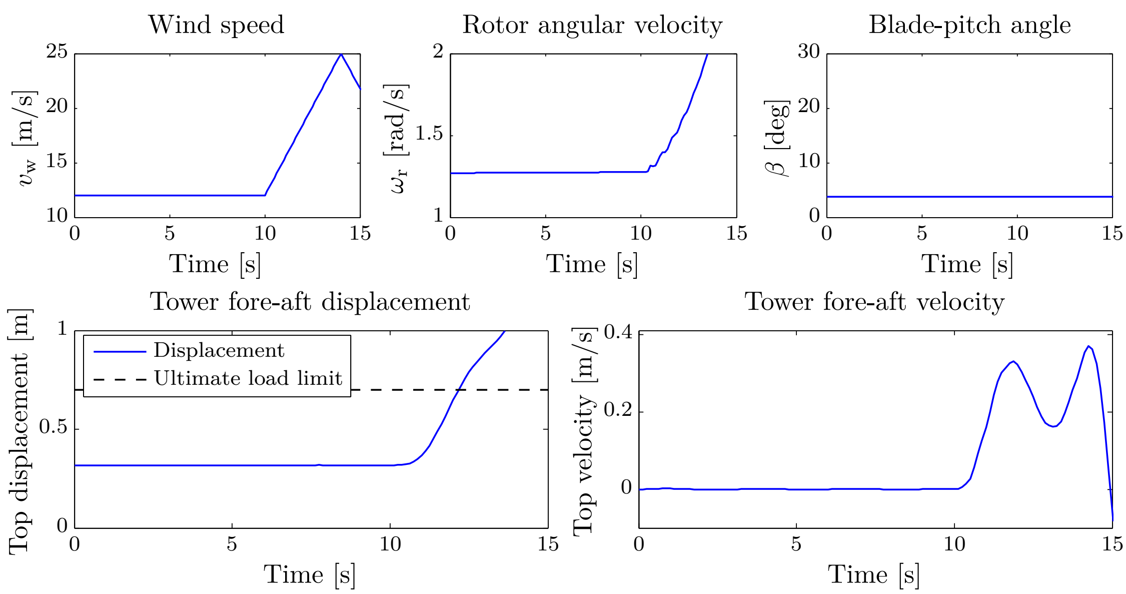


Figure 4.1: *Simulation with sudden increase in wind speed at time 10 s. The top plots show the horizontal hub height wind speed, rotor angular velocity and blade-pitch angle respectively. The bottom left plot shows the displacement of the tower top, with the dashed line indicating the ultimate load limit. The bottom right plot shows the velocity of the tower top. The wind turbine controller is turned off at time 10 s, such that the effect of the wind gust can be examined without the intervention of the control.*

To prevent damage to the tower, an emergency shutdown is introduced. The shutdown is performed by pitching the blades to 90° with a maximum rate of 8 deg/s. The shutdown is initiated when the tower top displacement reaches the ultimate load limit of 0.7 m. The effect of blade-pitching is discussed further in Chapter 6. Figure 4.2 illustrates the effect of the emergency shutdown. The red dashed lines indicate the time at which the emergency shutdown is initialised.

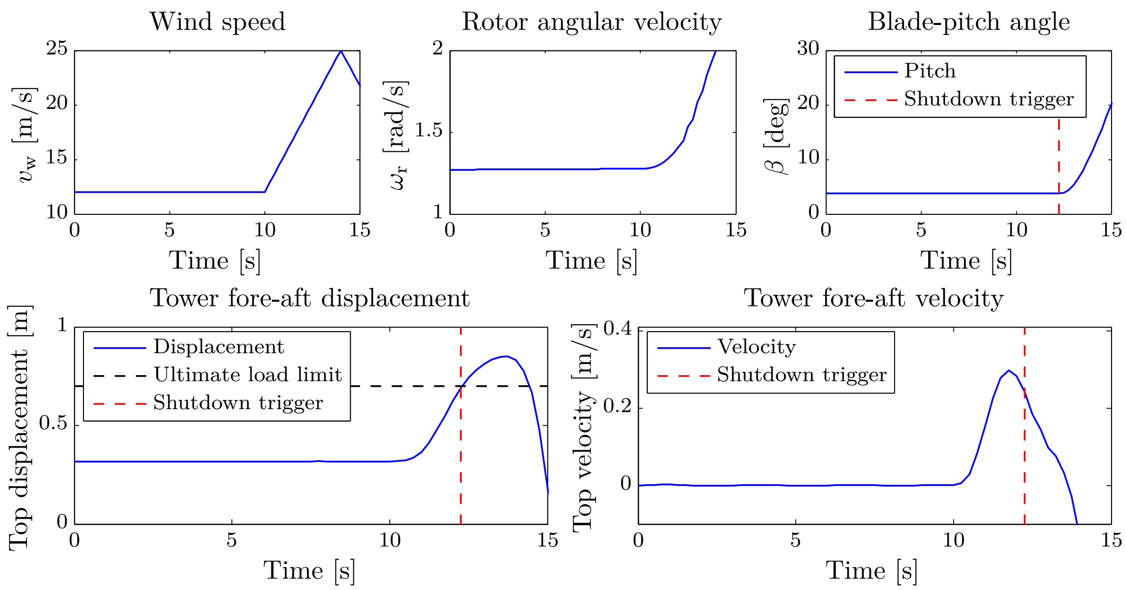


Figure 4.2: *Simulation of effect of emergency shutdown. The top plots show the horizontal hub height wind speed, rotor angular velocity and blade-pitch angle respectively. The bottom left plot shows the displacement of the tower top. The bottom right plot shows the velocity of the tower top. The black and red dashed lines indicate the ultimate load limit and the emergency shutdown trigger time respectively.*

It is clear from Figure 4.2 that this safety system does not prevent the exceedance of the tower ultimate load limit. As energy is stored in the velocity of the tower top (and possible other states), the initialisation of the shutdown is too late. The fact that this trigger strategy does not protect the wind turbine is in this case somewhat obvious; however similar problems could apply to less obvious cases. To prevent that the ultimate load limit is exceeded, either the tower top displacement trigger should be lowered or additional states should be included in the emergency shutdown trigger. The velocity of the tower top is an obvious state to include in the trigger. A trigger strategy which includes more than one state will be denoted a multivariate safety supervisor, whereas a trigger which only considers a single state will be denoted a univariate safety supervisor. From a theoretical perspective, an univariate safety supervisor would have to be very conservative in order to guarantee safety, if even possible. Even if the tower bending is zero, a high velocity of the tower top could cause the ultimate load limit to be possibly violated at a later time. Consequently, an emergency shutdown trigger based solely on the tower top displacement will theoretically never be able to guarantee that the ultimate load limit is not violated.

In Figure 4.3 the tower top displacement and velocity trajectory is illustrated. The left plot illustrates the trajectory of the shutdown in Figure 4.2. In the right plot a fictitious multivariate emergency shutdown trigger is introduced. The multivariate trigger initiates the emergency shutdown procedure, if the tower top displacement and velocity trajectory enters the region marked in grey. By considering both the tower top displacement and the velocity, the ultimate load limit is not exceeded. It should be noted that this obviously does not imply safety of the system in general. An illustration of the right plot in Figure 4.3 as a function of time, can be found in Appendix A.

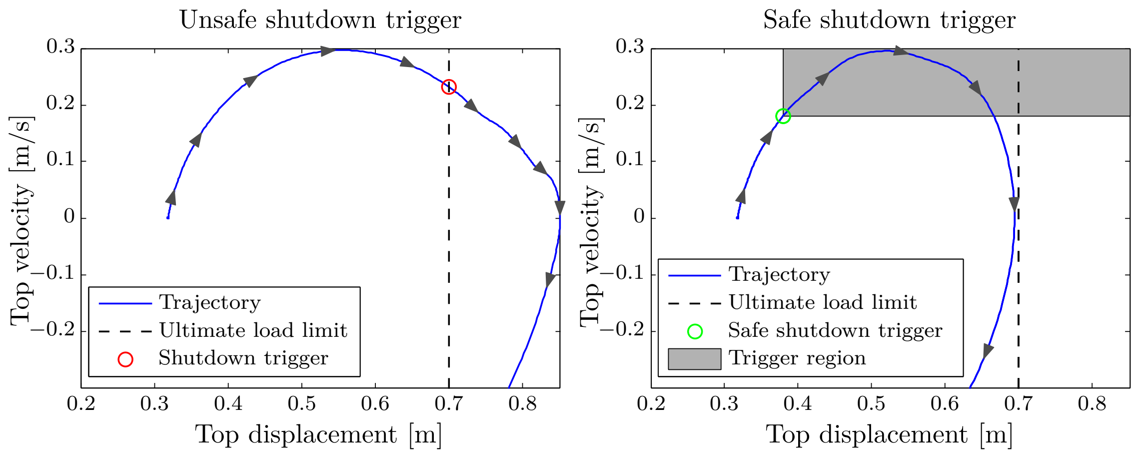


Figure 4.3: *The tower top fore-aft displacement is plotted against the tower fore-aft velocity. The dashed line indicates the ultimate load limit. The grey region illustrates an imaginary multivariate emergency shutdown trigger. The red and green circles mark the unsafe and safe trigger times respectively. As the pitch angle is changed to 90° in a continuous motion, no abrupt changes can be seen on the trajectory at the time of emergency shutdown trigger.*

As a wind turbine introduces several energy storing elements the calculation of an appropriate emergency shutdown trigger is not a trivial task and should possibly be a function of many states. As indicated in Figure 4.3 the safety system should not only trigger the shutdown procedure at the ultimate load limit but also in any region which could possibly cause the limit to be reached at a later time, if an emergency shutdown is initiated.

4.2 Aerodynamic Shutdown

In the following two situations, the effects of the emergency shutdown itself are examined trough simulation.

It is in [IEC01] noted that it is essential to consider effects arising from the emergency shutdown procedure itself. The following example demonstrates an emergency shutdown based on the aerodynamic braking principle only. This is done by pitching the blades to 90° with a pitch rate of 8°/s and turning off the generator torque. The wind speed is kept constant at 23 m/s. The shutdown procedure is initialised at time 10 s.

The rotor torque and rotor thrust are often described by the coefficients C_q and C_t. A positive C_q means that the rotor torque is positive and a positive C_t that a positive force is applied to the rotor, pushing it backwards. The coefficients will be described in detail in Section 6.3. Only the signs of the coefficients are of interest for now. Figure 4.4 illustrates how the pitching of the blades results in a negative rotor torque coefficient (C_q).

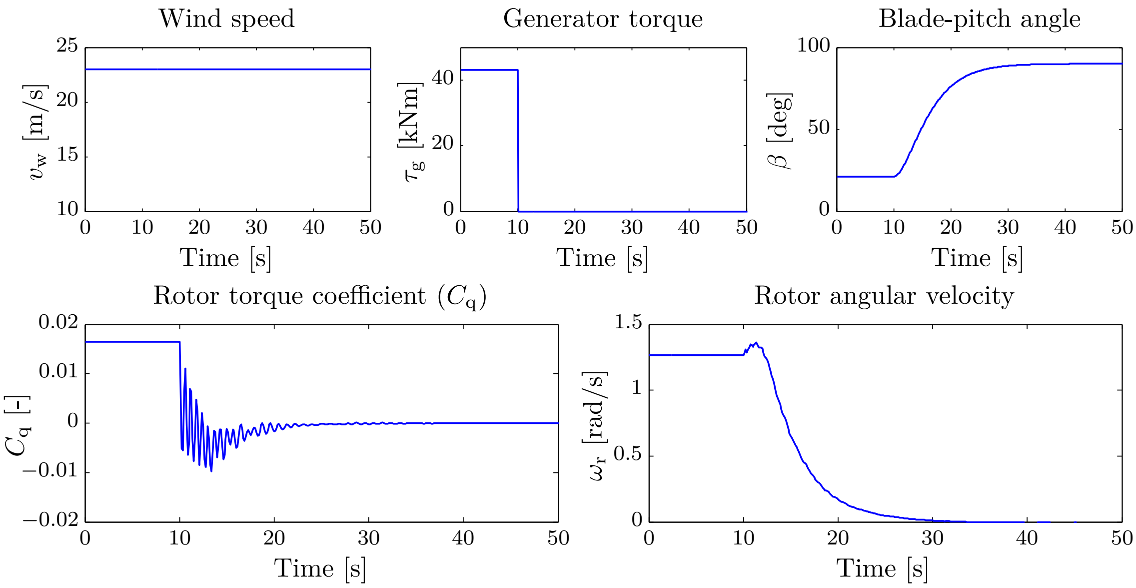


Figure 4.4: *Simulation of emergency shutdown using an aerodynamic braking principle. The top plots show the wind speed, generator torque and blade-pitch angle. The bottom left plot shows the aerodynamic torque coefficient (C_{q}) of the rotor. The bottom right plot shows the rotor angular velocity (ω_{r}). The short positive spike on the rotor velocity is due to the disconnection of the generator torque as the emergency shutdown is initialised.*

As illustrated in Figure 4.4, the pitching of the blades results in the torque constant (C_{q}) going negative, which successfully brings the rotor to a stop.

As the emergency shutdown illustrated in Figure 4.4 seems smooth and undramatic, an examination of some additional states reveals that the wind turbine has been under excessive stress during the shutdown. In Figure 4.5 the thrust coefficient (C_{t}), tower top fore-aft displacement and flapwise blade tip displacement (out-of-rotor-plane blade tip displacement) are illustrated.

As illustrated in Figure 4.5 the pitching of the blades results in the thrust coefficient C_{t} going from positive to negative. As a result, the thrust changes from forcing the rotor backwards, to driving the rotor forwards. The change in direction of the rotor force affects in particular the tower top displacement and the flapwise blade tip displacement. Prior to the initialisation of the emergency shutdown, the tower top is constantly forced backwards approximately 0.2 m. As the thrust coefficient changes the tower top is driven forwards, resulting in an oscillation of the tower top. The peak value of the tower top displacement reaches a magnitude of approximately 0.4 m. Likewise, the flapwise bending of the blades experiences a forward bending spike magnitude of almost 4 m.

In Figure 4.6 the values of the torque C_{q} and thrust C_{t} coefficients are illustrated as contours along the emergency shutdown trajectory. The emergency shutdown trajectory is given by the tip speed ratio (λ) and blade-pitch angle (β) (commonly used for wind turbines).

In the two top plots the tip speed ratio and blade-pitch angle trajectory are illustrated on the contours of the C_{q} and C_{t} coefficients. From the plots it can be seem that the trajectory enters the negative region of both coefficients as the blade-pitch angle is changed towards 90°. The separation of positive and negative C_{q} and C_{t} coefficients are illustrated by black lines denoted the zero levels. The shutdown is initiated at the black dot.

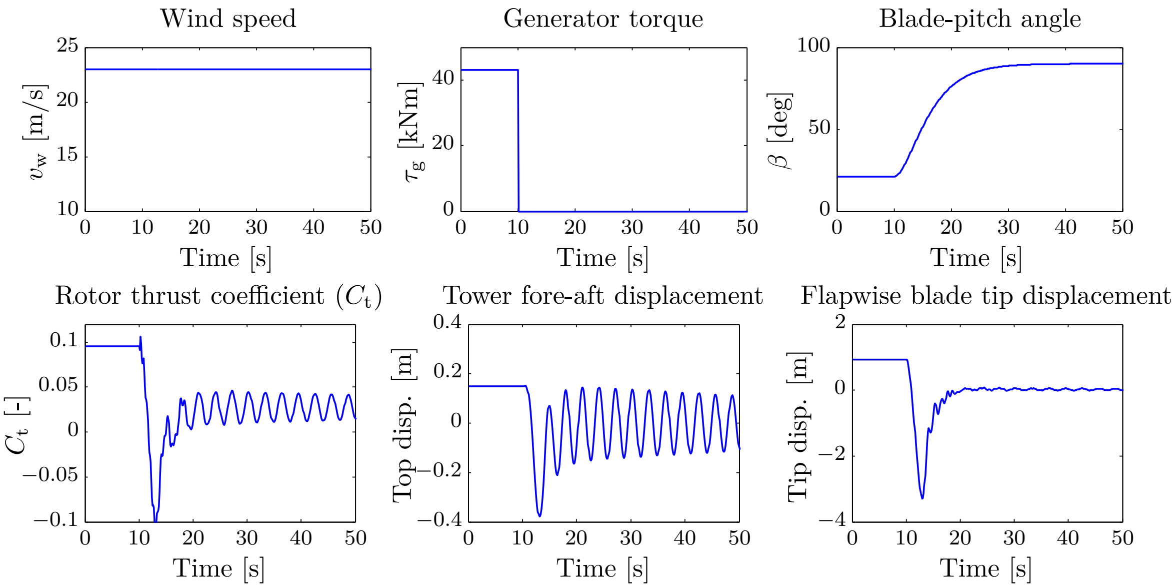


Figure 4.5: *Simulation of emergency shutdown using an aerodynamic braking principle. The top plots show the wind speed, generator torque and blade-pitch angle. The bottom left plot shows the aerodynamic thrust coefficient (C_t) of the rotor. The bottom middle plot shows the tower top fore-aft displacement. The bottom right plot shows the mean flapwise blade tip displacement of the three blades.*

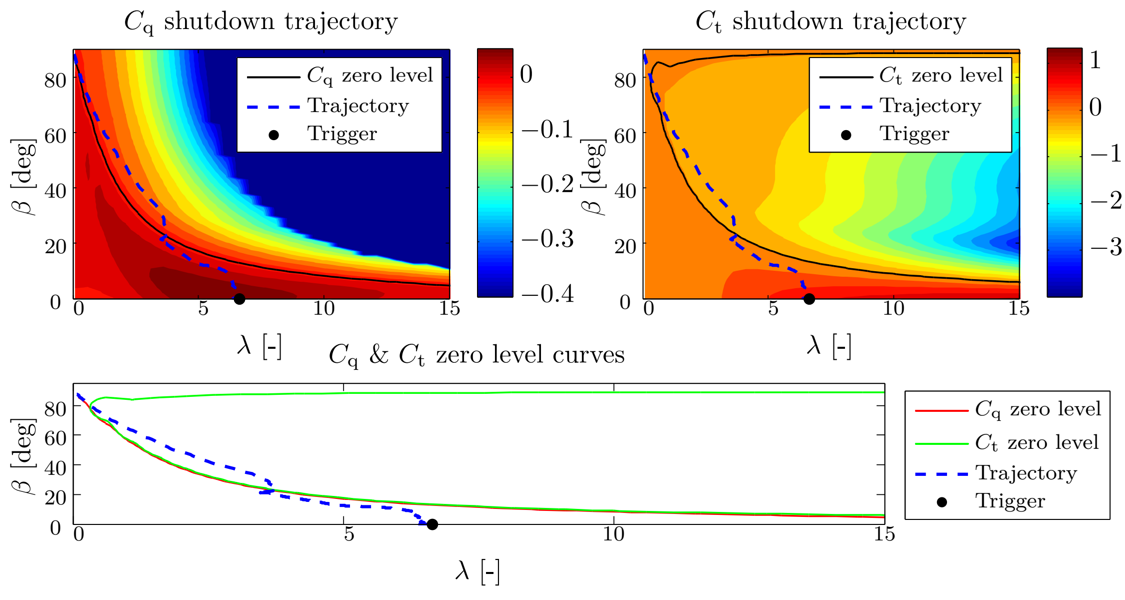


Figure 4.6: *Top left plot shows the shutdown trajectory compared to the C_q contours. Top right plot shows the shutdown trajectory compared to the C_t contours. In the bottom plot, the zero crossings of the C_q and C_t contours are compared to the shutdown trajectory.*

The bottom plot in Figure 4.6 compares the zero levels of the C_q and C_t contours with the shutdown trajectory. The comparison of the C_q and C_t zero levels reveals that the zero levels follow closely. Thus it is not possible to obtain af negative rotor torque (C_q) without at the same time generating a negative rotor thrust (C_t). Consequently it is on this specific wind turbine not possible to obtain a negative rotor torque to stop the rotor, without at the same time obtaining an unwanted negative thrust.

To reduce the unwanted effect of the negative thrust force, the emergency shutdown procedure could be designed such that the negative magnitude of the thrust is limited. In Figure 4.7 a fictitious shutdown trajectory is illustrated. By following such a trajectory in the emergency shutdown procedure, the magnitude of the negative thrust coefficient is reduced.

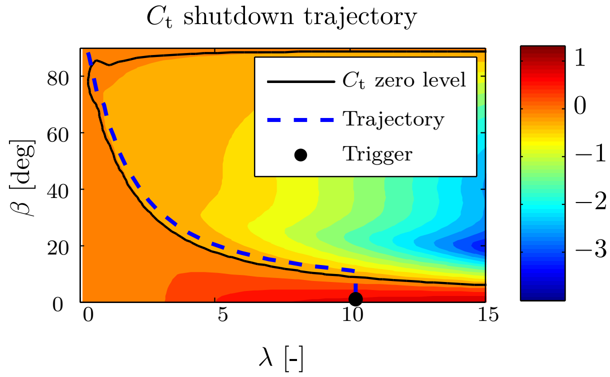


Figure 4.7: *Fictitious shutdown trajectory compared to the contours of the C_t-table.*

From the above situation an essential discovery was made in relation to the design of a safety supervisor. It was found that the emergency shutdown procedure itself can expose the wind turbine system to dangerous loads. Consequently, it cannot be assumed that the loads of the wind turbine are decreasing from the point of emergency shutdown initialisation. This discovery entails that the emergency shutdown procedure should be included in the safety supervisor design, such that the safety guarantee includes the trajectory which will be produced by the emergency shutdown procedure itself.

4.3 Mechanical Shutdown

In this example an emergency shutdown using a combination of aerodynamic and mechanical braking will briefly be discussed. As mentioned, mechanical braking is usually not used on variable blade-pitch with turbines, why this emergency shutdown procedure will primarily apply to smaller wind turbines.

Some wind turbines implement mechanical brakes on the drive train which can assist in the emergency shutdown. The mechanical brake can be installed on the high speed shaft, as illustrated in Figure 2.1. As the brake is applied, the torque is transferred to the rotor through the gearbox and the low speed shaft.

Figure 4.8 illustrates the wind speed, brake torque, blade-pitch angle, rotor angular velocity, drive train torsion and blade lead-lag tip displacement (in-rotor-plane blade tip displacement) during an emergency shutdown using a combination of aerodynamic and mechanical braking. The emergency shutdown procedure is initialised at time 10 s. By the introduction of mechanical braking, the drive train torsion and lead-lag blade tip displacement are in particular exposed to loads during the emergency shutdown.

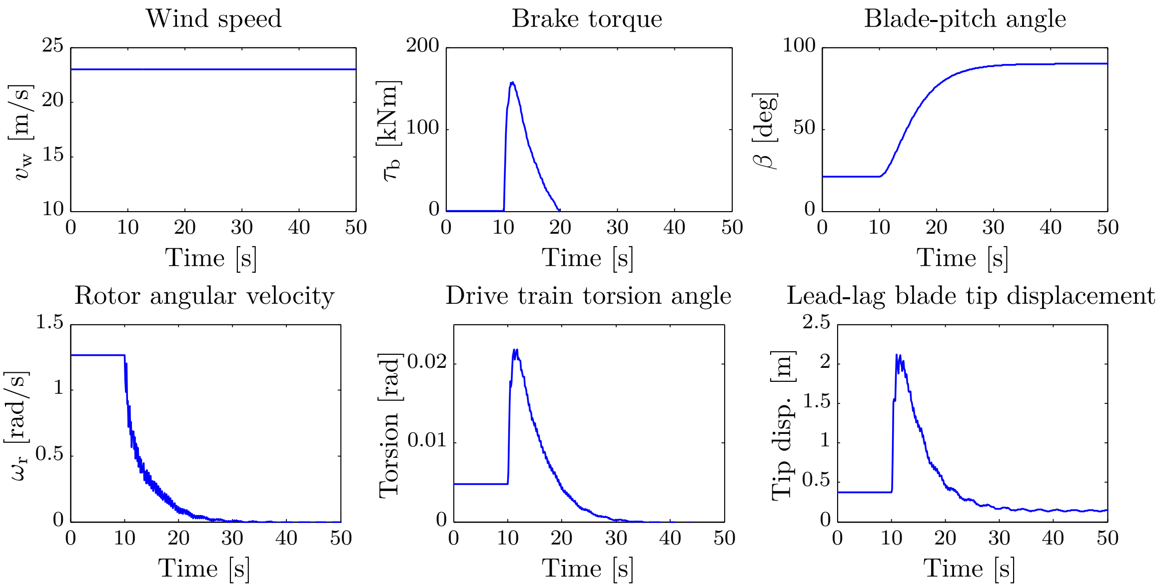


Figure 4.8: *Simulation of emergency shutdown using aerodynamic and mechanical braking. The top plots show the wind speed, brake torque and blade-pitch angle. The bottom left plot shows the angular velocity of the rotor. The bottom middle plot shows torsion angle of the drive train. The bottom right plot shows the mean lead-lag blade tip displacement of the three blades. The emergency shutdown is initiated at time 10 s.*

As in the example with aerodynamic braking only, this emergency shutdown procedure seems undramatic from the inspection of the rotor velocity only. However, the inspection of the drive train shaft torsion and lead-lag blade tip displacement reveals that the system has been undergoing stress during the shutdown.

In the above three simulation examples, it was found that the wind turbine is exposed to stress during the emergency shutdown procedure. Additionally it was found that the initialisation of the emergency shutdown procedure should be triggered in time such that the ultimate load limits cannot possibly be violated at a future time. Consequently, the design of a safety supervisor system should include the coupling of the wind turbine states as well as the trajectory produced by the emergency shutdown procedure itself. Additionally the safety supervisor should take the changing wind conditions into consideration, such that the wind turbine can be safely shut down given the stochastic behaviour of the wind speed.

In the following chapter, methods which can be used to design a safety supervisor system are discussed.

5 Safety Verification Methods

As described in the previous chapters, a safety system is a mandatory part of the wind turbine design, to ensure that the system is not damaged during operation. As the main purpose of the wind turbine is to produce power, it is desirable to keep the wind turbine operational for as much of the time as possible. This implies that the safety system must activate the emergency shutdown procedure in time to avoid violations of the ultimate load limits, but, at the same time, not be limiting the power production unnecessarily by being too conservative. In this chapter, different methods to identify *safety envelopes* will be discussed.

In [JF11] univariate safety supervisors monitor the rotor speed and tower acceleration. If the rotor speed or tower acceleration exceeds a given limit, the emergency shutdown procedure is initialised. It is in [JF11] noted that acceptable univariate threshold values can be difficult to establish. Additionally it is found that some structural elements can be difficult to protect using univariate threshold criteria (such as the drive train torsion). This kind of univariate safety supervisors are typical implementations of safety supervisors on wind turbines today. In Chapter 4 it was similarly found that the violation of a given ultimate load limit can be difficult to avoid based solely on univariate safety supervisors. It is difficult to tell which combination of system states that can result in a possible violation of a given ultimate load limit. Consequently, it seems difficult to develop an univariate safety supervisor, which guarantees safety in every imaginable situation. A practical implementation of an univariate safety supervisor can, in order to provide a safety guarantee in most situations, prove to be very conservative.

In Chapter 4 it was additionally found that the emergency shutdown procedure itself can produce unsafe trajectories. As a result, it is not sufficient to consider if a given state of the system is safe or unsafe. The trajectory produced by the emergency shutdown from the specific state should also be considered. The stochastic behaviour of the wind disturbance must additionally be included in the emergency shutdown trajectory, e.g. the trajectory should not be able to evolve to some state in the unsafe set, given any wind disturbance in some bounded set.

To resolve the above issues and to possibly improve the uptime of the wind turbines, this project seeks a multivariate safety supervisor system, which includes the shutdown trajectory and a stochastic bounded wind disturbance in the safety guarantee. The safety supervisor system should be developed in such a way that real time evaluation of the safety criterion is possible.

In the design of a multivariate safety supervisor system, the emergency shutdown, given an initial state, is classified as being either a safe or an unsafe emergency shutdown. To describe the region in which an emergency shutdown of the system is safe, the concept of safety envelopes is considered. An imaginary example in two dimensions is illustrated in Figure 5.1. The set $\mathcal{X}_\mathrm{u}$ denotes the unsafe set of the wind turbine, with the boundaries defined by the ultimate load limits of the system. If the system enters the unsafe set, it is assumed to get damaged. In the initial set $\mathcal{X}_0$, an emergency shutdown can be initialised without the system trajectory evolving to some state in the unsafe set $\mathcal{X}_\mathrm{u}$, given any stochastic disturbance in some bounded set. The initial set is consequently a possible safety envelope candidate. Throughout this thesis, the set $\mathcal{X}_0$ will be denoted either as a possible safety envelope or the initial set, depending on the context. The set $\mathcal{X}_\mathrm{n}$ is the set in which the wind turbine operates in normal conditions. In Figure 5.1 a fictitious system trajectory is illustrated by a dashed line, with the emergency shutdown initiated at the point marked by a red circle.

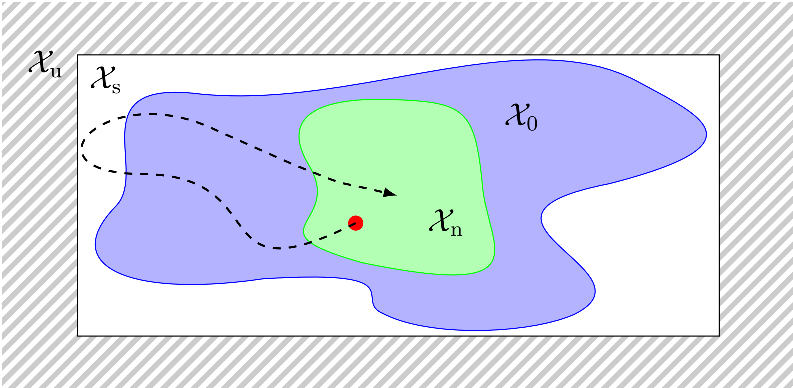


Figure 5.1: *Illustration of a fictitious state space of a system. The four sets $\mathcal{X}_\mathrm{u}$, $\mathcal{X}_\mathrm{s}$, $\mathcal{X}_0$ and $\mathcal{X}_\mathrm{n}$ denote the unsafe set, safe set, initial set and normal operation set of the system respectively. An emergency shutdown trajectory initialised in the red dot, is illustrated by a black dashed line. As the emergency shutdown trajectory is initialised in the initial set $\mathcal{X}_0$, the trajectory is guaranteed not to evolve to some state in the unsafe set $\mathcal{X}_\mathrm{u}$, given any stochastic disturbance in some bounded set.*

If the wind turbine is about to leave the initial set, the safety supervisor must trigger the emergency shutdown procedure. It is not tolerated that the wind turbine operates in regions, where the turbine cannot be shut down safely. Following this philosophy, it will at all times be possible to shut down the wind turbine without damaging the system.

To keep the wind turbine operational as much of the time as possible, it is desirable that the initial set $\mathcal{X}_0$ is as large as possible. If the initial set can be expanded, the frequency of emergency shutdowns is lowered, resulting in a higher power production.

5.1 Safety Envelope Identification Methods

In this section, methods used to identify a safety envelope are discussed. The objective is to find a method which can be used to identify a safety envelope of the wind turbine system, given a bounded disturbance.

The concepts of reachability and invariant sets are concepts which are closely connected to the search of safety envelopes. The concept of reachability considers the set of states which the system trajectory can reach given an initial state and a possible control signal. If the reachable set can be separated from the unsafe set $\mathcal{X}_\mathrm{u}$ given the control signal of the emergency shutdown procedure, then the system trajectory cannot reach the unsafe set, which guarantees the safety of the system. If the reachable set of a set of initial points $\mathcal{X}_0$ is separated from the unsafe set, then this initial set can be used as a safety envelope. As an exact description of such a reachable set for an arbitrary system is hard to determine, methods for over-approximating the set can be used.

Three principles which can be used to identify safety envelopes are discussed. The principles are respectively based on:

1. Identification using system measurements
2. Identification using model simulation
3. Identification using model examination and uncrossable state barriers

5.1.1 Identification using system measurements

Inspired by [Aga08] the safety envelope search can be based on measurement data obtained from a real wind turbine system and if necessary supported by data obtained through simulation. Using the available data, statistical extrapolation can possibly be used to calculate probabilities of the wind turbine entering the unsafe set $\mathcal{X}_\mathrm{u}$. This kind of approach is recommended by [IEC06] to predict ultimate loads. Given an emergency shutdown criterion, the probability of ultimate load limit exceedance can be calculated. The safety envelope should be found such that the probability of violation of the ultimate load limits is below some probability within the safety envelope.

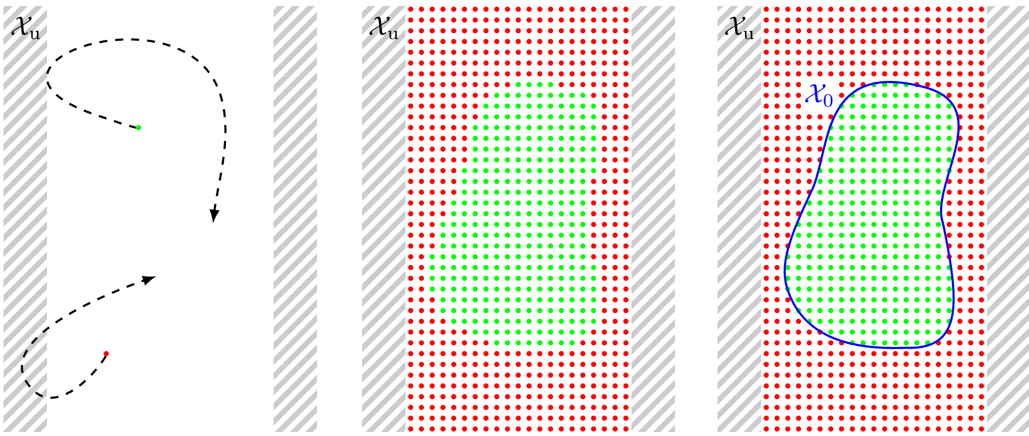
The advantage of the method is that it can be based solely on measurement data, if sufficient data is available. This eliminates the problem of model uncertainty. Further, the stochastic wind disturbance is somewhat directly included in the measurement data.

The disadvantage of the method is that a huge number of measurement data might be required to obtain a reliable safety envelope. Additionally, as the method is based on extrapolation, the reliability of the solution might be hard to determine. Further it might be very difficult to include the effect of the emergency shutdown itself in the safety envelope construction.

5.1.2 Identification using model simulation

By simulating trajectories of the emergency shutdowns from initial points in the state space distributed in some resolution, the safe trajectories can be separated from the unsafe trajectories. The boundary between the safe and unsafe initial points can then be used to construct a safety envelope. As the resolution of the simulation grid will be limited to some finite number, a criterion such as nearest neighbour should be used to determine the safety of intermediate points.

The construction of a safety envelope using simulation is illustrated in Figure 5.2 given a two dimensional system.



(a) *A safe and an unsafe emergency shutdown trajectory* **(b)** *Grid of safe and unsafe initial points* **(c)** *Safety envelope separates safe from unsafe initial points*

Figure 5.2: *Grid of simulations of system in two dimensions. Green dots indicate safe initial points. An emergency shutdown initialised in the green points, will produce a safe system trajectory. Red dots indicate unsafe points. An emergency shutdown initialised in the red points, will produce an unsafe system trajectory. The boundary of the safe points is used as safety envelope and as emergency shutdown criterion.*

The advantage of this method is that the true shape of the optimal safety envelope can be closely approximated by increasing the resolution of the simulation grid. As an arbitrary shape of the safety envelope can be obtained, the method will provide a close to optimal emergency shutdown criterion. This implies that the amount of emergency shutdowns is reduced to a minimal. Additionally, the method allows a direct inclusion of the emergency shutdown procedure in the safety envelope construction.

The primary disadvantage of the method is the time it takes to obtain a safety envelope. If a system in $\mathbb{R}^{12}$ is verified with a resolution of 100 in each dimension, it requires 10^{24} simulations. This number of simulations will take considerable time to produce, given the normal complexity of a wind turbine model. The `FAST` simulator uses approximately 15 s to simulate an emergency shutdown from a given initial state, on a modern PC. If the number of simulations is reduced, so is the resolution of the grid. Additionally it seems difficult to include the stochastic behaviour of the wind in the simulation, as the wind speed can change arbitrarily during the emergency shutdown procedure.

5.1.3 Identification using model examination and uncrossable state barriers

The system trajectories can be obtained directly from the system description. It is however in general difficult to obtain system solutions. As a consequence, Lyapunov theory has proven to be a powerful tool, as a Lyapunov candidate function provides information of the system, without the need of a solution. In the following, the concept of Lyapunov like functions, which can be used to construct a safety envelope, is discussed.

If an initial set $\mathcal{X}_0$ can be found to be positively invariant and exclusive from the unsafe set $\mathcal{X}_\mathrm{u}$, the system is guaranteed to be safe in $\mathcal{X}_0$. A set Ω is said to be positively invariant if, once the system is in Ω it will never leave it ($\forall x_0 \in \Omega$ the trajectories $x(t, x_0) \in \Omega$, $\forall t \geq 0$ [Kha02]). In Figure 5.3 an invariant set $\mathcal{X}_0$ is illustrated. If the system is initialised in $\mathcal{X}_0$, it will not be able to evolve to some state in the unsafe set $\mathcal{X}_\mathrm{u}$.

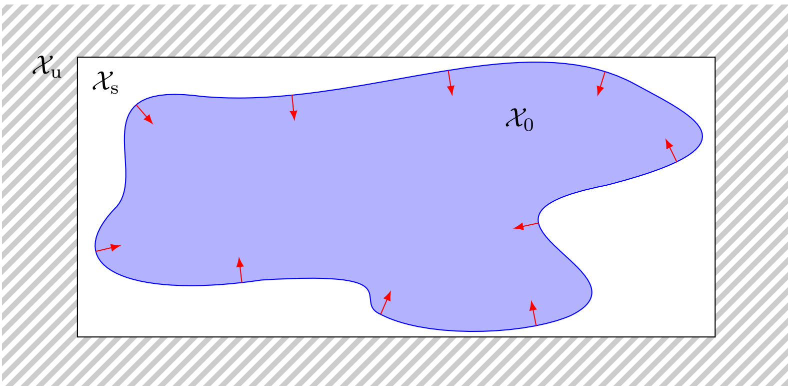


Figure 5.3: *The invariant set $\mathcal{X}_0$ is given in blue, with the red arrows indicating the direction of the vector field. Due to the direction of the system vector field, it is not possible to cross the boundary of the invariant set. Consequently, no system trajectory initialised in $\mathcal{X}_0$ will be able to evolve to some state in the unsafe set $\mathcal{X}_\mathrm{u}$.*

The Lyapunov equation enables the construction of a Lyapunov candidate function given a linear system description. The level sets of the Lyapunov function constitute invariant sets. Consequently, the safety envelope can directly be constructed from the level sets of the Lyapunov function, which are separated from the unsafe set, without the need of solutions to the system. As the modelling of a wind turbine includes highly non-linear parts (such as the aerodynamic properties) it seems difficult to model the system using a linear description only.

In [Pra06] it is proposed to design a Lyapunov-like scalar function which maps the system state $\mathbf{x}$ onto the set of real numbers, where the sign of the function is non-positive in the initial set $\mathcal{X}_0$ and positive in the unsafe set $\mathcal{X}_\mathrm{u}$, and safisfy certain restrictions on its time derivative. Such a function is denoted a barrier certificate. Recently proposed methods enable a search of such a barrier certificate given a polynomial system description and the sets being semi-algebraic (specified by polynomial equalities and inequalities). The search for a fixed degree polynomial barrier certificate can be defined as a sum of squares program (SOSP, described in Chapter 9), which in turn can be formulated as an SDP [Par03]. As a result, the existence of such a barrier provides a certificate that trajectories initialised in the initial set $\mathcal{X}_0$ cannot evolve to some state in $\mathcal{X}_\mathrm{u}$.

If the wind turbine can be modelled using a polynomial system description, the search of a safety envelope can be formulated as an SDP, which can be solved using existing software. The procedure in [Pra06] uses the barrier certificate method to *verify* the safety of a *given* set, why this method can be used to verify if a given initial set $\mathcal{X}_0$ is indeed a feasible safety envelope. This project does not seek a safety verification method, but rather a method for optimisation of the safety envelope size. However, as the barrier certificate search is formulated as an SDP, it should be possible to include an optimisation criterion. In [Pan10] a similar optimisation is performed using the sum of squares framework and Lyapunov theory to find the largest reachable set limited by a specified shape. In [SSE08] the unreachable set of a process is optimised from barrier certificates, given an initial set. To the author's knowledge, optimisation of the safe area using barrier certificates has not been made before.

The advantage of the barrier certificate method is that an optimised analytical safety envelope can be obtained without the need of system solutions. Additionally, the emergency shutdown procedure and a stochastic disturbance can directly be included in the search of safety envelope. The disadvantage of the method is that it is limited to polynomial model descriptions, and that the reliability of the resulting safety envelope will be limited by model uncertainties. Additionally the search of a safety envelope will be limited to a search of a set with some specified finite complexity. The blade-pitch procedure used in the emergency shutdown is static and can be modelled as an independent autonomous system, which can then be included in the method. As the barrier certificate method complies with the requirements to the safety envelope identification method, it seems to be worth pursuing. To the authors knowledge, the barrier certificate method using the sum of squares (SOS) framework has only been tested on a very few simple practical systems.

In the following chapter, a polynomial wind turbine model description will be developed. If it is possible to develop a reasonable model of the system using polynomials only, a safety supervisor can be constructed using barrier certificates and the SOS framework.

6 Wind Turbine Dynamic Model

In this chapter a dynamical model of a wind turbine will be developed. The model must be designed such that it can be used in the search of a safety envelope. The model is in Chapter 10 used in the search of a safety envelope. As no wind turbine is available, the model will be designed to resemble the fictitious NREL 5-MW wind turbine, implemented in the `FAST` wind turbine simulator.

To be able to model the wind turbine it is essential first to determine the effects of the wind turbine that should be modelled. The model objective is to be able to model the behaviour of a wind turbine during extreme conditions and shutdown. The model has to include the elements of the wind turbine which are exposed to significant loads during operation and the emergency shutdown procedure.

As discussed in Chapter 2.6, the emergency shutdown procedure is chosen to be based on the aerodynamic principle. To obtain the aerodynamic braking of the rotor, the blades are pitched to 90° using a static feed-forward blade-pitch angle procedure. This emergency shutdown principle was in Chapter 4 found to introduce loads to the tower and blades. Consequently, these loads should be included in the model.

According to [Han08] the three most important sources of loads on the wind turbine in normal operation are:

- Gravitational loading
- Inertial loading
- Aerodynamic loading

The gravitational loading is mostly due to the repetitive sinusoidal loading of the blades as a result of rotation of the rotor. As this load is mainly interesting when considering fatigue, it is considered non-essential with respect to the safety of the wind turbine.

The inertial loading occurs when the turbine is accelerated or decelerated. A safety shutdown will result in a hard deceleration of the rotor. As a result, the inertial loading must be included in the wind turbine model.

The Aerodynamic loading is due to the aerodynamic forces from the wind field. From a safety perspective, the wind field can be considered as an unknown disturbance, which can render the wind turbine unsafe. As the wind field will directly inflict loads on the structural components of the wind turbine, an aerodynamic model of the wind turbine must additionally be considered.

To reduce the amount of states considered in the safety system, it is chosen to consider structural components only. Oil temperature, generator temperature and electrical issues etc. will not be included in the safety system. Additionally it is assumed that the wind turbine is using a collective pitch strategy, that the wind turbine is aligned with the wind direction and that the wind field is uniform. These assumptions allow further simplification of the safety system and modelling, as issues such as yaw moments in the nacelle can be ignored.

The components to be considered in the design of the safety system should be based on the specific wind turbine model and type. The above considerations and assumptions together with the `FAST` simulations in Section 4 are used to identify the mechanical components which should be protected by the safety system.

Inspired by the NREL 5-MW reference wind turbine, the components which should be modelled are chosen to:

- Rotor speed
- Generator speed
- Drive train torsion
- Tower fore-aft bending
- Blade flapwise bending (out-of-rotor-plane bending)
- Blade lead-lag bending (in-rotor-plane bending)

As the aerodynamic braking is achieved by pitching of the rotor blades, the pitching procedure should be modelled. The pitch procedure must be modelled as an autonomous system. The dynamics of the generator should be considered, as the generator torque is set to zero when the emergency shutdown is initialised.

The actuators which should be modelled are:

- Blade-pitch system
- Generator torque

Additionally, the stochastic behaviour of the wind field should be modelled according to [IEC06], and included in the complete model as a disturbance.

The model will be divided into parts, which finally will be connected. In Figure 6.1 the model parts are illustrated as boxes and the interconnections of the parts as arrows.

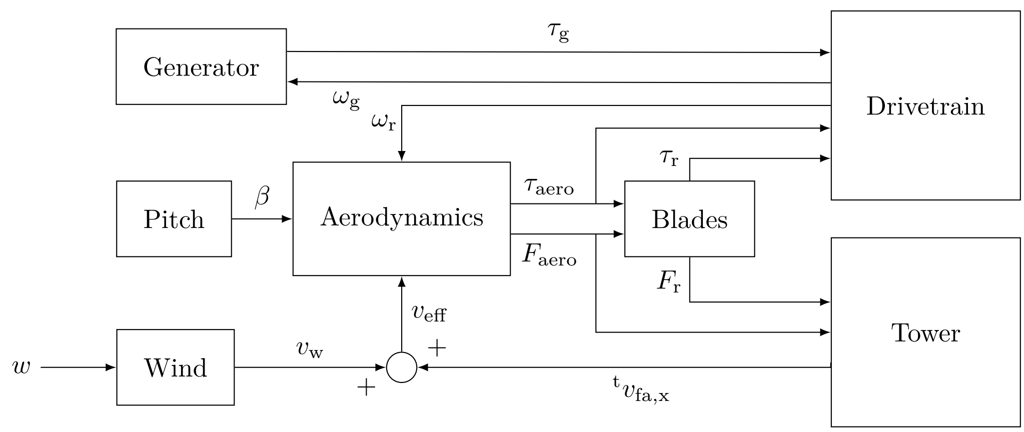


Figure 6.1: *Model parts given as boxes. The interconnections are given as arrows. The symbols will be introduced in the modelling sections, and can be found in the nomenclature. The wind disturbance w is the only external signal to the model.*

The system illustrated in Figure 6.1 is able to model an emergency shutdown trajectory given an initial state. The model can be used to test if a given initial state produces a safe or unsafe emergency shutdown trajectory. The objective of the model separates from conventional wind turbine models used for control, as it is not designed to model the behaviour of the wind turbine during normal operation. The blade-pitch will autonomously be taken from the initial value to 90°. The model will include an unknown bounded wind disturbance, as the only external signal to the model.

In the remaining of this chapter the model will be designed. First the mathematical structure of the model and the wind turbine coordinate systems will be defined. Subsequently, each of the model parts will be modelled individually. Finally the model parts are connected into one system.

An overview of the wind turbine modelling chapter is given below.

- **6.1** - Model Structure
- **6.2** - Coordinate Systems
- **6.3** - Aerodynamic Model
- **6.4** - Structural Model
  - **6.4.1** - Drive train
  - **6.4.2** - Blades
  - **6.4.3** - Tower
- **6.5** - Actuator Model
  - **6.5.2** - Blade-pitch actuator system
  - **6.5.1** - Generator
- **6.6** - Wind Model
- **6.7** - Model Composition

In the following section, the mathematical structure of the model will be specified.

6.1 Model Structure

The framework based on barrier certificates and the SOS decomposition described in Chapter 5 is limited to handle multivariate polynomials. The model must be consistent with this mathematical structure.

In particular, the wind turbine model should, in order to be used in later analysis, be described by a set of first order differential equations. The differential equations are limited to the class of multivariate polynomials.

The differential equations $\dot{x} = f(\mathbf{x})$ of the model must be on polynomial form given as

$$f(x_1, ..., x_\mathrm{n}) = \sum_i c_i m_i,\ c_i \in \mathbb{R},\ m_i \in \mathcal{M}(x_1, ..., x_\mathrm{n}), \tag{6.1}$$

where $\mathcal{M}(x_1, ..., x_n)$ is the set of finite products generated by the family $X = \{x_1, ..., x_\mathrm{n}\}$ and c_i is a constant term.

The polynomial $f(x_1, x_2)$ will in this specific case be given as a finite linear combination of monomials

$$f(x_1, x_2) = \sum_i c_i m_i = c_0 + c_1 x_1 + c_2 x_2 + c_3 x_1 x_2 + c_4 x_1^2 + c_5 x_2^2 + c_6 x_1^2 x_2 + ... ,$$

with $c_i \in \mathbb{R}$, and $m_i \in \mathcal{M}(x_1, x_2)$.

The complete model should be given on the form

$$\dot{\begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_\mathrm{n}(t) \end{bmatrix}} = \begin{bmatrix} f_1\left(x_1(t), \cdots, x_\mathrm{n}(t), d_1(t), \cdots, d_\mathrm{q}(t)\right) \\ f_2\left(x_1(t), \cdots, x_\mathrm{n}(t), d_1(t), \cdots, d_\mathrm{q}(t)\right) \\ \vdots \\ f_\mathrm{n}\left(x_1(t), \cdots, x_\mathrm{n}(t), d_1(t), \cdots, d_\mathrm{q}(t)\right) \end{bmatrix},$$

with the polynomials $\{f_1, f_2, \cdots, f_\mathrm{n}\}$ defined by (6.1) and the states and disturbances defined by $\mathbf{x} \in \mathbb{R}^\mathrm{n}$, $\mathbf{d} \in \mathbb{R}^\mathrm{q}$ respectively.

In the following section, the coordinate system used to model the wind turbine will be defined.

6.2 Coordinate Systems

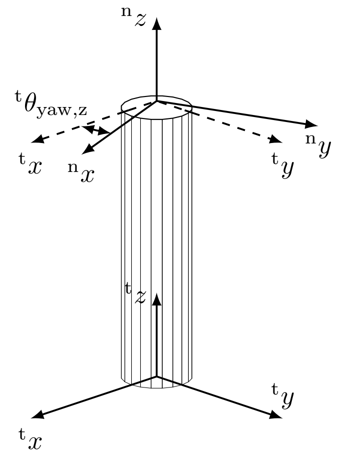
In this section, the coordinate systems which will be used in the modelling of the wind turbine will be defined.

It is chosen to define the coordinate systems according to [IEC01]. Four systems - tower coordinate system ($\boldsymbol{\mathcal{T}}$), nacelle coordinate system ($\boldsymbol{\mathcal{N}}$), hub coordinate system ($\boldsymbol{\mathcal{H}}$) and blade coordinate system ($\boldsymbol{\mathcal{B}}$) - are used to describe the motions and forces of the wind turbine.

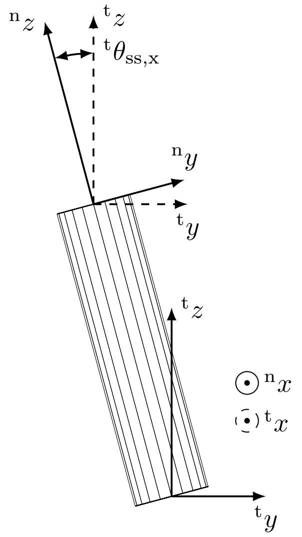
The following notation will be used to describe rotation and translation. An angle (θ) of some object in the nacelle coordinate system ($\boldsymbol{\mathcal{N}}$), around the x-axis will be denoted ${}^{\mathrm{n}}\theta_{\mathrm{name,x}}$, with *name* being the name of the object. A translational velocity parallel to the x-axis in the tower coordinate system ($\boldsymbol{\mathcal{T}}$) will similarly be denoted ${}^{\mathrm{t}}v_{\mathrm{name,x}}$. The notation of translations, e.g ${}^{\mathrm{n}}x_{\mathrm{name,x}}$ will be shortened to ${}^{\mathrm{n}}x_{\mathrm{name}}$. Some frequently used rotations or translations will be given specific names, such as the blade-pitch angle, which is denoted β.

The tower coordinate system $\boldsymbol{\mathcal{T}} = ({}^{\mathrm{t}}x, {}^{\mathrm{t}}y, {}^{\mathrm{t}}z)$ is placed at the base of the tower with ${}^{\mathrm{t}}z$ coaxial with the tower. The nacelle coordinate system $\boldsymbol{\mathcal{N}} = ({}^{\mathrm{n}}x, {}^{\mathrm{n}}y, {}^{\mathrm{n}}z)$ is placed in the nacelle such that ${}^{\mathrm{n}}x$ is aligned with the rotor axis and ${}^{\mathrm{n}}z$ is vertical, pointing up.

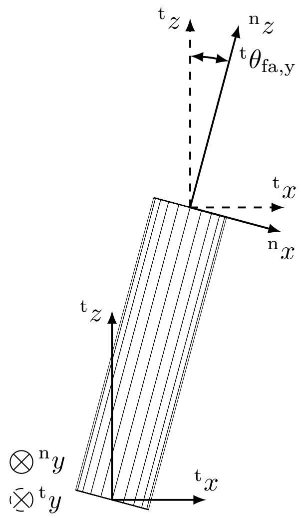
The ($\boldsymbol{\mathcal{T}}$) and ($\boldsymbol{\mathcal{N}}$) coordinate systems are illustrated in Figure 6.2. The naming is abused, as the tower fore-aft ${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$ and side-side ${}^{\mathrm{t}}\theta_{\mathrm{ss,x}}$ bending usually are defined relative to the nacelle direction. The yaw angle ${}^{\mathrm{t}}\theta_{\mathrm{yaw,z}}$ is, however, assumed to be zero.



(a) *Tower yaw rotation* ${}^{\mathrm{t}}\theta_z$



(b) *Tower side-side rotation* ${}^{\mathrm{t}}\theta_x$

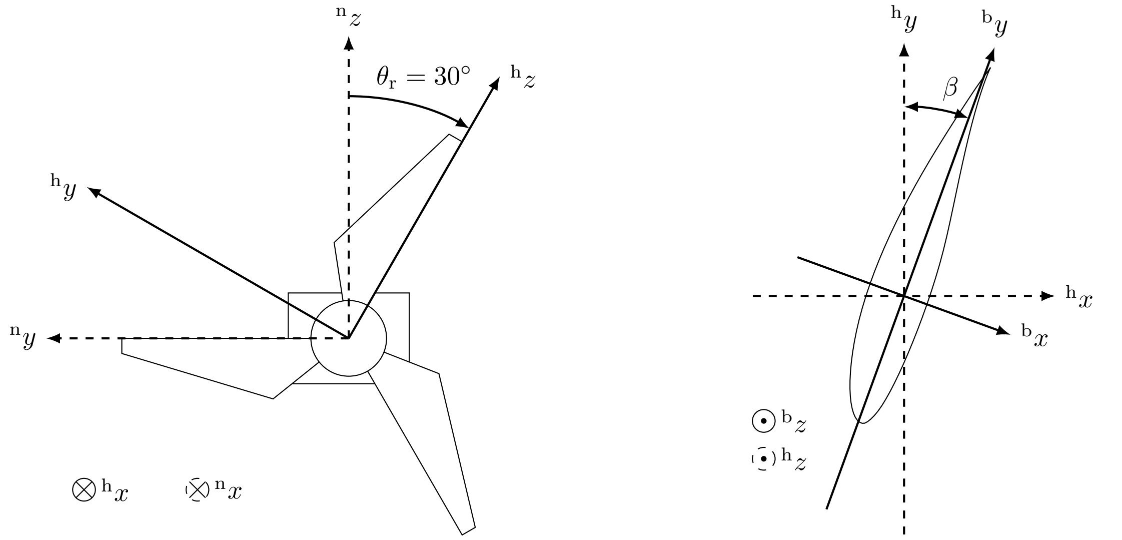


(c) *Tower fore-aft rotation* ${}^{\mathrm{t}}\theta_y$

Figure 6.2: *The tower system* $\boldsymbol{\mathcal{T}}$ *and nacelle system* $\boldsymbol{\mathcal{N}}$*. Rotations of the tower* ${}^{\mathrm{t}}\theta_z$*,*${}^{\mathrm{t}}\theta_x$ *and* ${}^{\mathrm{t}}\theta_y$ *are given in 6.2a, 6.2b and 6.2c respectively.*

The hub coordinate system $\boldsymbol{\mathcal{H}} = ({}^{\mathrm{h}}x, {}^{\mathrm{h}}y, {}^{\mathrm{h}}z)$ is placed in the nacelle fixed to the rotating shaft. This coordinate system has an angle $\theta_{\mathrm{r}} = {}^{\mathrm{n}}\theta_{\mathrm{az,x}}$ relative to the nacelle coordinate system. The angular velocity of the hub coordinate system in the nacelle coordinate system ${}^{\mathrm{n}}\omega_{\mathrm{r,x}}$ will be called the rotor angular velocity and be denoted ω_{r}. The blade coordinate system $\boldsymbol{\mathcal{B}} = ({}^{\mathrm{b}}x, {}^{\mathrm{b}}y, {}^{\mathrm{b}}z)$ is aligned along one of the blades with ${}^{\mathrm{b}}z$ along the chord. The angle ${}^{\mathrm{h}}y$ relative to ${}^{\mathrm{b}}y$ will be called the blade-pitch angle and be denoted β (β is defined positive towards feather). The blade-pitch angle is in accordance with standard practice measured in degrees.

In Figure 6.3 the hub and one blade are illustrated in the hub and blade coordinate systems respectively.



(a) *Hub coordinate system in the nacelle coordinate system*

(b) *Blade coordinate system in the hub coordinate system*

Figure 6.3: *The hub coordinate system $\mathcal{H}$ and the blade coordinate system $\mathcal{B}$. In the left plot the hub coordinate system is given in the nacelle coordinate system. In the right plot the blade-pitch angle is illustrated.*

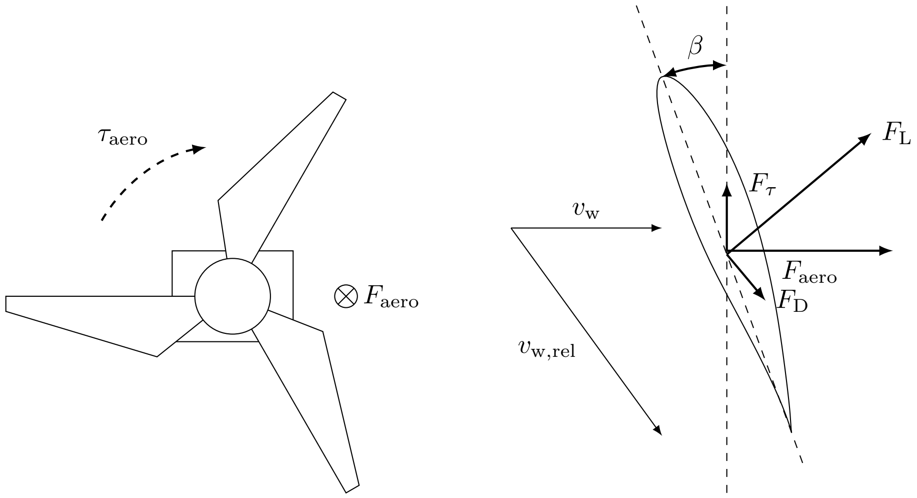
In the above section, the coordinate systems which will be used in the modelling of the wind turbine have been defined. In the following section, the aerodynamic model will be developed.

6.3 Aerodynamic Model

The aerodynamic model describes the connection between the wind and the resulting effects on the wind turbine, as illustrated in Figure 6.1 on Page 27.

The rotor of the wind turbine captures some of the kinetic energy in the wind, and converts it into mechanical energy, which in turn is turned into electrical energy through a generator. The aerodynamic forces acting on the wind turbine will be modelled according to [FDB07]. All forces will be described in the nacelle coordinate system $\mathcal{N}$.

A wind turbine rotor works by deflecting the wind by means of cambered blades and appropriate angles of attack, producing a lift force (F_{L}) perpendicular to the wind direction and a drag force (F_{D}) along the wind direction. An example cross-section of a wind turbine blade, with wind direction and resulting forces, is illustrated in Figure 6.4b.



(a) *Rotor effects* **(b)** *Cross-section of a wind turbine blade*

Figure 6.4: *Left the rotor, with the aerodynamic torque (τ_{aero}) and thrust force (F_{aero}), is shown. Right the aerodynamic lift (F_{L}) and drag (F_{D}) forces affecting the blade are shown. The forces can be resolved into a rotor force (F_{τ}) and rotor thrust (F_{aero}). The wind speed is denoted v_{w} and the wind speed relative to the rotation of the rotor denoted $v_{\text{w,rel}}$. The forces affecting the blade change with the blade-pitch angle (β).*

The lift and drag forces are dependent on the angle of attack. Different angles of attack can be achieved by pitching of the blades. The lift and drag forces can be resolved into the nacelle coordinates, one giving a thrust force (F_{aero}) along ${}^{\text{n}}x$ and one giving a torque τ_{aero} around ${}^{\text{n}}x$, as illustrated in Figure 6.4a. During normal operation a lift/drag ratio giving a high torque is wanted. During shutdown, the wind turbine can be actively stopped by pitching of the blades such that a negative torque is obtained.

An appropriate measure of the relative wind speed is the tip speed ratio, given in (6.2). The tip speed ratio λ is a unit-less number describing the ratio of the blade tip speed to the wind speed, given as

$$\lambda = \frac{R\omega_{\text{r}}}{v_{\text{w}}}, \tag{6.2}$$

where R and v_{w} denotes the rotor radius and horizontal hub height wind speed respectively.

The kinetic power P_{w} in the wind through the rotor coverage area A is given as

$$P_{\text{w}} = \frac{1}{2}\rho A {v_{\text{w}}}^3, \tag{6.3}$$

where ρ denotes the air density.

As the lift and drag forces are complex, the resulting power, thrust and torque are usually calculated offline as efficiency coefficients and used as lookup tables. The power coefficient (C_{p}) describes the amount of power that can be captured from the wind in (6.3). The power coefficient is usually written in terms of the collective blade-pitch β and the tip-speed ratio λ. The captured aerodynamic power is calculated as

$$P_{\text{aero}} = P_{\text{w}} C_{\text{p}}(\lambda, \beta) = \frac{1}{2}\rho A {v_{\text{w}}}^3 C_{\text{p}}(\lambda, \beta), \tag{6.4}$$

with $C_{\text{p}}(\lambda, \beta)$ typically given as a lookup table.

The torque delivered to the rotor can likewise be described using the torque coefficient (C_q) as

$$\tau_\mathrm{aero} = \frac{1}{2}\rho A R {v_\mathrm{w}}^2 C_\mathrm{q}(\lambda, \beta), \tag{6.5}$$

with $C_\mathrm{q}(\lambda, \beta)$ typically given as a lookup table.

The torque coefficient can be calculated from the power coefficient by

$$C_\mathrm{q} = C_\mathrm{p}/\lambda.$$

The aerodynamic thrust force is similarly described as

$$F_\mathrm{aero} = \frac{1}{2}\rho A {v_\mathrm{w}}^2 C_\mathrm{t}(\lambda, \beta), \tag{6.6}$$

with $C_\mathrm{t}(\lambda, \beta)$ typically given as a lookup table.

Lookup tables of C_p, C_q and C_t coefficients used in (6.4), (6.5) and (6.6) matching the aerodynamic properties of the NREL 5-MW wind turbine are generated using the software `WT_Perf` [Buh11]. The resulting tables are illustrated in Figure 6.5.

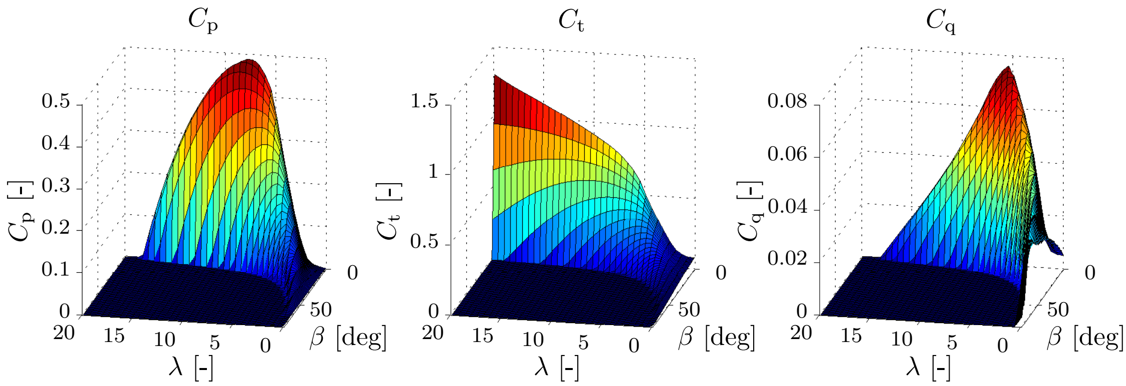


Figure 6.5: *Power (left), thrust (middle) and torque (right) coefficient lookup tables matching the aerodynamic properties of the NREL 5-MW wind turbine. Negative values in all tables have been set to zero.*

The power generated by the wind turbine is usually essential in the modelling. However from a safety perspective, the torque and thrust generated by the rotor are essential. In order to model the rotor torque and thrust force, Equation (6.5) and (6.6) must be implemented in the model. This implies according to Section 6.1 that the equations must be on polynomial form. Disregarding the lookup tables, the torque (6.5) and thrust (6.6) equations are on polynomial form. The lookup table will be approximated by polynomials. The tables in (6.5) and (6.6) are given as functions of λ and β. The definition of λ in (6.2) is not on polynomial form (as v_w in the denominator is variable). It is chosen to separate λ into the wind speed v_w and the angular velocity of the rotor ω_r. The polynomials representing the torque and thrust coefficients will, as a result, be given as functions of the three variables v_w, ω_r and β, given by

$$C_x(v_\mathrm{w}, \omega_\mathrm{r}, \beta),$$

with $C_x(v_\mathrm{w}, \omega_\mathrm{r}, \beta)$ being on polynomial form, as given in Equation (6.1).

Lookup tables of $C_\mathrm{q}(v_\mathrm{w}, \omega_\mathrm{r}, \beta)$ and $C_\mathrm{t}(v_\mathrm{w}, \omega_\mathrm{r}, \beta)$ coefficients, are generated using `WT_Perf`. The tables are found by calculating C_q and C_t for at range of v_w, ω_r and β, resulting in multidimensional matrices. As the approximation of a polynomial to the lookup tables is linear in the unknown coefficients, least squares can be used in the approximation. Details regarding the approximation can be found in Appendix B.

The normalised sum of squares errors using different polynomial degrees are illustrated in Figure 6.6.

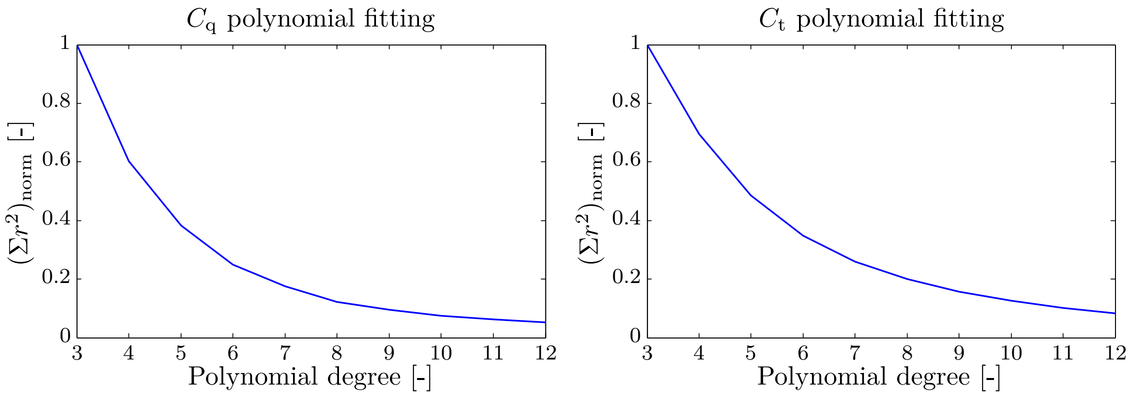


Figure 6.6: *Normalised sum of squares errors using different polynomial degrees. The left and right plots illustrate the C_q and C_t approximation errors respectively.*

The choice of polynomial degree in the approximation of C_q and C_t is a compromise between the accuracy of the approximation and the complexity of the resulting polynomial. In Figure 6.7 and 6.8 the C_q and C_t approximations using 10^{th} degree polynomials are illustrated. The surfaces illustrate the polynomial approximations to the lookup tables illustrated by black dots. The polynomial approximations are illustrated for 4 fixed values of the wind speed v_w.

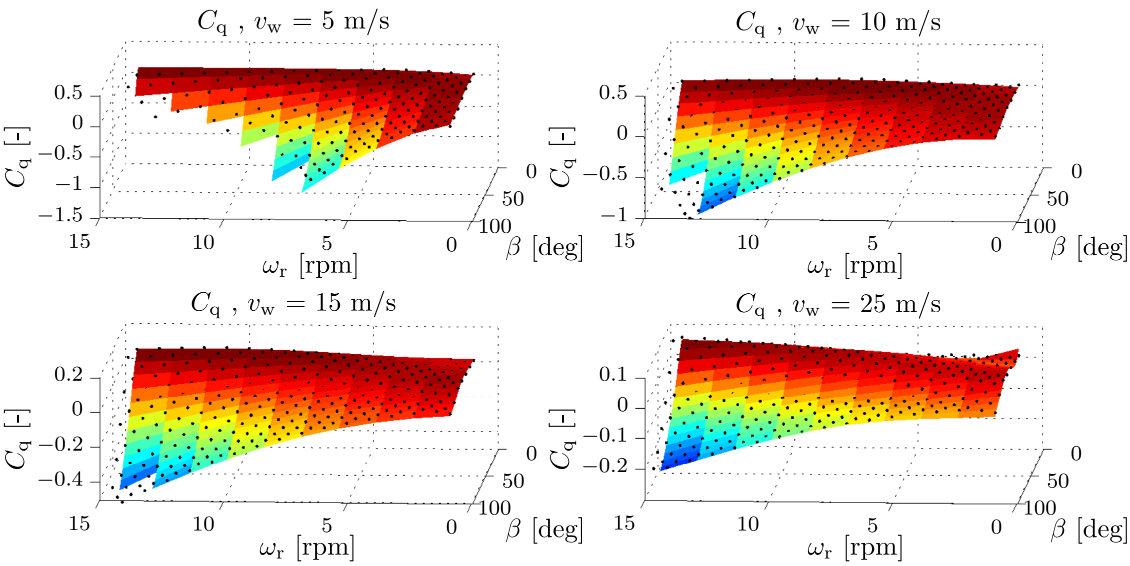


Figure 6.7: *Polynomial approximation of the C_q lookup table. The surface illustrates the polynomial approximation to the lookup table given as black dots. The approximation is illustrated for four fixed values of the wind speed v_w.*

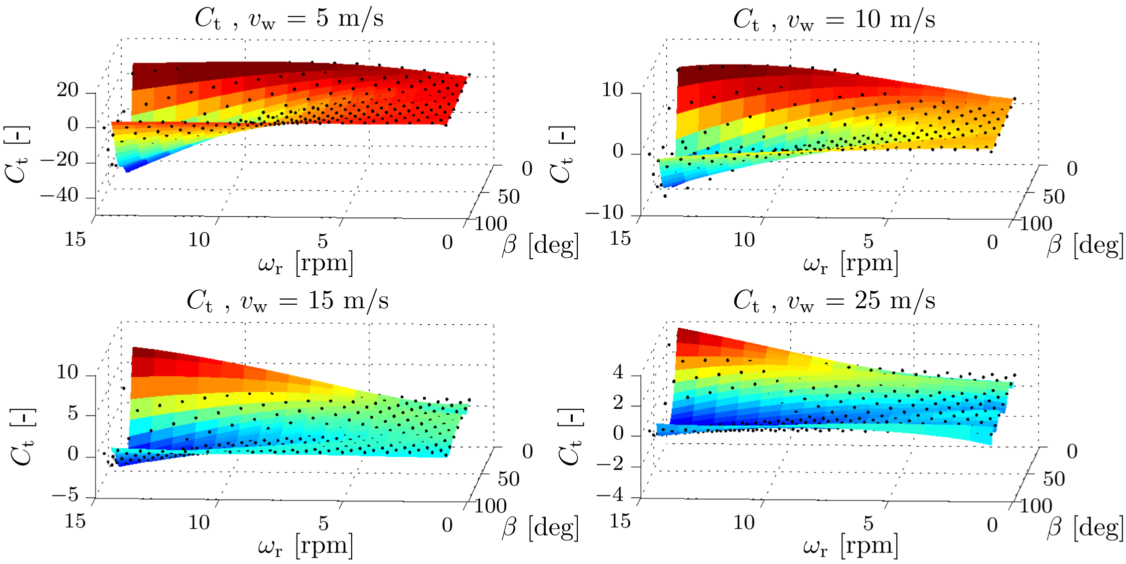


Figure 6.8: *Polynomial approximation of the C_t lookup table. The surface illustrates the polynomial approximation to the lookup table given as black dots. The approximation is illustrated for four fixed values of the wind speed v_w.*

The polynomial approximations illustrated in Figure 6.7 and 6.8 are valid in the wind interval $v_w = [3 \text{ m/s} ; 30 \text{ m/s}]$.

Using the polynomial approximation, the aerodynamic torque model is given as

$$\tau_{\text{aero}} = \frac{1}{2}\rho A R {v_w}^2 C_q(v_w, \omega_r, \beta), \tag{6.7}$$

with $C_q(v_w, \omega_r, \beta)$ being the polynomial approximation of the C_q lookup table.

Likewise, using the polynomial approximation, the aerodynamic thrust force model is given as

$$F_{\text{aero}} = \frac{1}{2}\rho A {v_w}^2 C_t(v_w, \omega_r, \beta), \tag{6.8}$$

with $C_t(v_w, \omega_r, \beta)$ being the polynomial approximation of the C_t lookup table.

Equation (6.7) and (6.8) are now on polynomial form and can be used in the model. In Section 6.4.3 the rotor will be connected to the top of the tower. As the tower top is not stationary, the effective wind speed experienced by the rotor will be a function of wind speed v_w and the fore-aft velocity of the tower top ${}^{t}v_{fa,x}$. The aerodynamic equations will as a result be functions of the effective wind speed v_{eff}

$$\tau_{\text{aero}} = \frac{1}{2}\rho A R {v_{\text{eff}}}^2 C_q(v_{\text{eff}}, \omega_r, \beta), \; F_{\text{aero}} = \frac{1}{2}\rho A {v_{\text{eff}}}^2 C_t(v_{\text{eff}}, \omega_r, \beta),$$

with $v_{\text{eff}} = v_w - {}^{t}v_{fa,x}$.

In the above section, a polynomial model of the aerodynamic torque and thrust force has been developed. The aerodynamic torque τ_{aero} and the aerodynamic thrust force F_{aero} are transferred to the mechanical structure of the wind turbine. In the following chapter, the model of the structural parts of the wind turbine will be developed.

6.4 Structural Model

The structural modelling of the wind turbine will be divided into subsystems which will later be connected. The subsystems include the drive train (Section 6.4.1), the blades (Section 6.4.2) and the tower (Section 6.4.3).

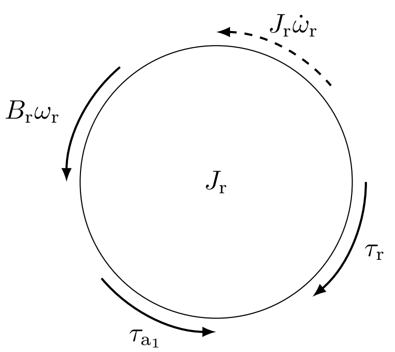
6.4.1 Drive train

In the following, the model of the drive train is developed. The purpose of the drive train is to connect the rotor to the generator. In most modern wind turbines the drive train includes a gearing, to increase the angular velocity of the rotor shaft to be suitable in the electrical generation.

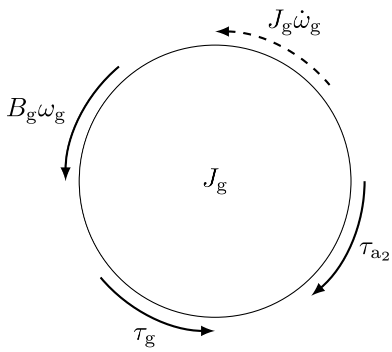
The drive train model is divided into three parts: the rotor, the gear and the generator, as in [SWBB11]. The rotor connects to the gearbox and the gearbox connects to the generator by rotating shafts. As the shafts are relatively elastic, the shafts will introduce dynamics. This will be modelled as a torsional spring. Both the rotor and the generator have an angular momentum. Each of the parts will be considered as free-body elements. The drive train is modelled in the nacelle coordinate system $\boldsymbol{\mathcal{N}}$. The complete calculations done in this chapter can be found in Appendix C.

The rotor is modelled as a rotational disc. The moment of inertia of the disc results in an angular momentum. The rotation of the disc is damped by a rotational viscous friction proportional to the angular velocity of the disc. The rotor is driven by the rotor torque τ_{r}. Finally the rotor is connected to the load torque of the gearbox τ_{a_1}.

The rotor and generator are illustrated as free body diagrams in Figure 6.9



(a) *Rotor*



(b) *Generator*

,

Figure 6.9: *Free body diagrams of the rotor and generator.*

where ω_{r} is the angular velocity of the rotor, B_{r} is the rotor friction, J_{r} is the inertia of the rotor, τ_{a_1} is the torque from the shaft, τ_{r} is the torque from the rotor, ω_{g} is the angular velocity of the generator, B_{g} is the generator friction, J_{g} is the inertia of the generator, τ_{a_2} is the torque from the shaft at the other side of the gearbox and τ_{g} is the applied torque from the generator.

From Figure 6.9a the model describing the rotor body can be found using D'Alembert's law,

$$J_{\mathrm{r}}\dot{\omega}_{\mathrm{r}} = \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \tau_{\mathrm{a}_1}. \tag{6.9}$$

The generator is driven by the torque from the gearbox. As with the rotor, the generator includes angular momentum and friction. Additionally the generator introduces a variable load torque τ_{g}.

The model of the generator is likewise given as,

$$J_g \dot{\omega}_g = \tau_{a_2} - B_g \omega_g - \tau_g. \tag{6.10}$$

The gearbox, including the rotational shafts, connects the rotor to the generator as illustrated in Figure 6.10. The rotor to gearbox and the gearbox to generator shafts are denoted a_1 and a_2 respectively. The gearbox gearing ratio is denoted N. The reference angles of the rotor and generator are denoted θ_r and θ_g respectively. It is assumed that the inertia of the gearbox is small compared to the inertia of the rotor and the generator, and is as a result set to zero.

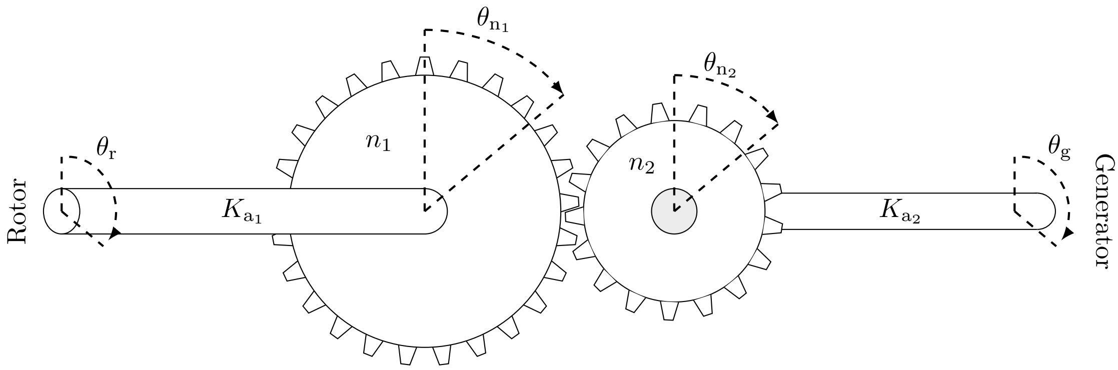


Figure 6.10: *The rotor is connected to the generator through two flexible shafts and a gearbox*

The gear ratio is given by the ratio of the number of teeth as

$$N = \frac{n_2}{n_1},$$

where n_1 is the number of teeth on the rotor gear and n_2 is the number of teeth on the generator gear. It should be noted that the choice of gear ratio results in $N < 1$.

The shafts are flexible with a stiffness K_{a_1} and K_{a_2}. Additionally damping in the torsion of the shafts is included. The torques delivered by the shafts are given as

$$\tau_{a_1} = K_{a_1}(\theta_r - \theta_{n_1}) + B_{a_1}(\omega_r - N\omega_g), \tag{6.11}$$

$$\tau_{a_2} = K_{a_2}\left(\frac{\theta_{n_1}}{N} - \theta_g\right), \tag{6.12}$$

where θ_{n_1} is the angle of the rotor gear, K_{a_1} is the stiffness coefficient of the rotor shaft, K_{a_2} is the stiffness coefficient of the generator shaft and B_{a_1} is the friction coefficient of the torsion, as illustrated in Figure 6.10.

The torque produced by the rotor is transferred to the generator through the two shafts and the gearing. The sum of the torques through the gear equals zero. The angle of the of the gearbox (θ_{n_1} in Figure 6.10) is found by

$$0 = K_{a_1}(\theta_r - \theta_{n_1}) + B_{a_1}(\omega_r - N\omega_g) - \left(K_{a_2}\left(\frac{\theta_{n_1}}{N} - \theta_g\right)\right)\frac{1}{N} \quad \Leftrightarrow$$

$$\theta_{n_1} = \frac{N(K_{a_1}N\theta_r + K_{a_2}\theta_g + B_{a_1}N(\omega_r - N\omega_g))}{K_{a_1}N^2 + K_{a_2}}. \tag{6.13}$$

In (6.13) the angle of the gearbox θ_{n_1} is given as a function of the rotor and generator angles and the rotor and generator angular velocities.

The interconnecting torques in (6.11) and (6.12) are substituted into (6.9) and (6.10), which becomes

$$J_\mathrm{r}\dot{\omega}_\mathrm{r} = \tau_\mathrm{r} - B_\mathrm{r}\omega_\mathrm{r} - \left[K_{\mathrm{a}_1}(\theta_\mathrm{r} - \theta_{\mathrm{n}_1}) + B_{\mathrm{a}_1}(\omega_\mathrm{r} - N\omega_\mathrm{g})\right], \tag{6.14}$$

$$J_\mathrm{g}\dot{\omega}_\mathrm{g} = K_{\mathrm{a}_2}\left(\frac{\theta_{\mathrm{n}_1}}{N} - \theta_\mathrm{g}\right) - B_\mathrm{g}\omega_\mathrm{g} - \tau_\mathrm{g}. \tag{6.15}$$

The angular position of the gear in (6.13) is substituted into (6.14) giving

$$\begin{aligned} J_\mathrm{r}\dot{\omega}_\mathrm{r} &= \tau_\mathrm{r} - B_\mathrm{r}\omega_\mathrm{r} - \left\{K_{\mathrm{a}_1}\left[\theta_\mathrm{r} - \frac{N(K_{\mathrm{a}_1}N\theta_\mathrm{r} + K_{\mathrm{a}_2}\theta_\mathrm{g} + B_{\mathrm{a}_1}N(\omega_\mathrm{r} - N\omega_\mathrm{g}))}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}\right] + B_{\mathrm{a}_1}(\omega_\mathrm{r} - N\omega_\mathrm{g})\right\} \\ &= \tau_\mathrm{r} - B_\mathrm{r}\omega_\mathrm{r} - \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}(\theta_\mathrm{r} - N\theta_\mathrm{g}) - \frac{B_{\mathrm{a}_1}K_{\mathrm{a}_1}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}(\omega_\mathrm{r} - N\omega_\mathrm{g}). \end{aligned} \tag{6.16}$$

The angular position of the gear in (6.13) is substituted into (6.15) giving

$$\begin{aligned} J_\mathrm{g}\dot{\omega}_\mathrm{g} &= K_{\mathrm{a}_2}\left(\frac{1}{N}\left(\frac{N(K_{\mathrm{a}_1}N\theta_\mathrm{r} + K_{\mathrm{a}_2}\theta_\mathrm{g} + B_{\mathrm{a}_1}N(\omega_\mathrm{r} - N\omega_\mathrm{g}))}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}\right) - \theta_\mathrm{g}\right) - B_\mathrm{g}\omega_\mathrm{g} - \tau_\mathrm{g} \\ &= \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}N(\theta_\mathrm{r} - N\theta_\mathrm{g}) + \frac{B_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}N(\omega_\mathrm{r} - N\omega_\mathrm{g}) - B_\mathrm{g}\omega_\mathrm{g} - \tau_\mathrm{g}. \end{aligned} \tag{6.17}$$

Identical constant terms are found in both (6.16) and (6.17). New coefficients describing the torsional angle, the total torsional spring constant and the total damping constant are introduced as

$$\theta_\Delta \triangleq \theta_\mathrm{r} - N\theta_\mathrm{g},\ K_\mathrm{a} \triangleq \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}},\ B_\mathrm{a} \triangleq \frac{B_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}, \tag{6.18}$$

where θ_Δ is the torsional angle, K_a is the total spring constant and B_a is the total friction constant.

By inserting (6.18) into (6.16) and (6.17) the state space equations for the entire drive train becomes

$$\begin{aligned} \dot{\omega}_\mathrm{r} &= J_\mathrm{r}^{-1}\left[\tau_\mathrm{r} - B_\mathrm{r}\omega_\mathrm{r} - K_\mathrm{a}\theta_\Delta - B_\mathrm{a}(\omega_\mathrm{r} - N\omega_\mathrm{g})\right], \\ \dot{\omega}_\mathrm{g} &= J_\mathrm{g}^{-1}\left[K_\mathrm{a}N\theta_\Delta + B_\mathrm{a}N(\omega_\mathrm{r} - N\omega_\mathrm{g}) - B_\mathrm{g}\omega_\mathrm{g} - \tau_\mathrm{g}\right], \\ \dot{\theta}_\Delta &= \omega_\mathrm{r} - N\omega_\mathrm{g}. \end{aligned} \tag{6.19}$$

The resulting states are the torsion of the shafts θ_Δ, the angular velocity of the rotor ω_r and the angular velocity of the generator ω_g. The model in (6.19) is linear, with the connection to the rotor torque τ_r being polynomial. Consequently, the model can be used directly, as the model complies with the required model structure defined in Section 6.1.

In Figure 6.11 the angular velocity of the rotor, the angular velocity of the generator and the shaft torsion are simulated, using the above simplified model, and compared to the `FAST` simulator. The behaviour of the wind and the blade-pitch angle are identical in the two simulations.

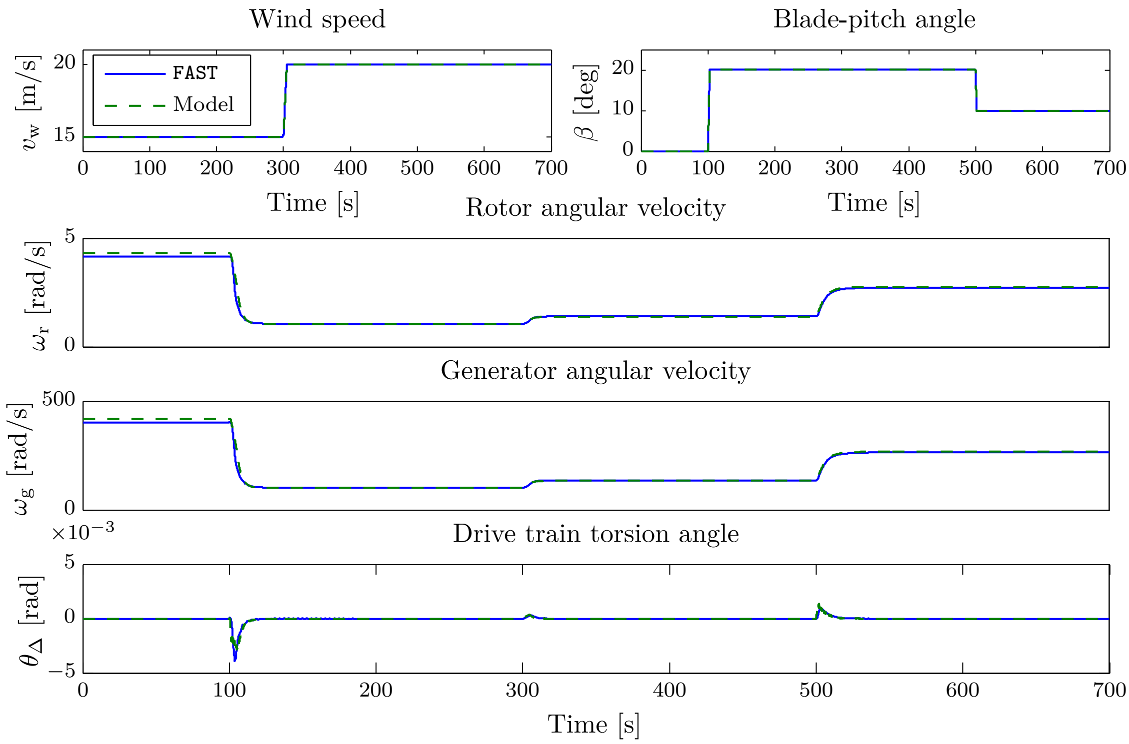


Figure 6.11: *Simulation results of rotor speed, generator speed and shaft torsion. The simplified model is compared to the FAST simulator. The behaviour of the wind and the blade-pitch angle are identical in both simulations. The simulation illustrates an extreme situation without generator torque.*

In the above section, a simplified model of a wind turbine drive train was developed. The drive train is driven by the torque from the rotor. The rotor torque is partly given by the aerodynamic model described in Section 6.3 and partly by the blade model developed in the following section.

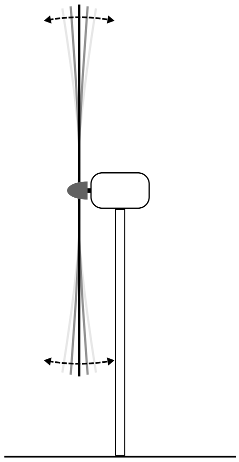
6.4.2 Blades

In this section the model of the wind turbine blades will be developed. The three blades form the rotor which is connected to the drive train and is affected by the wind. The connections of the blade model to the remaining model are illustrated in Figure 6.1 on page 27.

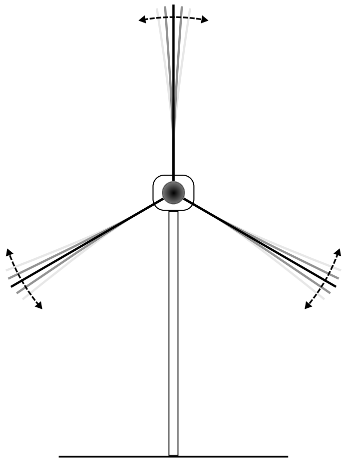
The blades of a wind turbine are relatively flexible and will consequently introduce additional dynamics to the system. According to [TGKP04] the bending of the blades should be considered a significant part of the rotor and drive train dynamics, actually being more dominant than the flexibility of the drive train shaft in relation to the dynamics of the system.

The bending of the blades is separated into motion parallel to the axis of rotation of the rotor and motion in the plane of rotation, referred to as flapwise and lead-lag bending respectively [JFM09]. Lead-lag motions introduce fluctuations in torque in the drive train. Equivalently, the flapwise motion introduces translational forces parallel to the axis of rotation. These forces will directly affect the bending of the wind turbine tower.

The flapwise and lead-lag bendings are illustrated in Figure 6.12.



(a) *Flapwise blade bending*



(b) *Lead-lag blade bending*

Figure 6.12: *Illustration of flapwise and lead-lag bending of the wind turbine blades*

To simplify the modelling of the blade bending, the blades will be considered being piecewise rigid. The motion of the blades is only allowed in *hinges* between the rigid pieces. This approach is known as a hinge-spring model. Additionally the motions of the three blades are assumed to be identical, such that the three blades can be considered as one object, i.e. a rotatory disc modelled in the hub coordinate system.

Both flapwise and lead-lag bending will be modelled as simple mass, spring and damper systems. Each blade is considered to be consisting of two rigid pieces connected by a hinge. The position of the hinge is denoted the *break point*. As the geometry of the blade is not uniform, the position of the break point along the blade might not be identical, when considering flapwise and lead-lag bending.

The simple hinged blade model is illustrated in Figure 6.13.

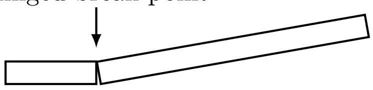


Figure 6.13: *Hinged blade model. The blade is composed by two rigid pieces, which can bend in the hinge, denoted the break point.*

In the following, the flapwise and lead-lag bending will be modelled using the hinged blade model principle.

Flapwise blade bending

Flapwise bending of the blades refers to the motion of the blades parallel to the axis of rotation of the rotor. In the case that the wind turbine is aligned with the wind direction, flapwise bending will additionally be parallel to the direction of the wind. According to [JFM09] the flapwise bending is the single factor which induces the largest load on the blades. The flapwise motion of the blades additionally introduces forces which affect the fore-aft motion of the tower and vice versa.

In Figure 6.14 the hinged model of the flapwise bending is illustrated. The mass M_{flap} is a fictitious mass of the blade beyond the break point.

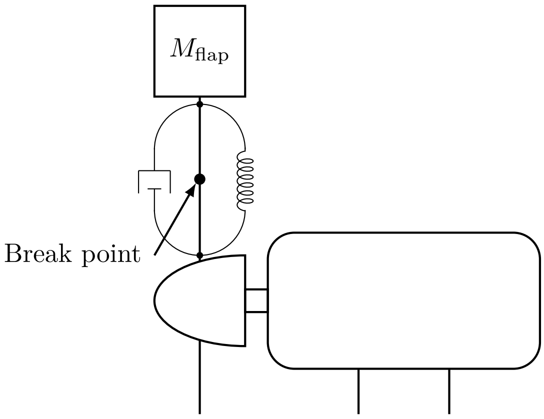
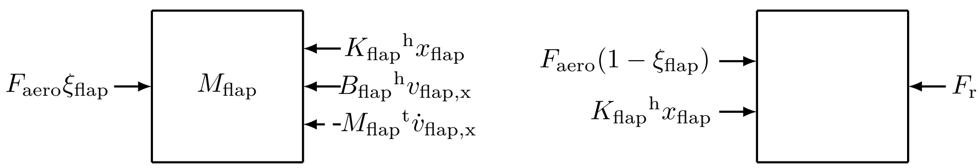


Figure 6.14: *Flapwise blade bending as mass, spring and damper system. The blade bends in the break point.*

The hinged blade is affected by the thrust force of the wind. Some of the wind will hit the hinged part of the blade and some the rigid part. The proportion of the wind force which affects the hinged part of the blade is denoted ξ_{flap}. The remaining wind force will affect the rigid part of the blade directly.

The load of the hinged spring is determined by the ${}^{\text{h}}x$ displacement of the blade tip. The position of the blade tip will be denoted ${}^{\text{h}}x_{\text{flap}}$. The velocity of the blade tip is likewise denoted ${}^{\text{h}}v_{\text{flap,x}}$ in the hub coordinate system $\boldsymbol{\mathcal{H}}$ and ${}^{\text{t}}v_{\text{flap,x}}$ in the tower coordinate system $\boldsymbol{\mathcal{T}}$. It is as mentioned, assumed that the motions of the three blades are identical.

The states of the system are the flapwise velocity of the tip mass and the flapwise displacement of the blade tip. The hinged part of the blade and the inner part of the blade are considered as two rigid bodies. The bodies are illustrated in Figure 6.15



(a) *Hinged part of the blades* **(b)** *Rigid part of the blades*

,

Figure 6.15: *Model of flapwise blade tip displacement separated into two rigid bodies.*

where K_{flap} is the spring constant of the blade flapping, B_{flap} is the damping of the blade flapping, ξ_{flap} is the proportion of the wind thrust which hits the hinged part of the blade, F_{r} is the total horizontal rotor force along ${}^{\text{n}}x$ delivered by the rotor and F_{aero} is the thrust of the wind field given in (6.8).

From Figure 6.15a the model of the hinged part of the blades can be found as

$$F_{\text{aero}}\xi_{\text{flap}} = K_{\text{flap}}{}^{\text{h}}x_{\text{flap}} + B_{\text{flap}}{}^{\text{h}}v_{\text{flap,x}} + M_{\text{flap}}{}^{\text{t}}\dot{v}_{\text{flap,x}}.$$

From Figure 6.15b the total thrust force from the rotor disc is given as

$$F_{\text{r}} = F_{\text{aero}}(1-\xi_{\text{flap}}) + K_{\text{flap}}{}^{\text{h}}x_{\text{flap}}. \tag{6.20}$$

As the rotor is connected to the tower, the rotor force F_r will be delivered to the tower structure.

The flapwise blade model is in state space form given as

$$\begin{aligned} {}^{\mathrm{t}}\dot{v}_{\mathrm{flap,x}} &= M_{\mathrm{flap}}^{-1}\left[F_{\mathrm{aero}}\xi_{\mathrm{flap}} - K_{\mathrm{flap}}{}^{\mathrm{h}}x_{\mathrm{flap}} - B_{\mathrm{flap}}{}^{\mathrm{h}}v_{\mathrm{flap,x}}\right], \\ {}^{\mathrm{h}}\dot{x}_{\mathrm{flap}} &= {}^{\mathrm{h}}v_{\mathrm{flap,x}}. \end{aligned} \tag{6.21}$$

To avoid describing the motion of the blades partly in the hub coordinate system $\boldsymbol{\mathcal{H}}$ and partly in the tower coordinate system $\boldsymbol{\mathcal{T}}$, all coordinates are rewritten with respect to the hub coordinate system. To do this the top of the tower is used as reference.

Assuming small bending angles of the tower, the transformation of coordinates is given as

$$\begin{aligned} {}^{\mathrm{t}}x_{\mathrm{flap}} &= {}^{\mathrm{h}}x_{\mathrm{flap}} + {}^{\mathrm{t}}x_{\mathrm{fa}}, \\ {}^{\mathrm{t}}v_{\mathrm{flap,x}} &= {}^{\mathrm{h}}v_{\mathrm{flap,x}} + {}^{\mathrm{t}}v_{\mathrm{fa,x}}, \end{aligned} \tag{6.22}$$

where ${}^{\mathrm{t}}x_{\mathrm{fa}}$ and ${}^{\mathrm{t}}v_{\mathrm{fa,x}}$ are the fore-aft displacement and velocity of the tower top in the tower coordinate system $\boldsymbol{\mathcal{T}}$ respectively.

Inserting (6.22) in (6.21) results in the flapwise blade state space equations given as

$$\begin{aligned} {}^{\mathrm{h}}\dot{v}_{\mathrm{flap,x}} &= M_{\mathrm{flap}}^{-1}\left[F_{\mathrm{aero}}\xi_{\mathrm{flap}} - K_{\mathrm{flap}}{}^{\mathrm{h}}x_{\mathrm{flap}} - B_{\mathrm{flap}}{}^{\mathrm{h}}v_{\mathrm{flap,x}}\right] - {}^{\mathrm{t}}\dot{v}_{\mathrm{fa,x}}, \\ {}^{\mathrm{h}}\dot{x}_{\mathrm{flap,x}} &= {}^{\mathrm{h}}v_{\mathrm{flap,x}}. \end{aligned} \tag{6.23}$$

The flapwise blade model introduces two additional states, the flapwise displacement and the velocity of the blade tip.

The blade flapping model in (6.23) satisfy the required model structure given in Section 6.1. The force induced by the flapwise motion can be linked to the tower model using Equation (6.20).

In the following, the blade lead-lag bending model will be developed.

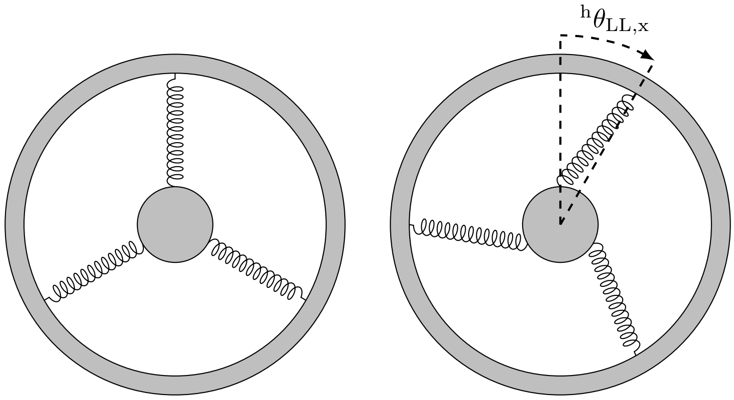
Lead-lag blade bending

The angular acceleration or deceleration of the rotor will result in a bending of the blades in the plane of rotation. As with the flapwise blade bending, the lead-lag blade bending will be considered equal for each blade. If the angle of the blade tips in the plane of rotation is positive, the blades are said to be leading the rotor. Likewise the blades are said to be lagging the rotor if the angle is negative.

The modelling of the blade bending is approximated by representing the rotor as a two inertia model as in [TGKP04]. The outer part of the blades act as a single inertia, while the inner part of the blades combined with the hub comprises the inner inertia. The separation point of the inner and outer part of the blade is the blade break point.

The lead-lag blade bending angle and angular velocity are given in the hub coordinate system $\boldsymbol{\mathcal{H}}$, and denoted ${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}$ and ${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}$ respectively. The blade tip angular velocity is in the nacelle coordinate system $\boldsymbol{\mathcal{N}}$ denoted ${}^{\mathrm{n}}\omega_{\mathrm{LL,x}}$.

The two inertia blade lead-lag model is illustrated in Figure 6.16. The inner disc represents the inertia of the inner rigid part of the blades. The outer disc represents the inertia of the outer hinged part of the blades. In accordance with the hinged blade model, the two inertias are linked by a spring and damper system.



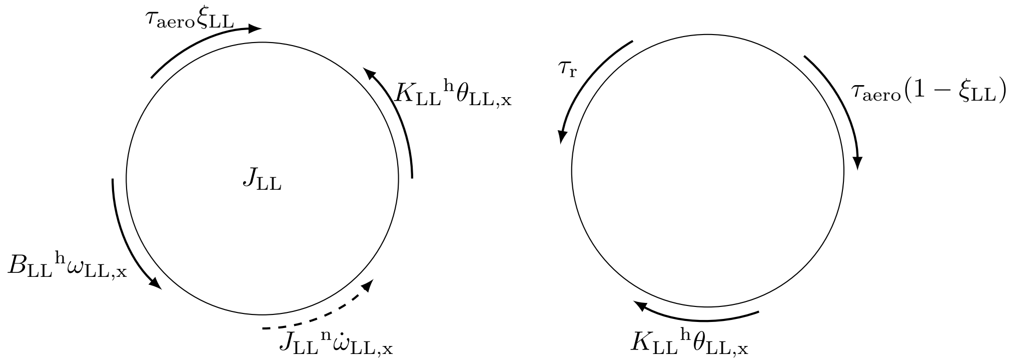
(a) *Inner and outer inertias are synchronous*

(b) *The blade tips lead the hub*

Figure 6.16: *The two inertia rotor model. In 6.16a the lead-lag angle is zero. In 6.16b the blade tips lead the inner part of the rotor, resulting in a positive lead-lag blade bend angle.*

The hinged lead-lag blade bending is affected by the aerodynamic torque of the wind. Some of the aerodynamic torque will affect the hinged part of the blade and some the rigid part. The proportion of the aerodynamic torque which affects the hinged part of the blade is denoted ξ_{LL}. The remaining aerodynamic torque will affect the inner rigid part of the rotor directly.

In Figure 6.17 the inner and the outer part of the rotor are separated into two bodies.



(a) *Outer hinged part of the blades*

(b) *Inner rigid part of the blades*

Figure 6.17: *Free body diagrams of the inner and outer blade parts.*

From Figure 6.17 the model equations are given as

$$\begin{aligned} \tau_{\mathrm{aero}}\xi_{\mathrm{LL}} &= J_{\mathrm{LL}}{}^{\mathrm{n}}\dot{\omega}_{\mathrm{LL,x}} + B_{\mathrm{LL}}{}^{\mathrm{h}}\omega_{\mathrm{LL,x}} + K_{\mathrm{LL}}{}^{\mathrm{h}}\theta_{\mathrm{LL,x}}, \\ \tau_{\mathrm{r}} &= \tau_{\mathrm{aero}}(1-\xi_{\mathrm{LL}}) + K_{\mathrm{LL}}{}^{\mathrm{h}}\theta_{\mathrm{LL,x}}. \end{aligned} \tag{6.24}$$

The lead-lag blade bending model is in state space form given as

$$\begin{aligned} {}^{\mathrm{n}}\dot{\omega}_{\mathrm{LL,x}} &= J_{\mathrm{LL}}^{-1}\left[\tau_{\mathrm{aero}}\xi_{\mathrm{LL}} - B_{\mathrm{LL}}{}^{\mathrm{h}}\omega_{\mathrm{LL,x}} - K_{\mathrm{LL}}{}^{\mathrm{h}}\theta_{\mathrm{LL,x}}\right], \\ {}^{\mathrm{h}}\dot{\theta}_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\omega_{\mathrm{LL,x}}. \end{aligned}$$

As with the blade flapping model, a change of coordinates are introduced, such that the system states are given in hub coordinates only. The change of coordinates are given as

$$
\begin{aligned}
{}^{\mathrm{n}}\theta_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\theta_{\mathrm{LL,x}} + \theta_{\mathrm{r}}, \\
{}^{\mathrm{n}}\omega_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\omega_{\mathrm{LL,x}} + \omega_{\mathrm{r}},
\end{aligned}
$$

where θ_{r} and ω_{r} denotes the rotor angle and angular velocity given in the nacelle coordinate system respectively.

The resulting state space description is given as

$$
\begin{aligned}
{}^{\mathrm{h}}\dot{\omega}_{\mathrm{LL,x}} &= J_{\mathrm{LL}}^{-1}\left[\tau_{\mathrm{aero}}\xi_{\mathrm{LL}} - B_{\mathrm{LL}}\,{}^{\mathrm{h}}\omega_{\mathrm{LL,x}} - K_{\mathrm{LL}}\,{}^{\mathrm{h}}\theta_{\mathrm{LL,x}}\right] - \dot{\omega}_{\mathrm{r}}, \\
{}^{\mathrm{h}}\dot{\theta}_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\omega_{\mathrm{LL,x}}.
\end{aligned}
\tag{6.25}
$$

The lead-lag blade model introduces the lead-lag bending angle ${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}$ and the angular velocity ${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}$ of the blade tips as additional states.

The blade lead-lag model in (6.25) satisfy the required model structure given in Section 6.1. The model can directly be combined with the drive-train model given in (6.19) by using (6.24).

In Figure 6.18 the flapwise blade model and the lead-lag blade model are simulated using varying wind speeds and a constant 15° pitch (β) angle and compared to a similar simulation using the `FAST` simulator. The `FAST` simulator considers individual bending of the three wind turbine blades. To get comparable results, the mean bending of the three blades is used.

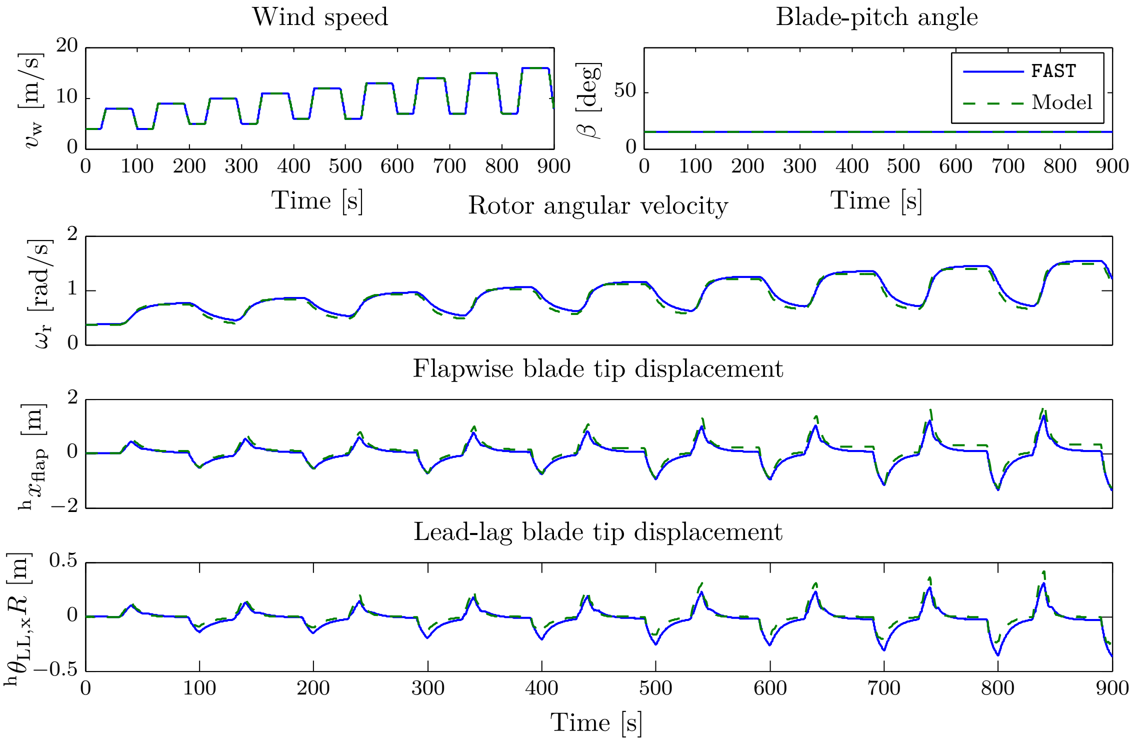


Figure 6.18: *Simulation results of blade bending. The result of the `FAST` simulation is given as the mean bending of the three blades. Note that the lead-lag angle is multiplied by the rotor radius R to obtain a lead-lag blade tip displacement, which can be compared to the blade flapwise tip displacement.*

From Figure 6.18 it seems that the flapwise and lead-lag simulation results are offset slightly compared to the `FAST` simulator. However, the flapwise and lead-lag blade models are considered sufficiently accurate.

In the above section, models of the flapwise and lead-lag bending of the blades have been developed. The models can be connected to the remaining model of the wind turbine as illustrated in Figure 6.1 on Page 27. In the following section, the wind turbine tower will be modelled.

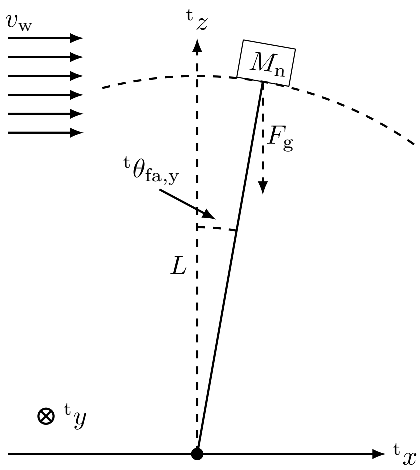
6.4.3 Tower

The wind turbine tower is affected by several different forces; aerodynamic forces from the rotor, acceleration and deceleration of the drive train and the gravitational force.

In the modelling of the tower it is assumed that the rotor axis is aligned with the wind direction. In this case the aerodynamic thrust force of the rotor will result in a motion of the tower along ${}^{\mathrm{t}}x$, which will be called the fore-aft motion of the tower. The generator torque and mechanical braking of the rotor will result in a side-side motion of the tower top along ${}^{\mathrm{t}}y$. As the side-side motion of the tower is considered insignificant in relation to emergency shutdown, the side-side effect will not be modelled.

The top of the tower will be modelled as a constant mass. The mass will be able to move along the ${}^{\mathrm{t}}x$-axis. The length of the tower is considered constant and the torsion of the tower is not considered, which results in one degree of freedom.

The dynamics of the tower will be modelled as a rigid lever connected to the ground by a hinge. The lever and hinge form a spring, mass and damper systems. The tower fore-aft bending along the ${}^{\mathrm{t}}x$-axis is illustrated in Figure 6.19

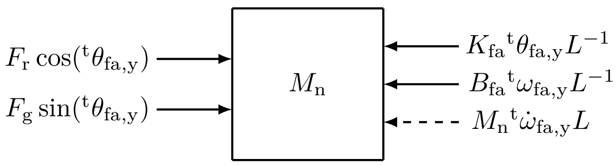


,

Figure 6.19: *Fore-aft motion of the tower given in the tower coordinate system $\mathcal{T}$*

where F_{g} denotes the gravitational force, M_{n} is the mass of the tower top, L is the length of the tower and ${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$ is the fore-aft angle of the tower bending.

The system illustrated in Figure 6.19 is given as a free-body diagram in Figure 6.20



,

Figure 6.20: *Forces affecting the tower top along the ${}^{\mathrm{t}}x$-axis (fore-aft) in the tower coordinate system $\mathcal{T}$*

where K_{fa} is the spring constant of the hinge and B_{fa} is the damping in the hinge.

From Figure 6.20 the tower system equations are found to

$$\begin{aligned} F_{\mathrm{r}}\cos({}^{\mathrm{t}}\theta_{\mathrm{fa,y}}) + F_{\mathrm{g}}\sin({}^{\mathrm{t}}\theta_{\mathrm{fa,y}}) &= K_{\mathrm{fa}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}}L^{-1} + B_{\mathrm{fa}}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}L^{-1} + M_{\mathrm{n}}{}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}}L \quad \Leftrightarrow \\ {}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} &= (M_{\mathrm{n}}L^2)^{-1}\left[F_{\mathrm{r}}L\cos({}^{\mathrm{t}}\theta_{\mathrm{fa,y}}) + F_{\mathrm{g}}L\sin({}^{\mathrm{t}}\theta_{\mathrm{fa,y}}) - K_{\mathrm{fa}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - B_{\mathrm{fa}}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}\right]. \end{aligned} \tag{6.26}$$

The system given in (6.26) is not on polynomial form. The system is simplified by introducing the following approximations $F_{\mathrm{r}}\cos({}^{\mathrm{t}}\theta_{\mathrm{fa,y}}) = F_{\mathrm{r}}$ and $F_{\mathrm{g}}\sin({}^{\mathrm{t}}\theta_{\mathrm{fa,y}}) = F_{\mathrm{g}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$. The approximations can be introduced under the assumption of small tower bending angles. The resulting state space description is given as

$$\begin{aligned} {}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} &= (M_{\mathrm{n}}L^2)^{-1}\left[F_{\mathrm{r}}L + F_{\mathrm{g}}L{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - K_{\mathrm{fa}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - B_{\mathrm{fa}}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}\right], \\ {}^{\mathrm{t}}\dot{\theta}_{\mathrm{fa,y}} &= {}^{\mathrm{t}}\omega_{\mathrm{fa,y}}. \end{aligned} \tag{6.27}$$

The state space description of the tower system given in (6.27) satisfy the required model structure given in Section 6.1.

In Figure 6.21 the tower bending is simulated using varying wind speeds and a constant 15° pitch angle (β) and compared to a similar simulation in the `FAST` simulator. The bending is in Figure 6.21 given as displacement of the tower top.

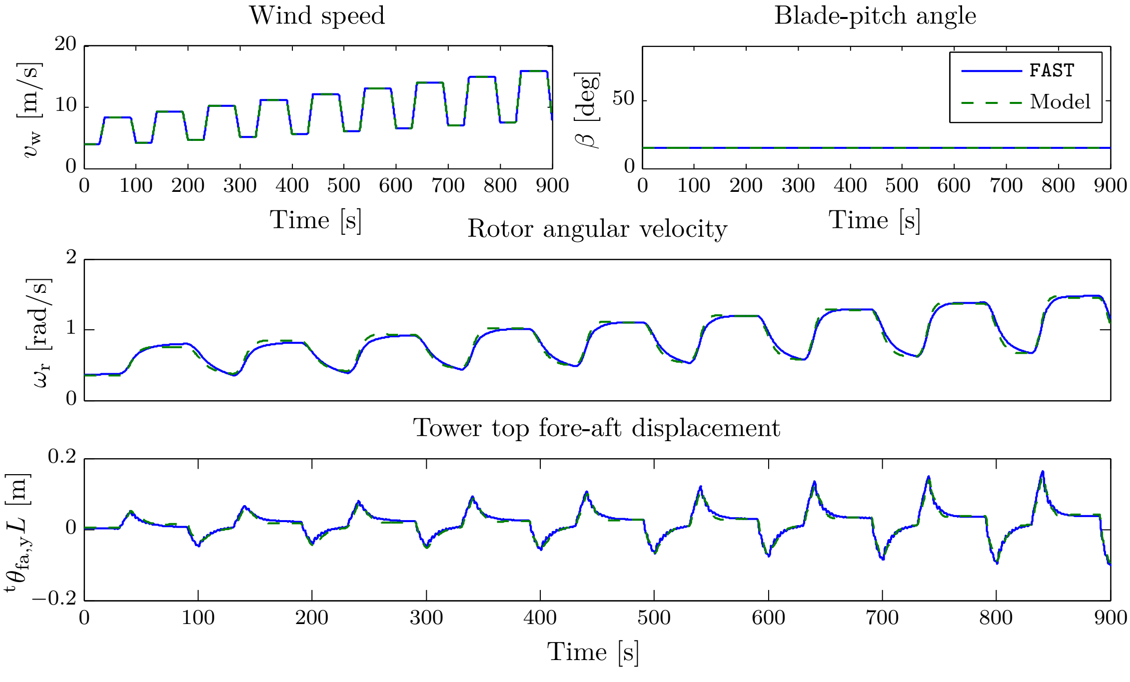


Figure 6.21: *Simulation results of tower bending with constant generator torque and blade-pitch.*

In the above section a model of the tower fore-aft bending has been developed. The model can be connected to the remaining model of the wind turbine as illustrated in Figure 6.1 on Page 27. In the following section, models of the wind turbine actuators will be developed.

6.5 Actuator Model

The actuators of a typical wind turbine include the blade-pitch, nacelle yaw, rotor brake and the generator torque. The actuators are controllable and can be used to control power production and to keep the wind turbine safe.

In Figure 6.22 the actuators of the wind turbine are illustrated. In individual blade-pitch wind turbines an individual pitch actuator will be assigned to each blade.

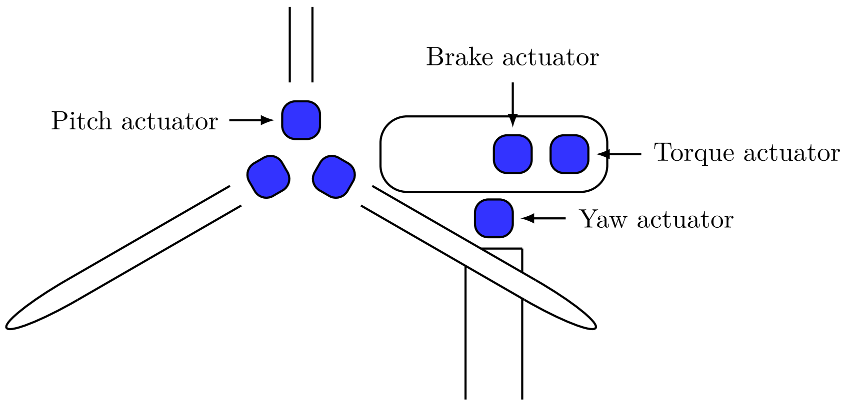


Figure 6.22: *Actuators of the wind turbine*

As mentioned in Section 2.6, the emergency shutdown procedure will be using blade-pitch only to stop the rotor. When the emergency shutdown procedure is initialised, the generator torque will be set to zero and the blade-pitch actuators will be activated. As the brake and yaw mechanisms are not used during the considered shutdown procedure, they will not be modelled. In the following sections, the generator torque and blade-pitch are considered, as these are active during emergency shutdown.

6.5.1 Generator

The generator torque should be set to zero when the emergency shutdown is initiated. According to the definition of the NREL 5-MW wind turbine, the time constant of the generator torque is very small compared to the dynamics of the wind turbine in general. Simulations show that the generator torque can be changed from a given value, during normal operation of the wind turbine, to zero within < 1 s. As a result, it is chosen not to consider the dynamics of the generator torque. When the emergency shutdown is initialised, the generator torque will simply be changed from the current value to zero instantaneously.

6.5.2 Blade-pitch actuator system

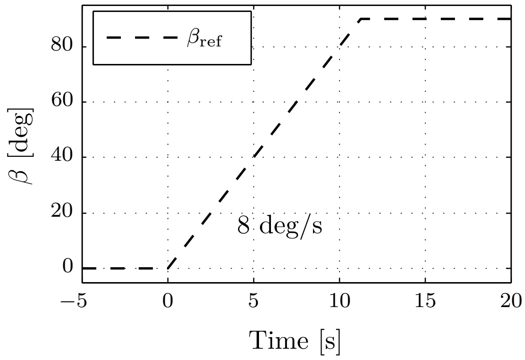
In the following a blade-pitch model will be developed.

The blade-pitch angle (β) is during normal operation used in the control of the rotor speed, as mentioned in Section 2.5. When an emergency shutdown procedure is initialised, a fixed pitch procedure will be executed such that the blade-pitch angle is taken to $\beta = 90°$.

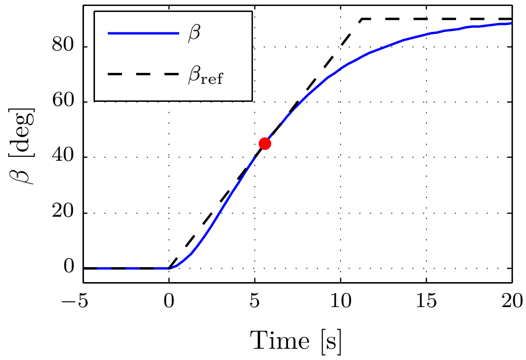
Due to the inertia of the blade masses and to avoid overloading of the pitch actuators, the blade-pitch mechanism is rate limited. The blade-pitch rate limit of the NREL 5-MW wind turbine is given in Table 2.1 to 8°/s. Although the NREL 5-MW wind turbine implements an individual blade-pitch mechanism, it is chosen to consider collective blade-pitching only.

To model the static pitching procedure, the pitching system is modelled as an autonomous system. In Figure 6.23a a static pitching procedure from 0° to 90° with a pitch rate of 8°/s is illustrated.

The objective of the blade-pitch model is to develop a dynamical model which resembles the procedure illustrated in Figure 6.23a.



(a) *Reference blade-pitch procedure with a pitch rate of 8°/s. The pitch angle is initialised at $\beta = 0°$.*



(b) *Second order dynamical system resembling the reference pitch procedure. The red circle marks the control point used in the search of model parameters.*

Figure 6.23: *Left, blade-pitch reference. Right, dynamic autonomous model of the static blade-pitch procedure.*

The model parameters will be designed such that the model resembles Figure 6.23a. The parameters will have no direct physical interpretation.

To resemble Figure 6.23a, the pitch procedure is modelled as a second order system. The linear system of the second order pitch system is given as

$$\begin{bmatrix} \dot{\omega}_\beta \\ \dot{\theta}_\beta \end{bmatrix} = \mathbf{A}_{\mathrm{pitch}} \begin{bmatrix} \omega_\beta \\ \theta\beta \end{bmatrix} = \begin{bmatrix} -a_{1,\beta} & -a_{2,\beta} \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \omega_\beta \\ \theta\beta \end{bmatrix}, \tag{6.28}$$

where the parameters $a_{1,\beta}$ and $a_{2,\beta}$ are unknown.

The objective is to find parameters $a_{1,\beta}$ and $a_{2,\beta}$ which result in a system that resembles 6.23a. As the blade-pitch rate is 8°/s, the pitch angle should reach $\beta = 45°$ at time $\frac{45°}{8°/\mathrm{s}} = 5.625$ s when the system is initialised in $\beta = 0°$. This is used as design criterion in the search of parameters.

To design the blade-pitch model the solution of the differential equations in (6.28) is found. As the system is coupled, the solution is not directly given. In order to reduce the linear system to an uncoupled system, a state transformation is introduced

$$\mathbf{P} = [\mathbf{v}_1, \mathbf{v}_2],$$

where $\mathbf{v}$ denotes the eigenvectors of the linear system (6.28) [Per00, 6].

Using the state transformation the system is decoupled

$$\tilde{\mathbf{A}}_{\mathrm{pitch}} = \mathbf{P}^{-1}\mathbf{A}_{\mathrm{pitch}}\mathbf{P} \;= \begin{bmatrix} f_1(a_{1,\beta}, a_{2,\beta}) & 0 \\ 0 & f_2(a_{1,\beta}, a_{2,\beta}) \end{bmatrix}.$$

The solution of the transformed decoupled system can be found directly, using the general solution to first order linear differential equations.

$$\begin{bmatrix} \tilde{\omega_\beta}(t) \\ \tilde{\theta_\beta}(t) \end{bmatrix} = \begin{bmatrix} e^{\tilde{\mathbf{A}}_{\mathrm{pitch}}(1,1)t} & 0 \\ 0 & e^{\tilde{\mathbf{A}}_{\mathrm{pitch}}(2,2)t} \end{bmatrix} \begin{bmatrix} \tilde{c}_1 \\ \tilde{c}_2 \end{bmatrix},$$

with the constants $\tilde{c}_1 = \tilde{\omega_\beta}(0)$ and $\tilde{c}_2 = \tilde{\theta_\beta}(0)$.

The solution to the original system can be found using the reverse transformation

$$\begin{bmatrix} \omega_\beta(t) \\ \theta_\beta(t) \end{bmatrix} = \mathbf{P} \begin{bmatrix} e^{\tilde{\mathbf{A}}_{\mathrm{pitch}}(1,1)t} & 0 \\ 0 & e^{\tilde{\mathbf{A}}_{\mathrm{pitch}}(2,2)t} \end{bmatrix} \mathbf{P}^{-1} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}.$$

To obtain a pitch model with 45° at time 5.625 s the system $\theta_\beta(5.625 \text{ s}) = 45°$ is solved with respect to $a_{1,\beta}, a_{2,\beta}$. As the equation has two unknowns, a constant $a_{1,\beta}$ is chosen iteratively to obtain real poles. The calculations can be found in Appendix D on Page 131.

The resulting system in the original coordinates is found to

$$\begin{bmatrix} \dot{\omega}_\beta \\ \dot{\theta}_\beta \end{bmatrix} = \begin{bmatrix} -0.6 & -0.0894 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \omega_\beta \\ \theta_\beta \end{bmatrix}. \tag{6.29}$$

The system in (6.29) is designed such that the angle goes to zero. During an emergency shutdown, the angle will go to 90°. To obtain this, an output equation is introduced as

$$\beta = -\theta_\beta + 90.$$

A simulation of the blade-pitch model with initial pitch angle $\beta = 0$ is illustrated in Figure 6.23b. The red circle in the plot marks the point $\theta_\beta(5.625 \text{ s}) = 45°$ used in the search of the model parameters.

The modelled behaviour of the actuators during an emergency shutdown is simulated using `FAST` and the NREL 5-MW controller. The emergency shutdown is initialised at time 50 s and illustrated in Figure 6.24. At time 50 s, the pitch procedure developed above is used to take the pitch angle of the NREL 5-MW wind turbine to 90°. Simultaneously, the generator torque is set to zero.

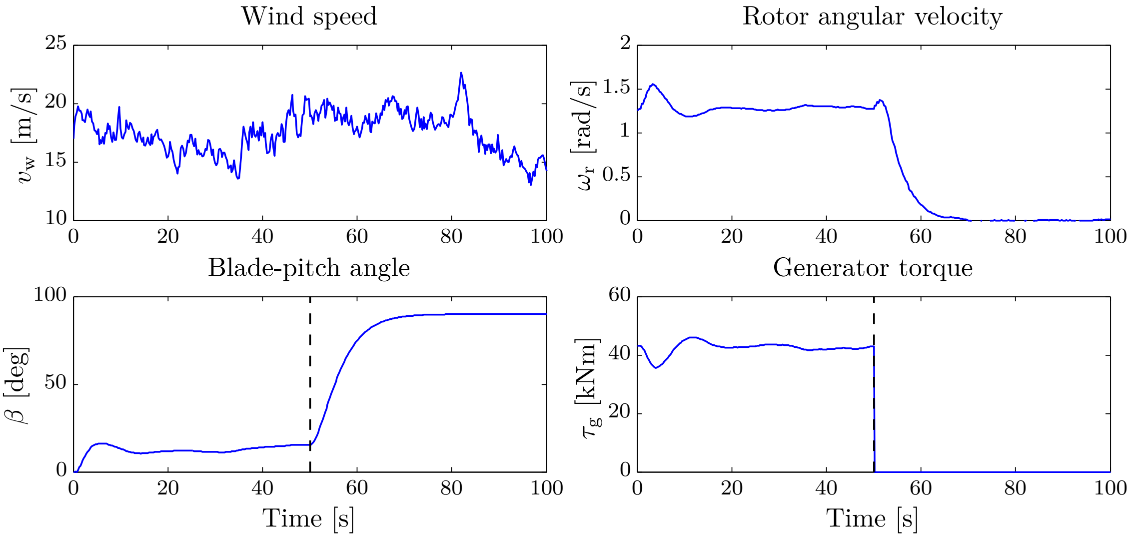


Figure 6.24: *The top plots show the horizontal hub height wind speed and the rotor angular velocity. The bottom plots illustrate the blade-pitch angle and generator torque. The dashed lines indicate the time of emergency shutdown initialisation. The blade-pitch model is used to take the pitch angle to 90°. The generator torque is set to zero when the emergency shutdown is initialised.*

6.6 Wind Model

In this section a wind model is described. The wind model will be used to model the disturbance from the stochastic wind field.

In relation to the safety of a wind turbine, the stochastic behaviour of the wind field can possibly render the wind turbine unsafe and damage the wind turbine structure. Consequently, the disturbance from the wind field should be included in the system safety guarantee.

The wind is characterised by its speed, direction and turbulence. The behaviour of the wind depends on numerous factors, such as height above ground, geographic location and climate. The motion of the wind is mainly driven by temperature differences. Close to the surface the wind speed and direction are affected by frictional forces which cause turbulence.

In Figure 6.25 the *van der Hoven* kinetic wind energy spectrum is illustrated [dH56].

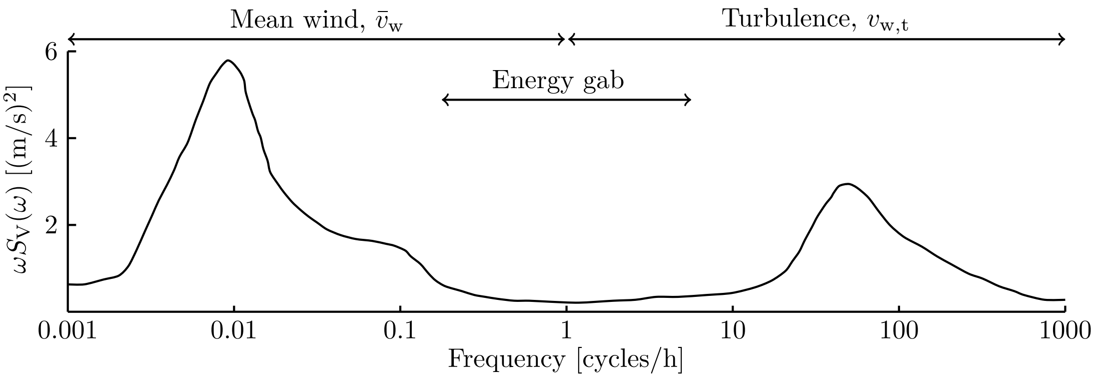


Figure 6.25: *Hoven spectrum [dH56]. The spectrum illustrates a typical kinetic wind energy distribution. $S_\mathrm{V}(\omega)$ is the power spectral density at the angular frequency ω. The product $\omega S_\mathrm{V}(\omega)$ yields a measure of the kinetic energy of the wind. The separation of the two energy peaks is denoted the* energy gab*, which ranges from 10 min to 2 h. The frequencies ω are plotted using a logarithmic scale and given in cycles per hour.*

The Hoven spectrum reveals that the kinetic energy of the wind exhibits two energy peaks separated by an energy gab. The low and high frequency peaks originate from the geostrophic flow and the local turbulence respectively. The specific peak frequencies depend on factors such as geographic position and local terrain. However the spectrum at different sites follow the same shape [FDB07].

The wind energy gab allows the separation of the wind speed into two components, the mean wind $\bar{v}_\mathrm{w}$ and the turbulent wind speed $v_\mathrm{w,t}$, given as

$$v_\mathrm{w} = \bar{v}_\mathrm{w} + v_\mathrm{w,t}, \tag{6.30}$$

where v_w is the wind speed experienced by the wind turbine.

As illustrated in Figure 6.25, turbulence is defined by the wind speeds above the energy frequency gab. These frequencies span from minutes to seconds. The high frequencies of the turbulence are essential when considering the aerodynamic loads and accordingly the safety of the wind turbine, as the turbulent wind speed can change suddenly.

As the mean wind speed changes slowly, it cannot cause sudden changes in the wind speed. Accordingly, the mean wind speed can be considered piecewise constant. This entails that the mean wind speed can be considered constant during an emergency shutdown of a few seconds.

In addition to the mean wind and the turbulence, the wind turbine itself introduces additional wind phenomena such as wind shear and tower shadow [Han08]. As many factors affect the wind field, the wind field model can be made arbitrarily complex. To simplify the modelling of the wind, it is chosen to consider a scalar wind field composed from a constant mean wind and a turbulence component. Additionally the wind shear, tower shadow etc. are neglected. As no specific geographical location is considered, the purpose of the wind model will be to model a typical wind situation.

In the following, a simple turbulence model will be described.

6.6.1 Turbulence model

The turbulence at a specific site is often described stochastically by its power spectrum density. Generally it is accepted to consider the turbulent wind field as a wide-sense stationary random process using approximation models such as the *Karman*, *Kaimal* or *Mann* models. These models approximate the power spectrum densities of the turbulence [FDB07].

The parameters of the spectrum models are highly dependent on the specific location of the wind turbine and should be experimentally obtained from measurements. The model of the turbulence spectrum density has to satisfy a range of requirements listed in [IEC06].

To model the turbulence a standard turbulence model will be used, specifically the Karman turbulence filter. This is essentially a simple low-pas filter, given as

$$H_{\mathrm{w,t}}(s) = \sigma_{\mathrm{V}} \frac{K_{\mathrm{V}}}{(1 + sT_{\mathrm{V}})^{5/6}},$$

where the filter parameters T_{V}, K_{V} and σ_{V} represent the turbulence frequency bandwidth, turbulence power and standard deviation of the turbulence respectively. These parameters should be obtained experimentally on the location of the wind turbine. The turbulence $v_{\mathrm{w,t}}(t)$ is generated by passing white noise $w(t)$ through the filter.

In [FDB07] the filter is approximated by a rational second order filter given as

$$H_{\mathrm{turb}}(s) \approx \sigma_{\mathrm{V}} K_{\mathrm{V}} \frac{0.4sT_{\mathrm{V}} + 1}{(sT_{\mathrm{V}} + 1)(0.25sT_{\mathrm{V}} + 1)}. \tag{6.31}$$

Some specifications of a typical wind field are in given in [FDB07] from which the following parameters can be calculated:

$$T_{\mathrm{V}} = 12.0, \quad K_{\mathrm{V}} = 4.2, \quad \sigma_{\mathrm{V}} = 2.4.$$

In Figure 6.26 the frequency response of the Karman filter (6.31) and a simulation of the wind field given a constant mean wind $\bar{v}_{\mathrm{w}} = 15$ m/s are illustrated. The cut-off frequency of the filter is just below 1000 cycles/h, which is similar to the Hoven spectrum.

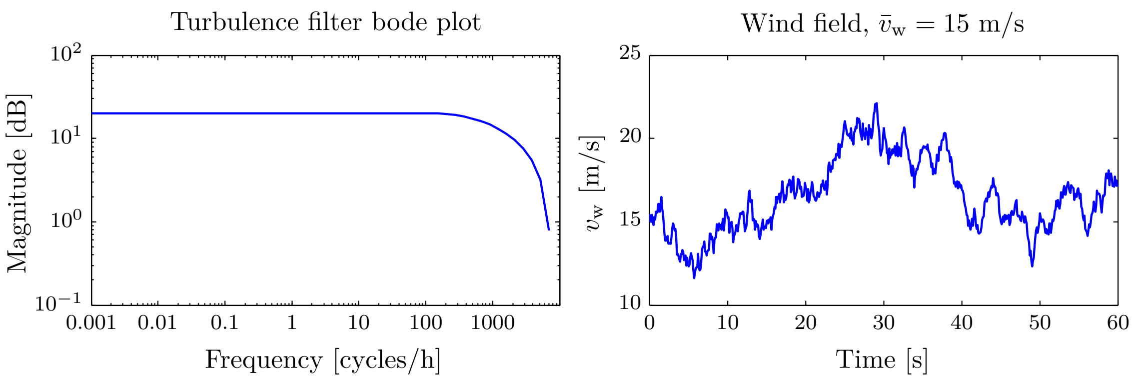


Figure 6.26: *Left the frequency response of the turbulence model is illustrated using a logarithmic scale. Right a simulation of the wind speed v_{w} is illustrated using a mean wind speed $\bar{v}_{\mathrm{w}} = 15$ m/s and white driving noise w.*

To be able to use the above wind model with the remaining model subsystems, the frequency domain model is using MATLAB transformed to state space form. The wind turbulence model in state space form is given by

$$\begin{bmatrix} \dot{v}_{\mathrm{w,t1}} \\ \dot{v}_{\mathrm{w,t2}} \end{bmatrix} = \begin{bmatrix} -0.42 & -0.22 \\ 0.13 & 0 \end{bmatrix} \begin{bmatrix} v_{\mathrm{w,t1}} \\ v_{\mathrm{w,t2}} \end{bmatrix} + \begin{bmatrix} 2 \\ 0 \end{bmatrix} w, \tag{6.32}$$

with $v_{\mathrm{w,t1}}$ and $v_{\mathrm{w,t2}}$ as internal turbulence states and w as the driving white noise. The turbulence wind component is given by

$$v_{\mathrm{w,t}} = 0.68 v_{\mathrm{w,t1}} + 1.14 v_{\mathrm{w,t2}}. \tag{6.33}$$

Using the (6.33) the total wind field can be calculated using (6.30).

In this section a simple wind model was developed, based on the Karman wind model. The model is used to filter the wind disturbance, such that high frequencies are removed.

In the above sections the model parts have been developed. In the following section, the parts are assembled into a single model description.

6.7 Model Composition

To form the complete model, each model equation must be given by known terms only. Ultimately the complete model should be given by known constant terms, states and disturbances only. As the model is autonomous, no input terms will be present.

A complete list of model states and disturbances is given in Table 6.1.

States and disturbances of the model			
Description	**Symbol**	**Unit**	**Type**
Drive train			
Rotor angular velocity	ω_{r}	rad/s	State
Generator angular velocity	ω_{g}	rad/s	State
Drive train torsion angle	θ_{Δ}	rad	State
Flapwise blade bending			
Flapwise blade tip velocity	${}^{\mathrm{h}}v_{\mathrm{flap,x}}$	m/s	State
Flapwise blade tip displacement	${}^{\mathrm{h}}x_{\mathrm{flap}}$	m	State
Lead-lag blade bending			
Lead-lag blade tip angular velocity	${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}$	rad/s	State
Lead-lag blade tip angle	${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}$	rad	State
Tower			
Tower fore-aft angular velocity	${}^{\mathrm{t}}\omega_{\mathrm{fa,y}}$	rad/s	State
Tower fore-aft angle	${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$	rad	State
Blade-pitch actuator system			
Blade-pitch angular velocity	ω_{β}	deg/s	State
Blade-pitch angle	θ_{β}	deg	State
Wind Model			
Wind turbulence component 1	$v_{\mathrm{w,t1}}$	m/s	State
Wind turbulence component 2	$v_{\mathrm{w,t2}}$	m/s	State
Driving turbulence noise	w	-	Disturbance

Table 6.1: *States and disturbances of the model*

In Appendix E the unknown terms of the model equations are substituted by known terms and the equations are manipulated, such that the linear and nonlinear terms appear clearly. The result of the model composition is given in Equation (6.34). The model is separated into a linear and a nonlinear part.

$$
\begin{bmatrix} \dot{\omega}_{\mathrm{r}} \\ \dot{\omega}_{\mathrm{g}} \\ \dot{\theta}_{\Delta} \\ {}^{\mathrm{h}}\dot{v}_{\mathrm{flap,x}} \\ {}^{\mathrm{h}}\dot{x}_{\mathrm{flap}} \\ {}^{\mathrm{h}}\dot{\omega}_{\mathrm{LL,x}} \\ {}^{\mathrm{h}}\dot{\theta}_{\mathrm{LL,x}} \\ {}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} \\ {}^{\mathrm{t}}\dot{\theta}_{\mathrm{fa,y}} \\ \dot{\omega}_{\beta} \\ \dot{\theta}_{\beta} \\ \dot{v}_{\mathrm{w,t1}} \\ \dot{v}_{\mathrm{w,t2}} \end{bmatrix}
=
\begin{bmatrix}
-\frac{B_{\mathrm{r}}+B_{\mathrm{a}}}{J_{\mathrm{r}}} & \frac{B_{\mathrm{a}}N}{J_{\mathrm{r}}} & -\frac{K_{\mathrm{a}}}{J_{\mathrm{r}}} & 0 & 0 & 0 & \frac{K_{\mathrm{LL}}}{J_{\mathrm{r}}} & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{B_{\mathrm{a}}N}{J_{\mathrm{g}}} & -\frac{BN^2+B_{\mathrm{g}}}{J_{\mathrm{g}}} & \frac{K_{\mathrm{a}}N}{J_{\mathrm{g}}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -N & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -\frac{B_{\mathrm{flap}}}{M_{\mathrm{flap}}} & -\frac{K_{\mathrm{flap}}(M_{\mathrm{n}}+M_{\mathrm{flap}})}{M_{\mathrm{flap}}M_{\mathrm{n}}} & 0 & 0 & \frac{B_{\mathrm{fa}}}{M_{\mathrm{n}}L} & -\frac{F_{\mathrm{g}}L-K_{\mathrm{fa}}}{M_{\mathrm{n}}L} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{B_{\mathrm{r}}+B_{\mathrm{a}}}{J_{\mathrm{r}}} & -\frac{B_{\mathrm{a}}N}{J_{\mathrm{r}}} & \frac{K_{\mathrm{a}}}{J_{\mathrm{r}}} & 0 & 0 & -\frac{B_{\mathrm{LL}}}{J_{\mathrm{LL}}} & -\frac{K_{\mathrm{LL}}(J_{\mathrm{r}}+J_{\mathrm{LL}})}{J_{\mathrm{r}}J_{\mathrm{LL}}} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{K_{\mathrm{flap}}}{M_{\mathrm{n}}L} & 0 & 0 & -\frac{B_{\mathrm{fa}}}{M_{\mathrm{n}}L^2} & \frac{F_{\mathrm{g}}L-K_{\mathrm{fa}}}{M_{\mathrm{n}}L^2} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.6 & -0.0894 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -0.42 & -0.22 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.13 & 0
\end{bmatrix}
\begin{bmatrix} \omega_{\mathrm{r}} \\ \omega_{\mathrm{g}} \\ \theta_{\Delta} \\ {}^{\mathrm{h}}v_{\mathrm{flap,x}} \\ {}^{\mathrm{h}}x_{\mathrm{flap}} \\ {}^{\mathrm{h}}\omega_{\mathrm{LL,x}} \\ {}^{\mathrm{h}}\theta_{\mathrm{LL,x}} \\ {}^{\mathrm{t}}\omega_{\mathrm{fa,y}} \\ {}^{\mathrm{t}}\theta_{\mathrm{fa,y}} \\ \omega_{\beta} \\ \theta_{\beta} \\ v_{\mathrm{w,t1}} \\ v_{\mathrm{w,t2}} \end{bmatrix}
$$

$$
+ \begin{bmatrix}
\frac{(1-\xi_{\mathrm{LL}})}{J_{\mathrm{r}}}\tau_{\mathrm{aero}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) \\
0 \\
0 \\
\frac{\xi_{\mathrm{flap}}(M_{\mathrm{n}}+M_{\mathrm{flap}})-M_{\mathrm{flap}}}{M_{\mathrm{flap}}M_{\mathrm{n}}}F_{\mathrm{aero}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) \\
0 \\
\frac{\xi_{\mathrm{LL}}(J_{\mathrm{r}}+J_{\mathrm{LL}})-J_{\mathrm{LL}}}{J_{\mathrm{r}}J_{\mathrm{LL}}}\tau_{\mathrm{aero}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) \\
0 \\
\frac{(1-\xi_{\mathrm{flap}})}{M_{\mathrm{n}}L}F_{\mathrm{aero}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) \\
0 \\
0 \\
0 \\
2w \\
0
\end{bmatrix}, \quad \text{with} \quad
\begin{aligned}
\tau_{\mathrm{aero}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) &= \tfrac{1}{2}\rho A R {v_{\mathrm{eff}}}^2 C_{\mathrm{q}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) \\
F_{\mathrm{aero}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) &= \tfrac{1}{2}\rho A {v_{\mathrm{eff}}}^2 C_{\mathrm{t}}(v_{\mathrm{eff}},\omega_{\mathrm{r}},\beta) \\
v_{\mathrm{eff}} &= v_{\mathrm{w}} - L\,{}^{\mathrm{t}}\omega_{\mathrm{fa,y}} \\
v_{\mathrm{w}} &= \bar{v}_{\mathrm{w}} + 0.68 v_{\mathrm{w,t1}} + 1.14 v_{\mathrm{w,t2}} \\
\beta &= 90^\circ - \theta_{\beta}
\end{aligned}
\tag{6.34}
$$

The constant parameters of the model in (6.34) are given in Table 6.2.

Model parameters		
Parameter	**Symbol**	**Value**
Aerodynamic Model		
Rotor radius	R	61.5 m
Rotor area	A	$11.88e3$ m^2
Air density	ρ	1.22521 kg/m^3
Drive train		
Gearing	N	1/97
Rotor inertia	J_{r}	$19.38e6$ kg $\cdot$ m^2
Generator inertia	J_{g}	534.12 kg $\cdot$ m^2
Rotor friction	B_{r}	$150e3$ Nm $\cdot$ s
Generator friction	B_{g}	0 Nm $\cdot$ s
Shaft damping	B_{a}	$12.15e6$ Nm/(rad/s)
Shaft stiffness	K_{a}	$15.00e6$ Nm/rad
Flapwise blade bending		
Flapwise blade mass	M_{flap}	$66.00e3$ kg
Flapwise stiffness	K_{flap}	$55.25e3$ N/m
Flapwise damping	B_{flap}	$250.00e3$ N/(m/s)
Flapwise break point factor	ξ_{flap}	0.5
Lead-lag blade bending		
Lead-lag blade inertia	J_{LL}	$12.40e6$ kg $\cdot$ m^2
Lead-lag stiffness	K_{LL}	$67.50e6$ Nm/rad
Lead-lag damping	B_{LL}	$300.00e6$ Nm/(rad/s)
Lead-lag break point factor	ξ_{LL}	0.51
Tower		
Tower height	L	87.6 m
Tower fictitious mass	M_{n}	$557.97e3$ kg
Tower fore-aft stiffness	K_{fa}	$10.13e9$ Nm/rad
Tower fore-aft damping	B_{fa}	$221.e6$ Nm/(rad/s)
Gravitational acceleration	g	9.82 m/s^2

Table 6.2: *Model parameters*

The model given in (6.34) has been designed to resemble the NREL 5-MW wind turbine implemented in the `FAST` wind turbine simulator. To test the validity of the model, it is compared to a simulation performed in `FAST`. In the simulation, the stochastic wind speed and autonomous blade-pitch are replaced by controlled inputs, such that the simulations can be compared. The blade-pitch angle sequence is chosen such that it resembles a series of emergency shutdowns.

In Figure 6.27 the equations given in (6.34) with parameters given in Table 6.2 are simulated and compared to a similar simulation in `FAST`. The wind speed v_{w} and the blade-pitch angle β are equal in both simulations. The aerodynamic functions $\tau_{\mathrm{aero}}(v_{\mathrm{eff}}, \omega_{\mathrm{r}}, \beta)$ and $F_{\mathrm{aero}}(v_{\mathrm{eff}}, \omega_{\mathrm{r}}, \beta)$ are given by 10^{th} order polynomial approximations as described in Section 6.3.

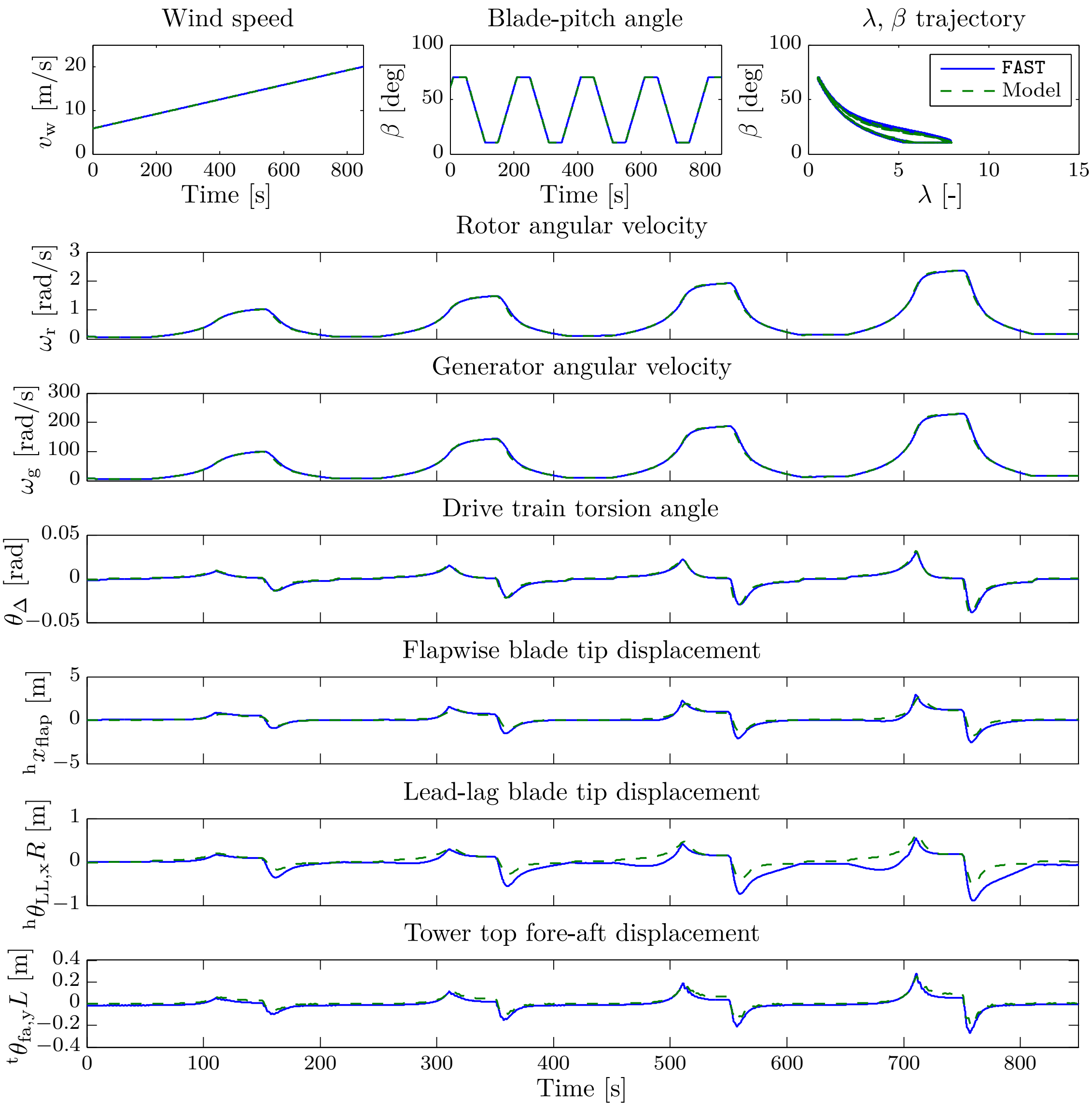


Figure 6.27: *Comparison of polynomial model simulation and* FAST *simulation. Both simulations share the same wind field and blade-pitch angle sequence. The lower 6 plots share a common time axis given below the bottom plot. It should be noted that the lead-lag blade bending and tower bending have been converted from angles to translations.*

The comparison in Figure 6.27 indicates that the model on polynomial form in general resembles the NREL 5-MW wind turbine, implemented in `FAST`, satisfactorily. It seems however that the lead-lag bending of the blades is either under modelled or that the parameters related to the lead-lag bending are not correct.

A similar simulation has been performed using a range of polynomial approximations of the aerodynamic lookup tables. This is done to examine the required order of the polynomials used in the approximation. The examination is given in Appendix F. From the examination it is clear that polynomials must be at least 9^{th} order to resemble the original aerodynamic lookup tables. To reduce the order of the polynomials, the ranges in with the approximations are valid could be reduced - e.g. the wind speed range could be limited to $v_w = [15\text{m/s} \; ; \; 25\text{m/s}]$.

The complete model has been assembled using the models of the subsystem. The complete model description was tested, and found sufficient. It has been shown that a reasonable polynomial model of a wind turbine can be developed, including polynomial approximations of aerodynamic properties.

Given a set of initial states, the autonomous pitch procedure will resemble a wind turbine emergency shutdown starting at the chosen initial state. By initiating the model in a given state, the solution to the model will provide a state trajectory of the emergency shutdown, using the static blade-pitch procedure. The trajectories of the model states from a given initial state are illustrated in Figure 6.28.

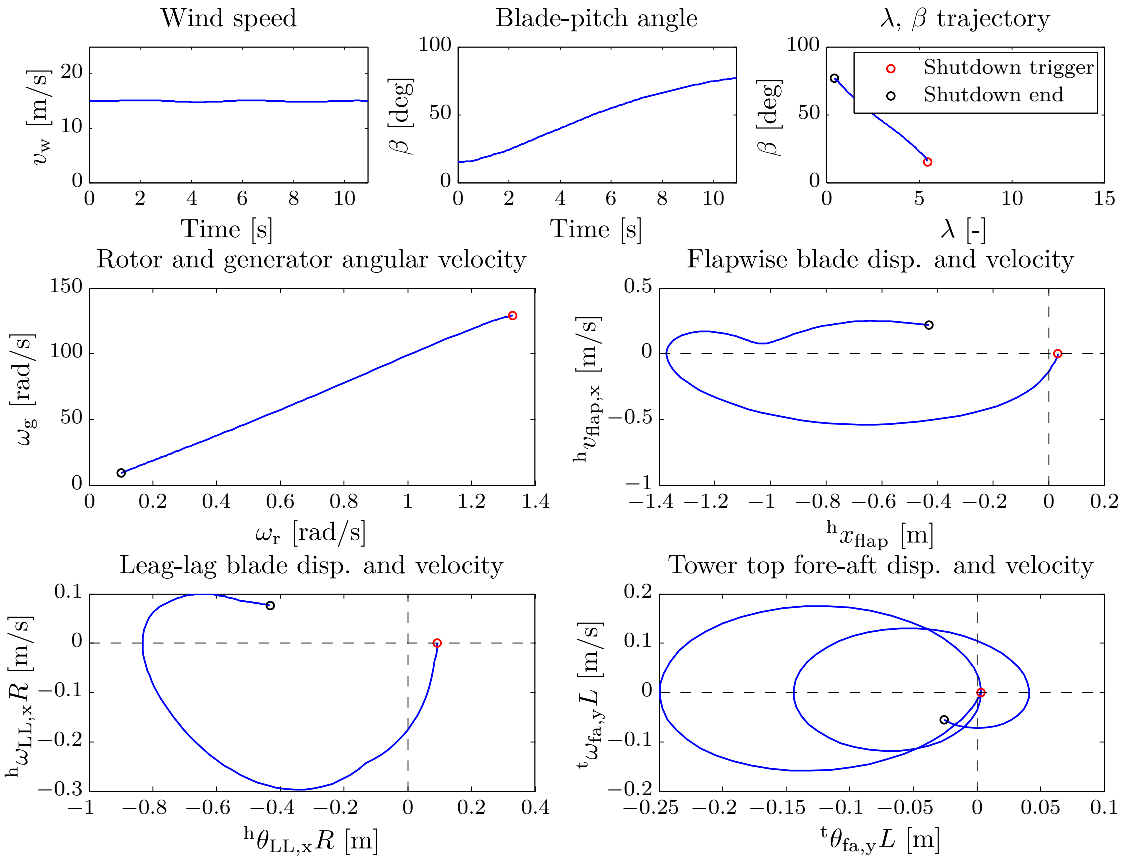


Figure 6.28: *Model trajectories from a given initial state, indicated by red circles. The pitch angle is autonomously taken from the initial angle of* $\beta = 15°$ *to* $\beta = 90°$*, according to the pitch model. The wind speed is constant 15 m/s. The simulation was stopped at the time when the rotor speed got below* 3 rpm (0.1 rad/s)*. The lead-lag blade bending and the tower bending have been converted from angles to translations, in order to simplify the comparison of the states.*

Figure 6.28 illustrates the use and purpose of the developed model. Using the model, it is possible to test if an emergency shutdown triggered at a specific state will produce trajectories which could damage the wind turbine or not. The shutdown model can be found on the enclosed DVD. A solution to a system as in (6.34) is in general difficult to obtain analytically. In the following Chapters, the barrier certificate method, which was shortly introduced in Section 5, will be used to design a wind turbine safety supervisor system, without the use of explicit solutions to the model equations.

7 Operation Analysis

In this chapter, practical considerations of the safety supervisor design will be discussed.

To recapitulate, the wind turbine safety supervisor should be able to distinguish when the system is safe and when it is unsafe. The developed model can be used to find trajectories of an emergency shutdown given an initial state. By studying the trajectories, it can be found whether a trigger of the emergency shutdown, from the initial state, is safe or unsafe. As this study cannot be performed for every initial state a method, which does not require the explicit solution to the system model, will be used. In Chapter 5 the concept of safety envelopes is introduced. If the system is in a safety envelope $\mathcal{X}_0$, an emergency shutdown, given the static pitch procedure, can be performed without violating the ultimate load limits of the wind turbine. To avoid that the wind turbine enters the unsafe set $\mathcal{X}_\mathrm{u}$, an emergency shutdown should be triggered no later than on the border of the safety envelope. To verify if an initial set $\mathcal{X}_0$ is safe or not, the barrier certificate and sum of squares framework can be used [PJP07]. This method handles polynomial system descriptions and will be used in the following chapters in the search of a safety envelope in which the wind turbine is safe - denoted the initial set $\mathcal{X}_0$. The safety envelope will be a subset of the safe set. The safety envelope can eventually be implemented in a safety supervisor, which monitors the system online and initiates an emergency shutdown if the wind turbine is about to leave the safety envelope. It should be emphasised that the safety envelope will be calculated given the static pitch procedure and a limited wind disturbance.

To be able to use the safety system in practice, the safety supervisor must be able to run in an online implementation. As a consequence, the calculations which are to be performed by the safety supervisor should be simple enough to enable online evaluation. Using the framework of barrier certificates, the safety evaluation is a matter of evaluating one to a few multivariate polynomials. The safety of the system is then directly given from the result. In the simple situation of a single safety envelope, the safety of the system is given by evaluation of a single polynomial.

The design of the safety supervisor system may require considerable calculations. As the calculations should be performed offline, the calculation time is not critical. However, the calculations should be possible to do on a modern PC in reasonable time. If the wind turbine system or the blade-pitch procedure is changed, the safety supervisor should be recalculated. The safety supervisor is however not dependent on the implementation of the control system. As a result, the control system can be changed without the need of a new safety supervisor, as mentioned in Section 1.4.

As the designed safety supervisor will be multivariate and model-based, the supervisor will require knowledge of the system states. This is in contrast to an univariate supervisor, which can be found on some wind turbines today. As mentioned in Section 1.4, a wind turbine safety system should be based only on safe life components, why the safety supervisor is limited to measurements from safe life sensors. Safe life sensors often include blade-pitch angle, acceleration of tower top, rotor velocity and strain of blades. Consequently, the safety supervisor is limited to measurements from the mentioned sensors. To make measurements of states (such as the drive train torsion) available, the states should either be estimated from the available sensors or an additional safe life sensor should be installed. The estimation, and validity of such an estimation, is out of the scope of this project. In the following, it will be assumed that full state information is available and reliable.

For the safety supervisor to be usable in practice, the safety supervisor system should be designed in accordance with the normal operation of the wind turbine. In the following section, the normal operation of the NREL 5-MW wind turbine will be examined. The information about the normal operation of the wind turbine will later be used in the search of a practical usable safety supervisor.

7.1 Normal Operation of NREL 5-MW

In this section the normal operation of the NREL 5-MW reference wind turbine is found. The knowledge of the normal operation region will later be used in the design of a safety supervisor system. In order for the safety envelope to be usable in practice, it should cover the normal operation best possible.

To find the normal operation of a given wind turbine, the wind field at the specific site should be taken into consideration. As no real wind measurements are available it is chosen to generate a wind field using the stochastic turbulent-wind field generator, `TurbSim` [NK11]. The generator is able to output a wind field which can be used in the simulation of the NREL 5-MW reference wind turbine in `FAST` and comply with the IEC-61400 standard. A wind field is generated using an increasing mean wind speed in the range from 5 m/s to the cut-out wind speed of 25 m/s. In Figure 7.1 the horizontal hub-height wind speed magnitude is illustrated. The generated wind field spans a time period of nearly 30 hours.

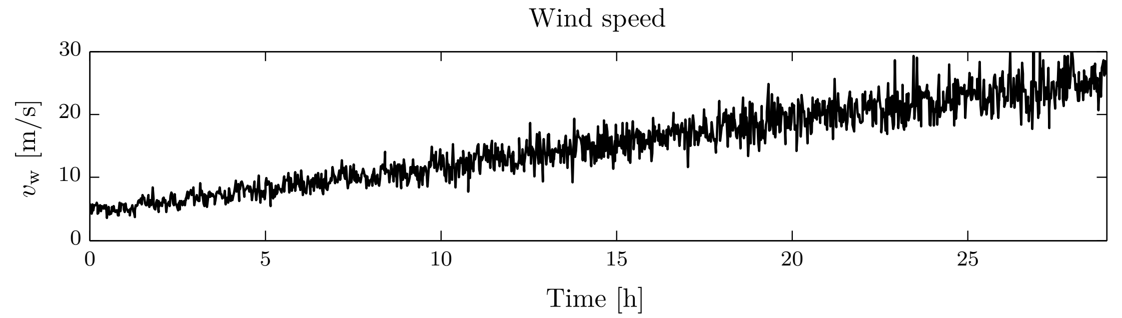


Figure 7.1: *Illustration of the horizontal hub-height wind speed magnitude. The mean wind speed spans the range from 5 m/s to 25 m/s. The wind field covers a time window of nearly 30 hours.*

A simulation is run using the NREL 5-MW wind turbine, the controller described in Section 2.5 and the generated wind field in Figure 7.1. During the simulation of nearly 30 hours, the safety critical states listed in Table 6.1 are measured.

A sample of the measurements during the 30 hour simulation is given as point clouds in Figure 7.2. It should be noted that the density of a cloud is dependent on the choice of wind field. In Appendix G the projections of the measurement cloud on every plane are illustrated.

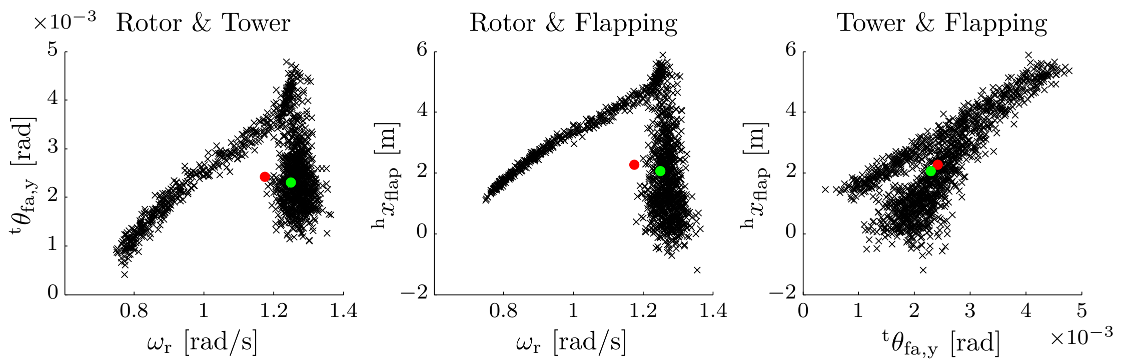


Figure 7.2: *Illustration of three selected point cloud projections from the normal operation simulation. The left point cloud illustrates the rotor velocity and tower top bending angle. The middle point cloud illustrates the rotor velocity and flapwise blade tip displacement. The right point cloud illustrates the tower top bending angle and flapwise blade tip displacement. The red and green circles indicate the mean and median points of the clouds.*

From Figure 7.2 (and Figure G.1 in Appendix G) it can be seen that some of the normal operation clouds seem to be composed by two chunks. This is due to the behaviour of the wind turbine controller. As described in Section 2.5, the control of the wind turbine is divided into regions. In region 2 the speed of the rotor is variable, while the speed of the rotor is kept constant in region 3 - which results in a separation of the normal operation clouds into two parts.

The mean, median and standard deviation of the measured states are given in Table 7.1.

Normal operation statistics			
State	**Mean**	**Median**	**Standard deviation**
ω_{r}	1.17 rad/s	1.25 rad/s	$163.11 \cdot 10^{-3}$ rad/s
ω_{g}	113.95 rad/s	121.27 rad/s	15.82 rad/s
θ_{Δ}	$13.62 \cdot 10^{-3}$ rad	$14.9 \cdot 10^{-3}$ rad	$53.15 \cdot 10^{-3}$ rad
${}^{\mathrm{h}}v_{\mathrm{flap,x}}$	≈ 0 m/s	≈ 0 m/s	$194.15 \cdot 10^{-3}$ m/s
${}^{\mathrm{h}}x_{\mathrm{flap}}$	2.27 m	2.01 m	1.46 m
${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}$	≈ 0 rad/s	≈ 0 rad/s	$901.34 \cdot 10^{-6}$ rad/s
${}^{\mathrm{h}}\theta_{\mathrm{LL,x}}$	$6.74 \cdot 10^{-3}$ rad	$6.9 \cdot 10^{-3}$ rad	$3.4206 \cdot 10^{-3}$ rad
${}^{\mathrm{t}}\omega_{\mathrm{fa,y}}$	≈ 0 rad/s	≈ 0 rad/s	$147.82 \cdot 10^{-6}$ rad/s
${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}$	$2.42 \cdot 10^{-3}$ rad	$2.3 \cdot 10^{-3}$ rad	$809.47 \cdot 10^{-6}$ rad

Table 7.1: *Mean, median and standard deviation of the measured states in the normal operation simulation*

The normal operation statistics given in Table 7.1 can be used in the search of a safety envelope. The mean and median measures provide information about the center of the normal operation region. These can be used to center the safety envelope such that a practical useable envelope is found. The mean value of the measurement clouds might in some cases be affected by a few extreme measurements, in which case the median could be a better measure. Additionally the standard deviation provides information about the scaling of the states, which can be used as weighting parameters in an optimisation of a safety envelope. The normal operation measurement data can be found on the enclosed DVD.

In the above section, statistics of the normal operation of the NREL 5-MW wind turbine were found. This information will later be used in the search of a practical safety envelope. In the following section, the ultimate load limits of the NREL 5-MW wind turbine will be defined.

7.2 Ultimate Load Limits

As defined in Section 1.2, the ultimate load limits of the wind turbine are a set of constraints which the system must not violate.

The ultimate load limits of a wind turbine should be based on structural calculations and experience. As this project is based on the fictitious NREL 5-MW wind turbine, no real ultimate load limits can be found. To obtain some realistic ultimate load limits of the NREL 5-MW, the limits will be based on the normal operation simulation described in Section 7.1.

To fit the framework of barrier certificates, the ultimate load limits must be given as semi-algebraic sets (i.e. polynomial equalities and inequalities) [PJP07]. Consequently, the ultimate load limits can be defined as polynomial functions of the system states, which are given in Table 6.1. As no specific constraints can be found from the definition of the NREL 5-MW in [JBMN09], it is chosen to define constraints on the flapwise blade tip displacement, lead-lag blade bending, tower fore-aft top bending, drive train torsion and the rotor angular velocity. This leaves the states of blade velocities, tower velocity and generator angular velocity unconstrained.

The ultimate load limits are chosen to be based on the 0.1% measurements with the highest numerical value, denoted $x_{0.1\%}$. Specifically the ultimate load limits are chosen to be $2x_{0.1\%}$, inspired by the ultimate load limit criteria typically used on aircrafts [NG00]. The $2x_{0.1\%}$ ultimate load limits of the tower bending and flapwise blade tip displacement are illustrated in Figure 7.3 - the remaining state histograms with ultimate load limits are given in Appendix H.

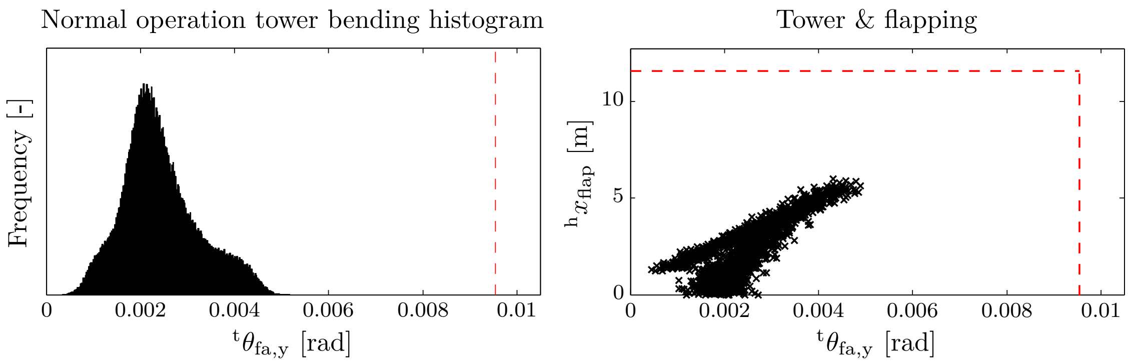


Figure 7.3: *Left a histogram of the tower top bending during the normal operation simulation is illustrated. Right the normal operation point cloud of tower bending and flapwise blade tip displacement is illustrated. On both plots, the $2x_{0.1\%}$ ultimate load limits are indicated by red dashed lines.*

The $2x_{0.1\%}$ ultimate load limits of the selected states, found from the normal operation, are listed in Table 7.2. The ultimate load limits of the drive train torsion, flapwise blade tip displacement, lead-lag blade bending and tower top fore-aft bending are considered equal in both directions (symmetric). This assumption might not be realistic in practice. It is chosen to consider only an upper ultimate load limit on the rotor angular velocity. As an $2x_{0.1\%}$ ultimate load limit on the rotor seems extreme, it is chosen to limit this specific state to $1.5x_{0.1\%}$.

State ultimate load limits			
State discription	**State**	**Limit**	**Value**
Rotor angular velocity ($1.5x_{0.1\%}$)	ω_{r}	$\gamma_{\mathrm{r}} = 2.025$ rad/s	$[- \; ; \; \gamma_{\mathrm{r}}]$
Generator angular velocity	ω_{g}	-	-
Drive train torsion angle ($2x_{0.1\%}$)	θ_{Δ}	$\gamma_{\Delta} = 441.42 \cdot 10^{-3}$ rad	$[-\gamma_{\Delta} \; ; \; \gamma_{\Delta}]$
Flapwise blade tip velocity	$^{\mathrm{h}}v_{\mathrm{flap,x}}$	-	-
Flapwise blade tip disp. ($2x_{0.1\%}$)	$^{\mathrm{h}}x_{\mathrm{flap}}$	$\gamma_{\mathrm{flap}} = 11.57$ m	$[-\gamma_{\mathrm{flap}} \; ; \; \gamma_{\mathrm{flap}}]$
Lead-lag blade tip angular velocity	$^{\mathrm{h}}\omega_{\mathrm{LL,x}}$	-	-
Lead-lag blade tip angle ($2x_{0.1\%}$)	$^{\mathrm{h}}\theta_{\mathrm{LL,x}}$	$\gamma_{\mathrm{LL}} = 26.00 \cdot 10^{-3}$ rad	$[-\gamma_{\mathrm{LL}} \; ; \; \gamma_{\mathrm{LL}}]$
Tower fore-aft angular velocity	$^{\mathrm{t}}\omega_{\mathrm{fa,y}}$	-	-
Tower fore-aft angle ($2x_{0.1\%}$)	$^{\mathrm{t}}\theta_{\mathrm{fa,y}}$	$\gamma_{\mathrm{fa}} = 9.54 \cdot 10^{-3}$ rad	$[-\gamma_{\mathrm{fa}} \; ; \; \gamma_{\mathrm{fa}}]$

Table 7.2: *Ultimate load limits of the system states*

The ultimate load limits define the boundary between the *safe set* $\mathcal{X}_{\mathrm{s}}$ and the *unsafe set* $\mathcal{X}_{\mathrm{u}}$. The safe set is defined by the ultimate load limits as

$$\mathcal{X}_\mathrm{s} = \left\{ \mathbf{x} \in \mathbb{R}^\mathrm{n} \;\middle|\; \begin{array}{cl} \omega_\mathrm{r} & \leq \gamma_\mathrm{r}, \\ |\theta_\Delta| & \leq \gamma_\Delta, \\ |{}^\mathrm{h}x_\mathrm{flap}| & \leq \gamma_\mathrm{flap}, \\ |{}^\mathrm{h}\theta_\mathrm{LL,x}| & \leq \gamma_\mathrm{LL}, \\ |{}^\mathrm{t}\theta_\mathrm{fa,y}| & \leq \gamma_\mathrm{fa} \end{array} \right\}.$$

The complement $\mathcal{X}_\mathrm{u} = \mathbb{R}^\mathrm{n} \setminus \mathcal{X}_\mathrm{s}$ forms the *unsafe set*. As the design of the safety supervisor system will be based on the system model, any model limitations should either be included in the unsafe set or be excluded from the state space in consideration (this will be done is Section 10.2).

In the above section, fictitious ultimate load limits of the NREL 5-MW wind turbine were defined. The limits define the *safe set* and will be used in the search of a safety envelope. In the following chapter the concept of barrier certificates is introduced, along with mathematical tools used in the barrier certificate framework.

8 Safe Operation Envelope

In this chapter the concepts of safety envelopes, barrier certificates and the methods which will be used in the optimisation of the safety envelopes are introduced. In the first section the concept of safety envelopes and barrier certificates are introduced using the familiar concept of linear Lyapunov functions and invariant sets. Subsequently a short survey of safety envelope search methods is given. Finally, some safety envelope optimization criteria are discussed. The methods are specified in detail in Chapter 9.

In the following, the concept of safety envelopes and barrier certificates are introduced using a simple linear example.

8.1 Concept of Safety Envelopes

If a system is initialised inside a safety envelope, the system is guaranteed not to evolve to some unsafe region of the state space. In the specific case of wind turbine emergency shutdowns, the envelope should guarantee that the wind turbine trajectory does not violate the ultimate load limits of the wind turbine, given an emergency shutdown initialised within the envelope. A similar concept of safety envelopes is used on aircrafts in order to ensure that the aircraft does not evolve to an unsafe region, which could damage the aircraft.

The wind turbine model is given by a set of polynomial differential equations on the form

$$\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t), \mathbf{d}(t)). \tag{8.1}$$

Let $\phi(t, \mathbf{x}_0, \mathbf{d}(t))$ denote the solution of equation (8.1) from an initial state $\mathbf{x}_0$ given some disturbance $\mathbf{d}(t)$ and the reachable map $\psi(t, \mathcal{X}_0, \mathcal{D}) = \{\phi(t, \mathbf{x}_0, \mathbf{d}(t)) \mid \mathbf{x}_0 \in \mathcal{X}_0, \mathbf{d}(t) \in \mathcal{D}\}$ denote the set-valued solution from all initial states. The total system is a 5-tuple consisting of $(\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_0, \mathcal{X}_\mathrm{u})$, where $\mathbf{f}$ is the vector field in (8.1), $\mathcal{X}$ is the state space, $\mathcal{D}$ is the disturbance set, $\mathcal{X}_0$ is the initial set and $\mathcal{X}_\mathrm{u}$ is the unsafe set provided in Section 7.2.

The concept of the safety envelope is illustrated in Figure 8.1. All shutdown trajectories initialised in $\mathcal{X}_0$ cannot evolve to some state in the unsafe set $\mathcal{X}_\mathrm{u}$ given some disturbance $\mathbf{d}(t)$ in a bounded set $\mathcal{D}$.

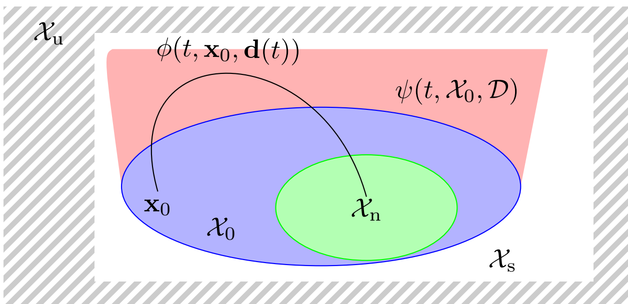


Figure 8.1: *The unsafe set $\mathcal{X}_\mathrm{u}$ is marked in grey, the normal operation $\mathcal{X}_\mathrm{n}$ in green, the initial set $\mathcal{X}_0$ in blue, the safe set $\mathcal{X}_\mathrm{s}$ in white and the reachable set $\psi(t, \mathcal{X}_0, \mathcal{D})$ in red. The reachable set should be separate from the unsafe set. An example trajectory is given as a black line initialised in $\mathbf{x}_0$.*

The safety of a system is defined in Definition 3.

Definition 3 (Safe system): *The system* $(\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_0, \mathcal{X}_\mathrm{u})$ *is defined as being safe, if all trajectories initialised in a set* $\mathcal{X}_0 \subseteq \mathcal{X}_\mathrm{s}$ *stays within the safe set* $(\psi(t, \mathcal{X}_0, \mathcal{D}) \subseteq \mathcal{X}_\mathrm{s},\ \forall t \geq 0)$.

The initial set $\mathcal{X}_0$ in Definition 3 forms a safety envelope. If a set $\mathcal{X}_0$ can be constructed, which guarantees the safety of the wind turbine, the boundary of such a set can be used as a shutdown criterion (recall that the safety envelope is found given an initialisation of the wind turbine emergency shutdown).

The method of barrier certificates can be used to *verify* if a given initial set is a safety envelope, without the need of calculating system trajectories. A barrier certificate is a function of state, satisfying a range of inequalities on the function itself and its Lie derivative along the flow of the system. The zero level of the barrier certificate separates the unsafe set from every trajectory initialised inside the zero level set. If a barrier certificate can be found given an initial set $\mathcal{X}_0$, then this initial set is safe and will be denoted a safety envelope [PJP07].

The objective of finding the largest possible safety envelope (denoted $\mathcal{X}_{0,\mathrm{opt}}$) of the system will not be pursued. Instead it is chosen to search for safety envelopes with bounded complexity. A safety envelope with some bounded complexity may not be unique. Consequently, the safety envelope should be chosen given some criterion, such as the safety envelope with the maximum volume,

$$\max \mathrm{vol}\ \mathcal{X}_0 \quad \text{s.t. } \psi(t, \mathcal{X}_0, \mathcal{D}) \subseteq \mathcal{X}_\mathrm{s}. \tag{8.2}$$

Optimization criteria related to emergency shutdowns of wind turbines are discussed in Section 8.3.

In the following, a simple example of a barrier certificate is given using the familiar concept of Lyapunov functions. The example is based on the Lyapunov equation in the search of a Lyapunov function.

Example 1 (Tower safety envelope): *An example of safety envelope construction using a Lyapunov function will be given. A sub-optimal solution to* (8.2) *will be found from an quadratic Lyapunov function, making* $\mathcal{X}_0$ *ellipse shaped. In the example a simplified version of the tower top fore-aft bending is considered. The ultimate load limit of the tower top bending used in the example is* $|{}^\mathrm{t}\theta_\mathrm{fa,y}| \leq \gamma_\mathrm{fa} = 4.77 \cdot 10^{-3}$ rad.

The tower model is in (6.27) *given as*

$$\begin{aligned}
{}^\mathrm{t}\dot{\omega}_\mathrm{fa,y} &= (M_\mathrm{n} L^2)^{-1} \left[F_\mathrm{r} L + F_\mathrm{g} L\, {}^\mathrm{t}\theta_\mathrm{fa,y} - K_\mathrm{fa}\, {}^\mathrm{t}\theta_\mathrm{fa,y} - B_\mathrm{fa}\, {}^\mathrm{t}\omega_\mathrm{fa,y}\right], \\
{}^\mathrm{t}\dot{\theta}_\mathrm{fa,y} &= {}^\mathrm{t}\omega_\mathrm{fa,y}.
\end{aligned}$$

The nonlinear external term F_r *will be neglected, such that the system becomes linear,*

$$\begin{bmatrix} {}^\mathrm{t}\dot{\omega}_\mathrm{fa,y} \\ {}^\mathrm{t}\dot{\theta}_\mathrm{fa,y} \end{bmatrix} = \begin{bmatrix} -\frac{B_\mathrm{fa}}{M_\mathrm{n} L^2} & \frac{F_\mathrm{g} L - K_\mathrm{fa}}{M_\mathrm{n} L^2} \\ 1 & 0 \end{bmatrix} \begin{bmatrix} {}^\mathrm{t}\omega_\mathrm{fa,y} \\ {}^\mathrm{t}\theta_\mathrm{fa,y} \end{bmatrix}.$$

A Lyapunov function $V(\mathbf{x})$ *of the tower system can be found using the Lyapunov equation*

$$\mathbf{PA} + \mathbf{A}^\mathrm{T}\mathbf{P} = -\mathbf{Q}. \tag{8.3}$$

Solving Equation (8.3) *for* $\mathbf{P}$ *given some positive definite matrix* $\mathbf{Q}$*, a Lyapunov function can be found as* $V(\mathbf{x}) = \mathbf{x}^\mathrm{T}\mathbf{P}\mathbf{x}$*, with the directional derivative of* $V(\mathbf{x})$ *given as* $\nabla V \mathbf{f}(\mathbf{x}) = \mathbf{x}^\mathrm{T}(\mathbf{PA} + \mathbf{A}^\mathrm{T}\mathbf{P})\mathbf{x}$.

Invariant sets can be derived from the Lyapunov function level sets. Given a Lyapunov function $V(\mathbf{x})$ *for the system, the set* $\Omega = \{({}^\mathrm{t}\omega_\mathrm{fa,y}, {}^\mathrm{t}\theta_\mathrm{fa,y}) \mid V(\mathbf{x}) \leq a\}$ *is invariant if* $\nabla V \mathbf{f}(\mathbf{x}) \leq 0$ *in* Ω

[Kha02]. As the Lyapunov function found using the Lyapunov equation is quadratic, the Lyapunov conditions hold globally and every level set of $V(\mathbf{x})$ is an invariant set.

Using `MATLAB` to determine the Lyapunov function for $\mathbf{Q} = \mathrm{diag}(500, 1)$ gives

$$
\begin{aligned}
V(\mathbf{x}) &= 2055{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}{}^2 + 4866{}^{\mathrm{t}}\theta_{\mathrm{fa,y}}{}^2 + 211{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}}, \\
\nabla V\mathbf{f}(\mathbf{x}) &= -{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}{}^2 - 500{}^{\mathrm{t}}\theta_{\mathrm{fa,y}}{}^2.
\end{aligned}
$$

The invariant level sets of the Lyapunov function can be used as safety envelopes. If the system is initialised within a given level set of $V(\mathbf{x})$, it will never be able to evolve to some state outside the level set. To obtain a safety envelope, the level set must separate the initial set from the unsafe set. This is obtained if the level set is in $\mathcal{X}_{\mathrm{s}}$. To visualise it, a function is defined as

$$B_{\mathrm{fa}}(\mathbf{x}) = V(\mathbf{x}) - a.$$

Figure 8.2 illustrates $B_{\mathrm{fa}}(\mathbf{x})$ using different values of a. This can be seen as lowering the Lyapunov function parabola in the safe set $\mathcal{X}_{\mathrm{s}}$. When the parabola is lowered, the zero level set generates a range of invariant ellipses.

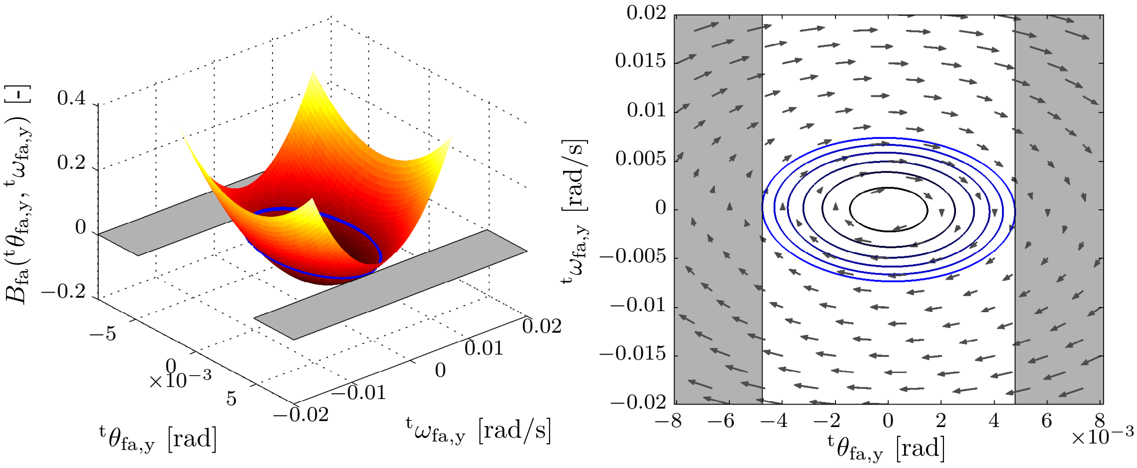


Figure 8.2: *Left the Lyapunov function parabola is lowered in the safe set. A zero level set is illustrated in blue. Right a range of zero level sets are illustrated. The vector field of the tower system is illustrated by arrows. In both plots the unsafe set $\mathcal{X}_{\mathrm{u}}$ is given in grey.*

From Figure 8.2 it is clear that the size of the zero level set of $B_{\mathrm{fa}}(\mathbf{x})$ depends on how much the parabola is lowered. The unsafe set needs to be in the exterior of the zero level set. The value of a for which the zero level set of $B_{\mathrm{fa}}(\mathbf{x}) = V(\mathbf{x}) - a$ is maximised given the choice of $\mathbf{Q}$, is found by solving $B_{\mathrm{fa}}({}^{\mathrm{t}}\omega_{\mathrm{fa,y}}, \gamma_{\mathrm{fa}}) = a$ and choosing a such that the resulting second order equation yields a single solution. In this way a is found to $a = 0.11$.

The maximum zero level ellipse of $B_{\mathrm{fa}}(\mathbf{x})$, denoted the Barrier is illustrated in Figure 8.3. Any initial set $\mathcal{X}_0$ which is in the interior of the barrier zero level ellipse is a safety envelope.

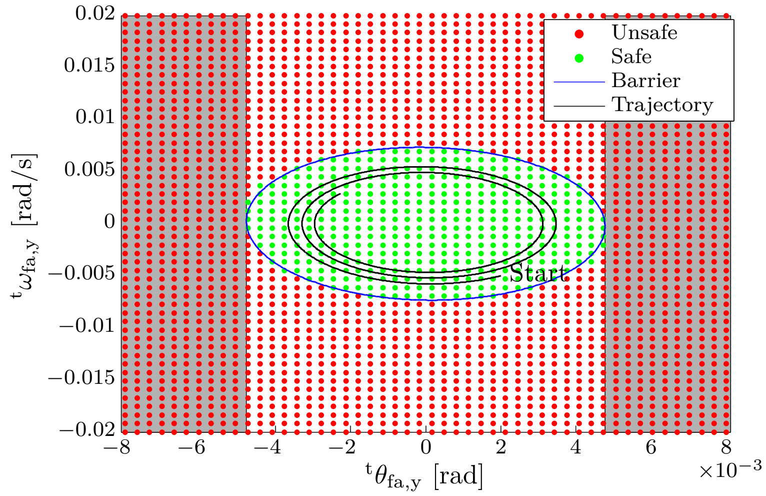


Figure 8.3: *Zero crossing of the barrier certificate, using the value of a which maximises the ellipse, is given in blue. The unsafe set $\mathcal{X}_u$ is given in grey. An arbitrary trajectory of the system initialised within the safety envelope is given in black. The green and red dots show simulated safe and unsafe initial states respectively.*

In Figure 8.3, the found safety envelope is compared to simulated safe and unsafe initial states. It should be noted that the orientation and shape of the ellipse are chosen arbitrarily through the choice of $\mathbf{Q}$.

The barrier $B_{fa}(\mathbf{x})$ has certain properties. As indicated in Figure 8.2, $B_{fa}(\mathbf{x})$ is positive in the unsafe set $\mathcal{X}_u$, non-positive in the interior of the ellipse and the directional derivative is non-positive.

The above example shows how a safety envelope can be designed using the Lyapunov equation in the case of a linear system description, without the need of system solutions. As the wind turbine model given in (6.34) is not on linear form, this Lyapunov equation approach cannot be used. In Chapter 9, the sum of squares framework is introduced. The framework allows a similar search of a barrier certificate when the vector field of the system is defined by polynomials and the sets (initial set $\mathcal{X}_0$, unsafe set $\mathcal{X}_u$, state space $\mathcal{X}$ and disturbance set $\mathcal{D}$) are semi-algebraic. The method handles uncertain disturbance input, which can be used to include the stochastic behaviour of the wind.

In the following section the methods, which will be used in the search of barrier certificates given a polynomial system description, are briefly introduced.

8.2 Safety Envelope Design Approach

This section introduces in short the methods which are used in the search of a safety envelope. In order to formulate a safety envelope search, which is computationally tractable, a number of methods are used.

Figure 8.4 illustrates the methods which will be used in the search of a safety envelope. The methods in white boxes are in [PJP07] used to formulate a safety verification of a given initial set $\mathcal{X}_0$. The methods in grey boxes are introduced in [SPW12] as a practical extension to the safety verification (in order to reduce the problem size).

Safety envelope	
Barrier cert.	Compositional barrier cert.
Positivstellensatz	
Sum of squares program (SOSP)	
Semidefinite programming (SDP)	
Decomposition	

Figure 8.4: *Methods which will be used in the search of a safety envelope. The top layer is the safety envelope itself. The problem of safety envelope design is propagated through the layers to form a semidefinite program, which can be solved on a PC.*

The concept of barrier certificates and the relation to safety envelopes were introduced in Example 1. This concept is formulated in [Pra06] and is introduced in the context of safety verification with disturbances in [PJP07]. A polynomial barrier certificate that separates the initial set $\mathcal{X}_0$ from the unsafe set $\mathcal{X}_\mathrm{u}$ should satisfy a range of conditions which can be stated as polynomial equalities and inequalities. These conditions can be transformed using the Positivstellensatz.

The Positivstellensatz states a relationship between a semi-algebraic set, and the existence of a certain polynomial [Las10]. 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 [Par03].

In [Par03] it is shown how a sum of squares decomposition can be computed using semidefinite programming (SDP). Consequently, the search of a sum of squares decomposition becomes tractable. The main result shows that the sum of squares procedure allows the search of solutions to the Positivstellensatz equation, with bounded complexity.

In [SPW12] the safety envelope verification is divided into smaller problems, which can be solved separately. Using this compositional method, the computational requirements of the calculations can be reduced. To obtain a solution which is valid for the complete system, the dual decomposition method is introduced.

To sum up, the validity of a barrier certificate can be examined using a polynomial identity from the Positivstellensatz. The existence of a solution to the Positivstellensatz identity can be cast as a sum of squares decomposition problem, which in turn can be transformed to a semidefinite program. A feasible solution to a semidefinite program can be searched for using existing SDP software.

In [PJP07] the sum of squares framework and barrier certificates are used to *verify* the safety of a given system. In the verification it is assumed that the initial set and the unsafe set are known. This verification produces an SDP feasibility problem. In the case of wind turbine safety supervisor design, it is desired to maximise the size of the safety envelope in order to keep the wind turbine operational without unnecessary emergency shutdowns. The safety validation problem should be changed to a safety envelope optimisation and validation problem. As an SDP can be formulated as an optimization problem with constraints, it is possible to include a safety envelope optimisation criterion in the SDP directly. This enables an optimization of the size of the envelope which satisfies the required conditions of the original safety validation problem. The SDP formalism is in general limited to linear optimization criteria.

In the following section possible optimization criteria, which can be used in the safety envelope search and which respect the limits of the SDP formulation, are examined. The criteria are chosen such that they make sense in the context of wind turbines.

8.3 Safety Envelope Optimisation Criteria

As mentioned in the above section, the method used to find barrier certificates is based on the concept of sum of squares and the use of SDP. Consequently, the search of a safety envelope should fit this framework.

Recall from Section 8.1, that the search of a safety envelope $\mathcal{X}_0$ has been limited to a search of a subset of the optimal safety envelope $\mathcal{X}_{0,\mathrm{opt}}$. The safety envelope is given as

$$\mathcal{X}_0 \subseteq \mathcal{X}_{0,\mathrm{opt}} \subseteq \mathcal{X}_\mathrm{s}.$$

In Figure 8.5 a range of different safety envelopes $\mathcal{X}_0$ are placed inside a fictitious optimal safety envelope $\mathcal{X}_{0,\mathrm{opt}}$. The shapes of the safety envelopes $\mathcal{X}_0$ are limited to circles.

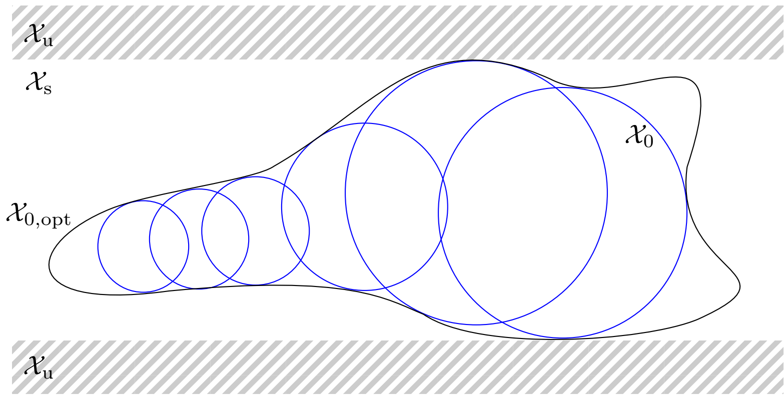


Figure 8.5: *A range of different safety envelopes $\mathcal{X}_0$ marked in blue are placed inside the optimal safety envelope $\mathcal{X}_{0,\mathrm{opt}}$ marked in black. The grey regions symbolise the unsafe set, $\mathcal{X}_\mathrm{u}$.*

As illustrated in Figure 8.5 the safety envelope $\mathcal{X}_0$, in the optimal safety envelope $\mathcal{X}_{0,\mathrm{opt}}$, given a specific shape of the safety envelope, is not unique. In order to select the safety envelope, a criterion is required. Such an optimisation criterion could be to select the safety envelope $\mathcal{X}_0$ with the largest volume in $\mathcal{X}_{0,\mathrm{opt}}$.

For the safety envelope to be useful, the practical problem must be taken into consideration. The main objective in the design of the safety envelope is to ensure safety of the wind turbine, while maintaining its operational uptime. The safety envelope should accordingly be designed with the objective of keeping the wind turbine operational.

To design a safety envelope which minimises the possibility of the system trajectory leaving it, the safety envelope should be designed with respect to the normal operation set $\mathcal{X}_\mathrm{n}$ of the wind turbine.

In Figure 8.6 a fictitious sampled normal operation set $\mathcal{X}_\mathrm{n}$ is illustrated. The safety envelope $\mathcal{X}_0$ is constructed with respect to the normal operation and the shape of the envelope is limited to the shape of an ellipse.

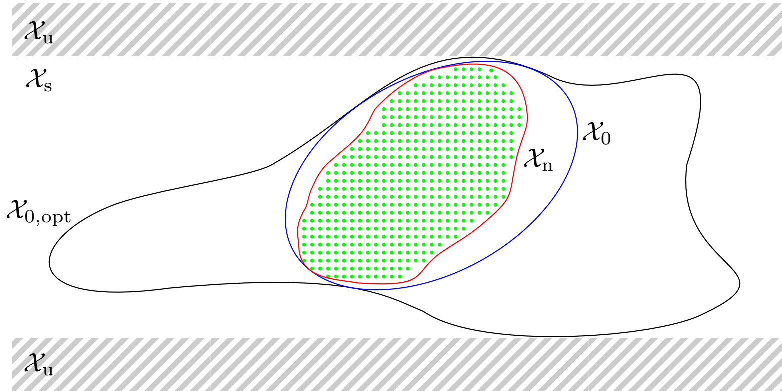


Figure 8.6: *The green circles symbolise measurements from the normal operation. The normal operation outline is given in red, $\mathcal{X}_{\mathrm{n}}$. The safety envelope $\mathcal{X}_0$ marked in blue, is placed inside the optimal safety envelope $\mathcal{X}_{0,\mathrm{opt}}$ marked in black. The grey regions symbolise the unsafe set, $\mathcal{X}_{\mathrm{u}}$.*

In Figure 8.6 the safety envelope covers the normal operation of the wind turbine. Using this choice of safety envelope, the possibility of the system trajectory leaving the safety envelope might be lower compared to the biggest volume envelope, even though the volume of the ellipse is smaller.

In Section 7.1 the normal operation of the NREL 5-MW wind turbine was found using a collective pitch controller and a varying wind field. Information from the normal operation such as mean value and orientation of the measurement point clouds can be used to choose a practical useable shape of the safety envelope.

8.3.1 Safety envelope optimisation formulation

As briefly introduced in Section 8.2, the search of a safety envelope is formulated as a semidefinite program. A standard SDP includes an optimisation of a linear cost function over symmetric positive semidefinite matrix variables.

The problem of minimising a linear function of variables $\mathbf{x} \in \mathbb{R}^{\mathrm{n}}$ is given as

$$\begin{aligned} \min_{\mathbf{x}} \quad & \mathbf{c}^{\mathrm{T}}\mathbf{x} \\ \text{s.t.} \quad & \mathbf{F}(\mathbf{x}) \succeq 0, \end{aligned}$$

where $\mathbf{F}(\mathbf{x}) \succeq 0$ is a matrix inequality that defines a convex feasible set [BV04]. Consequently, the safety envelope is restricted to be an LMI representable set with a linear optimisation criterion. In the following, optimisation criteria of a hyperellipsoid are considered.

8.3.2 Hyperellipsoid

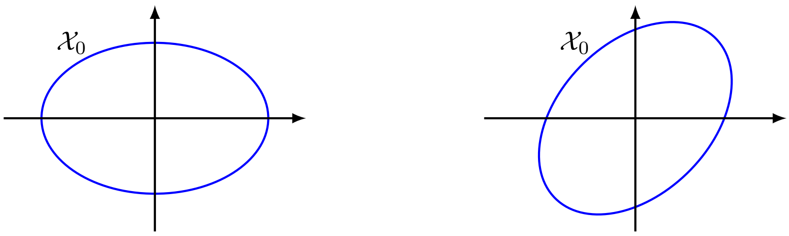
The hyperellipsoid is a simple geometric shape. The safety envelope $\mathcal{X}_0$ defined by a hyperellipsoid is given as

$$\mathcal{X}_0 = \{\mathbf{x} \in \mathbb{R}^{\mathrm{n}} | (\mathbf{x}-\mathbf{c})^{\mathrm{T}}\mathbf{E}(\mathbf{x}-\mathbf{c}) \leq 1\ ,\ \mathbf{E} = \mathbf{E}^{\mathrm{T}} \succ 0\}, \tag{8.4}$$

where $\mathbf{x}$ is the vector of variables, $\mathbf{c}$ is the vector defining the center of the hyperellipsoid and $\mathbf{E}$ is some positive symmetric matrix.

The hyperellipsoid allows the centre, scaling, orientation and shape as degrees of freedom. The scaling, orientation and shape of the hyperellipsoid are controlled by $\mathbf{E}$ in (8.4).

If $\mathbf{E}$ is limited to be diagonal $\mathbf{E} = \mathrm{diag}(a_{1,1}, a_{2,2}, ..., a_{\mathrm{n,n}})$ the hyperellipsoid axes will coincide with the Cartesian axes. An ellipse given by a diagonal $\mathbf{E}$ is illustrated in Figure 8.7a. An ellipse with off-diagonal elements different from zero in $\mathbf{E}$ can have an arbitrary orientation, which is illustrated in Figure 8.7b.



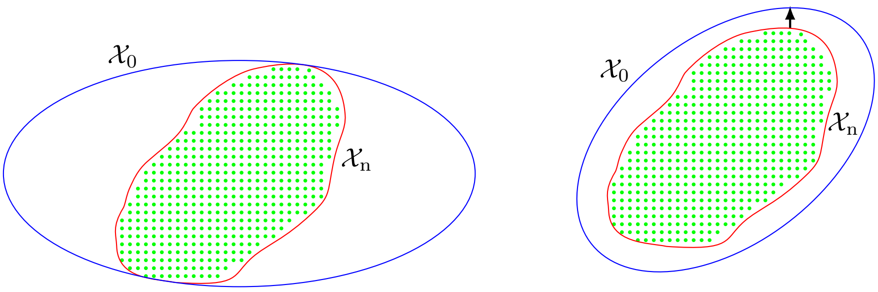
(a) *Locked orientation* **(b)** *Arbitrary orientation*

Figure 8.7: *The orientation of the ellipse is given by* $\mathbf{E}$. *Left the ellipse is given by diagonal* $\mathbf{E}$. *Right the ellipse is given by* $\mathbf{E}$ *with off-diagonal elements different from zero.*

8.3.3 Hyperellipsoid optimisation criteria

To obtain a safety envelope which best possible covers the normal operation, the safety envelope should be maximised according to some suitable measure.

In Figure 8.8 fictitious safety envelopes are respectively maximised according to the volume and the minimum distance to the normal operation.



(a) *Volume maximisation* **(b)** *Minimal distance maximisation*

Figure 8.8: *Left the safety envelope defined by an ellipse is optimised with respect to volume. Right the objective in the optimisation is to maximise the minimal distance to the normal operation set, which is given by an arrow. The normal operation is given as green circles symbolising measurement points. The normal operation outline is marked in red,* $\mathcal{X}_\mathrm{n}$. *The ellipse safety envelope* $\mathcal{X}_0$ *is given in blue.*

The disadvantage of maximising the volume of the safety envelope is that the distance to the normal operation might be small in some regions, or not even cover the normal operation. To minimise the probability of leaving the safety envelope, the measure of the minimal distance from the safety envelope to the normal operation could be used as optimisation criterion.

As mentioned, the optimisation of the safety envelope must be consistent with the SDP formulation. This limits the optimisation to be linear in the decision variables.

Maximum volume of hyperellipsoid

The volume of a hyperellipsoid defined as in (8.4) is given by the determinant of $\mathbf{E}$,

$$V_{\text{elip}} \propto \frac{1}{\sqrt{\det \mathbf{E}}}.$$

The volume of the hyperellipsoid can be maximised by maximising $\det \mathbf{E}^{-1}$ [Pan10]. This is a nonlinear optimisation problem. In [BV04] the optimisation problem is changed to become convex. This is done by introducing $\log\det \mathbf{E}^{-1}$. The resulting optimisation problem becomes

$$\begin{aligned} &\max\ \log\det \mathbf{E}^{-1} \\ &\text{s.t. } \mathbf{E} \succeq 0, \\ &\qquad \mathcal{X}_0(\mathbf{E}) \text{ is safe,} \end{aligned}$$

where both the objective and constraint are convex.

Both in the case of $\mathbf{E}$ having non zero off-diagonal elements and $\mathbf{E}$ being diagonal, the volume maximization is not linear. However as the optimisation is convex, it can in certain special cases be transformed to be linear by introducing additional constraints to the SPD problem as given in [BV04].

The above given optimisation criterion can be used to maximise the volume of the safety envelope when given as a hyperellipsoid. The optimisation optimises the true volume of the hyperellipsoid, but is only tractable in special cases.

Maximum sum of hyperellipsoid semi-principal axes

To relax the problem of finding the maximum volume of the safety envelope hyperellipsoid, the maximum sum of magnitudes of semi-principal axes of the hyperellipsoid can be considered.

The true volume of an hyperellipsoid is proportional to the magnitudes of the semi-principal axes as

$$V_{\text{elip}} \propto \prod_{i=1}^{\text{n}} \sigma_i,$$

where σ_i denotes the magnitudes of the semi-principal axes of the n dimensional hyperellipsoid. The eigenvalues of $\mathbf{E}^{-1}$ are the squares of the magnitudes of the semi-principal axes.

A maximisation of the *sum* of magnitudes of the semi-principal axes results in a measure which resembles the volume of the hyperellipsoid. In Figure 8.9 two ellipses with equal sums of magnitudes of the semi-principal axes are illustrated.

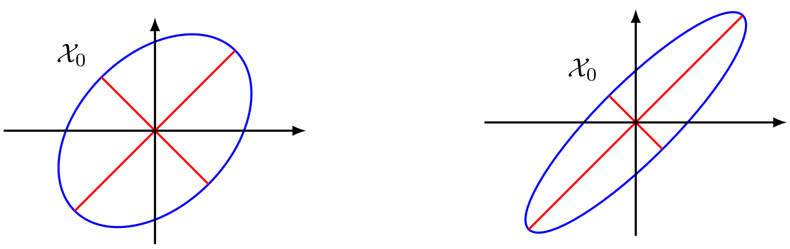


Figure 8.9: *The semi-principal axes are marked by red lines. The sums of magnitudes of the semi-principal axes of the ellipses are equal. The volume of the left ellipse is however approximately 1.5 times the volume of the right ellipse.*

In the special case of a real square matrix, the sum of eigenvalues equals the sum of diagonals of the matrix. As $\mathbf{E}^{-1}$ is square with real elements, the relationship between sum of eigenvalues and sum of diagonal elements can be exploited in the optimisation.

The eigenvalues of $\mathbf{E}^{-1}$ are denoted λ_i and the sum of diagonal elements by the trace of the matrix. The sum of eigenvalues equal the sum of diagonal elements

$$\sum_{i=1}^{\mathrm{n}} \lambda_i = \mathrm{Tr}\ \mathbf{E}^{-1}.$$

As the trace of the matrix $\mathbf{E}^{-1}$ is simply the sum of diagonals, this can easily be calculated. The maximisation of the semi-principal axes can in the SDP formulism be given as

$$\begin{aligned} &\min\ \mathrm{Tr}\ \mathbf{E} \\ &\text{s.t. } \mathbf{E} \succeq 0, \\ &\qquad \mathcal{X}_0(\mathbf{E}) \text{ is safe,} \end{aligned}$$

where the optimisation problem is linear in the objective.

The above objective of maximising the sum of magnitudes of the semi-principal axes is not identical to the objective of volume maximisation. However the trace of $\mathbf{E}$ does provide a similar measure and can directly be used in the SDP. In the following, an optimisation criterion which uses information from the normal operation is discussed.

Locked orientation and shape

In the following, the objective of maximising the minimal distance to the normal set is discussed, as illustrated in Figure 8.8b. As the true maximisation of the minimal distance to the normal operation set is difficult to formulate a similar measure will be used.

The idea of the following is to lock the orientation and shape of the safety envelope hyperellipsoid. The orientation is locked according to the shape of the normal operation.

The general shape of the normal operation can be found by calculating the covariance matrix of the measurements. The covariance matrix provides information about the orientation of the measurement point cloud. Choosing the hyperellipsoid matrix to be equal to the inverse of the covariance matrix locks the orientation and shape of the safety envelope.

The hyperellipsoid with orientation and shape defined by the normal operation covariance matrix is given by

$$\mathcal{X}_0 = \{\mathbf{x} \in \mathbb{R}^{\mathrm{n}} | (\mathbf{x} - \mathbf{c})^{\mathrm{T}} \mathbf{B} (\mathbf{x} - \mathbf{c}) < d\ ,\ d \geq 0\}, \tag{8.5}$$

with $\mathbf{B}$ being the inverse of the covariance matrix of the normal operation measurements and $\mathbf{c}$ being a measure of the center of the measurements, such as the mean or median.

Figure 8.10 illustrates two examples of normal operation locked ellipses. By adjusting d in (8.5), different level curves of (8.5) can be found.

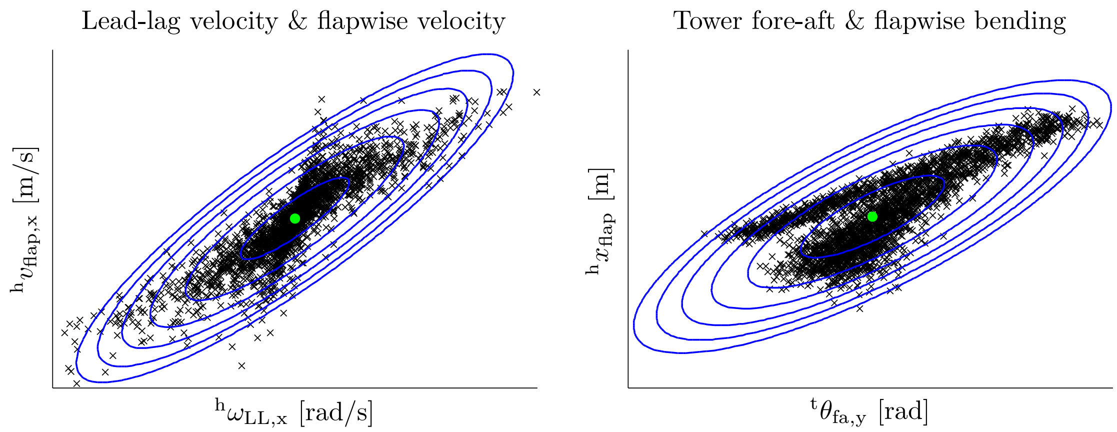


Figure 8.10: *Safety envelopes $\mathcal{X}_0$ are marked in blue. The normal operation point cloud projections onto the ${}^{\mathrm{h}}\omega_{\mathrm{LL,x}}, {}^{\mathrm{h}}v_{\mathrm{flap,x}}$ and ${}^{\mathrm{t}}\theta_{\mathrm{fa,y}}, {}^{\mathrm{h}}x_{\mathrm{flap}}$ planes are illustrated by black crosses. The medians of the point clouds are given as green dots. A range of ellipses are found using different values of d. The axes are given without units.*

As illustrated in Figure 8.10 the orientation and shape of the ellipse can be locked using the covariance matrix of the normal operation. The size of the ellipse can be maximised by adjusting d in (8.5). Defined as an SDP,

$$\begin{aligned} &\max\ d \\ &\text{s.t.}\ \ d \geq 0, \\ &\qquad \mathcal{X}_0(d) \text{ is safe.} \end{aligned}$$

The above optimisation objective is not equal to a maximisation of the minimal distance to the normal operation, as illustrated in Figure 8.8b. However, the optimisation provides a similar measure and can directly be formulated as an SDP, as the optimisation is linear. The covariance matrix of the normal operation measurement data can be found on the enclosed DVD.

8.3.4 Composite safety envelope

In the above, two different optimisation criteria have been discussed, respectively optimisation of the sum of magnitudes of semi-principal axes and the optimisation of the ellipse with locked orientation and shape. Several additional optimisation criteria could be formulated. Further the center of the hyperellipsoids could be chosen according to a range of criteria. As every envelope guarantees the safety of the system, independently of the optimisation criterion, the envelopes can be combined into one collective envelope, denoted $\mathcal{X}_{0,\mathrm{comp}}$.

In Figure 8.11 fictitious envelopes found using respectively trace and locked orientation in the optimisations are combined into one collective envelope.

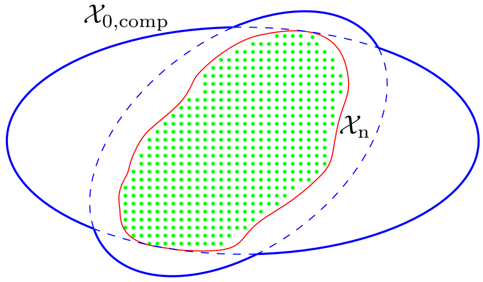


Figure 8.11: *Composed safety envelope $\mathcal{X}_{0,\mathrm{comp}}$ in solid blue. The safety envelope is composed by two ellipses. The normal operation measurements are given as green dots and bounded by the normal operation set in red.*

The system is safe as long as it is within at least one of the safety envelopes, as given in

$$\mathcal{X}_{0,\mathrm{comp}} = \bigcup_i \mathcal{X}_{0,i},$$

where $\mathcal{X}_{0,i} \subseteq \mathcal{X}_{0,\mathrm{opt}} \subseteq \mathcal{X}_\mathrm{s}$. If the state is in $\mathcal{X}_{0,\mathrm{comp}}$ then the system is safe.

The fact that the safety envelopes can be combined is useful in practice. Assume that it is found that the wind turbine is often shut down due to the states leaving the safety envelope in a given region of the state space. To reduce the frequency of the emergency shutdowns, a search of safety envelope in the specific region could be performed and the resulting envelope could be included in the combined envelope.

As mentioned in Section 2.5, the operational control of the wind turbine in power production mode is divided into regions given roughly by the wind speed. This is evident from the normal operation clouds given in Figure 7.2 and Figure G.1 in Appendix G. In order to cover normal operation, it might be beneficial or even necessary to design a safety envelope specifically to each region of the operational controller.

In Figure 8.12 the normal operation cloud of the rotor angular velocity and the tower top bending is separated into the measurements obtained in controller region 2 and region 3 respectively. Two ellipses are constructed according to the shape of the region 2 and region 3 measurements. Additionally a fictitious optimal safety envelope is illustrated.

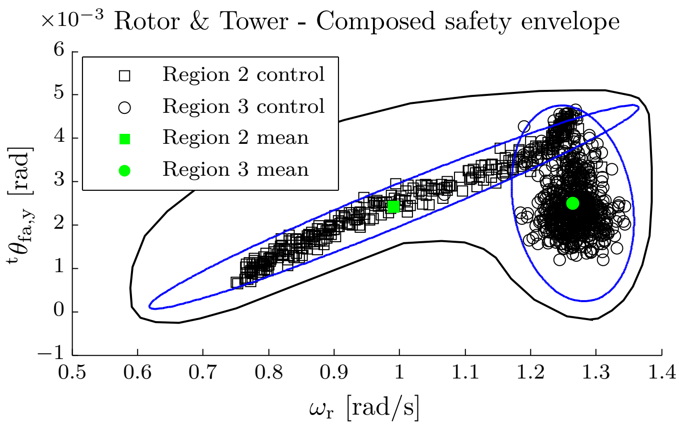


Figure 8.12: *Composed safety envelope designed according to the regions of the operational controller. The safety envelopes are given in blue. The optimal safety envelope $\mathcal{X}_{0,\mathrm{opt}}$ is given in black. The means of the normal operation in controller region 2 and region 3 are given by a green square and dot respectively.*

In the case illustrated in Figure 8.12 it is not possible to cover the normal operation using a single ellipse. By using ellipses designed specifically to each controller operation region, the normal operation is covered.

In this section some optimisation criteria of hyperellipsoids were introduced. The maximisations of volume and minimum distance to the normal operation set were relaxed to similar metrics, which can be formulated in an SDP.

The concept of safety envelopes, mathematical tools used in the search of a safety envelope and safety envelope optimisation criteria have been introduced. In the following chapter the search of ellipse shaped safety envelopes given the optimisation criteria found in this chapter, will be formulated.

9 Envelope Construction

In this chapter two different barrier certificates formulations are given. A safety envelope search is formulated using a convex barrier certificate description, the Positivstellensatz and SDP. Finally the computation of the resulting SDP is discussed.

9.1 Barrier Certificate Formulations

In this section two different barrier certificate formulations are given.

The barrier certificate guarantees that a trajectory initialised in the initial set $\mathcal{X}_0$ cannot evolve to the unsafe set $\mathcal{X}_\mathrm{u}$, given a piecewise continuous and bounded disturbance $d \in \mathcal{D}$. The barrier certificate formulation, which will be denoted the "strict barrier certificate", is given in Theorem 1.

Theorem 1 [PJP04]: *Given a system $(\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_0, \mathcal{X}_\mathrm{u})$, let $B(\mathbf{x})$ be a differentiable scalar function satisfying*

$$B(\mathbf{x}) \leq 0, \forall \mathbf{x} \in \mathcal{X}_0, \tag{9.1}$$

$$B(\mathbf{x}) > 0, \forall \mathbf{x} \in \mathcal{X}_\mathrm{u} \text{ and} \tag{9.2}$$

$$\nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, \mathbf{d}) < 0, \forall (\mathbf{x}, \mathbf{d}) \in \mathcal{X} \times \mathcal{D} \text{ s.t. B}(\mathbf{x}) = 0. \tag{9.3}$$

If such a function exists the system is safe.

In the above formulation the derivative along the flow of the system should be negative only on the zero level set of the barrier certificate. In this formulation of the barrier certificate, a trajectory initialised in the initial set $\mathcal{X}_0$ cannot cross the zero level set of the barrier certificate.

As will later be evident, the search of a barrier certificate satisfying the strict barrier certificate formulation in (9.3) is not convex. In the following a convex barrier certificate formulation is given.

In the following barrier certificate formulation the derivative constraint is changed to be negative everywhere in $\mathcal{X} \times \mathcal{D}$. As a result the formulation becomes convex. The convex barrier certificate formulation, which will be denoted the "weak barrier certificate", is given in Theorem 2.

Theorem 2 [PJP04]: *Given a system $(\mathbf{f}, \mathcal{X}, \mathcal{D}, \mathcal{X}_0, \mathcal{X}_\mathrm{u})$, let $B(\mathbf{x})$ be a differentiable scalar function satisfying*

$$\begin{aligned} B(\mathbf{x}) &\leq 0, \forall \mathbf{x} \in \mathcal{X}_0, \\ B(\mathbf{x}) &> 0, \forall \mathbf{x} \in \mathcal{X}_\mathrm{u} \text{ and} \\ \nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, \mathbf{d}) &\leq 0, \forall (\mathbf{x}, \mathbf{d}) \in \mathcal{X} \times \mathcal{D}. \end{aligned} \tag{9.4}$$

If such a function exists the system is safe.

In the above formulation of the barrier certificate, the derivate along the flow of the system should be non-positive everywhere in $\mathcal{X} \times \mathcal{D}$. As a result, every level set of the barrier certificate becomes an invariant set. In this formulation the barrier certificate is somewhat similar to a Lyapunov function, as demonstrated in Example 1. As the derivative constraint in (9.4) is clearly stricter than in (9.3), the weak barrier certificate formulation becomes conservative.

In Figure 9.1, the barrier certificate formulations in Theorem 1 (left) and Theorem 2 (right) are illustrated. The arrows indicate the derivative of the barrier certificates along the flow of the system with disturbances.

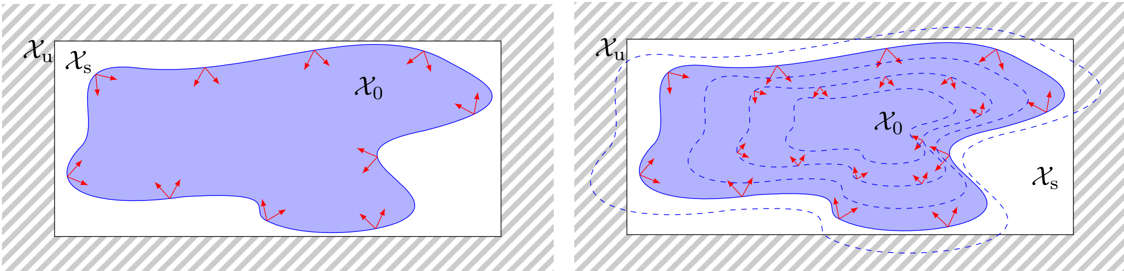


Figure 9.1: *Barrier certificate examples with arrows indicating the derivative* $\nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, \mathbf{d})$. *Left the derivative of the barrier certificate along the flow is non-positive on* $B = 0$. *Right the derivative of the barrier certificate along the flow is negative on* $\mathcal{X}$.

The constraints of the barrier certificate formulations can all be expressed as checking functions for negativity and non-negativity on the sets $(\mathcal{X}_0, \mathcal{X}_u, \mathcal{X} \times \mathcal{D})$. Checking global non-negativity of a function is in general a computational difficult problem. To relax the problem, the barrier certificate is limited to the class of multivariate polynomials with the sets being semi-algebraic. By using the special class of multivariate polynomials, the sums-of-squares polynomials, the problem of designing positive functions become computationally tractable [Par03]. In the following section the definition of general polynomials (which was shortly introduced in Section 6.1) and the sum of squares (SOS) polynomials will be defined.

9.2 Sum of Squares Polynomials

A general polynomial is given as a linear combination of monomials (finite products of variables)

$$f(\mathbf{x}) = \sum_i c_i m_i, \ \{c_i\} \subset \mathbb{R}, \ \{m_i\} \subset \mathcal{M}(\mathbf{x}),$$

where c_i is constant and m_i is from the family of monomials generated by $X = \{x_1, ..., x_n\}$.

The set of all polynomials in variables $\mathbf{x}$ will be denoted $\mathcal{R}_{\mathbf{x}}$. The degree of a monomial is defined as the sum of the exponents. The degree of a polynomial is defined as the maximum degree of its monomials. The set of all polynomials with degree k will be denoted $\mathcal{R}_{\mathbf{x}}^{\mathrm{k}}$.

A special class of polynomials is the sum of squares (SOS) polynomials. A given polynomial $F(\mathbf{x})$ is an SOS polynomial if it can be decomposed by a sum of squared polynomials

$$F(\mathbf{x}) = \sum_i f_i^2, \ f_i \in \mathcal{R}. \tag{9.5}$$

As the polynomial $F(\mathbf{x})$ can be decomposed by a sum of squared polynomials, it is guaranteed to be globally nonnegativ, $F(\mathbf{x}) \geq 0 \ \forall \mathbf{x} \in \mathbb{R}^{\mathrm{n}}$. An obvious necessary condition of the existence of the decomposition is that degree k of $F(\mathbf{x})$ is an even number.

The set of all polynomials in variables $\mathbf{x}$ which is SOS will be denoted $\Sigma_{\mathbf{x}}$, defined as

$$\Sigma_{\mathbf{x}} = \left\{ \ f \ \middle| \ f = \textstyle\sum_i f_i^2, \ f_i \in \mathcal{R}_{\mathbf{x}} \ \right\}.$$

It should be noted that the existence of an SOS decomposition of $f(x_1, ..., x_\mathrm{n})$ is only a sufficient condition of global nonnegativity. The set of positive polynomials and the set of SOS polynomials are only equal in special cases. Thus a function might be globally nonnegativ even though an SOS decomposition does not exist [Par03].

In the following section the search of a polynomial barrier certificate, being positive on semi-algebraic sets, is cast as a problem of finding a certain type of polynomial - using the Positivstellensatz.

9.3 Positivstellensatz

The Positivstellensatz' of Stengle and Putinar in the field of real algebraic geometry are key theorems in the construction of a barrier certificate using SOS decomposition. The Positivstellensatz' enable a transformation of a range of requirements as e.g. in Theorem 1, to a dual problem. Feasibility of the dual problem implies feasibility or infeasibility of the primal problem, depending on the choice of Positivstellensatz [Lal11].

To be able to utilize the Positivstellensatz' the concepts of monoids, cones and ideals have to be defined. Monoids, cones and ideals can be used to formulate inequalities, inequations and equalities of the primal problem.

Definition 4 (Multiplicative monoid): *Given $G = \{g_1, ..., g_\mathrm{t}\} \in \mathcal{R}$, the multiplicative monoid generated by the family G is defined by*

$$\mathcal{M}(g_1, .., g_\mathrm{t}) = \left\{ \prod_{i=1}^{\mathrm{t}} g_i^{l_i} \;\middle|\; l_i \in \mathbb{Z}_{\geq 0} \right\}.$$

The empty product is defined to be $\mathcal{M}(\emptyset) = 1$.

Given $\{g_1, g_2, g_3\} \in \mathcal{R}$ the multiplicative monoid is given as

$$\mathcal{M}(g_1, g_2, g_3) = \left\{ g_1^{k_1} g_2^{k_2} g_3^{k_3} \middle| k_1, k_2, k_3 \in \mathbb{Z}_{\geq 0} \right\}.$$

Definition 5 (Preordering): *Given $F = \{f_1, ..., f_\mathrm{r}\} \in \mathcal{R}$ the preordering $\mathcal{P}$ generated by the family F is a convex cone defined as*

$$\mathcal{P}(f_1, .., f_\mathrm{r}) = \left\{ \sum_{i=0}^{\mathrm{l}} s_i b_i \;\middle|\; l \in \mathbb{Z}_+,\ s_i \in \Sigma,\ b_i \in \mathcal{M}(f_1, ..., f_\mathrm{r}) \right\}. \tag{9.6}$$

A polynomial f in the preordering generated by two polynomials $\{f_1, f_2\}$ could be

$$\mathcal{P}(f_1, f_2) \ni f = s_0 + s_1 f_1 + s_2 f_2 + s_3 f_1 f_2 + s_4 f_1^5 + s_5 f_2^5. \tag{9.7}$$

The definition of the preordering (9.6) enables $f \in \mathcal{P}(f_1, f_2)$ to be an infinite sum of products, since an infinite combination of multiplicative monoids exists. It is, however, possible to reduce the unique expressions of the preordering to 2^r terms [Zac03]. The preordering in Example (9.7) can be reduced to

$$\begin{aligned} f &= s_0 + s_1 f_1 + s_2 f_2 + s_3 f_1 f_2 + s_4 f_1^2 f_1^2 f_1 + s_5 f_2^2 f_2^2 f_2 \\ &= s_0 + (s_1 + s_4 f_1^2 f_1^2) f_1 + (s_2 + s_5 f_2^2 f_2^2) f_2 + s_3 f_1 f_2 \\ &= s_0 + s_1' f_1 + s_2' f_2 + s_3 f_1 f_2. \end{aligned}$$

It should be noted that the term s_0 originates from the empty monoid product $\mathcal{M}(\emptyset) = 1$.

Definition 6 (Quadratic module): *A quadratic module $\mathcal{Q}$ generated by $\{f_1, ..., f_\mathrm{r}\} \in \mathcal{R}$ is a convex cone defined by*

$$\mathcal{Q}(f_1, .., f_\mathrm{r}) = \left\{ s_0 + \sum_{i=1}^{\mathrm{r}} s_i f_i \;\middle|\; s_i \in \Sigma \right\}. \tag{9.8}$$

From the definition it can be seen that the quadratic module is a preordering without cross products. Further it should be noted that the quadratic module is a finite sum of products, in contrary to the preordering. A polynomial f in the quadratic module generated by two polynomials $\{f_1, f_2\}$ is given as

$$\mathcal{Q}(f_1, f_2) \ni f = s_0 + s_1 f_1 + s_2 f_2.$$

Definition 7 (Ideal): *A polynomial ideal $\mathcal{I}$ generated by $H = \{h_1, ..., h_\mathrm{u}\} \in \mathcal{R}$ is defined by*

$$\mathcal{I}(h_1, .., h_\mathrm{u}) = \left\{ \sum_{k=1}^{\mathrm{u}} h_k f_k \;\middle|\; f_k \in \mathcal{R} \right\}.$$

The ideal is a finite sum of products. A polynomial h in the ideal generated by the two polynomials $\{h_1, h_2\}$ is given as

$$\mathcal{I}(h_1, h_2) \ni h = h_1 f_1 + h_2 f_2, \;\; f_1, f_2 \in \mathcal{R}.$$

The above definitions enable the introduction of the Positivstellensatz' theorems of Stengle and Putinar. The Positivstellensatz' are used to transform the primal problem of the barrier certificate search to a dual problem.

Stengle's Positivstellensatz states a relation between the emptiness of a semi-algebraic set and the solvability of a given polynomial identity.

Theorem 3 [Ste74]: *Given polynomials $\{f_1, ..., f_\mathrm{r}\}$, $\{g_1, ..., g_\mathrm{t}\}$ and $\{h_1, ..., h_\mathrm{u}\}$ in $\mathcal{R}$, the following statements are equivalent:*

1. The set

$$\mathbb{K} = \left\{ \mathbf{x} \in \mathbb{R}^\mathrm{n} \;\middle|\; \begin{array}{c} f_1(\mathbf{x}) \geq 0, ..., f_\mathrm{r}(\mathbf{x}) \geq 0, \;\{f_1, ..., f_\mathrm{r}\} \in \mathcal{R}_\mathbf{x} \\ g_1(\mathbf{x}) \neq 0, ..., g_\mathrm{t}(\mathbf{x}) \neq 0, \;\{g_1, ..., g_\mathrm{t}\} \in \mathcal{R}_\mathbf{x} \\ h_1(\mathbf{x}) = 0, ..., h_\mathrm{u}(\mathbf{x}) = 0, \;\{h_1, ..., h_\mathrm{u}\} \in \mathcal{R}_\mathbf{x} \end{array} \right\} \tag{9.9}$$

is empty.

2. There exist polynomials $g \in \mathcal{M}(g_1, ..., g_\mathrm{t})$, $f \in \mathcal{P}(f_1, .., f_\mathrm{r})$ and $h \in \mathcal{I}(h_1, .., h_\mathrm{u})$ such that

$$f + g^2 + h = 0. \tag{9.10}$$

Using Stengle's Positivstellensatz it is possible to change the problem from evaluation of the set $\mathbb{K}$ to a search of a solution to the polynomial in (9.10). If the dual problem is feasible, then the primal problem is infeasible

$$f + g^2 + h = 0 \quad \Rightarrow \quad \mathbb{K} = \emptyset. \tag{9.11}$$

If the set is given by inequality constraints only, they describe a compact set and generate an Archimedean quadratic module - Putinar's Positivstellensatz theorem can in these cases be used to reduce the number of free parameters [Las10]. If some polynomial $u(\mathbf{x})$ from the quadratic module generated by the inequalities makes $\{\mathbf{x} \in \mathbb{R}^\mathrm{n} | u(\mathbf{x}) \geq 0\}$ compact, the quadratic module is Archimedean. Considering only basic semi-algebraic sets, Putinar's Positivstellensatz gives certificates of positivity of polynomials.

Theorem 4 [Put93]: *Given polynomials* $\{f_1, ..., f_{\mathrm{r}}\} \in \mathcal{R}$*, polynomial* $F(x) \in \mathcal{R}$ *and the basic semi-algebraic set*

$$\mathbb{K} = \left\{ \mathbf{x} \in \mathbb{R}^{\mathrm{n}} \;\middle|\; f_1(\mathbf{x}) \geq 0, ..., f_{\mathrm{r}}(\mathbf{x}) \geq 0,\ \{f_1, ..., f_{\mathrm{r}}\} \in \mathcal{R} \right\}.$$

If the quadratic module $\mathcal{Q}(f_1, ..., f_{\mathrm{r}})$ *is Archimedean, then*

$$F(\mathbf{x}) > 0,\ \forall \mathbf{x} \in \mathbb{K} \quad \Leftrightarrow \quad F(\mathbf{x}) \in \mathcal{Q}(f_1, ..., f_{\mathrm{r}}).$$

Putinar's Positivstellensatz states that, if a polynomial $F(\mathbf{x}) \in \mathcal{R}_{\mathbf{x}}$ is strictly positive on $\mathbb{K}$ then $F(\mathbf{x}) \in \mathcal{Q}(f_1, ..., f_{\mathrm{r}})$. As defined in (9.8), the quadratic module $\mathcal{Q}$ is a finite sum of products. As a consequence, Putinar's Positivstellensatz can be used when possible to reduce the complexity of the barrier certificate construction.

A simple example of the usage of the Positivstellensatz is given in Appendix I.

The Positivstellensatz' of Stengle and Putinar can be used to transform the problem of finding a barrier certificate (as given in Theorem 1 and 2) over semi-algebraic sets, into a problem of solving polynomial equations. The search of a solution to the polynomial equations can be formulated as the existence of a sum of squares decomposition, which will be described in Section 9.5. In Stengle's Positivstellensatz the set $\mathbb{K}$ which should be *empty* is formulated. In Putinar's Positivstellensatz, the positivity of the barrier certificate over a set can be formulated more directly.

In the following section a tractable SOS decomposition of a polynomial is formulated.

9.4 Sum of Squares Decomposition

A result of [Par03] is that the existence of a sum of squares decomposition as given in (9.5) can be formulated as an LMI feasibility problem. This allows the search of such a decomposition using existing SDP algorithms and software. The possibility to search for an SOS decomposition of a polynomial can be used in many applications, as discussed in [Zac03]. Besides the possibility to search for a sum of squares decomposition of a given polynomial, the SDP formulation also allows a construction of a sum of squares decomposable polynomial - given some free parameters of the polynomial.

The search of a sum of squares decomposition is given in Theorem 5.

Theorem 5 [Par03]: *Given a set of polynomials* $\{p_i\} \subset \mathcal{R}$*, the existence of some* $\{a_i\} \subset \mathbb{R}$ *to satisfy*

$$p = p_0 + \sum_i a_i p_i \in \Sigma, \tag{9.12}$$

is an LMI feasibility problem.

A polynomial p of degree $2d$ can be written in the form

$$p = \mathbf{z}^{\mathrm{T}} \mathbf{Q} \mathbf{z}, \tag{9.13}$$

where $\mathbf{z}$ is a vector containing the monomials of the polynomial of degree $\leq d$ and $\mathbf{Q}$ is a symmetric matrix, called the Gramian. The Gram matrix is in general not unique. If some $\mathbf{Q} \succeq 0$ can be found satisfying (9.13), then the polynomial p is an SOS polynomial. In the case of a decomposition of a static polynomial, this becomes an LMI feasibility problem of finding some $\mathbf{Q}$ such that $p = \mathbf{z}^{\mathrm{T}}\mathbf{Q}\mathbf{z}$. In the case where the polynomial p contains some free parameters, these will be related to the entries of $\mathbf{Q}$. The LMI feasibility problem in this case becomes a problem of finding values of the free parameters (a_i in (9.12)), such that p becomes SOS. The latter formulation allows tractable answers to questions such as

Given $p_0, p_1 \in \mathcal{R}$, does there exist a $k \in \mathcal{R}$ such that

$$p_0 + kp_1 \in \Sigma. \tag{9.14}$$

The above question can be formulated as in (9.12) by writing the polynomial k as a linear combination of its monomials, $k = \sum_{j=1}^{s} a_j m_j$, where a_j are scalar variables and m_j are given polynomials (found from the monomials of k). Inserting the linear combination of k in (9.14), the problem becomes $p_0 + \sum_{j=1}^{s} a_j(m_j p_1) \in \Sigma$, with decision variables a_i and number of monomials s. This question is now on the form (9.12) and can as a result be formulated as an LMI feasibility problem. The above question is very similar to the problem of finding barrier certificates formulated by the Positivstellensatz' using SOS decomposition, as will be evident in Section 9.5.

It should be noted that the free parameters of p must be related affinely to the entries of $\mathbf{Q}$ in order for the problem to be defined as an LMI. Using the Positivstellensatz it can be noted that only the definition of the barrier certificate in Theorem 2 becomes LMI's.

The formulation of SOS decomposition problems on the form in (9.13) produces a number of decision variables in the corresponding LMI. The number of decision variables is given as $N_{\text{dec}} = \binom{n+2d}{2d}$, the length of the vector $\mathbf{z}$ given as $\binom{n+d}{d}$ and the size of $\mathbf{Q}$ given as $\binom{n+d}{d} \times \binom{n+d}{d}$ [Par03].

The transformation from the SOS conditions to an LMI can be done manually for small problems. In larger problems, it is necessary to automate the translation process. The `YALMIP` [Löf04] toolbox for `MATLAB` can be used to translate an SOS problem into an SDP, use a given SDP solver (in this case `SeDuMi` [Oli05]) to solve the problem and convert the solution back to the original SOS problem. As this process is done automatically, it can be assumed that an SOS decomposition problem can be solved directly. In the following an SOS decomposition problem will be denoted a Sum Of Squares Program (SOSP) (similar to a Semidefinite Program).

An SOSP is given as:

Sum Of Squares Program

$$\begin{aligned} &\min_{\{a_i\} \subset \mathbb{R}} \sum_{i=1}^{I} w_i a_i \\ &\text{s.t. } \; p_{j,0} + \sum_{i=1}^{I} a_i p_{j,i} \in \Sigma, \; \text{for } j = 1, \ldots, J \end{aligned} \tag{9.15}$$

The SOSP formulation in (9.15) define a convex optimisation problem, where a_i are scalar real decision variables, w_i are given constant real numbers and $p_{j,i}$ are given polynomials with fixed coefficients. If a problem can be formulated as in (9.15) it can be passed to an SDP using `YALMIP` and solved using standard software [PP05].

In this project, the SOS decomposition is used in relation to the Positivstellensatz, such that a feasible barrier certificate can be computed. In the following section the formulation of a search of polynomial barrier certificates using the Positivstellensatz' of Stengle and Putinar is described. Additionally it is given how the hyperellipsoidal shape of $\mathcal{X}_0$ is included in the search, using the optimisation criteria discussed in Section 8.3.

9.5 Polynomial Barrier Certificate

The Positivstellensatz' of Stengle and Putinar can be used to transform the requirements of the barrier certificate into the existence of a polynomial identity. The search of a barrier certificate has accordingly been transformed into a question of finding a solution to this polynomial identity. It turns out that the SOS decomposition described in Section 9.4, can be used to search for such a solution.

In this section, the sets $\mathcal{X}$, $\mathcal{X}_0$, $\mathcal{X}_\mathrm{u}$ and $\mathcal{D}$ are formulated as semi-algebraic sets, such that they can be included in the Positivstellensatz. Additionally it is shown how the ellipses described in Section 8.3 can be used as an initial set $\mathcal{X}_0$. Assuming that the barrier certificate is polynomial, an SOSP can be used to search for a feasible certificate. Finally it is shown how the optimisation criteria of the ellipse described in Section 8.3 can be included in the SOSP.

The sets in consideration must be semi-algebraic sets according to the formulating of the Positivstellensatz' (be given as polynomial equalities, inequalities and inequations),

$$\begin{aligned}
\mathcal{X} &= \{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid \mathbf{g}_\mathrm{X}(\mathbf{x}) \geq 0, \mathbf{g}_\mathrm{X}(\mathbf{x}) = 0, \mathbf{g}_\mathrm{X}(\mathbf{x}) \neq 0\}\,, \\
\mathcal{X}_0 &= \{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid \mathbf{g}_0(\mathbf{x}) \geq 0, \mathbf{g}_0(\mathbf{x}) = 0, \mathbf{g}_0(\mathbf{x}) \neq 0\}\,, \\
\mathcal{X}_\mathrm{u} &= \{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid \mathbf{g}_\mathrm{u}(\mathbf{x}) \geq 0, \mathbf{g}_\mathrm{u}(\mathbf{x}) = 0, \mathbf{g}_\mathrm{u}(\mathbf{x}) \neq 0\}\,, \\
\mathcal{D} &= \{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid \mathbf{g}_\mathrm{D}(\mathbf{x}) \geq 0, \mathbf{g}_\mathrm{D}(\mathbf{x}) = 0, \mathbf{g}_\mathrm{D}(\mathbf{x}) \neq 0\}\,,
\end{aligned} \tag{9.16}$$

where the equalities and inequalities are element-wise. A one variable polynomial $g(x)$ positive on $[\underline{x}, \overline{x}]$ can be constructed by $g(x) = (x - \underline{x})(\overline{x} - x)$ [PJP07].

In order to formulate the SOSP, the three conditions of the barrier certificates in Theorem 1, 2 should be put on form of the SOSP given in (9.15). In the following it is shown how the three conditions of the weak barrier certificate are formulated as an SOSP.

Condition 1 - Safe set

The first condition of the weak barrier certificate states that $B(\mathbf{x}) \leq 0,\ \forall \mathbf{x} \in \mathcal{X}_0$. As described in Section 8.3, the set $\mathcal{X}_0$ is chosen to be hyperellipsoidal, defined as $\mathcal{X}_0 = \left\{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid 1 - \mathbf{x}^\mathrm{T}\mathbf{E}\mathbf{x} \geq 0\right\}$. As a result, $\mathcal{X}_0$ is defined *inside* the ellipse, as illustrated in Figure 9.2.

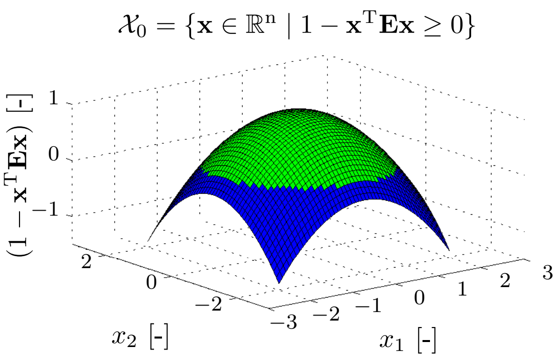


Figure 9.2: *Two dimensional initial set example. The parabola is nonnegative (green) in $\mathcal{X}_0$ and negative (blue) outside $\mathcal{X}_0$.*

The initial set $\mathcal{X}_0$ given by the ellipse (green in Figure 9.2) has a single polynomial inequality, making $\mathcal{X}_0$ compact in $\mathbb{R}^\mathrm{n}$. As a result, Putinar's Positivstellensatz can be used to transform the requirement of $B(\mathbf{x})$ to,

$$B(\mathbf{x}) \leq 0,\ \forall \mathbf{x} \in \mathcal{X}_0 \quad \Leftarrow \quad -B(\mathbf{x}) \in \mathcal{Q}(1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x}).$$

If some $-B(\mathbf{x})$ can be taken from the quadratic module $\mathcal{Q}(1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x})$, it is guaranteed to be negative on $\mathcal{X}_0$. An example $B(\mathbf{x})$ is illustrated in Figure 9.3.

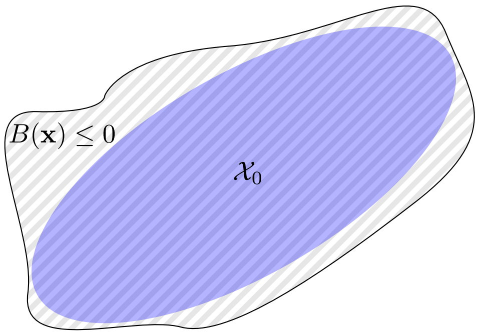


Figure 9.3: *By Putinar's Positivstellensatz, all polynomials which are negative on $\mathcal{X}_0$ are from the quadratic module $\mathcal{Q}(1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x})$.*

The resulting polynomial identity becomes (using the definition of the quadratic module in (9.8))

$$-B(\mathbf{x}) = s_0 + s_1(1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x}), \tag{9.17}$$

where $B(\mathbf{x}) \in \mathcal{R}_{\mathbf{x}}$ and $\{s_0, s_1\} \subset \Sigma_{\mathbf{x}}$. If some polynomial $B(\mathbf{x})$ and some SOS polynomials s_0 and s_1 can be found such that the above equation holds, then the barrier certificate is negative on the ellipse $\mathcal{X}_0$. If the objective is to maximise the initial set $\mathcal{X}_0$ (refer to Section 8.3), the term $(1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x})$ becomes a decision variable. In the case of maximisation of the trace, $\mathbf{E}$ becomes a decision matrix. In the optimisation using an ellipse with locked orientation and shape, the matrix $\mathbf{B}$ is static and the scalar variable d becomes a decision variable, $(d - \mathbf{x}^{\mathrm{T}}\mathbf{B}\mathbf{x})$ (can be interpreted as raising the polynomial illustrated in Figure 9.2).

As the quadratic module is generated by $1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x}$, which is a free polynomial, Equation (9.17) becomes a bilinear matrix inequality (BMI). Solvers for solving BMI's locally are applied with success in [SSE08]. It is however chosen to consider problems which are linear in the decision variables only. By setting the SOS variable s_1 in (9.17) to 1 (which is SOS) the problem becomes linear in the decision variables.

The resulting problem (by rearranging) becomes,

$$-B(\mathbf{x}) - (1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x}) \in \Sigma,$$

which comply with the SOSP defined in (9.15).

Condition 2 - Unsafe set

The second condition of the weak barrier certificate states that $B(\mathbf{x}) > 0,\ \forall(\mathbf{x}) \in \mathcal{X}_{\mathrm{u}}$. In this case the set $\mathcal{X}_{\mathrm{u}}$ is defined by the ultimate load limits of the system. The unsafe set can be defined by a number of state inequality constraints forming $\mathcal{X}_{\mathrm{u}} = \{\mathbf{x} \in \mathbb{R}^{\mathrm{n}} \mid \mathbf{g}_{\mathrm{u}} \geq 0\}$. As the ultimate load limits do not define a compact set, Putinar's Positivstellensatz cannot be used. Consequently Stengle's Positivstellensatz is used.

By the use of Stengle's Positivstellensatz, the set which should be *empty* is formulated. As the second condition of the strict barrier certificate states that $B(\mathbf{x})$ should be positive in $\mathcal{X}_\mathrm{u}$, the set which should be empty is constructed as all the points where $B(\mathbf{x})$ is non-positive in $\mathcal{X}_\mathrm{u}$. The set is $\mathbb{K}_\mathrm{u} = \{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid \mathbf{g}_\mathrm{u} \geq 0,\ -B(\mathbf{x}) \geq 0\}$. According to Stengle's formalism, the set is empty if zero can be taken from the preordering $\mathcal{P}(-B(\mathbf{x}), \mathbf{g}_\mathrm{u}(\mathbf{x}))$.

$$B(\mathbf{x}) > 0,\ \forall \mathbf{x} \in \mathcal{X}_\mathrm{u} \quad \Leftrightarrow \quad f = 0,\ f \in \mathcal{P}(-B(\mathbf{x}), \mathbf{g}_\mathrm{u}(\mathbf{x}))$$

If $\mathcal{X}_\mathrm{u}$ is defined by a single ultimate load limit, the preordering becomes

$$0 = s_0 - s_1 B(\mathbf{x}) + s_2 g_\mathrm{u}(\mathbf{x}) - s_3 B(\mathbf{x}) g_\mathrm{u}(\mathbf{x}).$$

If a polynomial $B(\mathbf{x}) \in \mathcal{R}_\mathbf{x}$ and some SOS polynomials $\{s_0, \ldots, s_3\} \subset \Sigma_\mathbf{x}$ can be found such that the above equation is satisfied, then the set is empty and the barrier certificate satisfy the unsafe set condition. The above problem is not linear in the decision variables. By manually picking $s_1 = 1$ and $s_3 = 0$, the problem becomes linear (but conservative). A barrier certificate which satisfy the condition related to the unsafe set is illustrated in Figure 9.4.

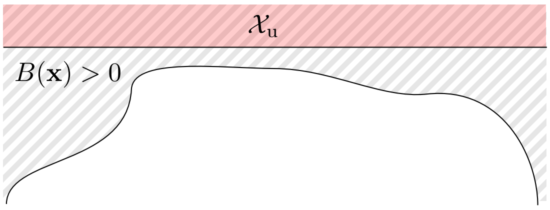


Figure 9.4: *By Stengle's Positivstellensatz, all polynomials which are positive on $\mathcal{X}_\mathrm{u}$ satisfies $f = 0,\ f \in \mathcal{P}(-B(\mathbf{x}), \mathbf{g}_\mathrm{u}(\mathbf{x}))$. The barrier certificate $B(\mathbf{x})$ is positive on $\mathcal{X}_\mathrm{u}$.*

The resulting SOSP becomes,

$$B(\mathbf{x}) - s_2 g_\mathrm{u}(\mathbf{x}) \in \Sigma,$$

which comply with the SOSP defined in (9.15). Several ultimate load limits (g_u's) can directely be included in the SOSP by formulating additional constraints. The problem of finding a $B(\mathbf{x})$ positive on $\mathcal{X}_\mathrm{u}$, when the nonlinear SOS terms are removed, is equivalent to $B(\mathbf{x}) \in \bigcap_i \mathcal{P}(g_{\mathrm{u},i})$.

Condition 3 - Derivative

The derivative condition of the weak barrier certificate states that,

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

where $\mathcal{X}$ defines the state space in consideration and $\mathcal{D}$ the set of disturbances. Using this formulation, the barrier derivative condition can be relaxed to only be satisfied in a part of the state space $\mathcal{X}$, which in practice can ease the search of a feasible barrier certificate.

Using Stengle's Positivstellensatz, the set which should be empty is formulated as the points at which the barrier derivative is positive in $\mathcal{X} \times \mathcal{D}$. The set is

$$\mathbb{K}_\nabla = \{\mathbf{x} \in \mathbb{R}^\mathrm{n} \mid \mathbf{g}_\mathrm{X} \geq 0,\ \mathbf{g}_\mathrm{D} \geq 0,\ \nabla B(\mathbf{x}) \mathbf{f}(\mathbf{x}, \mathbf{d}) \geq 0\}.$$

According to Stengle's formalism, the set is empty if zero can be taken from the preordering $\mathcal{P}(\nabla B(\mathbf{x}) \mathbf{f}(\mathbf{x}, \mathbf{d}), \mathbf{g}_\mathrm{X}(\mathbf{x}), \mathbf{g}_\mathrm{D}(\mathbf{x}))$,

$$\nabla B(\mathbf{x}) \mathbf{f}(\mathbf{x}, \mathbf{d}) \leq 0,\ \forall (\mathbf{x}, \mathbf{d}) \in \mathcal{X} \times \mathcal{D} \quad \Leftrightarrow \quad f = 0,\ f \in \mathcal{P}(\nabla B(\mathbf{x}) \mathbf{f}(\mathbf{x}, \mathbf{d}), \mathbf{g}_\mathrm{X}(\mathbf{x}), \mathbf{g}_\mathrm{D}(\mathbf{x})).$$

The concept of the barrier derivative being negative in the defined state space $\mathcal{X}$ is illustrated in Figure 9.5.

If $\mathcal{X}$ and $\mathcal{D}$ each are defined by a single polynomial inequality, the preordering becomes

$$\begin{aligned}0 = s_0 &+ s_1 \nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, d) + s_2 g_{\mathrm{X}} + s_3 g_{\mathrm{D}} \\ &+ s_4 \nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, d) g_{\mathrm{X}} + s_5 \nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, d) g_{\mathrm{D}} + s_6 g_{\mathrm{X}} g_{\mathrm{D}} \\ &+ s_7 \nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, d) g_{\mathrm{X}} g_{\mathrm{D}}.\end{aligned}$$

The terms with s_1, s_4, s_5 and s_7 contain products of unknown terms. As a result the SOS variables in these terms must be picked manually in order to obtain a linear problem. Choosing $s_1 = 1$ and the rest to be zero, resulting in

$$0 = s_0 + \nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, d) + s_2 g_{\mathrm{X}} + s_3 g_{\mathrm{D}} + s_6 g_{\mathrm{X}} g_{\mathrm{D}},$$

which is linear in the decision variables. The resulting SOSP becomes,

$$-\nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, d) - s_2 g_{\mathrm{X}} - s_3 g_{\mathrm{D}} - s_6 g_{\mathrm{X}} g_{\mathrm{D}} \in \Sigma,$$

which comply with the SOSP defined in (9.15). It should be noted that more limits on the state space and additional disturbances can directly be included in this program.

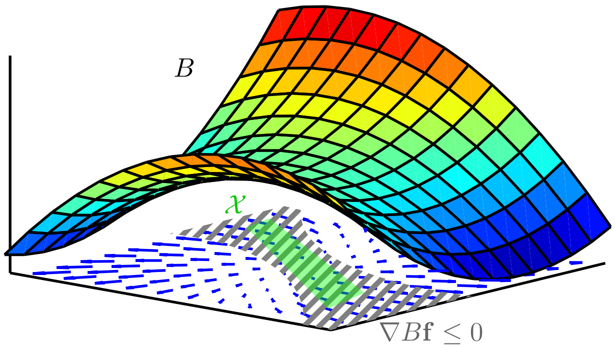


Figure 9.5: *By Stengle's Positivstellensatz, all polynomials which have a negative derivative (grey area) along the vector field (blue arrows) on $\mathcal{X}$ (green area), satisfy $f = 0$, where f is from the preordering $\mathcal{P}(\nabla B\mathbf{f}, \mathbf{g}_{\mathrm{X}}, \mathbf{g}_{\mathrm{D}})$.*

In the above, SOSPs of each weak barrier condition have been formulated. The SOSP defined in (9.15) enables multiple SOS constraints to be formulated in one SOSP. Thus it is possible to include the above three SOSPs into one program. If a barrier certificate $B(\mathbf{x})$ can be constructed which satisfy all SOS constraints, then this is a certificate that $\mathcal{X}_0$ is safe.

The optimisation criteria in (9.15) must be linear in the decision variables. Both the optimisation of the trace of $\mathbf{E}$ and the optimisation of the locked ellipse are linear in the decision variables. Consequently, both optimisation criteria can be formulated directly in the SOSP. In Figure 9.6 the optimisation of $\mathcal{X}_0$ is illustrated.

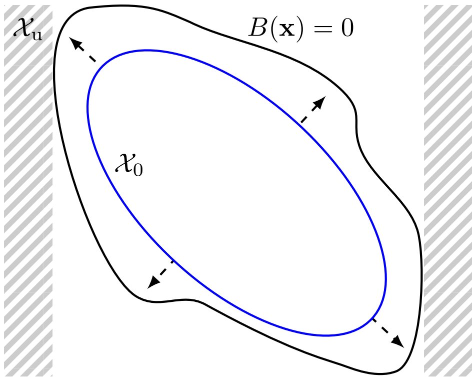


Figure 9.6: *Optimisation of initial set. The blue ellipse illustrate the initial set $\mathcal{X}_0$ which is being maximised. The black curve is the zero level set of the barrier certificate, which is a certificate for the safety of the initial set. The unsafe set $\mathcal{X}_\mathrm{u}$ is given in grey.*

The initial set $\mathcal{X}_0$ in Figure 9.6 can be enlarged as long as a feasible barrier certificate can be found (as long as the SOSP is able to find a feasible barrier certificate).

In the following an example of a barrier search using SOS is given. The example demonstrates how a barrier certificate can be obtained. The example uses the strict barrier certificate formulation, which is effectively relaxed to the weak barrier certificate in order to obtain a solvable problem.

Example 2 (Barrier certificate construction using SOS): *Consider the dynamical system in one state given as*

$$\dot{x}_1 = -x_1.$$

The state space $\mathcal{X}$, initial set $\mathcal{X}_0$ and unsafe set $\mathcal{X}_\mathrm{u}$ are given as

$$\begin{aligned}
\mathcal{X} &= \{x \in \mathbb{R}\}, \\
\mathcal{X}_0 &= \{x \in \mathbb{R} \mid |x| \leq 1\}, \\
\mathcal{X}_\mathrm{u} &= \{x \in \mathbb{R} \mid -4 < x < -2\}.
\end{aligned}$$

The objective is to examine if the initial set $\mathcal{X}_0$ is safe given an unsafe set $\mathcal{X}_\mathrm{u}$ using a barrier certificate.

The safe and unsafe sets are formulated as polynomial inequalities, using the technique given in (9.16)

$$\begin{aligned}
g_0(x_1) &= (x_1 - (-1))(1 - x_1) = 1 - x_1^2, \\
g_\mathrm{u}(x_1) &= (x_1 - (-4))(-2 - x_1) = -x_1^2 - 6x_1 - 8,
\end{aligned}$$

where $\mathcal{X}_0 = \{x \in \mathbb{R} \mid g_0(x_1) \geq 0\}$ and $\mathcal{X}_\mathrm{u} = \{x \in \mathbb{R} \mid g_\mathrm{u}(x_1) \geq 0\}$.

The initial set $\mathcal{X}_0$, unsafe set $\mathcal{X}_\mathrm{u}$, initial set polynomial $g_0(x_1)$, unsafe set polynomial $g_\mathrm{u}(x_1)$ and the vector field of the system are illustrated in Figure 9.7.

To find a barrier certificate that guarantees the separation of the initial set from the unsafe set, the strict barrier certificate formulation in Theorem 1 on Page 75 is used. To search for a barrier certificate, the requirements of the strict barrier certificate will be formulated using Stengle's and Putinar's Positivstellensatz'.

The barrier certificate should according to (9.1) *be non-positive in the initial set $\mathcal{X}_0$. As the polynomial defining $\mathcal{X}_0$ is compact, the requirement can be formulated using Putinar's Positivstellensatz. Given the closed set $\mathcal{X}_0 = \{x \in \mathbb{R} \mid g_0(x_1) \geq 0\}$, the barrier certificate $-B(x_1)$ is* *according to Putinar's Positivstellensatz positive on* $\mathcal{X}_0$ *if* $-B(x_1) \in \mathcal{Q}(g_0)$*, given as*

$$\mathcal{Q}(g_0) \ni -B(x_1) = s_0 + s_1 g_0(x_1),$$

where the polynomials $\{s_0, s_1\} \subset \Sigma_{x_1}$*. By rearranging, the requirement can be formulated as*

$$s_0 = -B(x_1) - s_1 g_0(x_1),$$

which is equivalent to testing if $-B(x_1) - s_1 g_0(x_1) \in \Sigma$.

The barrier certificate should according to (9.2) *be positive in the unsafe set* $\mathcal{X}_\mathrm{u}$*. As* $\mathcal{X}_\mathrm{u}$ *is also compact, Putinar's Positivstellensatz is used. Given the closed set* $\mathcal{X}_\mathrm{u} = \{x \in \mathbb{R} \mid g_\mathrm{u}(x_1) \geq 0\}$*, the barrier certificate* $B(x_1)$ *is according to Putinar's Positivstellensatz positive on* $\mathcal{X}_\mathrm{u}$ *if* $B(x_1) \in \mathcal{Q}(g_\mathrm{u})$*, given as*

$$\mathcal{Q}(g_\mathrm{u}) \ni B(x_1) = s_2 + s_3 g_\mathrm{u}(x_1),$$

where the polynomials $\{s_2, s_3\} \subset \Sigma_{x_1}$*. By rearranging, the requirement can be formulated as*

$$s_2 = B(x_1) - s_3 g_\mathrm{u}(x_1),$$

which is equivalent to testing if $B(x_1) - s_3 g_\mathrm{u}(x_1) \in \Sigma$.

The final requirement of the strict barrier certificate states that $\nabla B(x_1) f(x_1) < 0$ *on the zero level set of the barrier certificate. As this set description includes the equality constraint of the zero level set, Stengle's Positivstellensatz is used. In Stengle's formulation, the set which should* be empty *is formulated, as given in* (9.11).

The set

$$\mathbb{K} = \left\{ \mathbf{x} \in \mathbb{R} \;\middle|\; \begin{array}{c} \nabla B(x_1) f(x_1) \geq 0 \\ B(x_1) = 0 \end{array} \right\},$$

should be empty. This is equivalent to the existence of a solution to the polynomial $\mathcal{P}(\nabla B(x_1) f(x_1)) + \mathcal{I}(B(x_1)) = 0$*, given as*

$$s_4 + s_5 \nabla B(x_1) f(x_1) + B(x_1) f_1 = 0,$$

with the polynomials $\{s_4, s_5\} \subset \Sigma_{x_1}$ *and* $f_1 \subset \mathcal{R}_{x_1}$*. By rearranging, the requirement can be formulated as*

$$s_4 = -s_5 \nabla B(x_1) f(x_1) - B(x_1) f_1,$$

which is equivalent to testing if $-s_5 \nabla B(x_1) f(x_1) - B(x_1) f_1 \in \Sigma$.

The barrier certificate can now be found by choosing $\{s_1, .., s_5\} \subset \Sigma_{x_1}$ *and* $f_1 \in \mathcal{R}_{x_1}$ *such that*

$$\begin{aligned} &-B(x_1) - s_1 g_0(x_1), \\ &\;\; B(x_1) - s_3 g_\mathrm{u}(x_1), \\ &-s_5 \nabla B(x_1) f(x_1) - B(x_1) f_1, \end{aligned} \tag{9.18}$$

is SOS. The requirement in (9.18) *is not convex, as it includes products of free terms. By choosing* $s_5 = 1$ *and* $f_1 = 0$*, the requirement becomes* $-\nabla B(x_1) f(x_1) \in \Sigma$*, which is convex. This is effectively equivalent to the* weak *barrier certificate formulation, given in Theorem 2.*

In order to search for a barrier certificate $B(x_1)$*, the degree of the barrier certificate and SOS polynomials should be chosen. In order to obtain a barrier certificate,* $deg(B(x_1)) \geq 2$*. The SOS* *polynomials s_1, s_3 are chosen to the simplest case of scalars. With second order barrier certificate $B(x_1) = x_1^2 c_1 + x_1 c_2 + c_3$, the expressions by substitution become*

$$\begin{aligned} -x_1^2 c_1 - x_1 c_2 - c_3 - c_4(1 - x_1^2), \\ x_1^2 c_1 + x_1 c_2 + c_3 - c_5(-x_1^2 - 6x_1 - 8), \\ 2c_1 x_1^2 + c_2 x_1, \end{aligned} \tag{9.19}$$

which should be SOS, with $\{c_4, c_5\} \subset \Sigma_{x_1}$ and $\{c_1, c_2, c_3\} \subset \mathbb{R}$. If the expressions can be written as in (9.13) and $\{c_1, ..., c_5\}$ found such that $\mathbf{Q} \succeq 0$, then $B(x_1)$ is a certificate that the initial set $\mathcal{X}_0$ and the unsafe set $\mathcal{X}_\mathrm{u}$ are separated. The expressions in (9.19) on the form given in (9.13), with the vector $\mathbf{z} = [x_1, 1]^\mathrm{T}$ as the base of monomials, are

$$\mathbf{z}^\mathrm{T} \begin{bmatrix} c_4 - c_1 & \frac{-c_2}{2} \\ \frac{-c_2}{2} & -c_3 - c_4 \end{bmatrix} \mathbf{z}, \quad \mathbf{z}^\mathrm{T} \begin{bmatrix} c_1 + c_5 & \frac{c_2}{2} + 3c_5 \\ \frac{c_2}{2} + 3c_5 & c_3 + 8c_5 \end{bmatrix} \mathbf{z}, \quad \mathbf{z}^\mathrm{T} \begin{bmatrix} 2c_1 & \frac{c_2}{2} \\ \frac{c_2}{2} & 0 \end{bmatrix} \mathbf{z}, \tag{9.20}$$

where the matrices should be positive semidefinite simultaneously, in order for $B(x_1)$ to be a feasible barrier certificate. The search of $\{c_1, ..., c_5\}$ can according to (9.12) be formulated as an LMI feasibility problem, and solved using standard SDP solvers. As the example is very simple, the coefficients will be picked manually. A solution using the SDP solver `SeDuMi` can be found in Appendix K.

The coefficients $\{c_1, c_2, c_3\}$ belong to the quadratic barrier certificate. By inspection of the sets illustrated in Figure 9.7, it is obvious that $c_1 > 0$ and $c_3 < 0$, in order for the barrier certificate to be negative in the initial set and positive in the unsafe set. The SOS coefficients $\{c_4, c_5\}$ are chosen to positive scalars as $\mathbb{R}_{\geq 0} \subset \Sigma$. Substituting $\{c_1, c_2, c_3, c_4, c_5\} = \{\frac{1}{2}, 0, -1, 1, 1\}$ into (9.20) gives

$$\mathbf{z}^\mathrm{T} \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix} \mathbf{z}, \quad \mathbf{z}^\mathrm{T} \begin{bmatrix} \frac{3}{2} & 3 \\ 3 & 7 \end{bmatrix} \mathbf{z}, \quad \mathbf{z}^\mathrm{T} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \mathbf{z},$$

which are all positive semidefinite. As a result, an SOS decomposition of the expressions in (9.19) using the found coefficients exist. Inserting the coefficients in (9.19) gives

$$\begin{aligned} 1/2x_1^2, \\ 3/2x_1^2 + 6x_1 + 7, \\ x_1^2, \end{aligned}$$

where the first and third expressions are directly given as sums of squared polynomials. The second expression cannot directly be recognised as being SOS. By using $\mathbf{Q} = \mathbf{L}^\mathrm{T}\mathbf{L}$, the SOS decomposition can be found as

$$\begin{bmatrix} \frac{3}{2} & 3 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} 1.2247 & 2.4495 \\ 0 & 1.0000 \end{bmatrix}^\mathrm{T} \begin{bmatrix} 1.2247 & 2.4495 \\ 0 & 1.0000 \end{bmatrix}.$$

Using L, the SOS decomposition is found to $(1.2247x_1 + 2.4495)^2 + 1$, which is clearly a sum of squared polynomials.

The barrier certificate, using the found coefficients $\{c_1, c_2, c_3\}$, is given as $B(x_1) = \frac{1}{2}x_1^2 - 1$ and illustrated in Figure 9.7.

As a barrier certificate exist, no trajectory initialised in $\mathcal{X}_0$ can evolve to some state in $\mathcal{X}_\mathrm{u}$ and the system is accordingly safe.

In the above example the procedure of the barrier certificate search using SOS was given. A similar procedure will be used in the search of safety envelope of the wind turbine system. As the wind turbine system in relatively complex, this search cannot be performed by hand.

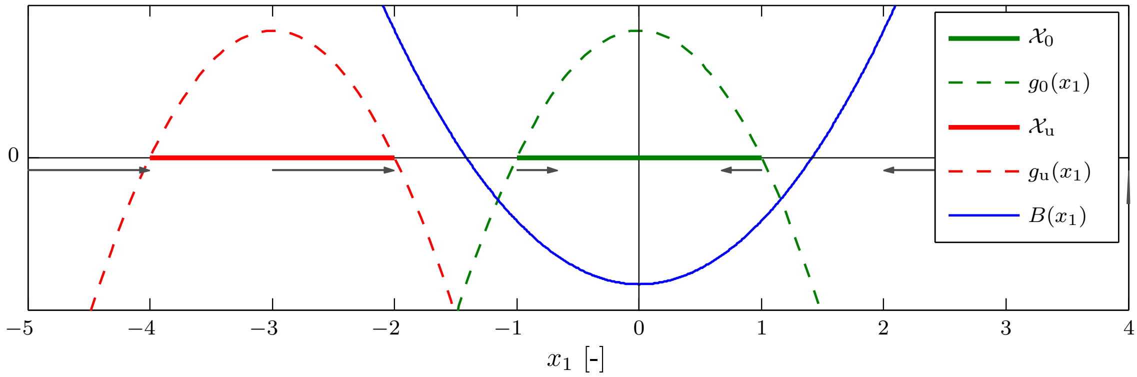


Figure 9.7: *The solid green and red lines illustrate the initial $\mathcal{X}_0$ and unsafe $\mathcal{X}_\mathrm{u}$ sets. The dashed green and red lines illustrate the initial $g_0(x_1)$ and unsafe $g_\mathrm{u}(x_1)$ polynomials, which are positive in the respective sets. The vector field of the system is given by grey arrows. The resulting barrier certificate is given in blue. The barrier certificate is negative in the safe set and positive in the unsafe set.*

In the following section, the SOSP solution search using the complete wind turbine model is discussed.

10 Computation of Safety Envelope

In this chapter, safety envelopes of the wind turbine system will be constructed. Initially the search of a single safety envelope of the complete wind turbine system is formulated as one SOSP. As the memory requirement of the complete SOSP is found to be very large, the wind turbine system is divided into subsystems from which separate safety envelopes are constructed. Finally the safety envelopes are assembled into a safety supervisor system, which is implemented and tested on the NREL 5-MW wind turbine in `FAST`.

10.1 Safety Envelope of Complete System

In this section the safety envelope search given the complete wind turbine system model in (6.34) is formulated in a single SOSP and the memory and computational requirements of the SOSP are examined. In order solve the SOSP on a standard PC, simplifications to the problem are introduced.

The complete polynomial model description in (6.34) includes 13 states with polynomial degree 12. The high polynomial degree of the model is due to the degree of the polynomial aerodynamic table approximations given in Section 6.3.

Using the weak barrier certificate formulation, the wind turbine safety envelope search can be formulated as demonstrated in Section 9.5. The SOSP of the safety envelope search, given the complete wind turbine system and the *trace* safety envelope optimisation criterion, is given in SOS Program 1.

SOS Program 1 Complete wind turbine system

$$
\begin{aligned}
\min \operatorname{Tr}\mathbf{E} \text{ over } & B \in \mathcal{R}_{\mathbf{x}},\ \mathbf{E} \in \mathbb{S}_{+}^{13},\ s_1, s_2, s_3, s_4, s_5 \in \Sigma_{\mathbf{x}},\ \mathbf{s}_{\mathrm{X,D}} \in \Sigma_{\mathbf{x},\mathbf{d}} \\
\text{s.t. } & B - s_1(\omega_{\mathrm{r}} - \gamma_{\mathrm{r}}) \in \Sigma \\
& B - s_2({\theta_{\Delta}}^2 - {\gamma_{\Delta}}^2) \in \Sigma \\
& B - s_3({}^{\mathrm{h}}{x_{\mathrm{flap}}}^2 - {\gamma_{\mathrm{flap}}}^2) \in \Sigma \\
& B - s_4({}^{\mathrm{h}}{\theta_{\mathrm{LL,x}}}^2 - {\gamma_{\mathrm{LL}}}^2) \in \Sigma \\
& B - s_5({}^{\mathrm{t}}{\theta_{\mathrm{fa,y}}}^2 - {\gamma_{\mathrm{fa}}}^2) \in \Sigma \\
& -B - (1 - \mathbf{x}^{\mathrm{T}}\mathbf{E}\mathbf{x}) \in \Sigma \\
& -\nabla B\mathbf{f} - \mathbf{s}_{\mathrm{X,D}}^{\mathrm{T}}\overline{\mathbf{g}}_{\mathrm{X,D}} \in \Sigma
\end{aligned}
$$

In SOS Program 1, $\mathbf{f}$ is the wind turbine system in (6.34), B is the barrier certificate, $\mathbf{E}$ is the matrix of the safety envelope ellipse, $\{\gamma_{\mathrm{r}},\ \gamma_{\Delta},\ \gamma_{\mathrm{flap}},\ \gamma_{\mathrm{LL}},\ \gamma_{\mathrm{fa}}\}$ are the ultimate load limits of the chosen states and $\overline{\mathbf{g}}_{\mathrm{X,D}}$ is a vector defining the state space and disturbance set. The bounded wind disturbance can be defined as an element in $\overline{\mathbf{g}}_{\mathrm{X,D}}$. Additionally, the state space $\mathcal{X}$ in consideration can be limited through $\overline{\mathbf{g}}_{\mathrm{X,D}}$, which in practice can ease the search of a feasible barrier certificate.

As the model $\mathbf{f}$ is of relative high dimension and the degrees of the polynomials are at the same time relative high, the SOSP becomes very large. A single constraint such as $s_1 \in \Sigma$ generates a matrix inequality constraint $\mathbf{Q}_1 \succeq 0$. With 13 states and polynomial degree $2d = 12$, the size of $\mathbf{Q}_1$ becomes

$$\binom{n+d}{d} \times \binom{n+d}{d} = \binom{13+12/2}{12/2} \times \binom{13+12/2}{12/2} = 27132 \times 27132.$$

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.

A set of linear matrix inequalities,

$$\mathbf{Q}_1 \succeq 0, \ldots, \mathbf{Q}_\mathrm{k} \succeq 0,$$

can be formulated as a single LMI and included as a single matrix inequality constraint. The resulting LMI can be constructed as

$$\mathbf{Q} = \mathrm{diag}\left(\mathbf{Q}_1, \ldots, \mathbf{Q}_\mathrm{k}\right) \succeq 0, \tag{10.1}$$

where the eigenvalues of $\mathbf{Q}$ are the union of the eigenvalues of $\mathbf{Q}_1, \ldots, \mathbf{Q}_\mathrm{k}$ [SW04].

It is clear from (10.1) that the size of $\mathbf{Q}$ increases with the number of matrix inequality constraints. As the safety envelope search in SOSP 1 produces several matrix inequality constraints, it is not possible to solve this complete SOSP on a regular PC.

In order to reduce the size of the problem, it is chosen to reduce the complexity of the model. In the model description given in (6.34) the wind disturbance enters through the wind turbulence model. As the wind turbulence model is considered the least important part of the model, it is removed. This implies that the disturbance enters the model unfiltered. By removing the wind turbulence model, the order of the complete model is reduced by two (reduced by two states).

The model in Chapter 6 was developed to handle wind speeds in the range $v_\mathrm{w} = [3 \text{ m/s} \ ; \ 30 \text{ m/s}]$. This resulted in high degree polynomial approximations of the aerodynamic tables (as they should span a large wind range). In order to reduce the required degree of the aerodynamic approximations, the wind range is limited to $v_\mathrm{w} = [15 \text{ m/s} \ ; \ 25 \text{ m/s}]$. This limitation allows reasonable approximations of the aerodynamic tables using 4^{th} degree polynomials. A comparison of the 4^{th} degree polynomial approximations to the original aerodynamic tables can be found in Appendix L. Using the above simplifications, the model is reduced to 11 states with a polynomial order of 6. These simplifications reduce the overall memory requirement to a few GB implemented in `MATLAB`, which allows the problem to be created. However, the SDP solvers use additional memory in setting up and solving the problem. Consequently, the problem is in spite of the model reduction, too large using a standard PC.

In Section 10.2 the simplified system model is separated into subsystems and separate safety envelopes of the subsystems are constructed. The problem with this technique is that the subsystem interconnections are not included in the safety guarantee. In Chapter 11 a recently proposed method of compositional barrier certificates, which can be used to verify safety of higher dimensional systems, is used to formulate the safety envelope search. Both techniques enable solutions to the resulting SOSPs to be obtained on a standard PC.

Ill-conditioning of SOSPs is often a problem. The problem of finding barrier certificates validating the safety of the wind turbine has also shown to be numerically difficult to compute. Albeit having reduced the problem size considerably, the SDP solver `SeDuMi` sometimes exits prematurely due to numerical issues. According to [LÖ9] a solution to an SDP (produced from the SOSP) does often not produce a strictly feasible SOS decomposition due to finite precision in the solver. As a result, the barrier certificates constructed using the SOSPs are in general not strictly certificates of safety. If a strictly feasible numerical certificate is required, the residuals of the SDP can be examined. This can be done using Theorem 8 in Appendix J. It is however in [Löf11] noted that a solution obtained from an SDP in most cases is sufficiently close to being feasible. In the following computations, the SOSPs will be slightly relaxed, such that better numerical results are obtained.

In the following section the problem is divided into subproblems which are solved individually.

10.2 Safety Envelopes of Separate Subsystems

The model is divided into subsystems which are considered individually. As the subsystems are considered 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 - such that the emergency shutdown procedure is included in this subsystem.

The subsystems and their interconnections are illustrated in Figure 10.1. The interconnections are given as arrows between the 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 not considered using this technique.

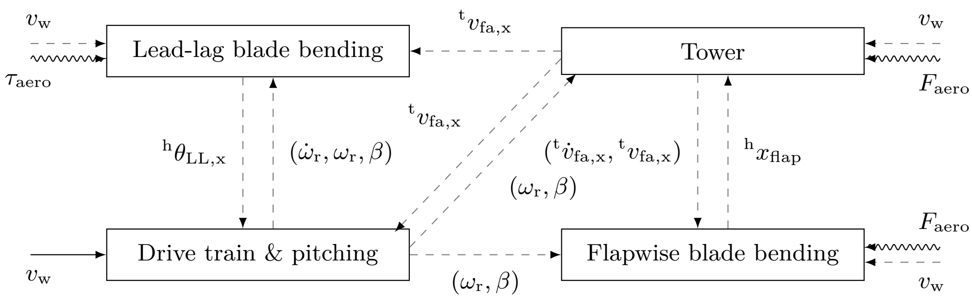


Figure 10.1: *The four separate subsystems are illustrated by boxes. The solid arrow is the real wind disturbance, the curly arrows the fictitious disturbances and the dashed arrows the interconnections which are not considered.*

As the interconnections are not considered, the subsystems do not interact. Consequently, it is only analysed whether a given subsystem is safe or not. To indirectly include the effects of the interconnections, some interconnections are replaced by unknown bounded disturbances. The choices of the unknown disturbances require practical knowledge, e.g. knowledge of the wind thrust force that affects the tower.

In the following, the safety envelopes of the four separate subsystems are computed.

10.2.1 Drive train & blade-pitching - safety envelope

The states of the drive train & blade-pitching subsystem are $\mathbf{x}_{\mathrm{r}} = [\omega_{\mathrm{r}}\ \omega_{\mathrm{g}}\ \theta_{\Delta}\ \theta_{\beta}\ \omega_{\beta}]^{\mathrm{T}}$. The drive train & blade-pitching subsystem will in the following be called the drive train subsystem for short. This subsystem incorporates the emergency shutdown procedure through the blade-pitch model and the aerodynamic functions. The drive train is in the complete model connected to the lead-lag bending of the blades and tower top velocity. The lead-lag bending of the blades affect the rotor torque, while the tower top velocity affects the wind speed experienced by the rotor. These interconnections are due to the separation of subsystems not included in the following drive train subsystem. The drive train subsystem is given as

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

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 $\beta = -\theta_{\beta} + 90$.

The state space $\mathcal{X}_{\mathrm{r}}$, unsafe set $\mathcal{X}_{\mathrm{u,r}}$ and disturbance set $\mathcal{D}_{\mathrm{r}}$ of the drive train subsystem are given as

$$\begin{aligned}
\mathcal{X}_{\mathrm{r}} &= \left\{ \mathbf{x} \in \mathbb{R}^5 \;\middle|\; \begin{array}{c} 0.5 \text{ rad/s} \le \omega_{\mathrm{r}} \le 3 \text{ rad/s},\\ 0.5 \cdot 97 \text{ rad/s} \le \omega_{\mathrm{g}} \le 3 \cdot 97 \text{ rad/s},\\ -0.5 \text{ rad} \le \theta_{\Delta} \le 0.5 \text{ rad},\\ 0^\circ \le \theta_{\beta} \le 90^\circ,\\ -20^\circ/\text{s} \le \omega_{\beta} \le 20^\circ/\text{s} \end{array} \right\},\\
\mathcal{X}_{\mathrm{u,r}} &= \left\{ \mathbf{x} \in \mathcal{X}_{\mathrm{r}} \;\middle|\; \omega_{\mathrm{r}} - \gamma_{\mathrm{r}} \ge 0 \right\} \cup \left\{ \mathbf{x} \in \mathcal{X}_{\mathrm{r}} \;\middle|\; {\theta_{\Delta}}^2 - {\gamma_{\Delta}}^2 \ge 0 \right\},\\
\mathcal{D}_{\mathrm{r}} &= \left\{ v_{\mathrm{w}} \in \mathbb{R} \;\middle|\; 15 \text{ m/s} \le v_{\mathrm{w}} \le 25 \text{ m/s} \right\},
\end{aligned} \tag{10.2}$$

where γ_{r} is the ultimate load limit of the rotor velocity and γ_{Δ} the ultimate load limit of the drive train torsion which are given in Section 7.2.

The state space in consideration has been limited such that only rotational speeds of the rotor in the interval [0.5 rad/s ; 3 rad/s] and the generator in the interval [$0.5 \cdot 97$ rad/s ; $3 \cdot 97$ rad/s] are considered. 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 β is limited to the interval $[0^\circ; 90^\circ]$. To facilitate the numerical solution it is found that the state space should be bounded in all dimensions. To obtain this, some fictitious state space bounds are constructed for the remaining states. These bounds are large enough to not impose additional restrictions to the practical solution. The wind disturbance is bounded such that it can only take values in the range 15 m/s to 25 m/s (due to the previously simplifications of the aerodynamic polynomial approximations).

To find a safety envelope of the drive train subsystem, the weak barrier certificate formulation is used. The technique demonstrated in Section 9.5 is used to transform the safety envelope optimisation into a tractable SOSP. The sets of the drive train given in (10.2) are transformed to the SOSP given in SOS Program 2. In the SOSP the trace optimisation criterion is used. The degrees of the SOS variables in (10.3) are chosen such that $\min(\deg s_1, \deg s_3) \ge \deg B_{\mathrm{r}}$ and $\min(\deg \mathbf{s}_{\mathrm{X,D}}) \ge \deg \mathbf{f}_{\mathrm{r}}$, where $\mathbf{f}_{\mathrm{r}}$ is the drive train subsystem [JWFP05]. The barrier certificate should be chosen to some predefined degree. It is in this case chosen to consider a quartic barrier certificate (if a feasible barrier certificate cannot be found, the degree can be increased).

SOS Program 2 Drive train subsystem

$$\begin{aligned}
e^* = &\min \operatorname{Tr} \mathbf{E}_{\mathrm{r}} \text{ over } B_{\mathrm{r}} \in \mathcal{R}^4_{\mathbf{x}_{\mathrm{r}}},\ \mathbf{E}_{\mathrm{r}} \in \mathbb{S}^5_+,\ s_1, s_3 \in \Sigma^4_{\mathbf{x}_{\mathrm{r}}},\ \mathbf{s}_{\mathrm{X,D}} \in \Sigma^6_{\mathbf{x}_{\mathrm{r}},\mathbf{d}_{\mathrm{r}}}\\
&\text{s.t. } B_{\mathrm{r}} - s_1(\omega_{\mathrm{r}} - \gamma_{\mathrm{r}}) \in \Sigma\\
&\quad B_{\mathrm{r}} - s_3({\theta_{\Delta}}^2 - {\gamma_{\Delta}}^2) \in \Sigma\\
&\quad - B_{\mathrm{r}} - (1 - \mathbf{x}_{\mathrm{r}}^{\mathrm{T}}\mathbf{E}_{\mathrm{r}}\mathbf{x}_{\mathrm{r}}) \in \Sigma\\
&\quad - \nabla B_{\mathrm{r}}\mathbf{f}_{\mathrm{r}} - \mathbf{s}_{\mathrm{X,D}}^{\mathrm{T}}\overline{\mathbf{g}}_{\mathrm{X,D}} \in \Sigma
\end{aligned} \tag{10.3}$$

The vector $\overline{\mathbf{g}}_{\mathrm{X,D}}$ in (10.3) contains all state space and disturbance polynomials designed from (10.2). The optimisation in SOSP 2 is quite big and turns out to be numerical difficult to calculate. To obtain a better numerical result a feasibility problem is formulated

$$\begin{aligned}&\text{Solve SOSP 2 as a feasibility problem}\\ &\text{s.t.}\quad \operatorname{Tr}\mathbf{E}_{\mathrm{r}} < 1.05e^{*}.\end{aligned} \tag{10.4}$$

In (10.4) the optimisation problem is changed to a feasibility problem. The trace of the initial set ellipse $\mathcal{X}_0$ obtained in SOSP 2 is made slightly larger (recall that the definition of $\mathbf{E}$ entails that a smaller trace enlarge $\mathcal{X}_0$) and it is verified if a feasible solution (feasible barrier certificate) can be found. The value 1.05 in (10.4) has been found through iteration such that a numerical acceptable result is obtained. The resulting initial set $\mathcal{X}_{0,\mathrm{r,Tr}}$ is found to

$$\mathcal{X}_{0,\mathrm{r,Tr}} = \left\{\mathbf{x}\in\mathcal{X}_{\mathrm{r}} \mid \mathbf{x}_{\mathrm{r}}^{\mathrm{T}}\mathbf{E}_{\mathrm{r}}\mathbf{x}_{\mathrm{r}} \leq 1\right\},$$
$$\mathbf{E}_{\mathrm{r}} = \begin{bmatrix} 0.23 & -4\cdot10^{-8} & -3.1\cdot10^{-8} & 7.38\cdot10^{-9} & -3.80\cdot10^{-8}\\ -4\cdot10^{-8} & 5.5\cdot10^{-7} & -1.16\cdot10^{-10} & -1.30\cdot10^{-11} & 1.07\cdot10^{-12}\\ -3.1\cdot10^{-8} & -1.16\cdot10^{-10} & 861.7 & -3.41\cdot10^{-12} & 5.97\cdot10^{-13}\\ 7.38\cdot10^{-9} & -1.30\cdot10^{-11} & -3.41\cdot10^{-12} & 0.56\cdot10^{-4} & -3.23\cdot10^{-11}\\ -3.80\cdot10^{-8} & 1.07\cdot10^{-12} & 5.97\cdot10^{-13} & -3.23\cdot10^{-11} & 0.13\cdot10^{-3} \end{bmatrix}.$$

The initial set $\mathcal{X}_{0,\mathrm{r,Tr}}$ can be used as a safety envelope of the drive train subsystem. The optimisation was computed on a 2.6 GHz AMD64, 96 GB ram computer and took 4 hours to complete.

The safety envelope $\mathcal{X}_{0,\mathrm{r,Tr}}$ is given as a five-dimensional hyperellipsoid. The hyperellipsoid is in Figure 10.2 projected onto three dimensions.

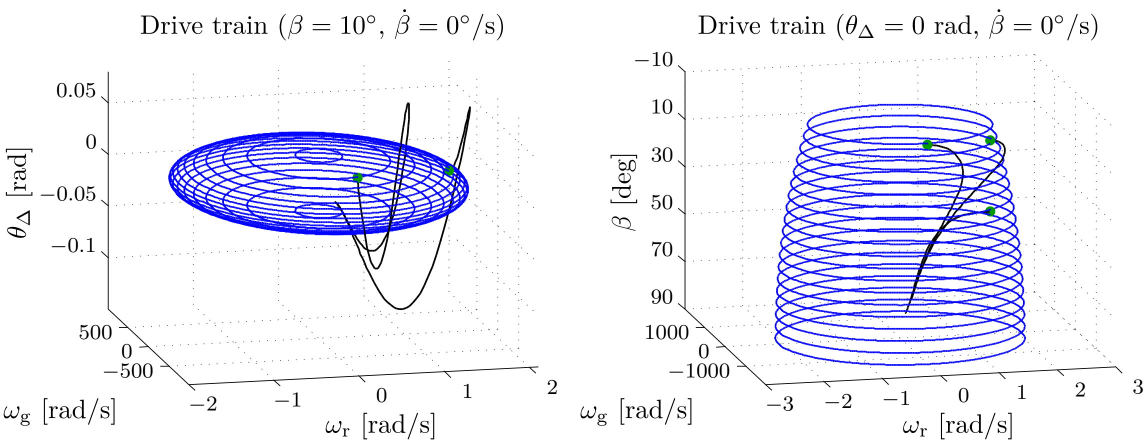


Figure 10.2: *Left $\mathcal{X}_{0,\mathrm{r,Tr}}$ given a constant blade-pitch angle and blade-pitch rate is illustrated. Right $\mathcal{X}_{0,\mathrm{r,Tr}}$ given a constant drive train torsion and blade-pitch rate is illustrated. On both plots, example system trajectories initialised in the safety envelopes are illustrated. The green dots indicate the initial points of the trajectories.*

The left plot in Figure 10.2 illustrates the drive train safety envelope given a constant blade-pitch angle $\beta = 10°$ and blade-pitch rate $\dot\beta = 0°$/s. If $\beta = 10°$ and $\dot\beta = 0°$/s, then the drive train, given an emergency shutdown, is safe if the system trajectory (of the drive train) is inside the ellipsoid. Two example system trajectories are initialised in the ellipsoid. Notice that the ultimate load limit of the rotor $\gamma_{\mathrm{r}} = 2.025$ rad/s is not violated. The right plot in Figure 10.2 illustrates the drive train safety envelope given a constant drive train torsion $\theta_\Delta = 0$ rad and blade-pitch rate $\dot\beta = 0°$/s. If $\theta_\Delta = 0$ and $\dot\beta = 0°$/s, then the system is safe, given an emergency shutdown, within the safety envelope (illustrated as a part of an ellipsoid). Three system trajectories are initialised within the ellipsoid. Notice that the diameter of the ellipsoid decreases as the blade-pitch angle goes towards zero. Consequently, the rotor angular velocities for which the system is safe, are dependent on the blade-pitch angle (if the blade-pitch angle is close to zero, the rotor may not rotate as fast).

An initial set optimisation using the locked ellipse optimisation criterion proved to numerically difficult given the drive train subsystem. Consequently, it is not possible to obtain a satisfactory safety envelope using the locked ellipse optimisation criterion.

The procedure demonstrated above will likewise be used for the following three subsystems.

10.2.2 Tower - safety envelope

The tower subsystem consists of the tower top bending angle and tower top angular velocity. The tower subsystem states are $\mathbf{x}_\mathrm{t} = [{}^\mathrm{t}\theta_\mathrm{fa,y}\ {}^\mathrm{t}\omega_\mathrm{fa,y}]^\mathrm{T}$. This subsystem is separated from the emergency shutdown procedure, which will consequently not be incorporated in the subsystem model. The tower model is connected to the aerodynamic thrust force F_aero (through the aerodynamic thrust function) and the flapwise blade tip displacement. The connection to the flapwise blade model will be neglected, while the aerodynamic thrust force will be included as an unknown bounded disturbance. The tower subsystem is given as

$$
\begin{aligned}
{}^\mathrm{t}\dot{\theta}_\mathrm{fa,y} &= {}^\mathrm{t}\omega_\mathrm{fa,y}, \\
{}^\mathrm{t}\dot{\omega}_\mathrm{fa,y} &= (M_\mathrm{n}L^2)^{-1}\left[F_\mathrm{aero}L + F_\mathrm{g}L\,{}^\mathrm{t}\theta_\mathrm{fa,y} - K_\mathrm{fa}\,{}^\mathrm{t}\theta_\mathrm{fa,y} - B_\mathrm{fa}\,{}^\mathrm{t}\omega_\mathrm{fa,y}\right],
\end{aligned}
$$

with F_aero as disturbance.

The state space $\mathcal{X}_\mathrm{t}$, unsafe set $\mathcal{X}_\mathrm{u,t}$ and disturbance set $\mathcal{D}_\mathrm{t}$ of the tower subsystem are given as

$$
\begin{aligned}
\mathcal{X}_\mathrm{t} &= \left\{\ \mathbf{x} \in \mathbb{R}^2 \ \middle|\ \begin{matrix} -0.01\ \mathrm{rad} \le {}^\mathrm{t}\theta_\mathrm{fa,y} \le 0.01\ \mathrm{rad}, \\ -0.02\ \mathrm{rad/s} \le {}^\mathrm{t}\omega_\mathrm{fa,y} \le 0.02\ \mathrm{rad/s} \end{matrix}\ \right\}, \\
\mathcal{X}_\mathrm{u,t} &= \left\{\ \mathbf{x} \in \mathcal{X}_\mathrm{t} \ \middle|\ {}^\mathrm{t}\theta_\mathrm{fa,y}{}^2 - \gamma_\mathrm{fa}{}^2 \ge 0\ \right\}, \\
\mathcal{D}_\mathrm{t} &= \left\{\ F_\mathrm{aero} \in \mathbb{R} \ \middle|\ F_\mathrm{aero}{}^2 - \gamma_{\mathrm{F}_\mathrm{aero}}{}^2 \le 0\ \right\},
\end{aligned}
$$

where $\gamma_{\mathrm{F}_\mathrm{aero}} = 10$ kN is the disturbance bound and γ_fa the ultimate load limit of the tower top bending given in Section 7.2. The specific choice of disturbance bound requires as mentioned some practical knowledge of the specific wind turbine.

Using the weak barrier certificate formulation, the tower subsystem safety envelope search is formulated as an SOSP. The $\mathcal{X}_\mathrm{0,t,Tr}$ trace optimisation given a quadratic barrier certificate is formulated in SOS Program 3.

SOS Program 3 Tower subsystem

$$
\begin{aligned}
e^* = &\min \operatorname{Tr}\mathbf{E}_\mathrm{t} \text{ over } B_\mathrm{t} \in \mathcal{R}^2_{\mathbf{x}_\mathrm{t}},\ \mathbf{E}_\mathrm{t} \in \mathbb{S}^2_+,\ s_1 \in \Sigma^2_{\mathbf{x}_\mathrm{t}},\ \mathbf{s}_\mathrm{X,D} \in \Sigma^2_{\mathbf{x}_\mathrm{t},\mathbf{d}_\mathrm{t}} \\
\text{s.t. } & B_\mathrm{t} - s_1({}^\mathrm{t}\theta_\mathrm{fa,y}{}^2 - \gamma_\mathrm{fa}{}^2) \in \Sigma \\
& -B_\mathrm{t} - (1 - \mathbf{x}_\mathrm{t}^\mathrm{T}\mathbf{E}_\mathrm{t}\mathbf{x}_\mathrm{t}) \in \Sigma \\
& -\nabla B_\mathrm{t}\mathbf{f}_\mathrm{t} - \mathbf{s}_\mathrm{X,D}^\mathrm{T}\overline{\mathbf{g}}_\mathrm{X,D} \in \Sigma
\end{aligned}
$$

As with the drive train, the solution e^* to the minimisation problem is relaxed and solved as a feasibility problem

$$\begin{aligned}&\text{Solve SOSP 3 as feasibility problem}\\&\text{s.t.}\quad \operatorname{Tr}\mathbf{E}_{\mathrm{t}} < 1.01e^*.\end{aligned}$$

The resulting initial set $\mathcal{X}_{0,\mathrm{t,Tr}}$ is found to

$$\mathcal{X}_{0,\mathrm{t,Tr}} = \left\{ \mathbf{x} \in \mathcal{X}_{\mathrm{t}} \;\middle|\; \begin{bmatrix} {}^{\mathrm{t}}\theta_{\mathrm{fa,y}} \\ {}^{\mathrm{t}}\omega_{\mathrm{fa,y}} \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} 11041 & 76 \\ 76 & 4590 \end{bmatrix} \begin{bmatrix} {}^{\mathrm{t}}\theta_{\mathrm{fa,y}} \\ {}^{\mathrm{t}}\omega_{\mathrm{fa,y}} \end{bmatrix} \leq 1 \right\}.$$

A similar SOSP is formulated using the locked ellipse optimisation, centered in the mean value of the normal operation measurements. The resulting initial set $\mathcal{X}_{0,\mathrm{t,Locked}}$ is found to

$$\mathcal{X}_{0,\mathrm{t,Locked}} = \\ \left\{ \mathbf{x} \in \mathcal{X}_{\mathrm{t}} \;\middle|\; \left(\begin{bmatrix} {}^{\mathrm{t}}\theta_{\mathrm{fa,y}} \\ {}^{\mathrm{t}}\omega_{\mathrm{fa,y}} \end{bmatrix} - \begin{bmatrix} 0.0025 \\ 0 \end{bmatrix} \right)^{\mathrm{T}} \begin{bmatrix} 1838.6 & -361.6 \\ -361.6 & 6400.9 \end{bmatrix} \cdot 10^3 \left(\begin{bmatrix} {}^{\mathrm{t}}\theta_{\mathrm{fa,y}} \\ {}^{\mathrm{t}}\omega_{\mathrm{fa,y}} \end{bmatrix} - \begin{bmatrix} 0.0025 \\ 0 \end{bmatrix} \right) \leq 60.7 \right\}.$$

The initial sets $\mathcal{X}_{0,\mathrm{t,Tr}}$ and $\mathcal{X}_{0,\mathrm{t,Locked}}$ can be used as safety envelopes of the tower subsystem. Note that this subsystem does not incorporate the emergency shutdown procedure and is accordingly only safe if the aerodynamic thrust force F_{aero} is in $\mathcal{D}_{\mathrm{t}}$ at all times. Both optimisations were done on a 2.6 GHz AMD64, 96 GB ram computer and took approximately 30 s to complete.

The safety envelopes $\mathcal{X}_{0,\mathrm{t,Tr}}$ and $\mathcal{X}_{0,\mathrm{t,Locked}}$ are illustrated in Figure 10.3.

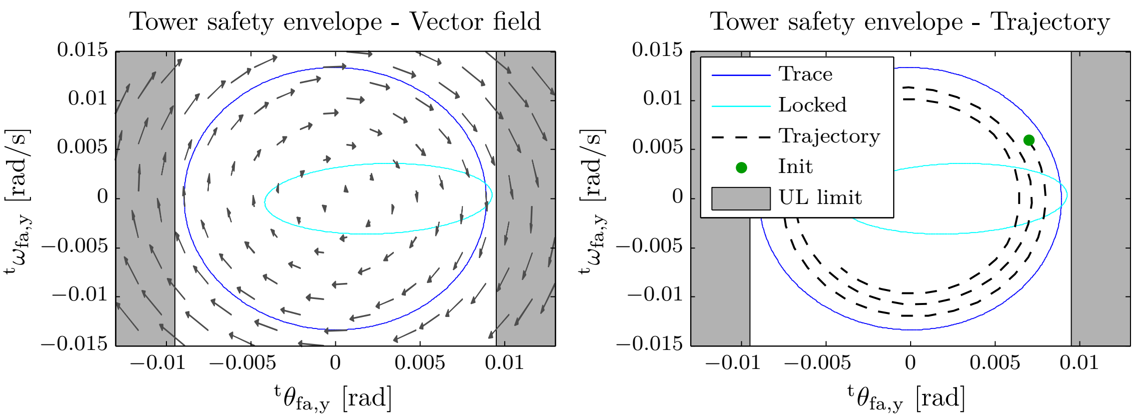


Figure 10.3: *Left the safety envelopes are illustrated along with the vector field of the system. Right an example trajectory is initialised inside the safety envelopes.*

In Figure 10.3 both the trace optimised ellipse and the optimised ellipse with locked orientation are illustrated. The left plot illustrates the safety envelopes along with the vector field of the tower subsystem. The right plot illustrates a trajectory initialised inside the safety envelope. Note that the locked ellipse $\mathcal{X}_{0,\mathrm{t,Locked}}$ is almost included in $\mathcal{X}_{0,\mathrm{t,Tr}}$. Consequently, the union of the safety envelopes is not significantly enlarged by the inclusion of the locked ellipse in this specific case.

10.2.3 Flapwise blade bending - safety envelope

The flapwise blade bending subsystem consists of the flapwise blade tip displacement and flapwise blade tip velocity. The flapwise blade bending subsystem states are $\mathbf{x}_{\mathrm{flap}} = [{}^{\mathrm{h}}x_{\mathrm{flap}} \;\; {}^{\mathrm{h}}v_{\mathrm{flap,x}}]^{\mathrm{T}}$. This subsystem is separated from the emergency shutdown procedure which will consequently not be incorporated in the subsystem model. The flapwise blade bending model is connected to the motion of the tower top and the aerodynamic thrust force F_{aero} (through the aerodynamic thrust function). The connection to the tower motion will be neglected, while the aerodynamic thrust force will be included as an unknown bounded disturbance. The flapwise blade bending subsystem is given as

$$\begin{aligned}
{}^{\mathrm{h}}\dot{x}_{\text{flap}} &= {}^{\mathrm{h}}v_{\text{flap,x}}, \\
{}^{\mathrm{h}}\dot{v}_{\text{flap,x}} &= M_{\text{flap}}^{-1}\left[F_{\text{aero}} - K_{\text{flap}}{}^{\mathrm{h}}x_{\text{flap}} - B_{\text{flap}}{}^{\mathrm{h}}v_{\text{flap,x}}\right],
\end{aligned}$$

with F_{aero} as disturbance.

The state space $\mathcal{X}_{\text{flap}}$, unsafe set $\mathcal{X}_{\text{u,flap}}$ and disturbance set $\mathcal{D}_{\text{flap}}$ of the flapwise blade bending subsystem are given as

$$\begin{aligned}
\mathcal{X}_{\text{flap}} &= \left\{ \quad \mathbf{x} \in \mathbb{R}^2 \;\middle|\; \begin{matrix} -15 \text{ m} \le {}^{\mathrm{h}}x_{\text{flap}} \le 15 \text{ m}, \\ -30 \text{ m/s} \le {}^{\mathrm{h}}v_{\text{flap,x}} \le 30 \text{ m/s} \end{matrix} \quad \right\}, \\
\mathcal{X}_{\text{u,flap}} &= \left\{ \quad \mathbf{x} \in \mathcal{X}_{\text{flap}} \;\middle|\; {}^{\mathrm{h}}x_{\text{flap}}{}^2 - \gamma_{\text{flap}}{}^2 \ge 0 \quad \right\}, \\
\mathcal{D}_{\text{flap}} &= \left\{ \quad F_{\text{aero}} \in \mathbb{R} \;\middle|\; F_{\text{aero}}{}^2 - \gamma_{\text{F}_{\text{aero}}}{}^2 \le 0 \quad \right\},
\end{aligned}$$

where $\gamma_{\text{F}_{\text{aero}}} = 10$ kN is the disturbance bound and γ_{flap} the ultimate load limit of the flapwise blade tip displacement given in Section 7.2.

Using the weak barrier certificate formulation, the flapwise blade bending subsystem safety envelope search is formulated as an SOSP. The $\mathcal{X}_{0,\text{flap,Tr}}$ trace optimisation given a quadratic barrier certificate is formulated in SOS Program 4.

SOS Program 4 Flapwise blade bending subsystem

$$\begin{aligned}
e^* = &\min \operatorname{Tr} \mathbf{E}_{\text{flap}} \text{ over } B_{\text{flap}} \in \mathcal{R}^2_{\mathbf{x}_{\text{flap}}},\ \mathbf{E}_{\text{flap}} \in \mathbb{S}^2_+,\ s_1 \in \Sigma^2_{\mathbf{x}_{\text{flap}}},\ \mathbf{s}_{\text{X,D}} \in \Sigma^2_{\mathbf{x}_{\text{flap}},\mathbf{d}_{\text{flap}}} \\
\text{s.t. } &B_{\text{flap}} - s_1({}^{\mathrm{h}}x_{\text{flap}}{}^2 - \gamma_{\text{flap}}{}^2) \in \Sigma \\
&- B_{\text{flap}} - (1 - \mathbf{x}_{\text{flap}}^{\mathrm{T}}\mathbf{E}_{\text{flap}}\mathbf{x}_{\text{flap}}) \in \Sigma \\
&- \nabla B_{\text{flap}}\mathbf{f}_{\text{flap}} - \mathbf{s}_{\text{X,D}}^{\mathrm{T}}\overline{\mathbf{g}}_{\text{X,D}} \in \Sigma
\end{aligned}$$

The solution e^* to the minimisation problem is relaxed and solved as a feasibility problem

$$\begin{aligned}
&\text{Solve SOSP 4 as feasibility problem} \\
&\text{s.t. } \operatorname{Tr} \mathbf{E}_{\text{flap}} < 1.01e^*
\end{aligned}$$

The resulting initial set $\mathcal{X}_{0,\text{flap,Tr}}$ is found to

$$\mathcal{X}_{0,\text{flap,Tr}} = \left\{ \mathbf{x} \in \mathcal{X}_{\text{flap}} \;\middle|\; \begin{bmatrix} {}^{\mathrm{h}}x_{\text{flap}} \\ {}^{\mathrm{h}}v_{\text{flap,x}} \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} 9.07 & 1.15 \\ 1.15 & 1.93 \end{bmatrix} \cdot 10^{-3} \begin{bmatrix} {}^{\mathrm{h}}x_{\text{flap}} \\ {}^{\mathrm{h}}v_{\text{flap,x}} \end{bmatrix} \le 1 \right\}.$$

A similar SOSP is formulated using the locked ellipse optimisation. The resulting initial set $\mathcal{X}_{0,\text{flap,Locked}}$ is found to

$$\begin{aligned}
&\mathcal{X}_{0,\text{flap,Locked}} = \\
&\left\{ \mathbf{x} \in \mathcal{X}_{\text{flap}} \;\middle|\; \left(\begin{bmatrix} {}^{\mathrm{h}}x_{\text{flap}} \\ {}^{\mathrm{h}}v_{\text{flap,x}} \end{bmatrix} - \begin{bmatrix} 2.32 \\ 0 \end{bmatrix} \right)^{\mathrm{T}} \begin{bmatrix} 0.43 & -0.06 \\ -0.06 & 2.17 \end{bmatrix} \left(\begin{bmatrix} {}^{\mathrm{h}}x_{\text{flap}} \\ {}^{\mathrm{h}}v_{\text{flap,x}} \end{bmatrix} - \begin{bmatrix} 2.32 \\ 0 \end{bmatrix} \right) \le 29.56 \right\}.
\end{aligned}$$

The initial sets $\mathcal{X}_{0,\text{flap,Tr}}$ and $\mathcal{X}_{0,\text{flap,Locked}}$ can be used as safety envelopes of the flapwise blade bending subsystem. Note that this subsystem does not incorporate the emergency shutdown procedure and is accordingly only safe if the aerodynamic thrust force F_{aero} is in $\mathcal{D}_{\text{flap}}$ at all times. Both optimisations were done on a 2.6 GHz AMD64, 96 GB ram computer and took approximately 30 s to complete.

The safety envelopes $\mathcal{X}_{0,\text{flap,Tr}}$ and $\mathcal{X}_{0,\text{flap,Locked}}$ are illustrated in Figure 10.4.

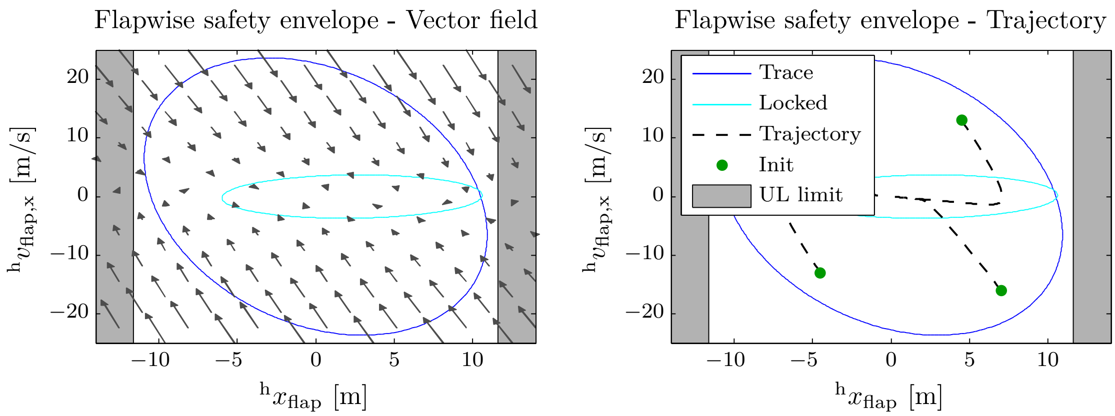


Figure 10.4: *Left the safety envelopes are illustrated along with the vector field of the system. Right example trajectories are initialised inside the safety envelopes.*

In Figure 10.4 both the trace optimised ellipse and the optimised ellipse with locked orientation are illustrated. The left plot illustrates the safety envelopes along with the vector field of the flapwise blade bending subsystem. The right plot illustrates trajectories initialised inside the safety envelope. As with the tower subsystem, the locked ellipse $\mathcal{X}_{0,\text{flap,Locked}}$ is almost included in $\mathcal{X}_{0,\text{flap,Tr}}$.

10.2.4 Lead-lag blade bending - safety envelope

The lead-lag blade bending subsystem consists of the lead-lag blade tip bending and lead-lag angular blade tip velocity. The lead-lag blade bending subsystem states are $\mathbf{x}_{\text{LL}} = [{}^{\mathrm{h}}\theta_{\text{LL,x}}\ {}^{\mathrm{h}}\omega_{\text{LL,x}}]^{\mathrm{T}}$. This subsystem is separated from the emergency shutdown procedure which will consequently not be incorporated in the subsystem model. The lead-lag blade bending model is connected to the aerodynamic torque τ_{aero} (through the aerodynamic torque function) and the motion of the drive train. The connection to the drive train will be neglected, while the aerodynamic torque will be included as an unknown bounded disturbance. The lead-lag blade bending subsystem is given as

$$\begin{aligned}
{}^{\mathrm{h}}\dot{\theta}_{\text{LL,x}} &= {}^{\mathrm{h}}\omega_{\text{LL,x}} \\
{}^{\mathrm{h}}\dot{\omega}_{\text{LL,x}} &= J_{\text{LL}}^{-1}\left[\tau_{\text{aero}} - B_{\text{LL}}{}^{\mathrm{h}}\omega_{\text{LL,x}} - K_{\text{LL}}{}^{\mathrm{h}}\theta_{\text{LL,x}}\right],
\end{aligned}$$

with τ_{aero} as disturbance.

The state space $\mathcal{X}_{\text{LL}}$, unsafe set $\mathcal{X}_{\text{u,LL}}$ and disturbance set $\mathcal{D}_{\text{LL}}$ of the lead-lag blade bending subsystem are given as

$$\begin{aligned}
\mathcal{X}_{\text{LL}} &= \left\{ \mathbf{x} \in \mathbb{R}^2 \;\middle|\; \begin{array}{c} -0.03 \text{ rad} \le {}^{\mathrm{h}}\theta_{\text{LL,x}} \le 0.03 \text{ rad}, \\ -0.2 \text{ rad/s} \le {}^{\mathrm{h}}\omega_{\text{LL,x}} \le 0.2 \text{ rad/s} \end{array} \right\}, \\
\mathcal{X}_{\text{u,LL}} &= \left\{ \mathbf{x} \in \mathcal{X}_{\text{LL}} \;\middle|\; {}^{\mathrm{h}}\theta_{\text{LL,x}}{}^2 - \gamma_{\text{LL}}{}^2 \ge 0 \right\}, \\
\mathcal{D}_{\text{LL}} &= \left\{ \tau_{\text{aero}} \in \mathbb{R} \;\middle|\; \tau_{\text{aero}}{}^2 - \gamma_{\tau_{\text{aero}}}{}^2 \le 0 \right\},
\end{aligned}$$

where $\gamma_{\tau_{\mathrm{aero}}} = 10$ kNm is the disturbance bound and γ_{LL} the ultimate load limit of the lead-lag blade tip bending given in Section 7.2.

Using the weak barrier certificate formulation, the lead-lag blade bending subsystem safety envelope search is formulated as an SOSP. The $\mathcal{X}_{0,\mathrm{LL},\mathrm{Tr}}$ trace optimisation given a quadratic barrier certificate is formulated in SOS Program 5.

SOS Program 5 Lead-lag blade bending subsystem

$$\begin{aligned}
e^* = & \min \operatorname{Tr} \mathbf{E}_{\mathrm{LL}} \text{ over } B_{\mathrm{LL}} \in \mathcal{R}^2_{\mathbf{x}_{\mathrm{LL}}},\ \mathbf{E}_{\mathrm{LL}} \in \mathbb{S}^2_+,\ s_1 \in \Sigma^2_{\mathbf{x}_{\mathrm{LL}}},\ \mathbf{s}_{\mathrm{X,D}} \in \Sigma^2_{\mathbf{x}_{\mathrm{LL}},\mathbf{d}_{\mathrm{LL}}} \\
\text{s.t. } & B_{\mathrm{LL}} - s_1({}^{\mathrm{h}}\theta_{\mathrm{LL,x}}{}^2 - \gamma_{\mathrm{LL}}{}^2) \in \Sigma \\
& - B_{\mathrm{LL}} - (1 - \mathbf{x}_{\mathrm{LL}}^{\mathrm{T}} \mathbf{E}_{\mathrm{LL}} \mathbf{x}_{\mathrm{LL}}) \in \Sigma \\
& - \nabla B_{\mathrm{LL}} \mathbf{f}_{\mathrm{LL}} - \mathbf{s}_{\mathrm{X,D}}^{\mathrm{T}} \overline{\mathbf{g}}_{\mathrm{X,D}} \in \Sigma
\end{aligned}$$

The solution e^* to the minimisation problem will be relaxed and the problem solved as a feasibility problem

$$\begin{aligned}
& \text{Solve SOSP 5 as feasibility problem} \\
& \text{s.t. } \operatorname{Tr} \mathbf{E}_{\mathrm{LL}} < 1.01 e^*
\end{aligned}$$

The resulting initial set $\mathcal{X}_{0,\mathrm{LL},\mathrm{Tr}}$ is found to

$$\mathcal{X}_{0,\mathrm{LL},\mathrm{Tr}} = \left\{ \mathbf{x} \in \mathcal{X}_{\mathrm{LL}} \;\middle|\; \begin{bmatrix} {}^{\mathrm{h}}\theta_{\mathrm{LL,x}} \\ {}^{\mathrm{h}}\omega_{\mathrm{LL,x}} \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} 1.65 & 0.04 \\ 0.04 & 0.15 \end{bmatrix} \cdot 10^3 \begin{bmatrix} {}^{\mathrm{h}}\theta_{\mathrm{LL,x}} \\ {}^{\mathrm{h}}\omega_{\mathrm{LL,x}} \end{bmatrix} \leq 1 \right\}.$$

A similar SOSP is formulated using the locked ellipse optimisation. The resulting initial set $\mathcal{X}_{0,\mathrm{LL},\mathrm{Locked}}$ is found to

$$\mathcal{X}_{0,\mathrm{LL},\mathrm{Locked}} = \left\{ \mathbf{x} \in \mathcal{X}_{\mathrm{LL}} \;\middle|\; \left(\begin{bmatrix} {}^{\mathrm{h}}\theta_{\mathrm{LL,x}} \\ {}^{\mathrm{h}}\omega_{\mathrm{LL,x}} \end{bmatrix} - \begin{bmatrix} 0.007 \\ 0 \end{bmatrix} \right)^{\mathrm{T}} \begin{bmatrix} 0.94 & -0.17 \\ -0.17 & 1.5 \end{bmatrix} \cdot 10^5 \left(\begin{bmatrix} {}^{\mathrm{h}}\theta_{\mathrm{LL,x}} \\ {}^{\mathrm{h}}\omega_{\mathrm{LL,x}} \end{bmatrix} - \begin{bmatrix} 0.007 \\ 0 \end{bmatrix} \right) \leq 30.09 \right\}.$$

The initial sets $\mathcal{X}_{0,\mathrm{LL},\mathrm{Tr}}$ and $\mathcal{X}_{0,\mathrm{LL},\mathrm{Locked}}$ can be used as safety envelopes of the lead-lag blade bending subsystem. Note that this subsystem does not incorporate the emergency shutdown procedure and is accordingly only safe if the aerodynamic torque τ_{aero} is in $\mathcal{D}_{\mathrm{LL}}$ at all times. Both optimisations were done on a 2.6 GHz AMD64, 96 GB ram computer and took approximately 30 s to complete.

The safety envelopes $\mathcal{X}_{0,\mathrm{LL},\mathrm{Tr}}$ and $\mathcal{X}_{0,\mathrm{LL},\mathrm{Locked}}$ are illustrated in Figure 10.5.

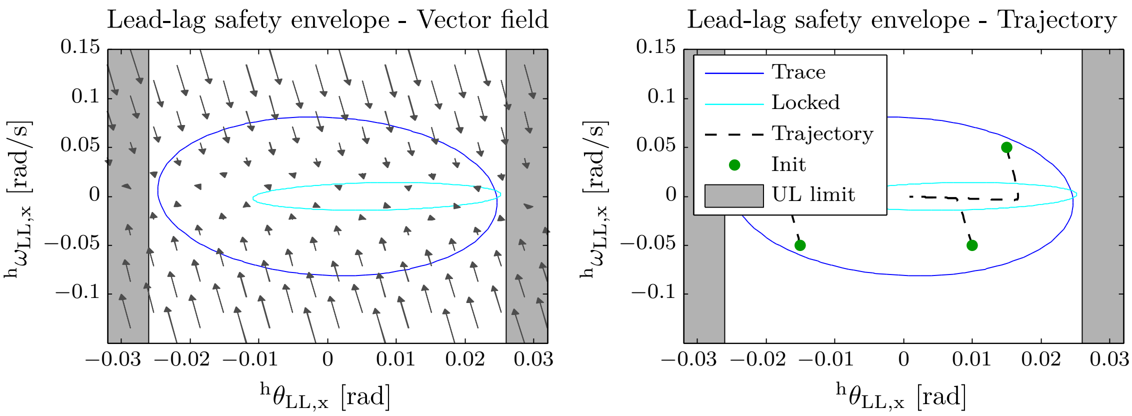


Figure 10.5: *Left the safety envelopes are illustrated along with the vector field of the system. Right example trajectories are initialised inside the safety envelopes.*

In Figure 10.5 both the trace optimised ellipse and the optimised ellipse with locked orientation are illustrated. The left plot illustrates the safety envelopes along with the vector field of the lead-lag blade bending subsystem. The right plot illustrates trajectories initialised inside the safety envelope. As with the tower and flapwise blade bending subsystems, the locked ellipse $\mathcal{X}_{0,\text{LL,Locked}}$ is almost included in $\mathcal{X}_{0,\text{LL,Tr}}$.

The SOSPs implemented in `MATLAB` with `YALMIP` can be found on the enclosed DVD.

In the following section, the separate safety envelopes found above will be combined into a safety supervisor system, implemented and tested on the NREL 5-MW wind turbine in `FAST`.

10.3 Implementation Results

In the above, safety envelopes of the drive train, tower, flapwise blade bending and lead-lag blade bending were found. These safety envelopes can be assembled into one safety supervisor system. In order for the system to be safe, the trajectory should be within at least one of the safety envelopes of each of the subsystems. Recall that the safety envelopes are designed using assumptions of the connections between the subsystems. Consequently, the safety supervisor does only ensure safety as long as these assumptions are satisfied.

The safety envelopes found in Section 10.2.1, 10.2.2, 10.2.3 and 10.2.4 can be combined into a safety supervisor system. The resulting safety supervisor system is given in (10.5).

$$\begin{aligned}
\mathcal{S}_{\text{r}} &= \begin{cases} \text{Safe}, & \mathbf{x}_{\text{r}} \in \mathcal{X}_{0,\text{r,Tr}} \\ \text{Unsafe}, & \text{else} \end{cases} \\
\mathcal{S}_{\text{t}} &= \begin{cases} \text{Safe}, & \mathbf{x}_{\text{t}} \in \mathcal{X}_{0,\text{t,Tr}} \cup \mathcal{X}_{0,\text{t,Locked}} \\ \text{Unsafe}, & \text{else} \end{cases} \\
\mathcal{S}_{\text{flap}} &= \begin{cases} \text{Safe}, & \mathbf{x}_{\text{flap}} \in \mathcal{X}_{0,\text{flap,Tr}} \cup \mathcal{X}_{0,\text{flap,Locked}} \\ \text{Unsafe}, & \text{else} \end{cases} \\
\mathcal{S}_{\text{LL}} &= \begin{cases} \text{Safe}, & \mathbf{x}_{\text{LL}} \in \mathcal{X}_{0,\text{LL,Tr}} \cup \mathcal{X}_{0,\text{LL,Locked}} \\ \text{Unsafe}, & \text{else} \end{cases}
\end{aligned} \tag{10.5}$$

If one of the safety conditions $\{\mathcal{S}_{\text{r}}, \mathcal{S}_{\text{t}}, \mathcal{S}_{\text{flap}}, \mathcal{S}_{\text{LL}}\}$ in (10.5) become *unsafe*, then the emergency shutdown procedure should be initialised immediately. The safety condition should be evaluated continuously. This does in practice entail that the polynomial safety envelope functions of the subsystems should be continuously evaluated. The signs of the results determine if an emergency shutdown should be triggered or not.

As the safety needs to be continuously verified, evaluation of the polynomials needs to be fast to compute. To test the safety of the system the seven polynomials of the subsystem envelopes should be evaluated. This evaluation involves 74 multiplications and 57 summations.

In the following, the safety supervisor system in (10.5) is implemented on the NREL 5-MW wind turbine in `FAST`. When the system is safe, the control of the wind turbine is given by the NREL 5-MW controller. When an unsafe situation is detected by the safety supervisor, the emergency shutdown procedure is initialised.

It should be noted that the NREL 5-MW model in `FAST` is far more complex than the model developed in Chapter 6. To be able to use the safety supervisor system, the mean of the lead-lag blade bendings and the mean of the flapwise blade tip displacements are considered. A wind field with a mean wind speed of 20 m/s is produced using `TurbSim`. The wind field produced by `TurbSim` is 3-dimensional, whereas the wind assumed by the safety supervisor is scalar.

The initial test of the safety supervisor system is to verify that the wind turbine can operate in normal operation without the emergency shutdown being triggered by the supervisor. A 30 minute test is performed in `FAST` with the safety supervisor being active. During the 30 minute test, the wind turbine is not shut down by the safety supervisor. As the wind turbine is not shut down during the simulation, it seems that the safety supervisor is not too conservative to allow normal operation, which is very important in relation to power production.

Four safety critical situations are simulated, each coupled with an illustration (illustrations on Page 102 and onwards). Each figure is divided into two parts, the top part illustrating the *signals* of the system and the bottom part the evaluation of the safety supervisor system. In the top part eight signals are illustrated over time, respectively the wind disturbance, the controllable generator torque and blade-pitch angle and five safety critical system states. In the bottom part, the safety critical states of each subsystem are illustrated in the state space. Safety envelopes optimised according to the trace are given in blue and the safety envelopes with locked shape and orientation in light blue (cyan). The emergency shutdown is triggered if a system trajectory leaves the safety envelopes. The point of an event (error or external event) is given in pink, and the trigger of the emergency shutdown in green. The safety critical situations tested are:

1. Blade-pitch controller error (Figure 10.6)

   Situation of error in the blade-pitch angle control. At a given point in time, an error occurs in the control of the blade-pitch, such that the rate of the blade-pitch angle stays at 0.5°/s towards $\beta = 0°$. This error results in an increase of the rotor angular velocity. A simulation of the pitch error and the trigger of the emergency shutdown is illustrated in Figure 10.6. In the figure it can be seen that the emergency shutdown is triggered by the safety envelope of the drive train subsystem (the drive train state trajectory reaches the edge of the safety envelope). In this case the emergency shutdown supervisor manages to shut down the wind turbine without any state evolving to the unsafe set.

2. Wind gust (Figure 10.7)

   Situation with wind gust. At a given point in time, a wind gust hits the rotor. The frequency of the wind gust is approximately 1/3 Hz, which is in the turbulence range of the Hoven spectrum in Figure 6.25 (which seems to be close to the NREL 5-MW tower resonance frequency). The wind gust results in an oscillation of the tower top. In Figure 10.7 it can be seen that the emergency shutdown is triggered by the safety envelope of the tower subsystem. Note that the angular velocity of the rotor is not noticeably affected by the wind gust, why this situation would be difficult to detect using a simple rotor overspeed guard. In this case the emergency shutdown supervisor manages to shut down the wind turbine without any state evolving to the unsafe set.

3. Generator failure (Figure 10.8)

   Situation with failure in the generator torque. The failure could be due to a power grid failure or a fault in the generator itself. The failure of the generator results in a 1.5 s absence of generator torque. In Figure 10.8 it can be seen that the 1.5 s generator failure causes in particular a lead-lag bending of the wind turbine blades. The remaining states do not deviate significantly. The emergency shutdown is triggered by the lead-lag safety envelope. In this case the emergency shutdown supervisor manages to shut down the wind turbine without any state evolving to the unsafe set.

4. Blade-pitch controller error & generator failure (Figure 10.9)

   Situation with a combination of a blade-pitch controller error and a generator failure. The error in the blade-pitch system causes the rate of the blade-pitch to stay at 4°/s towards $\beta = 0°$. At the same time the generator torque goes towards zero. In Figure 10.9 it can be seen that the emergency shutdown is triggered by the lead-lag safety envelope (additionally the safety envelope of the drive train is close to trigger the emergency shutdown). The safety supervisor system does in this case not manage to keep lead-lag blade bending within the ultimate load limits. Consequently, the blades are potentially damaged.

In three of the four above safety critical situations, the safety supervisor system is able to trigger the emergency shutdown of the NREL 5-MW wind turbine prior to the system being damaged. In safety critical situation 4, the safety supervisor is not able to prevent the system state from entering the unsafe set. The reason that the emergency shutdown is not initialised in time, is either due to modelling uncertainties (difference between the NREL 5-MW model implemented in `FAST` and the model developed in Chapter 6) or that the couplings of the subsystems have not been included in the construction of safety envelopes. As the polynomial model of the NREL 5-MW is very simple compared to the implementation in `FAST`, it is assumed that other situations can be found for which the safety supervisor system does not ensure safety of the system. In Section 13.1 it is briefly discussed how modelling uncertainties can be included in the safety guarantee. An implementation of the safety supervisor in `SIMULINK` can be found on the enclosed DVD.

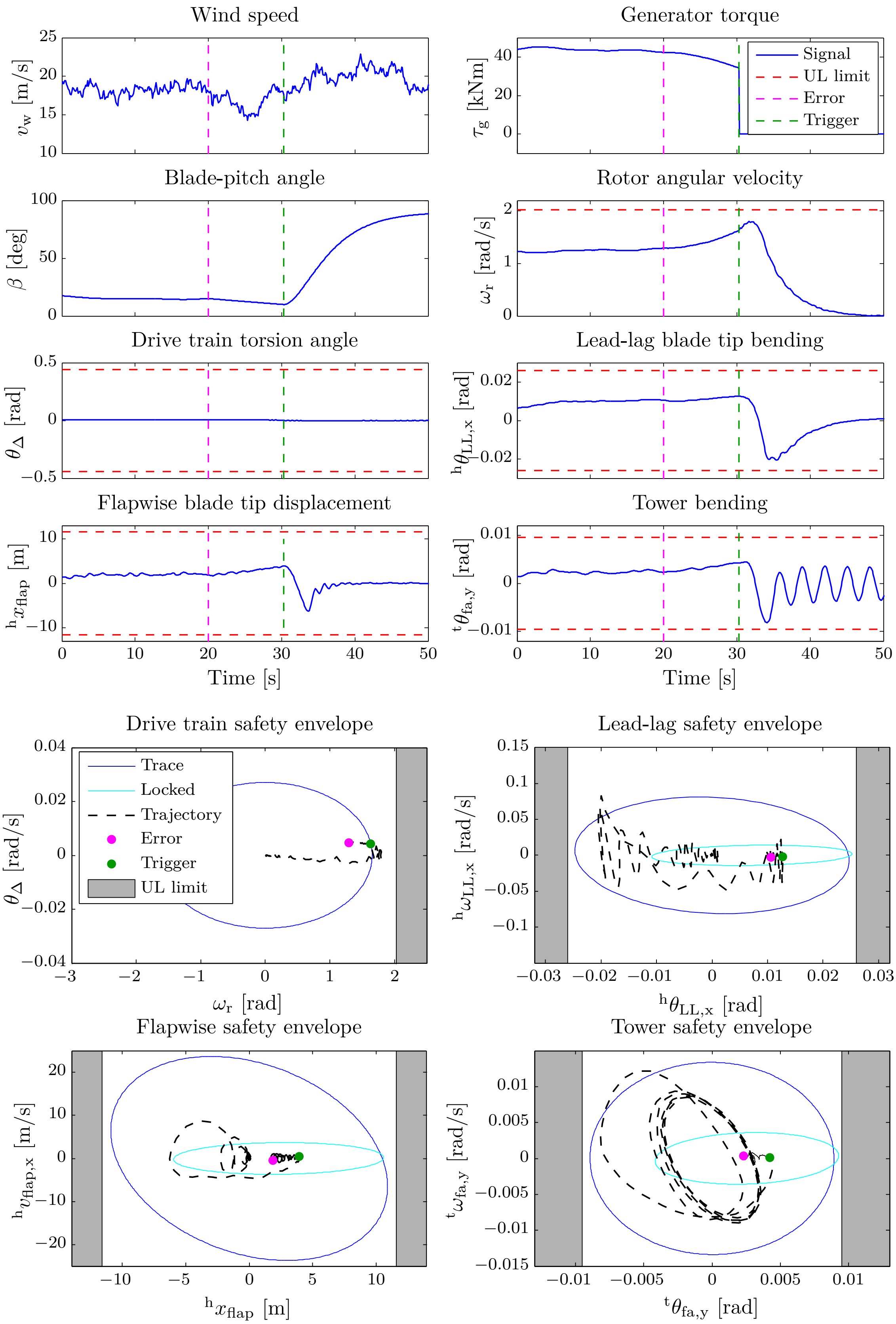


Figure 10.6: *Safety critical situation 1. Top 8 plots show the evolution of states over time. In the bottom 4 plots, the state trajectories of the subsystems are illustrated. A pitch control error is introduced.*

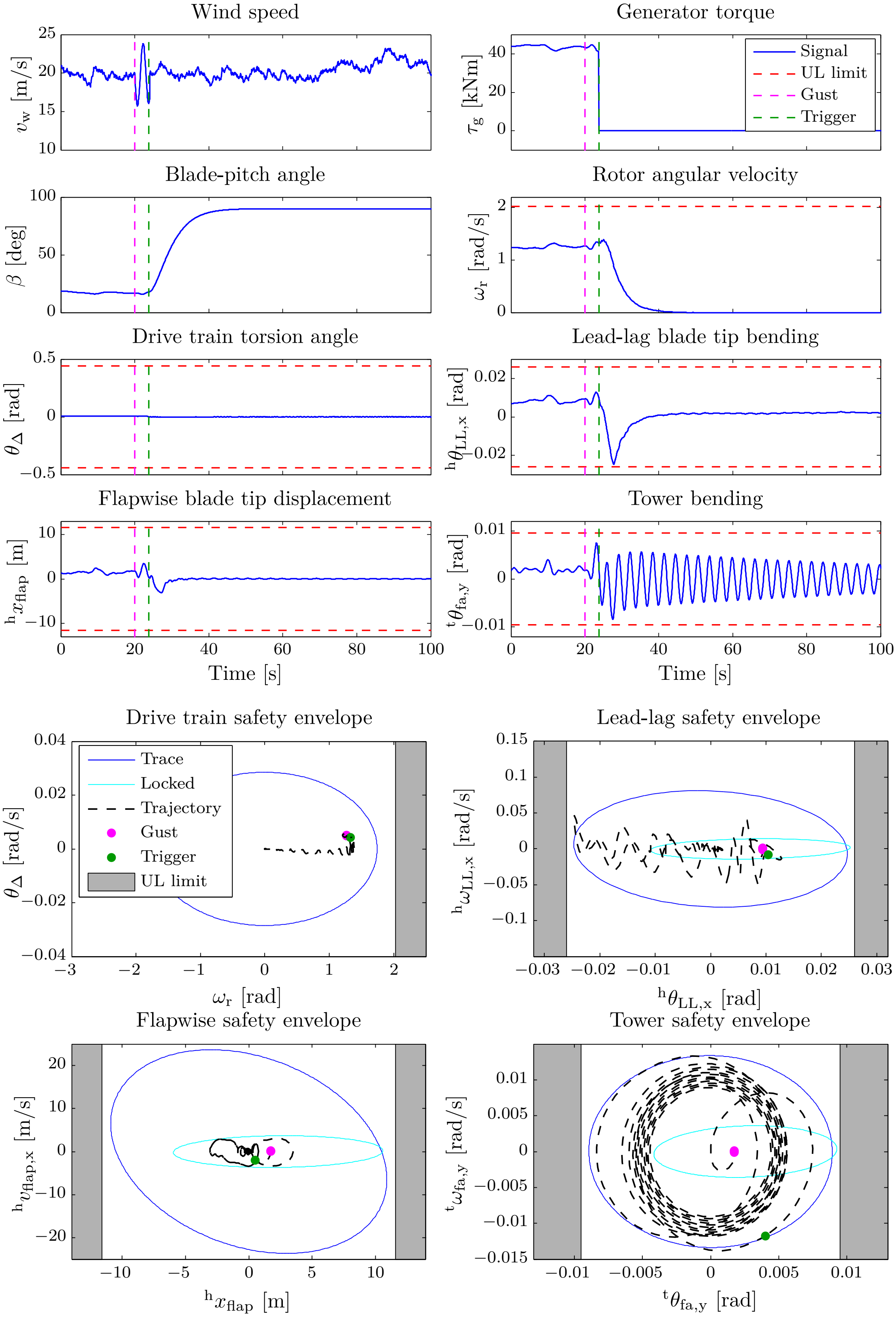


Figure 10.7: *Safety critical situation 2. Top 8 plots show the evolution of states over time. In the bottom 4 plots, the state trajectories of the subsystems are illustrated. A wind gust is introduced.*

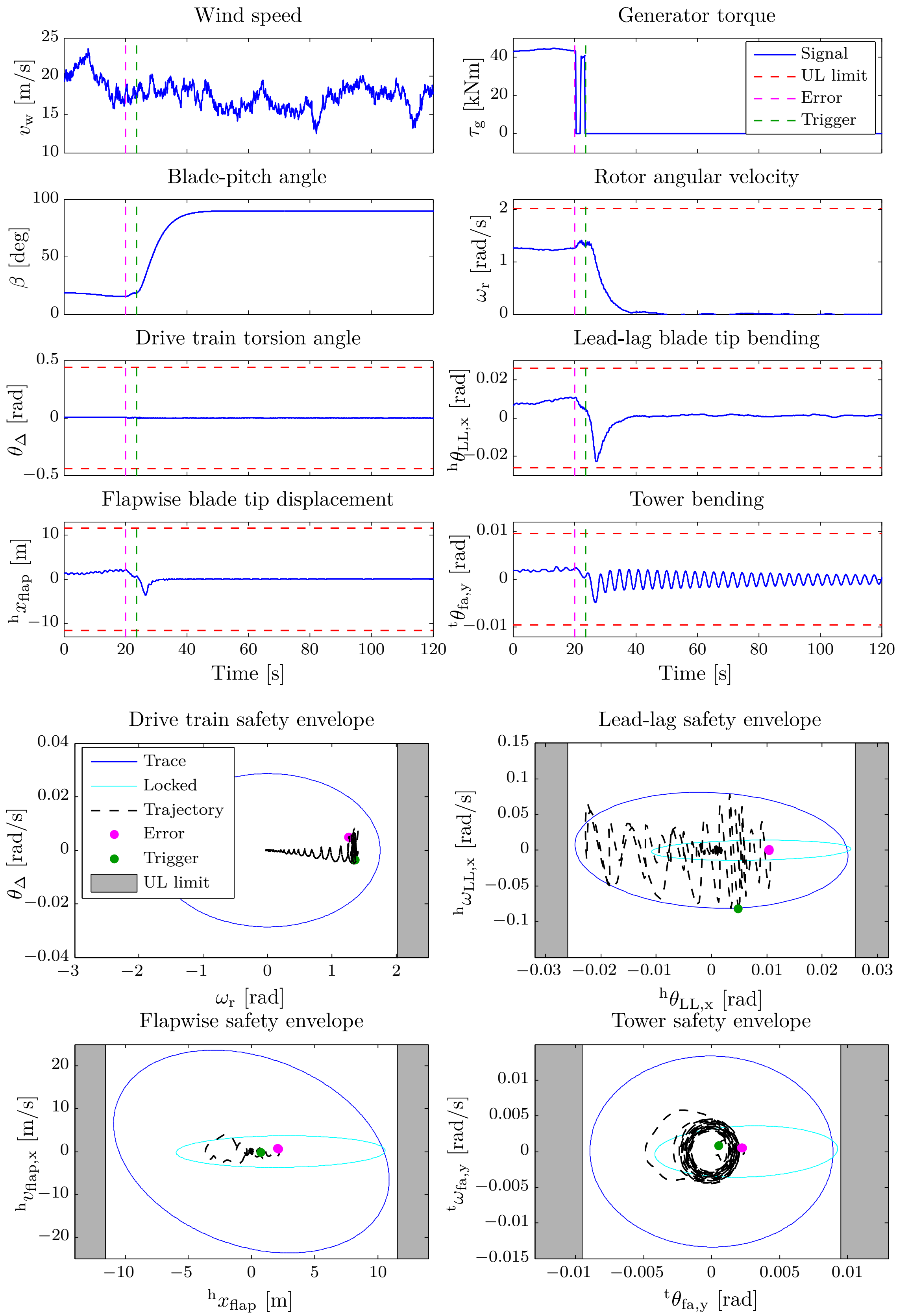


Figure 10.8: *Safety critical situation 3. Top 8 plots show the evolution of states over time. In the bottom 4 plots, the state trajectories of the subsystems are illustrated. A generator torque failure is introduced.*

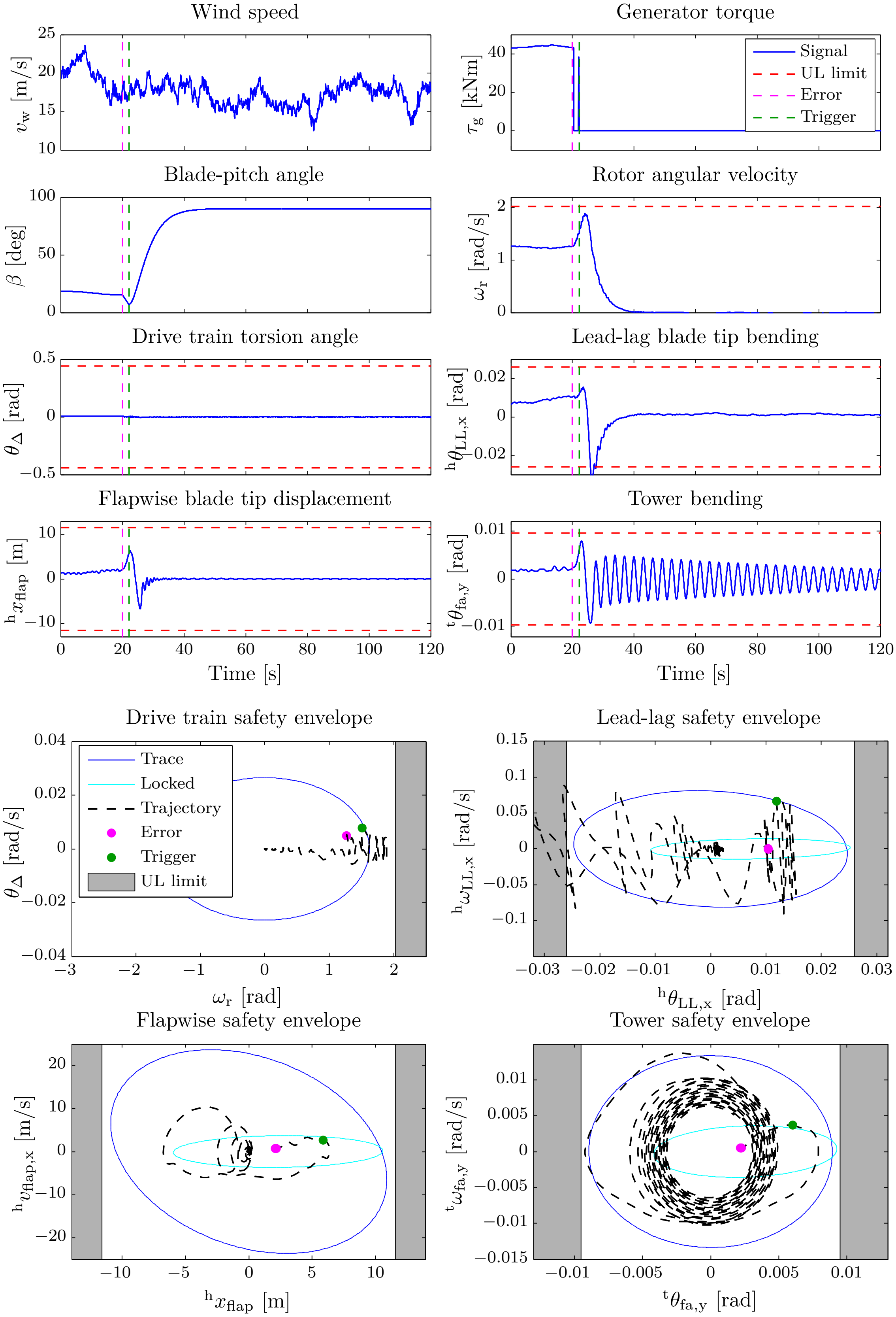


Figure 10.9: *Safety critical situation 4. Top 8 plots show the evolution of states over time. In the bottom 4 plots, the state trajectories of the subsystems are illustrated. A pitch control error and a generator torque failure are introduced.*

11 Compositional Safety Envelope Construction

In this chapter, safety verification and optimisation using compositional barrier certificates are described. In Section 10.1 the SOSP of the complete safety envelope search was formulated and found too large for computation on a regular PC. In Section 10.2 the system was separated into subsystems, for which individual safety envelopes were constructed. Using this technique, no interconnections of the subsystems were included in the safety envelope construction.

In this chapter, a compositional barrier certificate method is considered. The compositional barrier certificate method considers a system as a composition of coupled subsystems (with subsystems similar to in Section 10.2) with constraints between them. In [BXMM08] it is noted that decomposition methods can provide substantial computational savings if the problem size grows more than linear - which is the case with sum of squares decomposition problems. As a result, the compositional barrier certificate method can be used to obtain a barrier certificate which is valid given the complete system, but with lower computational complexity (reduced memory requirements). This can be seen as a practical computational extension to the barrier certificate formulation.

The compositional barrier certificate method proposed in [SPW12] uses an iterative method in the safety verification computation. This entails that the SOSPs of the subsystems should be calculated a number of times. A single computation of the drive train & blade-pitching SOSP was in Section 10.2.1 completed in approximately 4 hours. To reduce the computation time, some simplifications will be introduced. In the simulations performed in Section 10.3, the ultimate load limits of the drive train torsion and flapwise blade tip displacement were not close to being violated in any of the simulated situations. As a result, these will not be included in the following calculations.

In the following, the compositional barrier certificate method is used to include the effects of the emergency shutdown procedure in each of the subsystems (which were not possible in Section 10.2). This entails that the aerodynamic functions ($F_{\text{aero}}(v_{\text{w}}, \omega_{\text{r}}, \beta)$, $\tau_{\text{aero}}(v_{\text{w}}, \omega_{\text{r}}, \beta)$) should be included in each subsystem, with the rotor angular velocity ω_{r} and blade-pitch angle β as interconnected variables (from the drive train & pitching subsystem). The wind is assumed to be static at $v_{\text{w}} = 20$ m/s. The wind turbine subsystem separation is illustrated in Figure 11.1.

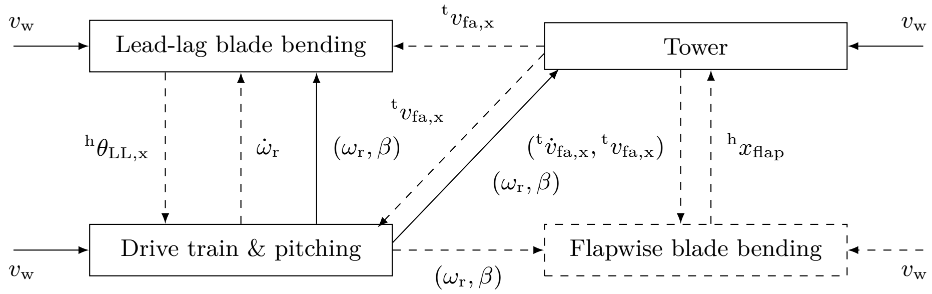


Figure 11.1: *Wind turbine system separated into four subsystems with interconnections. The solid boxes are included in the safety envelope search. The interconnections are given by arrows. The solid arrows are the interconnections which are included in the safety envelope search.*

The considered subsystems $\mathcal{I} = \{\text{Drive train, Tower, Lead-lag blade bending}\}$, with output maps (denoted $\mathbf{y}$) and input maps (denoted $\mathbf{u}$), are given as

$$\text{Drive train}: \begin{cases} \dot{\omega}_\mathrm{r} = \left(J_\mathrm{r} + N^{-1}J_\mathrm{g}\right)^{-1}\left[\tau_\mathrm{aero} - B_\mathrm{r}\omega_\mathrm{r}\right] \\ \dot{\theta}_\beta = \omega_\beta \\ \dot{\omega}_\beta = -0.6\omega_\beta - 0.0894\theta_\beta \\ \mathbf{y}_\mathrm{r} = \begin{bmatrix} \omega_\mathrm{r} \\ \theta_\beta \end{bmatrix} \end{cases}$$

$$\text{Tower}: \begin{cases} {}^\mathrm{t}\dot{\theta}_\mathrm{fa,y} = {}^\mathrm{t}\omega_\mathrm{fa,y}, \\ {}^\mathrm{t}\dot{\omega}_\mathrm{fa,y} = (M_\mathrm{n}L^2)^{-1}\left[F_\mathrm{aero}L + F_\mathrm{g}L{}^\mathrm{t}\theta_\mathrm{fa,y} - K_\mathrm{fa}{}^\mathrm{t}\theta_\mathrm{fa,y} - B_\mathrm{fa}{}^\mathrm{t}\omega_\mathrm{fa,y}\right] \\ \mathbf{u}_\mathrm{t} = \begin{bmatrix} \omega_\mathrm{r} \\ \beta \end{bmatrix} \end{cases}$$

$$\text{Lead-lag blade bending}: \begin{cases} {}^\mathrm{h}\dot{\theta}_\mathrm{LL,x} = {}^\mathrm{h}\omega_\mathrm{LL,x} \\ {}^\mathrm{h}\dot{\omega}_\mathrm{LL,x} = J_\mathrm{LL}^{-1}\left[\tau_\mathrm{aero}\xi_\mathrm{LL} - B_\mathrm{LL}{}^\mathrm{h}\omega_\mathrm{LL,x} - K_\mathrm{LL}{}^\mathrm{h}\theta_\mathrm{LL,x}\right] \\ \mathbf{u}_\mathrm{LL} = \begin{bmatrix} \omega_\mathrm{r} \\ \beta \end{bmatrix} \end{cases}$$

with $\tau_\mathrm{aero} = \frac{1}{2}\rho A R {v_\mathrm{w}}^2 C_\mathrm{q}(v_\mathrm{w}, \omega_\mathrm{r}, \beta)$, $F_\mathrm{aero} = \frac{1}{2}\rho A {v_\mathrm{w}}^2 C_\mathrm{t}(v_\mathrm{w}, \omega_\mathrm{r}, \beta)$ and $\beta = -\theta_\beta + 90$.

The three resulting subsystems each have 4^th degree polynomial vector fields. The state spaces in consideration are defined as in Section 10.2.

11.1 Compositional Barrier Certificate

The compositional barrier certificate method can be used to verify the safety of a system given as an interconnection of multiple subsystems. This method can be seen as a decomposition of the safety verification described in Chapter 9.

The safety verification using compositional barrier certificates splits up the system into subsystems which are connected through some coupling constraints. The interconnections of the subsystems are formulated by input and output maps. An interconnection input to the i^th system will be given by $\mathbf{u}_i \in \mathcal{U}_i$ and an output of a subsystem as $\mathbf{y}_i$. The input and output maps of the subsystems define a relation between the subsystems.

If the system can be decomposed into interconnected subsystems with input and output maps, the safety of the system can be verified using Theorem 6.

Theorem 6 [SPW12]: *Given a system $(\{\mathbf{f}_i\}, \{\mathcal{X}_i\}, \{\mathcal{U}_i\}, \{\mathcal{D}_i\}, \{\mathcal{X}_{0,i}\}, \{\mathcal{X}_{\mathrm{u},i}\})$, if a family of scalar differentiable functions $\{B_i(\mathbf{x}_i)\}$ exists, satisfying for all $i \in \mathcal{I}$*

$$\begin{aligned} B_i(\mathbf{x}_i) + \tau_{0,i} \leq 0,\ \forall \mathbf{x}_i \in \mathcal{X}_{0,i}, \\ B_i(\mathbf{x}_i) - \tau_{\mathrm{u},i} > 0,\ \forall \mathbf{x}_i \in \mathcal{X}_{\mathrm{u},i} \text{ and} \\ \nabla B_i(\mathbf{x}_i)\mathbf{f}_i(\mathbf{x}_i, \mathbf{u}_i, \mathbf{d}_i) + \tau_{\mathrm{w},i}(\mathbf{u}_i, \mathbf{y}_i) \leq 0,\ \forall (\mathbf{x}_i, \mathbf{u}_i, \mathbf{d}_i) \in \mathcal{X}_i \times \mathcal{U}_i \times \mathcal{D}_i \end{aligned} \tag{11.1}$$

with $\tau_0 = \sum_i \tau_{0,i} \geq 0$, $\tau_\mathrm{u} = \sum_i \tau_{\mathrm{u},i} \geq 0$ and $\tau_\mathrm{w}(\mathbf{u}, \mathbf{y}) = \sum_i \tau_{\mathrm{w},i}(\mathbf{u}_i, \mathbf{y}_i) \geq 0$, then the system is safe, with $B(\mathbf{x}) = \sum_i B_i(\mathbf{x}_i)$ as the certificate.

The sets $\mathcal{X}$, $\mathcal{D}$, $\mathcal{X}_0$ and $\mathcal{X}_\mathrm{u}$ are constructed from the Cartesian products of the sets of the subsystems

$$\mathcal{X} = \bigtimes_{i\in\mathcal{I}} \mathcal{X}_i, \quad \mathcal{D} = \bigtimes_{i\in\mathcal{I}} \mathcal{D}_i, \quad \mathcal{X}_0 = \bigtimes_{i\in\mathcal{I}} \mathcal{X}_{0,i}, \quad \mathcal{X}_\mathrm{u} = \bigtimes_{i\in\mathcal{I}} \mathcal{X}_{\mathrm{u},i}.$$

The barrier certificate subproblems in Theorem 6 can be considered equal to the weak barrier certificate with constraints on a few shared variables τ_0, τ_u and $\tau_\mathrm{w}(\mathbf{u},\mathbf{y})$. Note that the subproblems are almost separable. As a result, the subproblems can be formulated as individual SOSPs with some shared complicating constraints.

11.1.1 Compositional barrier certificate using SOS

Using the locked ellipse optimisation criterion, the compositional safety envelope optimisation of the system can using Theorem 6 be formulated as a range of SOSPs

$$\begin{aligned} &\min\ -\sum_{i\in\mathcal{I}} d_i \text{ over } \begin{array}{l}\{d_i\}\in\mathbb{R},\ \{B_i\}\in\mathcal{R}_{\mathbf{x}_i},\ \{\alpha_i\}\in\mathbb{R},\\ \{\gamma_i\}\in\mathcal{R}_{\mathbf{u}_i,\mathbf{y}_i},\ \{s_{\mathrm{u},i}\}\in\Sigma_{\mathbf{x}_i},\ \{\mathbf{s}_{\mathrm{X,D,U},i}\}\in\Sigma_{\mathbf{x}_i,\mathbf{d}_i,\mathbf{u}_i}\end{array}\\ &\text{s.t. } \forall i\in\mathcal{I}: \begin{cases} -B_i(\mathbf{x}_i)-(d_i-(\mathbf{x}_i-\mathbf{c}_i)^\mathrm{T}\mathbf{B}_i(\mathbf{x}_i-\mathbf{c}_i))-\alpha_i\in\Sigma\\ B_i(\mathbf{x}_i)-s_{\mathrm{u},i}g_{\mathrm{u},i}\in\Sigma\\ -\nabla B_i(\mathbf{x}_i)\mathbf{f}_i(\mathbf{x}_i,\mathbf{u}_i)-\mathbf{s}_{\mathrm{X,D,U},i}^\mathrm{T}\bar{\mathbf{g}}_{\mathrm{X,D,U},i}-\gamma_i\in\Sigma\end{cases}\end{aligned} \tag{11.2}$$

with $\alpha=\sum_i\alpha_i\geq 0$, $\gamma=\sum_i\gamma_i\geq 0$ and $\mathbf{B}_i$ being the matrix defining the locked ellipse of subsystem i.

The polynomial degree of the interconnection variable γ_i should be larger or equal to the polynomial degree of the vector field, with respect to $\mathbf{u}_i$ and $\mathbf{y}_i$.

The SOSPs in (11.2) are very similar to the SOSPs computed in Section 10.2. The only difference is the complication variables α_i and polynomial functions γ_i, which should satisfy the complicating constraints. Note that free variables of the unsafe conditions $\tau_{\mathrm{u},i}$ from (11.1) are set to zero.

In (11.2) the individual safety envelopes are optimised such that the zero crossings d_i of the locked ellipses are maximised. The compositional objective becomes to maximise $\sum_{i\in\mathcal{I}} d_i$. Note that the unsafe set $\mathcal{X}_\mathrm{u}$ is defined as the Cartesian product of $\mathcal{X}_{\mathrm{u},i}$.

As with the original barrier certificate formulation, the compositional barrier certificate formulation is formulated to *verify* the safety of a given initial set $\mathcal{X}_0$. The objective of the wind turbine safety envelope construction is however to maximise a variable (and in advance unknown) safety envelope. As the weak barrier certificate formulation is used, a possible safety envelope can be constructed by $\mathcal{X}_0\subseteq\{\mathbf{x}\in\mathcal{X}|B(\mathbf{x})\leq 0\}$ with $B(\mathbf{x})=\sum_i B(\mathbf{x}_i)$. As the barrier certificate in general can be of high polynomial degree, it is desirable to formulate the safety envelope using the ellipses. From (11.2) it is given that $-B_i(\mathbf{x}_i)-(d_i-(\mathbf{x}_i-\mathbf{c}_i)^\mathrm{T}\mathbf{B}_i(\mathbf{x}_i-\mathbf{c}_i))-\alpha_i\geq 0$ which is equivalent to

$$\sum_{i\in\mathcal{I}}((\mathbf{x}_i-\mathbf{c}_i)^\mathrm{T}\mathbf{B}_i(\mathbf{x}_i-\mathbf{c}_i)-d_i)\geq B(\mathbf{x})+\alpha, \tag{11.3}$$

with $\alpha\in\mathbb{R}_{\geq 0}$.

From (11.3) it is given that the sum of ellipses can be used as a (possibly conservative) safety envelope of the composed system. A safety envelope defined by a sum of locked ellipses is given as

$$\mathcal{X}_0=\left\{\mathbf{x}\in\mathcal{X}\,\middle|\,\sum_{i\in\mathcal{I}}(\mathbf{x}_i-\mathbf{c}_i)^\mathrm{T}\mathbf{B}_i(\mathbf{x}_i-\mathbf{c}_i)\leq\sum_{i\in\mathcal{I}} d_i\right\}. \tag{11.4}$$

By maximising $\sum_i d_i$ in (11.4), the composed safety envelope is maximised.

To obtain a feasible result of the decomposed SOSPs, some algorithm should be used to secure that the complicating constraints are satisfied. In the following section the dual decomposition method will be used to solve the problem (as done in [SPW12]).

11.2 Barrier Certificate through Dual Decomposition

The subsystems in (11.2) are not separable due to the complicating constraints. By using a decomposition method, the subsystems can be split up into separable problems, which can be solved individually. To obtain a feasible solution, some master algorithm should coordinate the subproblems.

Consider a compositional system with k problems

$$\begin{aligned} \min_{\mathbf{x}_1,\dots,\mathbf{x}_\mathrm{k}} \ & f_1(\mathbf{x}_1) + \dots + f_\mathrm{k}(\mathbf{x}_\mathrm{k}) \\ \text{s.t. } & \mathbf{x}_1 \in \mathcal{C}_1, \dots, \mathbf{x}_\mathrm{k} \in \mathcal{C}_\mathrm{k} \\ & \mathbf{h}_1(\mathbf{x}_1) + \dots + \mathbf{h}_\mathrm{k}(\mathbf{x}_\mathrm{k}) \leq 0, \end{aligned} \tag{11.5}$$

with $\mathcal{C}$ being local feasibility constraints and $\mathbf{h}_1, \dots, \mathbf{h}_k$ defining the complicating constraints.

By forming the Lagrangian dual problem of (11.5), the problem becomes separable. To obtain a feasible solution, a master algorithm, scaling the *cost* of the shared variables (interpreted as shared resources), can be used [BXMM08].

The Lagrangian of (11.5) is $\Lambda(\mathbf{x}_1, \dots, \mathbf{x}_\mathrm{k}, \boldsymbol{\lambda}) = f_1(\mathbf{x}_1) + \dots + f_\mathrm{k}(\mathbf{x}_\mathrm{k}) + \boldsymbol{\lambda}^\mathrm{T}\left(\mathbf{h}_1(\mathbf{x}_1) + \dots + \mathbf{h}_\mathrm{k}(\mathbf{x}_\mathrm{k})\right)$, which forms the Lagrangian dual function

$$\varphi(\boldsymbol{\lambda}) = \inf_{\mathbf{x}_1 \in \mathcal{C}_1, \dots, \mathbf{x}_\mathrm{k} \in \mathcal{C}_\mathrm{k}} \Lambda(\mathbf{x}, \boldsymbol{\lambda}) = \inf_{x_1 \in \mathcal{C}_1} \Big(f_1(\mathbf{x}_1) + \boldsymbol{\lambda}^\mathrm{T}\mathbf{h}_1(\mathbf{x}_1) \Big) + \dots + \inf_{\mathbf{x}_\mathrm{k} \in \mathcal{C}_\mathrm{k}} \Big(f_\mathrm{k}(\mathbf{x}_\mathrm{k}) + \boldsymbol{\lambda}^\mathrm{T}\mathbf{h}_\mathrm{k}(\mathbf{x}_\mathrm{k}) \Big).$$

The dual function is separable, and the dual problem $\sup_{\lambda \geq 0} \varphi(\boldsymbol{\lambda})$ can be solved by means of coordinating costs of the constraints to the subproblems.

11.2.1 Polynomial compositional barrier certificate

Problem (11.2) is on the same form as (11.5), with α_i and γ_i as complicating constraints and $-\sum_i d$ as objective function.

To be able to verify the feasibility of the complicating constraint $\gamma = \sum_i \gamma_i \geq 0$, the polynomials γ_i will be limited to being quadratic in the inputs and outputs [TPM09],

$$\gamma_i = \begin{bmatrix} \mathbf{u}_i \\ \mathbf{y}_i \end{bmatrix}^\mathrm{T} \boldsymbol{\Gamma}_i \begin{bmatrix} \mathbf{u}_i \\ \mathbf{y}_i \end{bmatrix},$$

where $\boldsymbol{\Gamma}_i$ is a diagonal matrix. Let $\overline{\gamma}_i$ denote the diagonal elements of $\boldsymbol{\Gamma}_i$. For $\boldsymbol{\Gamma}_i$ to be positive definite, the elements of $\overline{\boldsymbol{\gamma}}_i$ must be positive. Note that the quadratic choice of γ_i does not comply with the requirement of γ_i being of the same (or higher) order of the vector field. The problem is however still solvable, as the state space is limited.

The Lagrangian of (11.2) is

$$\Lambda_i(\mathbf{x}_i, \boldsymbol{\lambda}) = -d_i + \lambda_1(-\alpha_i) + \boldsymbol{\lambda}_2^\mathrm{T}(-\overline{\boldsymbol{\gamma}}_i),$$

where $\boldsymbol{\lambda} = [\lambda_1, \boldsymbol{\lambda}_2]^\mathrm{T}$ are the dual variables. The Lagrangian dual function is

$$\begin{aligned} \varphi(\boldsymbol{\lambda}) = & \sum_i \left(\inf_{\mathbf{x}_i, \alpha_i, \gamma_i} \Lambda_i(\mathbf{x}_i, \boldsymbol{\lambda}) \right) \\ & \text{s.t. } \{B_i\} \text{ satisfying (11.2),} \end{aligned} \tag{11.6}$$

with the dual (master) problem

$$\sup_{\lambda \geq 0} \varphi(\boldsymbol{\lambda}). \tag{11.7}$$

Note that the optimisations in (11.6) are given for a constant $\boldsymbol{\lambda}$ (cost). If the complicating constraints are satisfied, the dual variables $\boldsymbol{\lambda}$ can be slacked for a better solution. If they are not satisfied, the costs $\boldsymbol{\lambda}$ must be adjusted.

The SOSP in (11.2) formulated as Lagrangian duals is given in SOS Program 6. Notice that the i programs can be computed separately, but that the complication constraints might not be satisfied.

SOS Program 6 Compositional subsystem

$$\begin{aligned}
\varphi_i(\boldsymbol{\lambda}) \;&= \min \; -d_i - \boldsymbol{\lambda}^{\mathrm{T}}[\alpha_i \; \overline{\gamma}_i]^{\mathrm{T}} \text{ over } \begin{array}{l} d_i \in \mathbb{R},\; B_i^4 \in \mathcal{R}_{\mathbf{x}_i},\; \alpha_i \in \mathbb{R}, \\ \overline{\gamma}_i \in \mathbb{R}^2,\; s_{\mathrm{u},i} \in \Sigma^4_{\mathbf{x}_i},\; \mathbf{s}_{\mathrm{X,D,U},i} \in \Sigma^4_{\mathbf{x}_i,\mathbf{d}_i} \end{array} \\
\text{s.t.} \;& -B_i - (d_i - (\mathbf{x}_i - \mathbf{c}_i)^{\mathrm{T}}\mathbf{B}_i(\mathbf{x}_i - \mathbf{c}_i)) - \alpha_i \in \Sigma \\
& B_i - s_{\mathrm{u},i} g_{\mathrm{u},i} \in \Sigma \\
& -\nabla B_i \mathbf{f}_i - \mathbf{s}^{\mathrm{T}}_{\mathrm{X,D,U},i}\overline{\mathbf{g}}_{\mathrm{X,D,U},i} - \begin{bmatrix} \mathbf{u}_i \\ \mathbf{y}_i \end{bmatrix}^{\mathrm{T}} \operatorname{diag}(\overline{\gamma}_i) \begin{bmatrix} \mathbf{u}_i \\ \mathbf{y}_i \end{bmatrix} \in \Sigma
\end{aligned}$$

To solve the dual (master) problem (11.7), the subgradient method will be used. A subgradient can, given a constant Lagrange multiplier, be found from the optimal values of the complicating variables. Let α_i^* and $\overline{\gamma}_i^*$ denote the optimal values from an optimisation given some $\boldsymbol{\lambda}$. The function $\mathbf{g}(\boldsymbol{\lambda}) = [\sum_i \alpha_i^*(\boldsymbol{\lambda}); \sum_i \overline{\gamma}_i^*(\boldsymbol{\lambda})] \in \partial\varphi(\boldsymbol{\lambda})$ is then a subgradient at $\boldsymbol{\lambda}$, where $\partial\varphi(\boldsymbol{\lambda})$ denotes the subdifferential at $\boldsymbol{\lambda}$. Updating $\boldsymbol{\lambda}$ according to

$$\boldsymbol{\lambda}^{(l+1)} = \left(\boldsymbol{\lambda}^{(l)} - a^{(l)}\mathbf{g}(\boldsymbol{\lambda}^{(l)})\right)_+, \tag{11.8}$$

with an appropriate diminishing step size $a^{(l)}$, the costs $\boldsymbol{\lambda}^{(l)}$ will converge to the optimal. The master algorithm controlling the cost ($\boldsymbol{\lambda}$) is illustrated in Figure 11.2. A cost $\boldsymbol{\lambda}$ is broadcasted by the master algorithm and the results are returned by the subproblems (in this case the SOSPs).

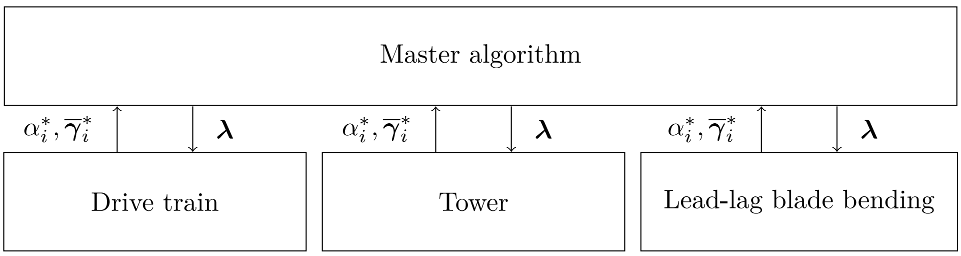


Figure 11.2: *Using dual decomposition, all subproblems can be solved in parallel, with a master algorithm (in this case the subgradient method) distributing costs of the shared variables.*

The algorithm is run until the dual variables have settled, and the best solution is used. It should be noted that, using the subgradient method the result is not guaranteed to improve at each iteration. Additionally, the solution is not guaranteed to be feasible at each iteration. The dual decomposition algorithm is given in Algorithm 1. As with the SOSPs in Section 10.2, the solution of a given SOSP will be relaxed (post-processed) to a feasibility problem, to obtain a better numerical result.

Algorithm 1 Dual algorithm to solve (11.2)

---

1. Initialise $l = 0$ and $\boldsymbol{\lambda}^0$.
2. Each subproblem is solved in parallel by computing SOS Program 6, and the solutions α^* and γ^* are reported.
3. The master algorithm updates the constraint costs with the subgradient iterate (11.8), and broadcasts the new costs $\boldsymbol{\lambda}^{(l+1)}$.
4. Update $l \leftarrow l + 1$ and go to step 2 (if costs have settled, go to step 5)
5. Post-process with objective relaxation and feasibility verification.

11.2.2 Computation

In the following, a compositional safety envelope of the drive train, tower and lead-lag blade bending subsystems will be constructed. This is done using the SOSP formulation given in SOS Program 6 and by updating the dual variables using the subgradient method given in (11.8). The procedure will be executed as in Algorithm 1.

The sets $\mathcal{X}_i$ and $\mathcal{X}_{\mathrm{u},i}$ of the subsystems will be defined as in Section 10.2, with $\mathcal{X}$ and $\mathcal{X}_{\mathrm{u}}$ given by the Cartesian products of the subsystem sets.

Algorithm 1 is initialised in $\boldsymbol{\lambda}^0 = [0.5, 0.5, 0.5]$ and the step size of the subgradient given as $a^{(l)} = \frac{0.01}{10+l}$. In Figure 11.3 the iterative results of Algorithm 1 are illustrated. The best objective is denoted d^* and the Lagrange multipliers are illustrated as functions of iterate number l.

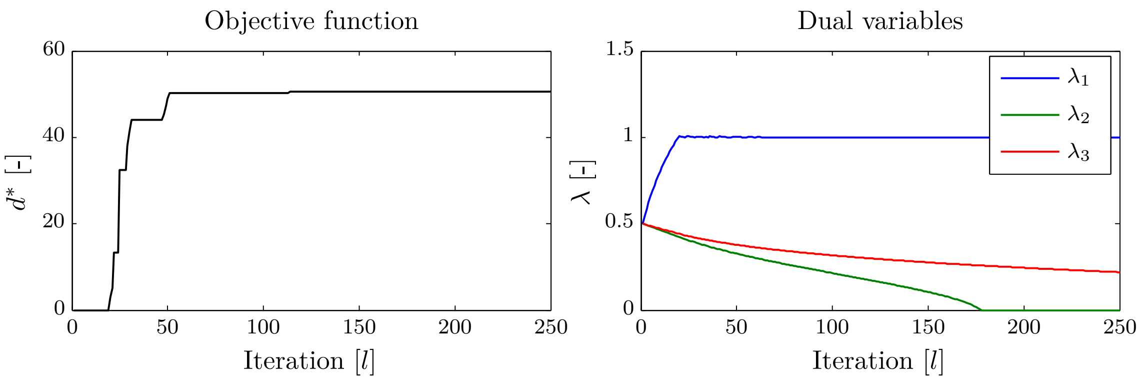


Figure 11.3: *Left plot shows the best results of the objective d^* obtained up to iterate l. The right plot shows the evolution of the Lagrangian multipliers as function of iterate number l.*

The computation was run on a 2.6 GHz AMD64, 96 GB ram computer and took 14 hours to complete. The optimisation script implemented in `MATLAB` with `YALMIP` can be found on the enclosed DVD.

The optimal value $d^* = \sum_i d_i$ is, as in Section 10.2, relaxed and solved as a feasibility problem $d_i > 0.75 d_i^*$ to obtain a better numerical result (post-processing step in Algorithm 1). The resulting feasible value is found to $d = \sum_i d_i = 35.47$.

In the following Section the above found barrier certificate will be tested on the NREL 5-MW wind turbine in `FAST`. This is done to examine if a practical useable result has been obtained. Notice that the assembled unsafe set $\mathcal{X}_\mathrm{u}$ is defined by the Cartesian product $\mathcal{X}_\mathrm{u} = \mathcal{X}_\mathrm{u,r} \times \mathcal{X}_\mathrm{u,t} \times \mathcal{X}_\mathrm{u,LL}$ of the subsystems.

To design a safety envelope which is safe for each subsystem ultimate load limits separately, several different compositional barrier certificates must be constructed using the unsafe sets

$$\mathcal{X}_\mathrm{u,1} = \mathcal{X}_\mathrm{u,r} \times \mathbb{R}^{\mathrm{n_t}} \times \mathbb{R}^{\mathrm{n_{LL}}}, \quad \mathcal{X}_\mathrm{u,2} = \mathbb{R}^{\mathrm{n_r}} \times \mathcal{X}_\mathrm{u,t} \times \mathbb{R}^{\mathrm{n_{LL}}}, \quad \mathcal{X}_\mathrm{u,3} = \mathbb{R}^{\mathrm{n_r}} \times \mathbb{R}^{\mathrm{n_t}} \times \mathcal{X}_\mathrm{u,LL},$$

where n_r, n_t and n_LL are the dimensions of the respective subsystem state spaces. A composed safety envelope can be constructed by the intersection of the computed safety envelopes, $\mathcal{X}_0 = \bigcap_i \mathcal{X}_{0,i}$.

11.3 Implementation Results

In this section the safety supervisor found using the compositional barrier certificate method is implemented and tested on the NREL 5-MW wind turbine implemented in `FAST`.

A safety envelope can, as described in Section 11.1, be constructed as

$$\mathcal{X}_0 = \left\{ (\mathbf{x}_\mathrm{r}, \mathbf{x}_\mathrm{t}, \mathbf{x}_\mathrm{LL}) \in \mathcal{X}_\mathrm{r} \times \mathcal{X}_\mathrm{t} \times \mathcal{X}_\mathrm{LL} \middle| \sum_i \big((\mathbf{x}_i - \mathbf{c}_i)^\mathrm{T} \mathbf{B}_i (\mathbf{x}_i - \mathbf{c}_i) \big) - d \le 0 \right\}.$$

To prevent that the system enters the unsafe set $\mathcal{X}_\mathrm{u}$, the safety supervisor should trigger an emergency shutdown when the sum of the evaluated safety envelopes becomes positive.

The resulting safety supervisor system is given in (11.9).

$$\mathcal{S} = \begin{cases} \text{Safe}, & \mathbf{x} \in \mathcal{X}_0 \\ \text{Unsafe}, & \text{else} \end{cases} \tag{11.9}$$

If $\mathcal{S}$ becomes *unsafe*, the safety supervisor should trigger an emergency shutdown.

As the safety needs to be continuously verified, evaluation of the polynomials needs to be fast to compute. To test the safety of the system, a second order polynomial in seven variables is evaluated. The evaluation involves 18 multiplications and 34 summations.

In the following, the safety supervisor system in (11.9) is implemented on the NREL 5-MW wind turbine in `FAST`. When the system is safe, the control of the wind turbine is given by the NREL 5-MW controller. When an unsafe situation is detected by the safety supervisor, the emergency shutdown procedure is initialised.

The four safety critical situations from Section 10.3 are tested. Additionally a normal operation simulation with no controller faults or external extreme conditions is illustrated in Appendix M (to verify that the safety supervisor does not shut down the wind turbine during normal operation). The four safety critical situations are listed below, each coupled with a figure. The figures are separated into two parts. The top part illustrates the *signals* of the system. The bottom part illustrates the evaluation of the safety condition $\sum_i \big((\mathbf{x}_i - \mathbf{c}_i)^\mathrm{T} \mathbf{B}_i (\mathbf{x}_i - \mathbf{c}_i) - d_i \big)$ (if the result of the evaluation becomes positive, the emergency shutdown is triggered).

1. Blade-pitch controller error (Figure 11.4)

   The compositional safety supervisor is able to detect the safety critical situation and safely shut down the wind turbine.

2. Wind gust (Figure 11.5)

   The compositional safety supervisor is able to detect the safety critical situation and safely shut down the wind turbine.

3. Generator failure (Figure 11.6)

   The compositional safety supervisor is able to detect the safety critical situation and safely shut down the wind turbine.

4. Blade-pitch controller error & generator failure (Figure 11.7)

   The compositional safety supervisor is able to detect the safety critical situation and safely shut down the wind turbine.

The safety supervisor designed using the compositional barrier certificate method is able to safely shut down the wind turbine in all four safety critical situations. This is in contrary to the safety supervisor designed using the separate safety envelopes, which was not able to detect the combination of pitch and generator fault. As the safety system is designed according to the Cartesian product of the unsafe sets of the subsystems, it is expected that situations can be found for which the safety system does not manage to keep the system safe. An implementation of the safety supervisor in `SIMULINK` can be found on the enclosed DVD.

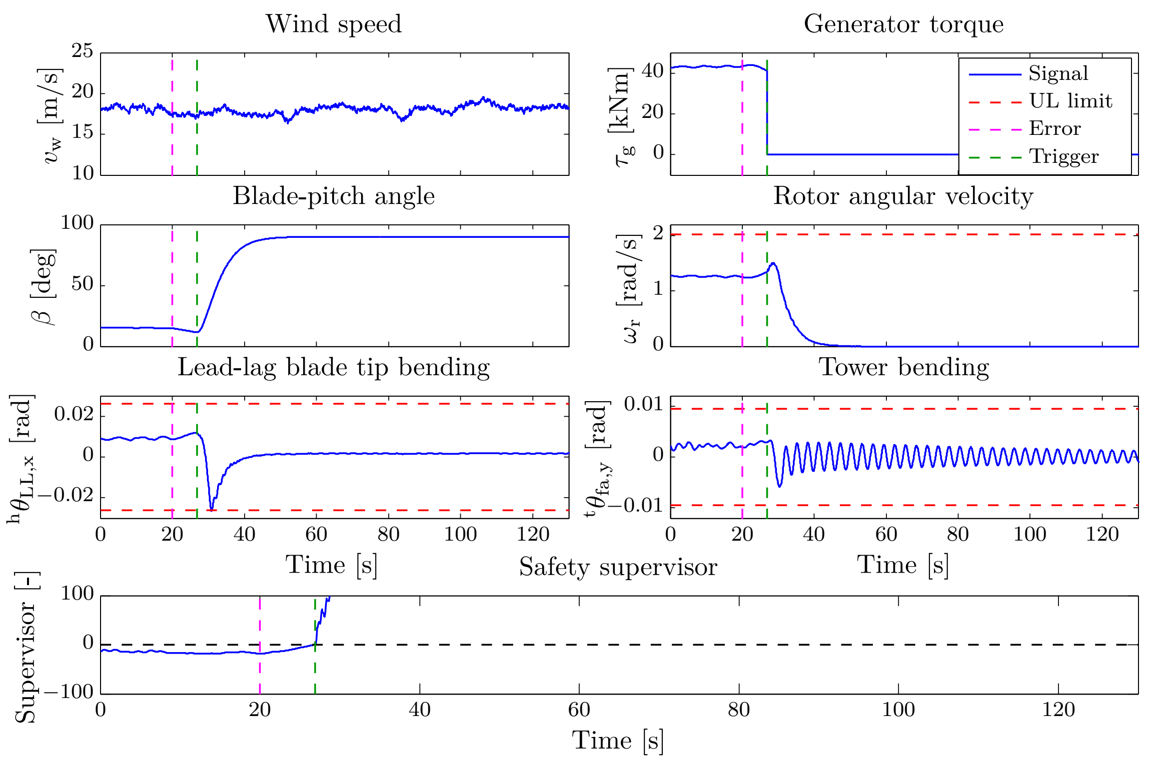


Figure 11.4: *Safety critical situation 1. Top 6 plots show system signals. Bottom plot shows evaluation of safety supervisor. A pitch control error is introduced.*

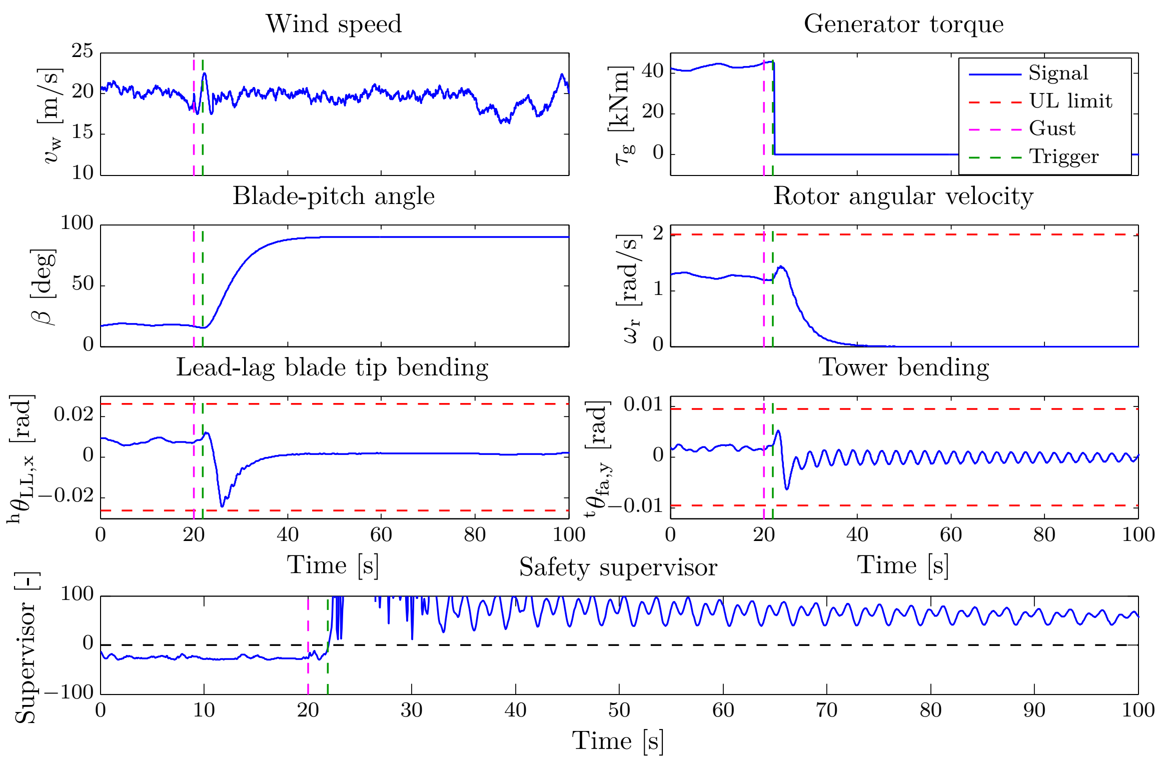


Figure 11.5: *Safety critical situation 2. Top 6 plots show system signals. Bottom plot shows evaluation of safety supervisor. A wind gust is introduced.*

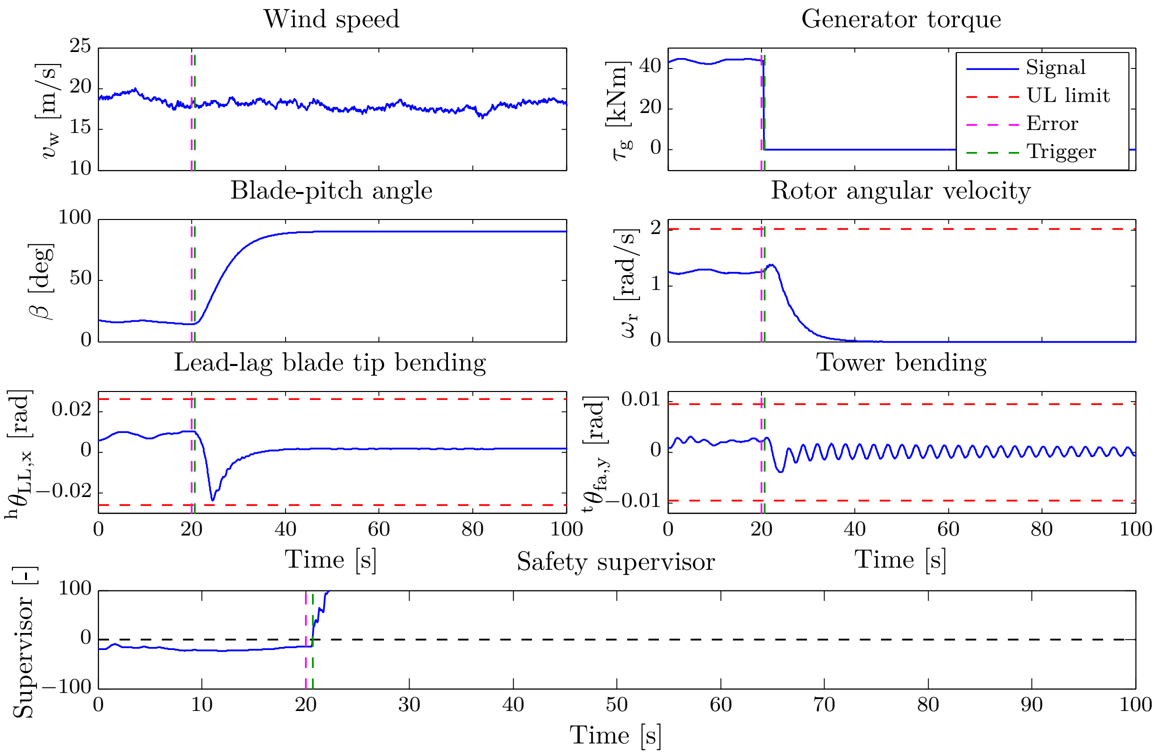


Figure 11.6: *Safety critical situation 3. Top 6 plots show system signals. Bottom plot shows evaluation of safety supervisor. A generator torque failure is introduced.*

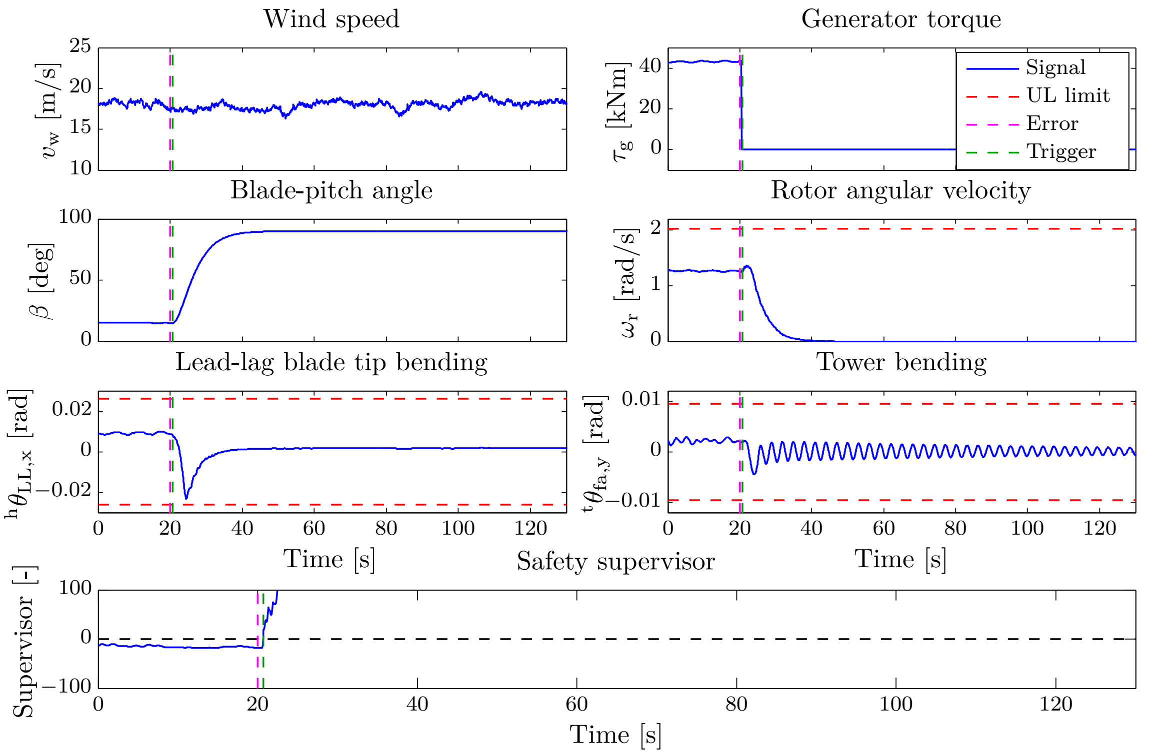


Figure 11.7: *Safety critical situation 4. Top 6 plots show system signals. Bottom plot shows evaluation of safety supervisor. A pitch control error and generator torque failure is introduced.*

12 Conclusion

The scope of this project is to design a safety supervisor system for a wind turbine. The objective of the safety supervisor design is to improve the safety guarantee of large wind turbines while at the same time keeping the number of emergency shutdowns low, such that the power production is not interrupted unnecessarily. The design of the safety supervisor system is based on the fictitious NREL 5-MW wind turbine, which represents a realistic large multi-megawatt wind turbine. An existing reference variable-speed, variable-blade-pitch controller is used to control the wind turbine power production in normal operation.

The IEC-61400 standard specify requirements to the external conditions for which a given wind turbine should be able to stay safe. In the specific case of the NREL 5-MW wind turbine, it is found that the wind turbine in operation should be able to handle wind gusts up to 35 m/s. Consequently, this requirement should be included in the design of the safety supervisor system. The IEC-61400 standard additionally provides some recommendations to how a safety system can be implemented using a safety supervisor which triggers an emergency shutdown when the condition of the wind turbine system is about to become unsafe. It is in IEC-61400 noted that the emergency shutdown procedure itself is important to consider when the safety supervisor system is designed.

From an examination of the NREL 5-MW wind turbine, it is found that the wind turbine experiences considerable loads during an emergency shutdown. Additionally it is found that a safety supervisor should be able to include the energy of the system and the emergency shutdown procedure itself, in the emergency shutdown trigger - in order to avoid that the ultimate load limits of the wind turbine are violated. These results indicate that a conventional rotor overspeed guard is a possible insufficient safety supervisor implementation, given a large wind turbine. Accordingly, it is chosen to consider a multivariate safety supervisor system.

Safety Verification Methods

To design a multivariate safety supervisor system which includes the stochastic behaviour of the wind and the emergency shutdown procedure itself in the safety guarantee, methods based on measurements, simulations and system model examination are considered. It is found that Lyapunov-like methods can provide information about the safety of the system, without the need of explicit knowledge of the system trajectories. Additionally, such a formulation allows inclusion of a wind disturbance and the emergency shutdown procedure in the safety guarantee.

Due to primarily the aerodynamic properties of the wind turbine a linear model description is found insufficient. As a result, familiar methods, such as the Lyapunov equation, cannot be used to examine the system. A similar concept based on barrier certificates is considered. The barrier certificate method enables safety verification of a set in the state space, without the need of explicit knowledge of system trajectories. If the system is found to be safe in some subset of the safe set, this set is denoted a safety envelope.

The safety envelope search using barrier certificates is a model-based method. To use the SOS framework, a polynomial model of the wind turbine system must be developed.

Modelling

To limit the complexity of the safety supervisor design, it is chosen to consider only the safety of specific structural parts of the wind turbine. The specific components which are included in the safety guarantee are found partly from observations of NREL 5-MW wind turbine simulations and partly from literature (experiences from other wind turbines).

The model includes the dynamics of the structural components which are found to be exposed to significant loads during normal operation and the emergency shutdown itself. The modelled components include the aerodynamic properties of the rotor, a two-mass drive train, the tower fore-aft bending, the blade flapwise bending, the blade lead-lag bending, the pitch procedure during emergency shutdown and a scalar wind model. The model parts are assembled into one complete 13-state polynomial model. The aerodynamic model includes polynomial approximations of the aerodynamic properties of the rotor, which are often given as lookup tables. To approximate the aerodynamic properties relatively high order polynomials are required to obtain a satisfactory approximation.

The model is developed as an autonomous model of the emergency shutdown procedure, with a single disturbance input from the wind. The resulting model can be used to find emergency shutdown trajectories from a given initial state. Using the model it can be examined if an emergency shutdown initiated in a given initial state produces a safe or unsafe shutdown trajectory. The model parameters are found partly from the specification of the NREL 5-MW wind turbine and partly through simulation.

The polynomial model is compared to the NREL 5-MW wind turbine implemented in `FAST` and is found to replicate the modelled dynamics satisfactory. This result shows that it is possible to obtain a reasonable dynamic model of the specific NREL 5-MW wind turbine using a polynomial system description only. This is considered essential, as it enables a search of safety envelopes using barrier certificates.

Operation Analysis

From the polynomial system description a theoretical safety supervisor system can be found. In practice the safety system should be designed with respect to the normal operation of the wind turbine system. To obtain some knowledge of the normal operation of the wind turbine, the system states are measured during typical external conditions. The knowledge of the normal operation enables a search of a safety supervisor system which is designed specifically towards the normal operation of the wind turbine. A natural objective in this case is to design a safety system which covers the normal operation region best possible; as this entails that the frequency of emergency shutdowns is lowered.

Safe Operation Envelope

It is chosen to consider safety envelopes limited to the shape of hyperellipsoids. The hyperellipsoid allows the center, scaling, orientation and shape as degrees of freedom. Additionally it is found that a range of optimisation criteria of a hyperellipsoid can be formulated in an SDP. In particular it is found that an optimisation of the trace of the hyperellipsoid can be formulated in an SDP. This measure resembles an optimisation of the volume of the hyperellipsoid. Additionally it is chosen to consider hyperellipsoids with locked center, orientation and shape, found from the normal operation of the wind turbine. It is found that the combination of trace optimised hyperellipsoids and hyperellipsoids locked to the normal operation provide a reasonable criterion to design practical useable safety envelopes and consequently a practical usable safety supervisor system. As a safety envelope can be obtained by an union of safety envelopes, the two optimisation criteria can be combined into one safety supervisor system.

Computation of Safety Envelope

The search of safety envelopes is formulated using the Positivstellensatz and sum of squares decomposition. The resulting problem becomes a sum of squares program, which can be passed as an SDP. The sum of squares program is formulated as an optimisation problem in which the safety envelope, shaped as a hyperellipsoid, is maximised. This is in contrary to the verification problems for which the barrier certificate method is originally proposed.

It is found that the developed 13-state wind turbine system produces a very large sum of squares program. Unfortunately, the program cannot be solved when formulated directly from the 13-state wind turbine system on a standard PC. When the sum of squares program is formulated as an SDP, the resulting program requires considerable memory and computation time. Additionally it is found that large sum of squares programs often produce numerical difficult problems, which are difficult to solve accurately on a standard PC.

To obtain a problem which can be computed in practice, the wind turbine system model is separated into parts. In this way the model parts can be individually formulated as sum of squares programs of reasonable size. Safety envelopes matching each model part using trace and locked hyperellipse optimisation criteria are found. This relaxation of the safety envelope search problem enables the search of separate safety envelopes to be computed on a standard PC in reasonable time. The disadvantage of this relaxation technique is that the interconnections of the model parts should be formulated manually as bounded disturbances, which requires some practical knowledge of the system in order to maintain the validity of the safety guarantee.

Safety envelopes of each of the separate model parts are found using sum of squares and barrier certificates. Trajectories initialised in a range of initial points within the safety envelopes are tested and found to be safe. Additionally the resulting safety supervisor system designed using the safety envelopes are implemented and tested in `FAST`. The safety supervisor system manages to shut down the wind turbine prior to any exceedance of ultimate load limits in three out of four situations. In the case of two coincident safety critical events, the safety supervisor system is not able to initialise the emergency shutdown procedure in time to avoid exceedance of the ultimate load limits. Additionally as modelling uncertainties are not included in the design of the safety supervisor, it cannot be guaranteed that the safety system implemented on the NREL 5-MW wind turbine in `FAST` provides a valid safety guarantee in every situation.

Compositional Safety Envelope

In order to obtain a safety supervisor system calculated from the complete wind turbine system (in contrary to separate model parts), the recently proposed method of compositional barrier certificates is utilised. Using this method, the interconnections of the model parts are included directly in the formulation of the problem. The compositional barrier certificate method is used in association with the dual decomposition method to iteratively obtain a feasible safety envelope. The disadvantage of this strategy is that the sum of squares programs should be solved a number of times, in order to obtain a feasible solution. In practice it is found that the sum of squares programs of the model parts should be solved approximately 100 times. As the calculation time of the drive train subsystem is approximately 4 hours, this result in significant computation time. In order to reduce the computation time, simplifications to the model parts are implemented.

Using the simplified model parts, the compositional barrier certificate method enables a search of safety envelopes which are valid for the complete system to be computed in practice on a standard PC. If a system can be separated into small easily solved system parts with a few interconnections between the parts - the compositional method seems to be a very advantageous barrier certificate search method in practice.

The safety supervisor system designed using the compositional barrier certificate method and the Cartesian product of the unsafe sets, is implemented and tested on the NREL 5-MW wind turbine in `FAST`. The results show that it is reasonable to assume that a practical useable safety supervisor system can be designed using this method.

Overall Conclusion

Given the results obtained in this project, it can be concluded that a multivariate model-based safety supervisor system can improve the safety guarantee and possibly improve the uptime of large wind turbines, compared to simple univariate safety supervisors often used today. The implemented safety supervisor showed ability to commence emergency shutdowns prior to unsafe situations and to stay passive during normal operation of the wind turbine. Using the concept of safety envelopes and barrier certificates the ultimate load limits of several safety critical components, the emergency shutdown procedure itself and the stochastic disturbance of the wind field can be directly formulated in a computationally tractable search of a safety supervisor system.

In practice, it is found that the barrier certificate method using sum of squares programs sometimes produce numerical difficult problems, which complicates the search of valid safety supervisor systems. Using the recent proposed method of compositional barrier certificates, the computational requirements of the sum of squares programming are lowered, which allow the search of safety envelopes on relative large problems. It seems, however, that the numerical aspect of solving sum of squares programs is still immature.

In general the combination of a polynomial model description, safety envelopes, barrier certificates and sum of squares programming provide a framework which is very suitable in relation to safety supervisor design. By combining the theoretical power of the framework with practical system knowledge and experience, the framework can in its current state be used in the design of safety supervisor systems.

As the safety system design is model-based, the validity of the safety guarantee is limited by model uncertainties and measurement errors. In order to obtain a practical valid safety guarantee, the possible model and measurement uncertainties must be included in the design of the safety supervisor system.

In the following chapter some suggestions to further work and some inspirational suggestions to solutions to the limitations of the results obtained in the project are proposed.

13 Future Work

In order to make the safety envelopes applicable to real wind turbines, further work needs to be conducted. In the proposed method, no regards is taken towards model uncertainties. This chapter contains ideas to make the safety envelope robust towards model uncertainties. Furthermore, it is shown how different barrier certificates from different models can be composed into one safety criteria (e.g. in the case of varying mean wind speeds).

13.1 Robust Safety Envelope

In this section model uncertainties included in the safety guarantee are briefly examined.

The safety envelopes designed in Chapter 10 and 11 are valid given that the system model is an exact representation of the real wind turbine system. As a consequence, the safety envelopes will not necessarily guarantee the safety of the physical wind turbine system. The model uncertainty will be a result of several factors, such as simplifications of the model, parameter uncertainties, insufficient model structure and time varying system parameters. It is assumed that the real system description is unknown but in the family of possible models [STCS98].

In the following, the class of model parameter uncertainties is included in the construction of safety envelope. The vector of uncertain parameters in the dynamical system is given as $\boldsymbol{\delta} = (\delta_1, ..., \delta_{\mathrm{p}})$. Two different cases of parameter uncertainties are considered:

- Time-invariant uncertainties
- Time-varying uncertainties

In the case of time-invariant parameter uncertainties, the parameters $\boldsymbol{\delta}$ are considered as being fixed but unknown. The case of time-varying parameter uncertainties considers an unknown and time varying vector $\boldsymbol{\delta}(t)$, belonging to the uncertainty set $\delta(t) \in \Delta, \forall t$. In many practical situations it seems reasonable to assume that a combination of time-invariant uncertainties and time-varying uncertainties are present. The class of time-invariant uncertainties can be included in the class of time-varying uncertainties by including an additional constraint of zero rate of change, on the relevant uncertain parameters [SW04].

Given a vector of parameter uncertainties, the dynamical system becomes

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \boldsymbol{\delta}(t)),$$

where the elements in $\boldsymbol{\delta}$ are either fixed or time-varying.

If the parameters $\boldsymbol{\delta}(t)$ coincide with the system state terms, the system becomes non-linear even if f is linear. In the case with f being polynomial as e.g.

$$\dot{x}_1 = \delta_1 x_1^2 + \delta x_2 + \delta_3,$$

the system, with introduction of varying $\boldsymbol{\delta}$, stays polynomial. As the system description stays polynomial, the search of a safety envelope can be formulated using barrier certificates and the SOS framework. Given the varying uncertainty $\boldsymbol{\delta} \in \Delta$, the weak barrier certificate formulation in

(9.4) becomes

$$B(\mathbf{x}) \leq 0, \forall(\mathbf{x}) \in \mathcal{X}_0,$$
$$B(\mathbf{x}) > 0, \forall(\mathbf{x}) \in \mathcal{X}_\mathrm{u},$$
$$\nabla B(\mathbf{x})\mathbf{f}(\mathbf{x}, \boldsymbol{\delta}, \mathbf{d}) \leq 0, \forall(\mathbf{x}, \boldsymbol{\delta}, \mathbf{d}) \in \mathcal{X} \times \Delta \times \mathcal{D},$$

where only the differential constraint is different from the original weak barrier certificate formulation. The parameter uncertainty set Δ is given as an semi-algebraic set as in (9.16), such that $\mathbf{g}_\Delta \geq 0$ in Δ.

Using Stengle's Positivstellensatz, the set which should be empty becomes

$$\mathbb{K} = \left\{ \mathbf{x} \in \mathbb{R} \;\middle|\; \begin{array}{c} \nabla B(\mathbf{x}) f(\mathbf{x}) \geq 0 \\ \mathbf{g}_\Delta \geq 0 \end{array} \right\},$$

which is equivalent to

$$-s_0 \nabla B(\mathbf{x}) f(\mathbf{x}, \boldsymbol{\delta}, \mathbf{d}) - \sum_{i=1}^{p} g_{\Delta,i} s_i \in \Sigma$$

with $\{s_0, ..., s_\mathrm{p}\} \subset \Sigma$. If a feasible solution to the resulting SOSP can be found, then the initial set $\mathcal{X}_0$ is a safety envelope to the system, which is valid given any parameter in Δ.

13.2 Wind Span

An implementation of a safety supervisor system should guarantee the safety of the wind turbine system in the wind span defined by the IEC-61400 standard, as described in Chapter 3. A centrally computed SOSP given the entire wind span becomes very large.

In order to reduce the size of the safety envelope search, the aerodynamic polynomial approximations are in Chapter 10 limited to cover a part of the wind field range. Specifically the safety envelope search is limited to cover the wind range v_w = [15m/s ; 25m/s]. This simplification allows the search of safety envelope to be achievable. Assuming that a reliable measurement of the mean wind is available, the ranges of the 50 years wind gusts can be separated according to a specific mean wind speed.

Wind gusts given a range of different mean wind speed, calculated using Equation (3.1), are illustrated in Figure 13.1.

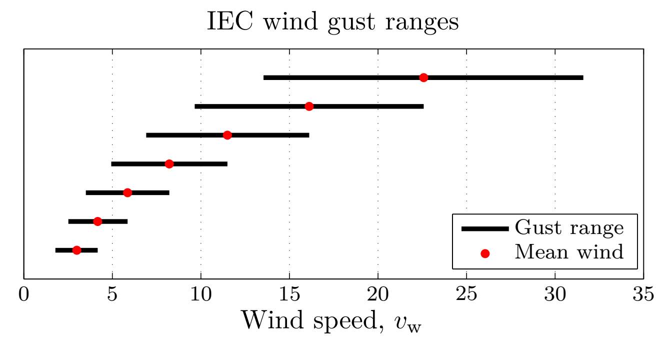


Figure 13.1: *The 50 years wind speed gusts (V_e50) calculated for a range of mean wind speeds.*

By separating the wind field into parts of the wind field range and constructing safety envelopes for each part, the entire operational mean wind speed range can be covered by the safety supervisor.

The concern using this concept is the validity of the safety guarantee when the mean wind speed changes from one safety envelope design to another.

A possible solution might be to consider the system as a hybrid system. In [PJP07] safety verification of hybrid systems using barrier certificates is discussed. To verify the safety of the hybrid system, barrier certificates are constructed from a set of functions, where each function corresponds to a discrete location of the system (in this case a mean wind speed). The functions are linked through discrete transition conditions, which take care of the transitions between the continuous systems. The approach is similar to stability analysis of hybrid systems using a range of Lyapunov functions.

Theorem 7 [PJP07]: *Let $l \in L$ be a finite set of discrete locations,* $\mathrm{Init}(l) = \{\mathbf{x} \in \mathcal{X} : (l, \mathbf{x}) \in \mathcal{X}_0\}$*,* $\mathrm{Unsafe}(l) = \{\mathbf{x} \in \mathcal{X} : (l, \mathbf{x}) \in \mathcal{X}_\mathrm{u}\}$*,* $\mathrm{Guard}(l, l')$ *define the possible transitions from location l to l' with reset map* $\mathrm{Reset}(l, l')$*. Suppose there exists a collection of functions $\{B_l(\mathbf{x}) : l \in L\}$ which for all $l \in L$, $l \neq l'$, satisfy*

$$\begin{aligned}
B_l(\mathbf{x}) &\leq 0, \forall \mathbf{x} \in \mathrm{Init}(l), \\
B_l(\mathbf{x}) &> 0, \forall \mathbf{x} \in \mathrm{Unsafe}(l), \\
\nabla B_l(\mathbf{x}) f_l(\mathbf{x}, \mathbf{d}) &< 0, \forall (\mathbf{x}, \mathbf{d}) \in \mathcal{I}(l) \times \mathcal{D}(l) \\
&\quad \text{such that } B_l(\mathbf{x}) = 0, \\
B_{l'}(\mathbf{x}') &\leq 0, \forall \mathbf{x}' \in \mathrm{Reset}(l, l')(\mathbf{x}) \\
&\quad \text{for all } \mathbf{x} \in \mathrm{Guard}(l, l') \text{ s.t. } \mathrm{B_l}(\mathbf{x}) \leq 0.
\end{aligned}$$

Then the safety of the system is guaranteed.

If it is possible to construct barrier certificates of each of the systems defined by a mean wind speed and a turbulence disturbance, and the barrier certificates satisfy Theorem 7, then the systems is guaranteed to be safe within the combined mean wind span.

Bibliography

[Aga08] Puneet Agarwal. *Structural Reliability of Offshore Wind Turbines.* PhD thesis, University of Texas, 2008.

[Buh11] Marshall Buhl. *NWTC Design Codes: WT_Perf (17-February-2011)*, 2011.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex Optimisation.* Cambridge University Press, 1. edition edition, 2004.

[BXMM08] Stephen Boyd, Lin Xiao, Almir Mutapcic, and Jacob Mattingley. Notes on Decomposition Methods. *Notes*, 2008.

[dH56] Isaac Van der Hoven. Power Spectrum of Horizontal Wind Speed in the Frequency Range from 0.0007 to 900 Cycles Per Hour. *Journal of meteorology*, 14(1):160–164, 1956.

[FDB07] Ricardo J. Mantz Fernando D. Bianchi, Hernan De Battista. *Wind Turbine Control Systems.* Springer, 2007.

[Han08] Martin O. L. Hansen. *Aerodynamics of Wind Turbines.* Earthscan, 2. edition edition, 2008.

[Hau06] Erich Hau. *Wind Turbines, Fundamentals, Technologies, Application, Economics.* Springer, 2nd edition edition, 2006.

[IEC01] (IEC) International Electrotechnical Commission. Elproducerende vindmøller - del 13: Måling af mekaniske laster. Technical report, Dansk Standard, 2001. IEC 61400-13.

[IEC06] (IEC) International Electrotechnical Commission. Elproducerende vindmøller - del 1: Konstruktionskrav. Technical report, Dansk Standard, 2006. IEC 61400-1.

[JB07] J M Jonkman and M L Buhl. Loads Analysis of a Floating Offshore Wind Turbine Using Fully Coupled Simulation Preprint. Technical Report June, NREL, 2007.

[JBMN09] J Jonkman, S Butterfield, W Musial, and G Scott Nrel. Definition of a 5-MW Reference Wind Turbine for Offshore System Development. Technical Report February, NREL, 2009.

[JF11] Kathryn E. Johnson and Paul A. Fleming. Development, implementation, and testing of fault detection strategies on the National Wind Technology Centers controls advanced research turbines. *Mechatronics*, 21(4):728–736, June 2011.

[JFM09] J. G. McGowan J. F. Manwell. *Wind Energy Explained, Theory, Design And Application.* Wiley, 2009.

[JJ05] Jason M Jonkman and Marshall L Buhl Jr. FAST User Guide. *Contract*, 2005.

[Jon10] Jason Jonkman. *NWTC Design Codes: FAST (05-November-2010)*, 2010.

[JWFP05] Z. Jarvis-Wloszek, R. Feeley, and A. Packard. Controls Applications of Sum of Squares Programming. *POSITIVE POLYNOMIALS IN CONTROL*, 1(Vol.312):20, 2005.

[Kha02] Hassan K. Khalil. *Nonlinear Systems.* Pearson Education, 3. edition edition, 2002.

[Lö09] Johan Löfberg. Pre- and Post-processing Sum-of-squares Programs in Practice. *IEEE Transactions on Automatic Control*, 54(5):1007–1011, 2009.

[Lal11] Sanjay Lall. Sums of Squares. Technical report, Lecture slides, 2011.

[Las10] Jean B. Lasserre. *Moments, Positive Polynomials and Their Applications.* Imperial College Press, 2010.

[Löf04] J. Löfberg. Yalmip : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[Löf11] Johan Löfberg. Strictly feasible sum-of-squares solutions. URL, February 2011.

[NG00] M. Neubauer and G. Gunther. Aircraft Loads. Technical Report November, Daimler-Chrysler Aerospace GmbH, 2000.

[NK11] Bonnie Jonkman Neil Kelley. *NWTC Design Codes: TurbSim (03-February-2011)*, 2011.

[NRE11] NREL. http://www.nrel.gov/, 2011.

[Oli05] Imre P Olik. Addendum to the sedumi user guide version 1.1. Technical Report 11, SeDuMi, 2005.

[Pan10] Rohit Pandita. *Dynamic Flight Envelope Assessment with Flight Safety Applications.* PhD thesis, University of Minnesota, 2010.

[Par03] Pablo A Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming*, 96(2):293–320, May 2003.

[Per00] Lawrence Perko. *Differential Equations and Dynamical Systems.* Springer, 3. edition edition, 2000.

[PJP04] Stephen Prajna, A. Jadbabaie, and G.J. Pappas. Stochastic safety verification using barrier certificates. *2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601)*, pages 929–934 Vol.1, 2004.

[PJP07] Stephen Prajna, Ali Jadbabaie, and George J. Pappas. A Framework for Worst-Case and Stochastic Safety Verification Using Barrier Certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, August 2007.

[PP05] Antonis Papachristodoulou and Stephen Prajna. A Tutorial on Sum of Squares Techniques for Systems Analysis. *Control*, pages 2686–2700, 2005.

[Pra06] Stephen Prajna. Barrier Certificates for Nonlinear Model Validation. *Automatica*, 42(1):117–126, January 2006.

[Put93] Mihai Putinar. Positive Polynomials on Compact Semi-Algebraic Sets. *Indiana University Mathematics Journal*, 42(3):13, 1993.

[SPW12] Christoffer Sloth, George J. Pappas, and Rafael Wisniewski. Compositional safety analysis using barrier certificates. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, HSCC '12, pages 15–24, New York, NY, USA, 2012. ACM.

[SSE08] G A Shah, C Sonntag, and S Engell. A Barrier Certificate Approach to the Verification of the Safe Operation of a Chemical Reactor. *Proceedings of the 17th World Congress*, 17(1):6932–6937, 2008.

[STCS98] Palle Andersen Steen Tøffner-Clausen and Jakob Stoustrup. Robust procesregulering, October 1998. ISSN 0908-1208, 3. edition.

[Ste74] Gilbert Stengle. A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Mathematische Annalen*, 207(2):87–97, 1974.

[SW04] Carsten Scherer and Siep Weiland. *Linear Matrix Inequalities in Control.* Lecture Notes, 2004.

[SWBB11] Mohsen Soltani, Rafael Wisniewski, Per Brath, and Stephen Boyd. Load Reduction of Wind Turbines Using Receding Horizon Control. *Proceedings IEEE Multi-Conference on Systems and Control*, CCA 2011(1):pages 852–857, 2011.

[TGKP04] Daniel J Trudnowski, Andrew Gentile, Jawad M Khan, and Eric M Petritz. Fixed-Speed Wind-Generator and Wind-Park Modeling for Transient Stability Studies. *Power*, 19(4):1911–1917, 2004.

[TPM09] Ufuk Topcu, Andrew K. Packard, and Richard M. Murray. Compositional stability analysis based on dual decomposition. *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, pages 1175–1180, December 2009.

[WWE10] WWEC. World Wind Energy Report 2010. *October*, 2010.

[Zac03] Zachary William Jarvis-Wloszek. *Lyapunov Based Analysis and Controller Synthesis for Polynomial Systems using Sum-of-Squares Optimization.* PhD thesis, University of California, Berkeley, 2003.

Emergency Shutdown Trigger A

In this appendix the tower top displacement and velocity trajectory illustrated in the right plot in Figure 4.3, is given as a function of time.

The tower top displacement and tower top velocity during the safe emergency shutdown trigger are illustrated in Figure A.1. The safe emergency shutdown trigger is given by red dashed lines.

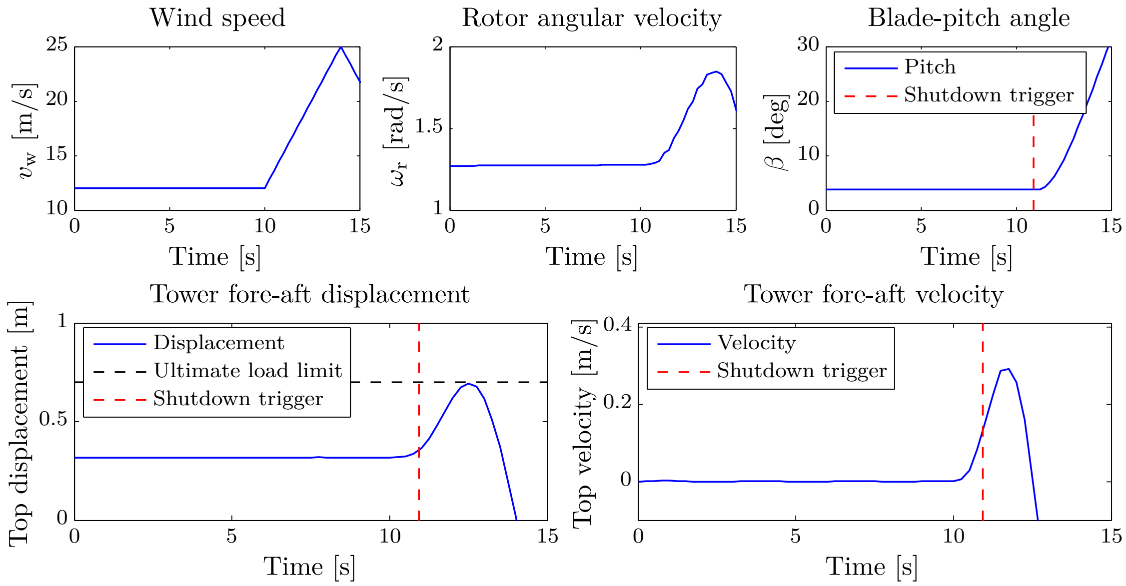


Figure A.1: *Simulation of emergency shutdown trigger. The top plots show the horizontal hub height wind speed, rotor angular velocity and blade-pitch angle respectively. The bottom left plot shows the displacement of the tower top. The bottom right plot shows the velocity of the tower top. The black and red dashed lines indicate the ultimate load limit and the emergency shutdown trigger time respectively.*

From Figure A.1 it can be seen that the ultimate load limit of the tower is not exceeded. The chosen multivariate emergency shutdown trigger manages to keep the tower safe during the increase in wind speed. It should be noted that this emergency shutdown trigger is not guaranteed to keep the system safe in general.

B Aerodynamic Table Approximation

In this appendix the polynomial approximations of C_t and C_q tables can be found. The results are presented in Section 6.3.

The C_t and C_q lookup tables takes 3 inputs, the wind speed v_w, the rotor angular velocity ω_r and the blade-pitch angle β. The output of the tables are the thrust C_t and torque C_q coefficients respectively.

In Section 6.3 the lookup tables are approximated by a range of polynomials with different order. The approximations are done using linear least squares. Least squares can be used in the approximation as the approximation problem is linear in the coefficients.

The number of free coefficients in the approximation is depending on the order of the polynomial and the number of variables. The total number of coefficients can be found using

$$c_\mathrm{tot} = \binom{2d+m}{2d} = \frac{(2d+m)!}{2d!m!}, \tag{B.1}$$

where m is the number of variables and $n = 2d$ is the order of the polynomial [Par03]. Each coefficient is multiplied by a monomial with order equal to or less than the order of the polynomial. In Figure B.1 the number of coefficients is plotted with growing polynomial order and 3 variables.

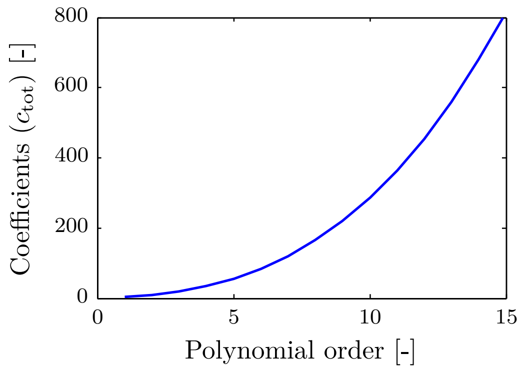


Figure B.1: *The number of coefficients in a n-order polynomial with 3 variables.*

Below the approximation of a 2$^\mathrm{nd}$ order polynomial to a lookup table is be given. As the polynomial order is 2 and the number of variables is 3, the total number of coefficients to be found is using (B.1) found to $c_\mathrm{tot} = 10$.

The i points $(C_{\mathrm{x},i}, v_{\mathrm{w},i}, \omega_{\mathrm{r},i}, \beta_i)$ in the lookup table are inserted in the polynomial structure. Given a 2$^\mathrm{nd}$ order polynomial structure with 10 coefficients and i lookup table points, the i polynomials can be written as

$$\begin{aligned}
C_{\mathrm{x},1} &= c_1 v_{\mathrm{w},1}^2 + c_2 \omega_{\mathrm{r},1}^2 + c_3 \beta_1^2 + c_4 v_{\mathrm{w},1}\omega_{\mathrm{r},1} + c_5 v_{\mathrm{w},1}\beta_1 + c_6 \omega_{\mathrm{r},1}\beta_1 + c_7 v_{\mathrm{w},1} + c_8 \omega_{\mathrm{r},1} + c_9 \beta_1 + c_{10} \\
C_{\mathrm{x},2} &= c_1 v_{\mathrm{w},2}^2 + c_2 \omega_{\mathrm{r},2}^2 + c_3 \beta_2^2 + c_4 v_{\mathrm{w},2}\omega_{\mathrm{r},2} + c_5 v_{\mathrm{w},2}\beta_2 + c_6 \omega_{\mathrm{r},2}\beta_2 + c_7 v_{\mathrm{w},2} + c_8 \omega_{\mathrm{r},2} + c_9 \beta_2 + c_{10} \\
&\vdots \\
C_{\mathrm{x},i} &= c_1 v_{\mathrm{w},i}^2 + c_2 \omega_{\mathrm{r},i}^2 + c_3 \beta_i^2 + c_4 v_{\mathrm{w},i}\omega_{\mathrm{r},i} + c_5 v_{\mathrm{w},i}\beta_i + c_6 \omega_{\mathrm{r},i}\beta_i + c_7 v_{\mathrm{w},i} + c_8 \omega_{\mathrm{r},i} + c_9 \beta_i + c_{10}.
\end{aligned} \tag{B.2}$$

The i polynomials in (B.2), can be written as a linear system

$$\begin{bmatrix} C_{\mathrm{x},1} \\ C_{\mathrm{x},2} \\ \vdots \\ C_{\mathrm{x},i} \end{bmatrix} = \begin{bmatrix} v_{\mathrm{w},1}^2 & \omega_{\mathrm{r},1}^2 & \beta_1^3 & v_{\mathrm{w},1}\omega_{\mathrm{r},1} & v_{\mathrm{w},1}\beta_1 & \omega_{\mathrm{r},1}\beta_1 & v_{\mathrm{w},1} & \omega_{\mathrm{r},1} & \beta_1 & 1 \\ v_{\mathrm{w},2}^2 & \omega_{\mathrm{r},2}^2 & \beta_2^3 & v_{\mathrm{w},2}\omega_{\mathrm{r},2} & v_{\mathrm{w},2}\beta_2 & \omega_{\mathrm{r},2}\beta_2 & v_{\mathrm{w},2} & \omega_{\mathrm{r},2} & \beta_2 & 1 \\ \vdots \\ v_{\mathrm{w},i}^2 & \omega_{\mathrm{r},i}^2 & \beta_i^3 & v_{\mathrm{w},i}\omega_{\mathrm{r},i} & v_{\mathrm{w},i}\beta_i & \omega_{\mathrm{r},i}\beta_i & v_{\mathrm{w},i} & \omega_{\mathrm{r},i} & \beta_i & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \\ c_9 \\ c_{10} \end{bmatrix}.$$

The coefficients of the overdetermined system can be approximated using linear least squares, given as

$$\mathbf{A}^{\dagger}_{(\mathrm{v_w},\omega_\mathrm{r},\beta)}\mathbf{c}_\mathrm{x} = \mathbf{c}, \tag{B.3}$$

where $\mathbf{A}_{(\mathrm{v_w},\omega_\mathrm{r},\beta)}$ is the matrix containing the input values, $\mathbf{c}_\mathrm{x}$ is the vector of output values and $\mathbf{c}$ is the vector of unknown coefficients.

The least squares solution to (B.3) is found using `MATLAB`. The script used in Section 6.3 in the approximation of C_t and C_q with a range of different polynomial orders, can be found on the enclosed DVD.

Results of the least squares approximation are illustrated in Figure 6.7 and 6.8 in Section 6.3.

C Drive Train Calculations

In this appendix the calculations done in the design of the drive train model can be found. Details about the modelling of the drive train can be found in Section 6.4.1.

The drive train system is given by the following equations

$$J_{\mathrm{r}}\dot{\omega}_{\mathrm{r}} = \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \tau_{\mathrm{a}_1}, \tag{C.1}$$
$$J_{\mathrm{g}}\dot{\omega}_{\mathrm{g}} = \tau_{\mathrm{a}_2} - B_{\mathrm{g}}\omega_{\mathrm{g}} - \tau_{\mathrm{g}}. \tag{C.2}$$

The torques delivered by the shafts are given as

$$\tau_{\mathrm{a}_1} = K_{\mathrm{a}_1}(\theta_{\mathrm{r}} - \theta_{\mathrm{n}_1}) + B_{\mathrm{a}_1}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}), \tag{C.3}$$
$$\tau_{\mathrm{a}_2} = K_{\mathrm{a}_2}\left(\frac{\theta_{\mathrm{n}_1}}{N} - \theta_{\mathrm{g}}\right). \tag{C.4}$$

The sum of the torques through the gear equals zero. The angle of the of the gearbox (θ_{n_1} in Figure 6.10) is found by

$$\begin{aligned} K_{\mathrm{a}_1}(\theta_{\mathrm{r}} - \theta_{\mathrm{n}_1}) + B_{\mathrm{a}_1}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}) &= \left(K_{\mathrm{a}_2}\left(\frac{\theta_{\mathrm{n}_1}}{N} - \theta_{\mathrm{g}}\right)\right)\frac{1}{N} \Leftrightarrow \\ \theta_{\mathrm{n}_1} &= \frac{N(K_{\mathrm{a}_1}N\theta_{\mathrm{r}} + K_{\mathrm{a}_2}\theta_{\mathrm{g}} + B_{\mathrm{a}_1}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}))}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}. \end{aligned} \tag{C.5}$$

The torque τ_{a_1} given in (C.3) is substituted into (C.1)

$$J_{\mathrm{r}}\dot{\omega}_{\mathrm{r}} = \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \left[K_{\mathrm{a}_1}(\theta_{\mathrm{r}} - \theta_{\mathrm{n}_1}) + B_{\mathrm{a}_1}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})\right]. \tag{C.6}$$

The angle of the gearbox θ_{n_1} in (C.5) is substituted into (C.6)

$$\begin{aligned} J_{\mathrm{r}}\dot{\omega}_{\mathrm{r}} =& \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \left\{K_{\mathrm{a}_1}\left[\theta_{\mathrm{r}} - \left(\frac{N(K_{\mathrm{a}_1}N\theta_{\mathrm{r}} + K_{\mathrm{a}_2}\theta_{\mathrm{g}} + B_{\mathrm{a}_1}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}))}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}\right)\right] + B_{\mathrm{a}_1}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})\right\} \\ =& \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \left[\frac{K_{\mathrm{a}_1}\theta_{\mathrm{r}}(K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2})}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}} - \frac{K_{\mathrm{a}_1}^2N^2\theta_{\mathrm{r}} + K_{\mathrm{a}_1}K_{\mathrm{a}_2}\theta_{\mathrm{g}}N + K_{\mathrm{a}_1}B_{\mathrm{a}_1}N^2(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}\right] \\ &- \frac{B_{\mathrm{a}_1}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})(K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2})}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}} \\ =& \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_1}(\theta_{\mathrm{r}} - N\theta_{\mathrm{g}}) + B_{\mathrm{a}_1}K_{\mathrm{a}_1}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}} \\ =& \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}(\theta_{\mathrm{r}} - N\theta_{\mathrm{g}}) - \frac{B_{\mathrm{a}_1}K_{\mathrm{a}_1}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}). \end{aligned} \tag{C.7}$$

The torque τ_{a_2} in (C.4) is substituted into (C.2)

$$J_{\mathrm{g}}\dot{\omega}_{\mathrm{g}} = K_{\mathrm{a}_2}\left(\frac{\theta_{\mathrm{n}_1}}{N} - \theta_{\mathrm{g}}\right) - B_{\mathrm{g}}\omega_{\mathrm{g}} - \tau_{\mathrm{g}}. \tag{C.8}$$

The angle of the gearbox θ_{n_1} in (C.5) is substituted into (C.8)

$$\begin{aligned}
J_{\mathrm{g}}\dot{\omega}_{\mathrm{g}} &= K_{\mathrm{a}_2}\left(\frac{1}{N}\left(\frac{N(K_{\mathrm{a}_1}N\theta_{\mathrm{r}} + K_{\mathrm{a}_2}\theta_{\mathrm{g}} + B_{\mathrm{a}_1}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}))}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}\right) - \theta_{\mathrm{g}}\right) - B_{\mathrm{g}}\omega_{\mathrm{g}} - \tau_{\mathrm{g}} \\
&= \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}N(\theta_{\mathrm{r}} - N\theta_{\mathrm{g}}) + B_{\mathrm{a}_1}K_{\mathrm{a}_2}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}} - B_{\mathrm{g}}\omega_{\mathrm{g}} - \tau_{\mathrm{g}} \\
&= \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}N(\theta_{\mathrm{r}} - N\theta_{\mathrm{g}}) + \frac{B_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}) - B_{\mathrm{g}}\omega_{\mathrm{g}} - \tau_{\mathrm{g}}. \qquad \text{(C.9)}
\end{aligned}$$

Identical constant terms are found in both (C.7) and (C.9). These are collected into new constants given as

$$K_{\mathrm{a}} \triangleq \frac{K_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}, \qquad \text{(C.10)}$$

$$B_{\mathrm{a}} \triangleq \frac{B_{\mathrm{a}_1}K_{\mathrm{a}_2}}{K_{\mathrm{a}_1}N^2 + K_{\mathrm{a}_2}}. \qquad \text{(C.11)}$$

The new constants (C.10) and (C.11) are substituted into (C.7) and (C.9), resulting in the following system equations

$$\begin{aligned}
J_{\mathrm{r}}\dot{\omega}_{\mathrm{r}} &= \tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - K_{\mathrm{a}}(\theta_{\mathrm{r}} - N\theta_{\mathrm{g}}) - B_{\mathrm{a}}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}), \\
J_{\mathrm{g}}\dot{\omega}_{\mathrm{g}} &= K_{\mathrm{a}}N(\theta_{\mathrm{r}} - N\theta_{\mathrm{g}}) + B_{\mathrm{a}}N(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}}) - B_{\mathrm{g}}\omega_{\mathrm{g}} - \tau_{\mathrm{g}}.
\end{aligned}$$

The above calculations are used in the modelling of the wind turbine drive train described in Section 6.4.1.

D Blade-Pitch Model Calculations

In this appendix the calculations done in the design of the blade-pitch model can be found. The calculations are done partly using `MATLAB`.

The original system is in symbolic form given as

$$\mathbf{A}_{\text{pitch}} = \begin{bmatrix} -a_{1,\beta} & -a_{2,\beta} \\ 1 & 0 \end{bmatrix}.$$

The eigenvectors of the system are found to be

$$\mathbf{P} = [\mathbf{v}_1, \mathbf{v}_2] = \begin{bmatrix} -\frac{\mathrm{a}_{1,\beta}}{2} - \frac{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}{2} & \frac{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}{2} - \frac{\mathrm{a}_{1,\beta}}{2} \\ 1 & 1 \end{bmatrix}.$$

The decoupled system $\tilde{\mathbf{A}}_{\text{pitch}}$ is found using the above state transformation,

$$\tilde{\mathbf{A}}_{\text{pitch}} = \mathbf{P}^{-1}\mathbf{A}_{\text{pitch}}\mathbf{P}$$

$$= \begin{bmatrix} -\frac{1}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} & \frac{1}{2} - \frac{\mathrm{a}_{1,\beta}}{2\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} \\ \frac{1}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} & \frac{\mathrm{a}_{1,\beta}}{2\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} + \frac{1}{2} \end{bmatrix} \begin{bmatrix} -a_{1,\beta} & -a_{2,\beta} \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -\frac{\mathrm{a}_{1,\beta}}{2} - \frac{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}{2} & \frac{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}{2} - \frac{\mathrm{a}_{1,\beta}}{2} \\ 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{2\,\mathrm{a}_{2,\beta}}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} - \frac{\mathrm{a}_{1,\beta}}{2} - \frac{\mathrm{a}_{1,\beta}{}^2}{2\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} & 0 \\ 0 & \frac{\mathrm{a}_{1,\beta}{}^2}{2\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} - \frac{2\,\mathrm{a}_{2,\beta}}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}} - \frac{\mathrm{a}_{1,\beta}}{2} \end{bmatrix}.$$

As the transformed system $\tilde{\mathbf{A}}_{\text{pitch}}$ is now decoupled, the solutions to the first order differential equations can be found directly. By using the invers transformation, the solution to the original system is found

$$\begin{bmatrix} \omega_\beta(t) \\ \theta_\beta(t) \end{bmatrix} = \mathbf{P} \begin{bmatrix} e^{\tilde{\mathbf{A}}_{\text{pitch}}(1,1)t} & 0 \\ 0 & e^{\tilde{\mathbf{A}}_{\text{pitch}}(2,2)t} \end{bmatrix} \mathbf{P}^{-1} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

The initial conditions are given by c_1 and c_2. The initial conditions is set to $c_1 = 0$ and $c_2 = 90$.

$$\omega_\beta(t) = -\frac{90\,\mathrm{a}_{2,\beta}\left(\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}{}^2\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}} - \mathrm{e}^{\frac{4\,\mathrm{a}_{2,\beta}\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}}\right)}{\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}\,t}{2}}\,\mathrm{e}^{\frac{2\,\mathrm{a}_{2,\beta}\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}}\,\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}{}^2\,t}{2\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}}\sqrt{\mathrm{a}_{1,\beta}{}^2 - 4\,\mathrm{a}_{2,\beta}}}$$

$$\theta_\beta(t) =$$
$$45\left(\mathrm{e}^{\frac{4\,\mathrm{a}_{2,\beta}\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}}}\,\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}-\mathrm{a}_{1,\beta}\,\mathrm{e}^{\frac{4\,\mathrm{a}_{2,\beta}\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}}}+\right.$$
$$\left.\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}{}^2\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}}}\,\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}+\mathrm{a}_{1,\beta}\,\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}{}^2\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}}}\right)$$
$$\left(\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}\,t}{2}}\,\mathrm{e}^{\frac{2\,\mathrm{a}_{2,\beta}\,t}{\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}}}\,\mathrm{e}^{\frac{\mathrm{a}_{1,\beta}{}^2\,t}{2\,\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}}}\,\sqrt{\mathrm{a}_{1,\beta}{}^2-4\,\mathrm{a}_{2,\beta}}\right)^{-1} \tag{D.1}$$

The time $t = 5.625$ and the solution $\theta_\beta(t) = 45$ is substituted into (D.1). The value of the constant $a_{1,\beta}$ is iteratively found, and inserted into (D.1), such that the resulting system yields real eigenvalues. In (D.2) $a_{1,\beta} = 0.6$.

$$0 =$$
$$\frac{\mathrm{e}^{\frac{11.3\,\mathrm{a}_{2,\beta}}{\sqrt{0.4-4.0\,\mathrm{a}_{2,\beta}}}-\frac{1.0}{\sqrt{0.4-4.0\,\mathrm{a}_{2,\beta}}}-1.7}\,\left(45.0\,\sqrt{0.4-4.0\,\mathrm{a}_{2,\beta}}-27.0\right)}{\sqrt{0.36-4.0\,\mathrm{a}_{2,\beta}}}+$$
$$\frac{\mathrm{e}^{\frac{1.0}{\sqrt{0.4-4.0\,\mathrm{a}_{2,\beta}}}-\frac{11.3\,\mathrm{a}_{2,\beta}}{\sqrt{0.36-4.0\,\mathrm{a}_{2,\beta}}}-1.7}\,\left(45.0\,\sqrt{0.4-4.0\,\mathrm{a}_{2,\beta}}+27.0\right)}{\sqrt{0.36-4.0\,\mathrm{a}_{2,\beta}}}-45.0 \tag{D.2}$$

Equation (D.2) is solved using `MATLAB`, resulting in $a_{2,\beta} = 0.089$.

The constants $a_{1,\beta}$ and $a_{2,\beta}$ are inserted into the original system

$$\begin{bmatrix}\dot{\omega}_\beta\\ \dot{\theta}_\beta\end{bmatrix} = \begin{bmatrix}-0.6 & -0.0894\\ 1 & 0\end{bmatrix}\begin{bmatrix}\omega_\beta\\ \theta\beta\end{bmatrix}. \tag{D.3}$$

The eigenvalues of the system in (D.3) are $\lambda = [-0.3250 - 0.2750]^{\mathrm{T}}$.

The system in (D.3) is designed such that the blade-pitch angle goes from some value to zero. During an emergency shutdown, the angle will go to 90°. To obtain this an output equation is designed

$$\beta = -\theta_\beta + 90.$$

A simulation of the system can be found in Figure 6.23b on Page 47.

E Model Composition

In this appendix the composition of the model subsystems will be done. In Section 6.7 the final model is presented. The model subsystems are developed in Chapter 6.

The model subsystems include:

- Drive train
- Flapwise blade bending
- Lead-lag blade bending
- Tower
- Blade-pitch actuator system
- Wind Model

The model subsystems should be assembled into one complete state space model. To do this, the model equations must only be dependent on states, inputs and disturbances. In the following each subsystem will be made ready for the final composition. This is done by substitution and rearranging of the equations.

Drive train

The drive train model equations from Section 6.4.1 are given as

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

with τ_g as input. The term τ_r is given in Equation (6.24) as $\tau_\mathrm{r} = \tau_\mathrm{aero}(1-\xi_\mathrm{LL}) + {K_\mathrm{LL}}^\mathrm{h}\theta_\mathrm{LL,x}$. Substitution by τ_r gives

$$\begin{aligned}
\dot{\omega}_\mathrm{r} &= J_\mathrm{r}^{-1}\left[\tau_\mathrm{aero}(1-\xi_\mathrm{LL}) + {K_\mathrm{LL}}^\mathrm{h}\theta_\mathrm{LL,x} - B_\mathrm{r}\omega_\mathrm{r} - K_\mathrm{a}\theta_\Delta - B_\mathrm{a}(\omega_\mathrm{r} - N\omega_\mathrm{g})\right],\\
\dot{\omega}_\mathrm{g} &= J_\mathrm{g}^{-1}\left[K_\mathrm{a}N\theta_\Delta + B_\mathrm{a}N(\omega_\mathrm{r} - N\omega_\mathrm{g}) - B_\mathrm{g}\omega_\mathrm{g} - \tau_\mathrm{g}\right],\\
\dot{\theta}_\Delta &= \omega_\mathrm{r} - N\omega_\mathrm{g}.
\end{aligned}$$

The drive train equations are expanded and simplified to

$$\begin{aligned}
\dot{\omega}_\mathrm{r} &= \frac{1-\xi_\mathrm{LL}}{J_\mathrm{r}}\tau_\mathrm{aero} + \frac{K_\mathrm{LL}}{J_\mathrm{r}}^\mathrm{h}\theta_\mathrm{LL,x} + \frac{B_\mathrm{a}N}{J_\mathrm{r}}\omega_\mathrm{g} - \frac{B_\mathrm{r}+B_\mathrm{a}}{J_\mathrm{r}}\omega_\mathrm{r} - \frac{K_\mathrm{a}}{J_\mathrm{r}}\theta_\Delta,\\
\dot{\omega}_\mathrm{g} &= \frac{K_\mathrm{a}N}{J_\mathrm{g}}\theta_\Delta + \frac{B_\mathrm{a}N}{J_\mathrm{g}}\omega_\mathrm{r} - \frac{B_\mathrm{a}N^2+B_g}{J_\mathrm{g}}\omega_\mathrm{g} - \frac{1}{J_\mathrm{g}}\tau_\mathrm{g},\\
\dot{\theta}_\Delta &= \omega_\mathrm{r} - N\omega_\mathrm{g},
\end{aligned}$$

where τ_aero is input from the aerodynamic model and τ_g is an external input.

Flapwise blade bending

The flapwise blade bending model equations given in (6.23) are given as

$$\begin{aligned} {}^{\mathrm{h}}\dot{v}_{\mathrm{flap,x}} &= M_{\mathrm{flap}}^{-1}\left[F_{\mathrm{aero}}\xi_{\mathrm{flap}} - K_{\mathrm{flap}}{}^{\mathrm{h}}x_{\mathrm{flap}} - B_{\mathrm{flap}}{}^{\mathrm{h}}v_{\mathrm{flap,x}}\right] - {}^{\mathrm{t}}\dot{v}_{\mathrm{fa,x}}, \\ {}^{\mathrm{h}}\dot{x}_{\mathrm{flap}} &= {}^{\mathrm{h}}v_{\mathrm{flap,x}}, \end{aligned} \tag{E.1}$$

with external input F_{aero} and the term ${}^{\mathrm{t}}\dot{v}_{\mathrm{fa,x}}$ from the tower equations. The term ${}^{\mathrm{t}}\dot{v}_{\mathrm{fa,x}}$ can be found from Equation (6.27) to

$$ {}^{\mathrm{t}}\dot{v}_{\mathrm{fa,x}} = L{}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} = (M_{\mathrm{n}}L)^{-1}\left[F_{\mathrm{r}}L + F_{\mathrm{g}}L{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - K_{\mathrm{fa}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - B_{\mathrm{fa}}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}\right], $$

with F_{r} given in Equation (6.20) to

$$ F_{\mathrm{r}} = F_{\mathrm{aero}}(1-\xi_{\mathrm{flap}}) + K_{\mathrm{flap}}{}^{\mathrm{h}}x_{\mathrm{flap}}. $$

The terms are substituted into (E.1)

$$\begin{aligned} {}^{\mathrm{h}}\dot{v}_{\mathrm{flap,x}} &= M_{\mathrm{flap}}^{-1}\left[F_{\mathrm{aero}}\xi_{\mathrm{flap}} - K_{\mathrm{flap}}{}^{\mathrm{h}}x_{\mathrm{flap}} - B_{\mathrm{flap}}{}^{\mathrm{h}}v_{\mathrm{flap,x}}\right] \\ &\quad - (M_{\mathrm{n}}L)^{-1}\left[(F_{\mathrm{aero}}(1-\xi_{\mathrm{flap}}) + K_{\mathrm{flap}}{}^{\mathrm{h}}x_{\mathrm{flap}})L + F_{\mathrm{g}}L{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - K_{\mathrm{fa}}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - B_{\mathrm{fa}}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}\right], \\ {}^{\mathrm{h}}\dot{x}_{\mathrm{flap}} &= {}^{\mathrm{h}}v_{\mathrm{flap,x}}. \end{aligned}$$

The flapwise bending equations are expanded and simplified to

$$\begin{aligned} {}^{\mathrm{h}}\dot{v}_{\mathrm{flap,x}} &= \frac{\xi_{\mathrm{flap}}(M_{\mathrm{n}} + M_{\mathrm{flap}}) - M_{\mathrm{flap}}}{M_{\mathrm{flap}}M_{\mathrm{n}}}F_{\mathrm{aero}} - \frac{K_{\mathrm{flap}}(M_{\mathrm{n}} + M_{\mathrm{flap}})}{M_{\mathrm{flap}}M_{\mathrm{n}}}{}^{\mathrm{h}}x_{\mathrm{flap}} - \frac{B_{\mathrm{flap}}}{M_{\mathrm{flap}}}{}^{\mathrm{h}}v_{\mathrm{flap,x}} \\ &\quad - \frac{F_{\mathrm{g}}L - K_{\mathrm{fa}}}{M_{\mathrm{n}}L}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} + \frac{B_{\mathrm{fa}}}{M_{\mathrm{n}}L}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}, \\ {}^{\mathrm{h}}\dot{x}_{\mathrm{flap}} &= {}^{\mathrm{h}}v_{\mathrm{flap,x}}, \end{aligned}$$

where F_{aero} is given by the nonlinear aerodynamic model.

Lead-lag blade bending

The lead-lag blade bending model equations in (6.25) are given as

$$\begin{aligned} {}^{\mathrm{h}}\dot{\omega}_{\mathrm{LL,x}} &= J_{\mathrm{LL}}^{-1}\left[\tau_{\mathrm{aero}}\xi_{\mathrm{LL}} - B_{\mathrm{LL}}{}^{\mathrm{h}}\omega_{\mathrm{LL,x}} - K_{\mathrm{LL}}{}^{\mathrm{h}}\theta_{\mathrm{LL,x}}\right] - \dot{\omega}_{\mathrm{r}}, \\ {}^{\mathrm{h}}\dot{\theta}_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\omega_{\mathrm{LL,x}}, \end{aligned} \tag{E.2}$$

with the term τ_{aero} from the aerodynamic model and $\dot{\omega}_{\mathrm{r}}$ from the drive train equations. The term

$$ \dot{\omega}_{\mathrm{r}} = J_{\mathrm{r}}^{-1}\left[\tau_{\mathrm{r}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - K_{\mathrm{a}}\theta_{\Delta} - B_{\mathrm{a}}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})\right], $$

given in (6.19) is substituted into (E.2), giving

$$\begin{aligned} {}^{\mathrm{h}}\dot{\omega}_{\mathrm{LL,x}} &= J_{\mathrm{LL}}^{-1}\left[\tau_{\mathrm{aero}}\xi_{\mathrm{LL}} - B_{\mathrm{LL}}{}^{\mathrm{h}}\omega_{\mathrm{LL,x}} - K_{\mathrm{LL}}{}^{\mathrm{h}}\theta_{\mathrm{LL,x}}\right] \\ &\quad - J_{\mathrm{r}}^{-1}\left[\tau_{\mathrm{aero}}(1-\xi_{\mathrm{LL}}) + K_{\mathrm{LL}},{}^{\mathrm{h}}\theta_{\mathrm{LL,x}} - B_{\mathrm{r}}\omega_{\mathrm{r}} - K_{\mathrm{a}}\theta_{\Delta} - B_{\mathrm{a}}(\omega_{\mathrm{r}} - N\omega_{\mathrm{g}})\right], \\ {}^{\mathrm{h}}\dot{\theta}_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\omega_{\mathrm{LL,x}}. \end{aligned}$$

The lead-lag bending equations are expanded and simplified to

$$\begin{aligned} {}^{\mathrm{h}}\dot{\omega}_{\mathrm{LL,x}} &= \frac{\xi_{\mathrm{LL}}(J_{\mathrm{r}} + J_{\mathrm{LL}}) - J_{\mathrm{LL}}}{J_{\mathrm{r}}J_{\mathrm{LL}}}\tau_{\mathrm{aero}} - \frac{B_{\mathrm{LL}}}{J_{\mathrm{LL}}}{}^{\mathrm{h}}\omega_{\mathrm{LL,x}} - \frac{K_{\mathrm{LL}}(J_{\mathrm{r}} + J_{\mathrm{LL}})}{J_{\mathrm{r}}J_{\mathrm{LL}}}{}^{\mathrm{h}}\theta_{\mathrm{LL,x}} \\ &\quad + \frac{B_{\mathrm{r}} + B_{\mathrm{a}}}{J_{\mathrm{r}}}\omega_{\mathrm{r}} + \frac{K_{\mathrm{a}}}{J_{\mathrm{r}}}\theta_{\Delta} - \frac{B_{\mathrm{a}}N}{J_{\mathrm{r}}}\omega_{\mathrm{g}}, \\ {}^{\mathrm{h}}\dot{\theta}_{\mathrm{LL,x}} &= {}^{\mathrm{h}}\omega_{\mathrm{LL,x}}, \end{aligned}$$

where τ_{aero} is input from the nonlinear aerodynamic model.

Tower

The tower model equations in (6.27) are given as

$$\begin{aligned}
{}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} &= (M_{\mathrm{n}}L^2)^{-1}\left[F_{\mathrm{r}}L + F_{\mathrm{g}}L\,{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - K_{\mathrm{fa}}\,{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - B_{\mathrm{fa}}\,{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}\right],\\
{}^{\mathrm{t}}\dot{\theta}_{\mathrm{fa,y}} &= {}^{\mathrm{t}}\omega_{\mathrm{fa,y}},
\end{aligned}$$

with F_{r} given in Equation (6.20) to

$$F_{\mathrm{r}} = F_{\mathrm{aero}}(1-\xi_{\mathrm{flap}}) + K_{\mathrm{flap}}\,{}^{\mathrm{h}}x_{\mathrm{flap}}.$$

Substitution by F_{r} gives

$$\begin{aligned}
{}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} &= (M_{\mathrm{n}}L^2)^{-1}\left[(F_{\mathrm{aero}}(1-\xi_{\mathrm{flap}}) + K_{\mathrm{flap}}\,{}^{\mathrm{h}}x_{\mathrm{flap}})L + F_{\mathrm{g}}L\,{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - K_{\mathrm{fa}}\,{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - B_{\mathrm{fa}}\,{}^{\mathrm{t}}\omega_{\mathrm{fa,y}}\right],\\
{}^{\mathrm{t}}\dot{\theta}_{\mathrm{fa,y}} &= {}^{\mathrm{t}}\omega_{\mathrm{fa,y}}.
\end{aligned}$$

The tower equations are expanded and simplified to

$$\begin{aligned}
{}^{\mathrm{t}}\dot{\omega}_{\mathrm{fa,y}} &= \frac{(1-\xi_{\mathrm{flap}})}{M_{\mathrm{n}}L}F_{\mathrm{aero}} + \frac{K_{\mathrm{flap}}}{M_{\mathrm{n}}L}{}^{\mathrm{h}}x_{\mathrm{flap}} + \frac{F_{\mathrm{g}}L - K_{\mathrm{fa}}}{M_{\mathrm{n}}L^2}{}^{\mathrm{t}}\theta_{\mathrm{fa,y}} - \frac{B_{\mathrm{fa}}}{M_{\mathrm{n}}L^2}{}^{\mathrm{t}}\omega_{\mathrm{fa,y}},\\
{}^{\mathrm{t}}\dot{\theta}_{\mathrm{fa,y}} &= {}^{\mathrm{t}}\omega_{\mathrm{fa,y}},
\end{aligned}$$

where F_{r} is input from the nonlinear aerodynamic model and flapwise blade bending.

Blade-pitch actuator system

The blade-pitch model is in (6.29) given as

$$\begin{aligned}
\dot{\omega}_{\beta} &= -0.6\omega_{\beta} - 0.0894\theta_{\beta},\\
\dot{\theta}_{\beta} &= \omega_{\beta}.
\end{aligned}$$

The blade-pitch model is in linear form, and only dependent on states. Consequently, the model can directly be inserted into the final model of the wind turbine.

Wind Model

The wind model is in (6.32) given as

$$\begin{aligned}
\dot{v}_{\mathrm{w,t1}} &= -0.4167v_{\mathrm{w,t1}} - 0.2222v_{\mathrm{w,t2}} + 2w\\
\dot{v}_{\mathrm{w,t2}} &= 0.1250v_{\mathrm{w,t1}}
\end{aligned}$$

The wind model is in linear form, and only dependent on states. Consequently, the model can directly be inserted into the final model of the wind turbine.

The subsystems are now dependent on either states or nonlinear terms. The final model is given in Section 6.7 on Page 51.

Polynomial Model Validation

F

In this appendix the complete model using polynomial approximations of aerodynamic lookup tables is compared to the model using the original lookup tables directly. The polynomial approximations of the aerodynamic lookup tables are described in Section 6.3 on Page 30. The approximation method is described in Appendix B.

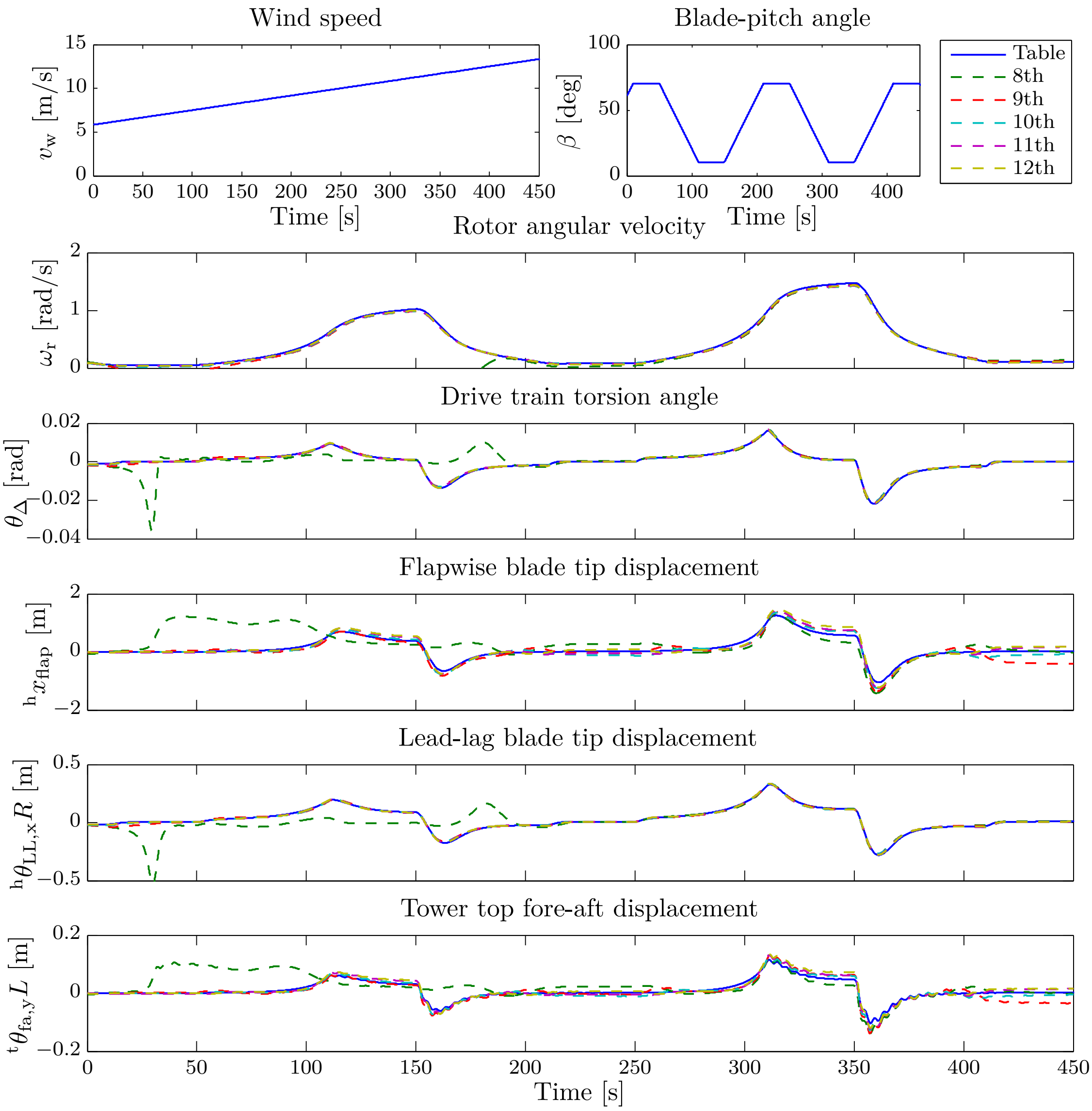


Figure F.1: *Comparison of model simulation using lookup tables and a range of polynomial approximations. The wind speed v_w and pitch angle β are identical in all simulations. Polynomial approximations using 8^{th} to 12^{th} order polynomials are shown. The five lower plots share the time axis given in the last plot.*

The model given in (6.34) on Page 53 is simulated, used a controlled wind speed v_w and blade-pitch angle β (the wind turbulence model and autonomous pitch procedure are not used). The simulation of the model is performed using the original aerodynamic lookup tables as well as a range of polynomial approximations. In Figure F.1 the simulations are compared. The results of the comparison are discussed in Section 6.7 on Page 6.7.

G Normal Operation

Figure G.1 illustrates point clouds of the normal operation simulation using the NREL 5-MW wind turbine with control system activated. The point clouds are projected onto each plane in the state space. As nine states were measured during the simulation, this results in 81 projections.

Figure G.1: *Point cloud projections of the normal operation simulation. Each plot illustrates the point cloud projected onto the given plane. The mean-values of the clouds are marked by red circles. Note that the names of the states have been shortened in order to fit all projections into one page.*

Each projection in Figure G.1 is labelled *[state1,state2]*, with the states being one of the nine states. The first state (*state1*) is given along the x-axis, whereas the second state (*state2*) is given along the y-axis.

Ultimate Load Limits H

In this appendix, the ultimate load limits of the states are illustrated along with the state histograms obtained from the normal operation simulation. The histograms are explained in detail in Section 7.2.

In Figure H.1 the remaining histograms of Section 7.2 are illustrated. The ultimate load limits illustrated are $2x_{0.1\%}$, except from the ultimate load limit of the rotor angular velocity, which has been chosen to $1.5x_{0.1\%}$.

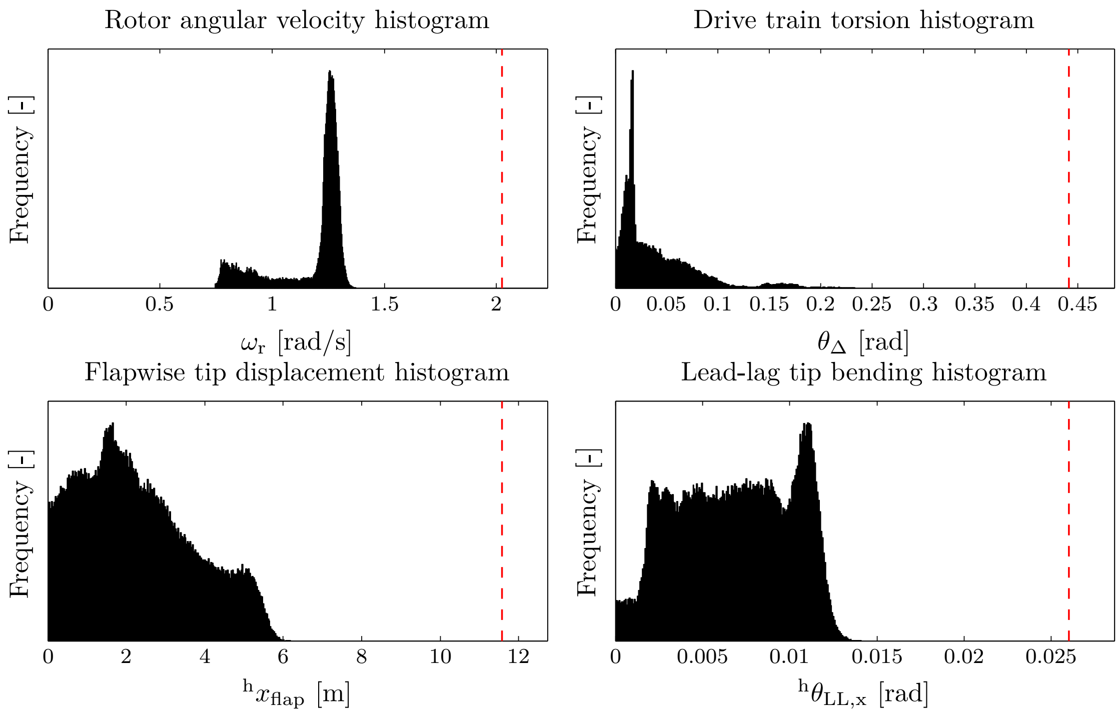


Figure H.1: *Normal operation histograms from the top left the rotor angular velocity, drive train torsion, flapwise blade tip displacement and lead-lag blade tip bending. The red dashed lines illustrate the ultimate load limits.*

The ultimate load limit values are given in Table 7.2 on Page 60.

I Positivstellensatz Example

In this appendix a very simple example of the usage of the Positivstellensatz, described in Section 9.3, is given.

Consider two polynomials given by

$$\begin{aligned} f_1(x_1) &= -x_1^2 - 3x_1 - 1, \\ f_2(x_1) &= -x_1^2 + 3x_1 - 1. \end{aligned} \tag{I.1}$$

A semi-algebraic set defined by the polynomials in (I.1) is given by

$$\mathbb{K} = \left\{ \; x_1 \in \mathbb{R} \; \middle| \; \begin{array}{c} f_1(x_1) \geq 0 \\ f_2(x_1) \geq 0 \end{array} \; \right\} \tag{I.2}$$

The objective is to find if there exist a solution to (I.2) in $\mathbb{R}$.

Using the Positivstellensatz defined in (9.9), this question can be formulated as the existence of a polynomial identity given in (9.10). If this polynomial identity exists, this is a certificate that the set in (I.2) is empty, i.e. there is no solution in $\mathbb{R}$ which satisfy the inequality constraints.

The polynomial identity is given by

$$f + g^2 + h = 0.$$

As no equalities or inequations are used in the description of the set (I.2), the identity is simplified as

$$f = 0, \tag{I.3}$$

where f is generated by the preordering $\mathcal{P}(f_1, f_2)$. If 0 belongs to the preordering $\mathcal{P}(f_1, f_2)$, then this is a certificate that the set (I.2) is empty, i.e. no solution in $\mathbb{R}$ satisfy the inequalities defined by $f_1(x_1)$ and $f_2(x_1)$. With the preordering the identity becomes

$$s_0 + s_1 f_1 + s_2 f_2 + s_3 f_1 f_2 = 0,$$

with $\{s_0, ..., s_3\} \subset \Sigma$.

Recall that the preordering is infinite, but can be reduced to 2^r unique terms (in this case four terms). The difficult part now becomes to find $\{s_0, ..., s_3\} \subset \Sigma$ such that the identity is valid. In this very simple case, the SOS variables can easily be picked by hand.

Substituting $f_1(x_1)$, $f_2(x_1)$ and rearranging, the identity becomes

$$s_0 = -s_1(-x_1^2 - 3x_1 - 1) - s_2(-x_1^2 + 3x_1 - 1) - s_3(-x_1^2 - 3x_1 - 1)(-x_1^2 + 3x_1 - 1)$$

which is equivalent to showing that

$$-s_1(-x_1^2 - 3x_1 - 1) - s_2(-x_1^2 + 3x_1 - 1) - s_3(-x_1^2 - 3x_1 - 1)(-x_1^2 + 3x_1 - 1) \in \Sigma$$

As $\mathbb{R}_+ \subset \Sigma$, the SOS polynomials are chosen as positive constants for simplicity. Picking $s_1 = 1$, $s_2 = 1$ and $s_3 = 0$, the identity becomes

$$2x_1^2 + 3x_1 + 1 + x_1^2 - 3x_1 + 1 = x_1^2 + 2.$$

As $2x_1^2 + 2$ is clearly a sum of squares, a solution to the identity in (I.3) exists, which bears witness to the fact that the set defined in (I.2) is empty. Consequently, the answer to the objective is that not solution in $\mathbb{R}$ exist which satisfy the inequalities.

In Figure I.1 the polynomials in I.1 are illustrated. From the figure it is obvious that no solution in $\mathbb{R}$ satisfy the inequalities defined by $f_1(x_1) \geq 0,\ f_2(x_1) \geq 0$.

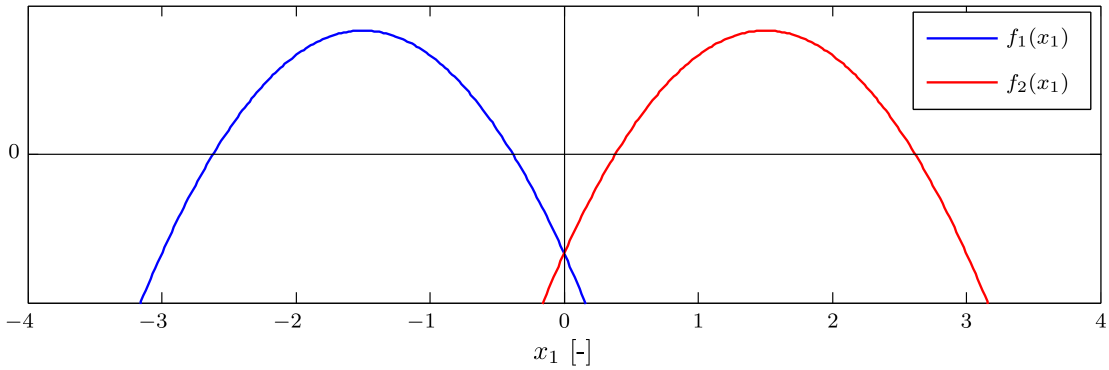


Figure I.1: *Illustration of the polynomial inequalities $f_1(x_1)$ and $f_2(x_1)$ which define a semi-algebraic set.*

J SOS Numerical Considerations

In this appendix, the feasibility of the solution to an SOSP solved in `YALMIP` is described.

The problem of finding the SOS decomposition of a polynomial equals an LMI feasibility problem of finding a $\mathbf{Q}$ such that

$$\mathbf{A}(\mathbf{Q}) = \mathbf{b}, \ \mathbf{Q} \succeq 0,$$

where $\mathbf{A}(\mathbf{Q})$ is the equality constraints between the polynomials and the SOS decomposition. Using SDP, the equality $\mathbf{A}(\mathbf{Q}) = \mathbf{b}$ will not be exactly satisfied. If the Gramian $\mathbf{Q}$ is "sufficiently" positive definite, the polynomial is an SOS. The Gramian is however often close to being singular, which have to be taking in to consideration.

Theorem 8 [LÖ9]: *Let* $\mathbf{r}$ *be the residuals from the SDP solving the sum of squares decomposition* $f = \mathbf{z}^{\mathrm{T}}\mathbf{Q}\mathbf{z}$, $\mathbf{Q} \in \mathbb{S}^{\mathrm{M}}$. *If* $\lambda_{\min}(\mathbf{Q}) \geq M||\mathbf{r}||_{\infty}$, *the polynomial is an SOS.*

K SOS Calculation Example

In this appendix Example 2 in Section 9.5 is expressed as an LMI [SW04][BV04] and solved using the popular LMI solver `SeDuMi`.

Three matrix inequality constraints in Example 2 on Page 85 are given as

$$\mathbf{F}^{(1)} = \begin{bmatrix} c_4 - c_1 & \frac{-c_2}{2} \\ \frac{-c_2}{2} & -c_3 - c_4 \end{bmatrix} \succeq 0, \quad \mathbf{F}^{(2)} = \begin{bmatrix} c_1 + c_5 & \frac{c_2}{2} + 3c_5 \\ \frac{c_2}{2} + 3c_5 & c_3 + 8c_5 \end{bmatrix} \succeq 0, \quad \mathbf{F}^{(3)} = \begin{bmatrix} 2c_1 & \frac{c_2}{2} \\ \frac{c_2}{2} & 0 \end{bmatrix} \succeq 0.$$

Additionally the scalar coefficients c_4 and c_5 are limited to be SOS. This implies that $\{c_4, c_5\} \subset \mathbb{R}_{x\geq 0} \subset \Sigma$, which can be written as a set of linear constraints

$$c_4 \geq 0, \quad c_5 \geq 0. \tag{K.1}$$

The objective is to find a feasible solution $\mathbf{c} = [c_1\ c_2\ c_3\ c_4\ c_5]^{\mathrm{T}}$, which satisfies the above constraints.

To find a $\mathbf{c}$ which satisfies the constraints, the problem is expressed as an LMI feasibility problem. The LMI feasibility problem on standard form is given as

$$\mathbf{F}(\mathbf{c}) = \mathbf{F}_0 + \sum_i c_i \mathbf{F}_i \succeq 0, \tag{K.2}$$

where $\mathbf{F}_i = \mathbf{F}_i^{\mathrm{T}} \in \mathbb{R}^{\mathrm{n}\times\mathrm{n}}$ and $\mathbf{c}$ is the variable.

The constrains $\mathbf{F}^{(1)}$, $\mathbf{F}^{(2)}$ and $\mathbf{F}^{(3)}$ can be put on LMI form (K.2) as

$$\begin{aligned}
\mathbf{F}^{(1)}(\mathbf{c}) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + c_1 \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 & -\frac{1}{2} \\ -\frac{1}{2} & 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix} + c_4 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + c_5 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \succeq 0, \\
\mathbf{F}^{(2)}(\mathbf{c}) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + c_1 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + c_4 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + c_5 \begin{bmatrix} 1 & 3 \\ 3 & 8 \end{bmatrix} \succeq 0, \qquad \text{(K.3)} \\
\mathbf{F}^{(3)}(\mathbf{c}) &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + c_1 \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + c_4 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + c_5 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \succeq 0.
\end{aligned}$$

The matrix inequalities in (K.3) can be combined into one LMI by

$$\begin{aligned}
\mathbf{F}(\mathbf{c}) &= \begin{bmatrix} \mathbf{F}^{(1)}(\mathbf{c}) & 0 & 0 \\ 0 & \mathbf{F}^{(2)}(\mathbf{c}) & 0 \\ 0 & 0 & \mathbf{F}^{(3)}(\mathbf{c}) \end{bmatrix} \\
&= \begin{bmatrix} c_4 - c_1 & -\frac{c_2}{2} & 0 & 0 & 0 & 0 \\ -\frac{c_2}{2} & -c_3 - c_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & c_1 + c_5 & \frac{c_2}{2} + 3c_5 & 0 & 0 \\ 0 & 0 & \frac{c_2}{2} + 3c_5 & c_3 + 8c_5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2c_1 & \frac{c_2}{2} \\ 0 & 0 & 0 & 0 & \frac{c_2}{2} & 0 \end{bmatrix} \succeq 0,
\end{aligned} \tag{K.4}$$

where $\mathbf{F}(\mathbf{c}) = \mathbf{F}(\mathbf{c})^{\mathrm{T}}$ and the eigenvalues of $\mathbf{F}(\mathbf{c})$ are the union of the eigenvalues of $\mathbf{F}^{(1)}$, $\mathbf{F}^{(2)}$ and $\mathbf{F}^{(3)}$.

Finally the linear constraints given in (K.1) should be included in the LMI. Linear inequalities can be expressed as a diagonal LMI by including the inequalities in the diagonal of an LMI

$$\mathbf{a}_1^{\mathrm{T}}\mathbf{x} \le b_1, \ldots, \mathbf{a}_{\mathrm{k}}^{\mathrm{T}}\mathbf{x} \le b_{\mathrm{k}} \Leftrightarrow \mathrm{diag}(b_1 - \mathbf{a}_1^{\mathrm{T}}\mathbf{x}, \ldots, b_{\mathrm{k}} - \mathbf{a}_{\mathrm{k}}^{\mathrm{T}}\mathbf{x}) \succeq 0. \tag{K.5}$$

Using (K.5) the linear constraints in (K.1) are expressed as an LMI

$$\mathbf{F}^{(4)} = \mathrm{diag}(c_4, c_5) \succeq 0. \tag{K.6}$$

Including (K.6) in (K.4) the final LMI becomes

$$\tilde{\mathbf{F}}(\mathbf{c}) = \begin{bmatrix} \mathbf{F}^{(1)}(\mathbf{c}) & 0 & 0 & 0 \\ 0 & \mathbf{F}^{(2)}(\mathbf{c}) & 0 & 0 \\ 0 & 0 & \mathbf{F}^{(3)}(\mathbf{c}) & 0 \\ 0 & 0 & 0 & \mathbf{F}^{(4)}(\mathbf{c}) \end{bmatrix} \succeq 0. \tag{K.7}$$

The LMI in (K.7) can be solved using standard LMI software such as `SeDuMi`. If the LMI can be solver, this implies that a vector $\mathbf{c}$ exists such that the resulting matrix becomes positive semidefinite. A $\mathbf{c}$ that satisfies the constraint is a feasible solution to the LMI problem.

A feasible solution to K.7 is found using the solver `SeDuMi`. The resulting coefficients are found to $\{c_1, c_2, c_3, c_4, c_5\} = \{0.6844, 0.0000, -1.4521, 1.0682, 0.3824\}$. By substitution of the coefficients, the eigenvalues of the matrix inequalities are found to $\mathbf{F}^{(1)} = [0.3838, 0.3839]$, $\mathbf{F}^{(2)} = [0.1584, 2.5160]$, $\mathbf{F}^{(3)} = [0.0000, 1.3687]$ and $\mathbf{F}^{(4)} = [1.0682, 0.3824]$. As the eigenvalues are non-negative, the matrix inequality constraints are satisfied. The linear constraints in (K.1) are also satisfied.

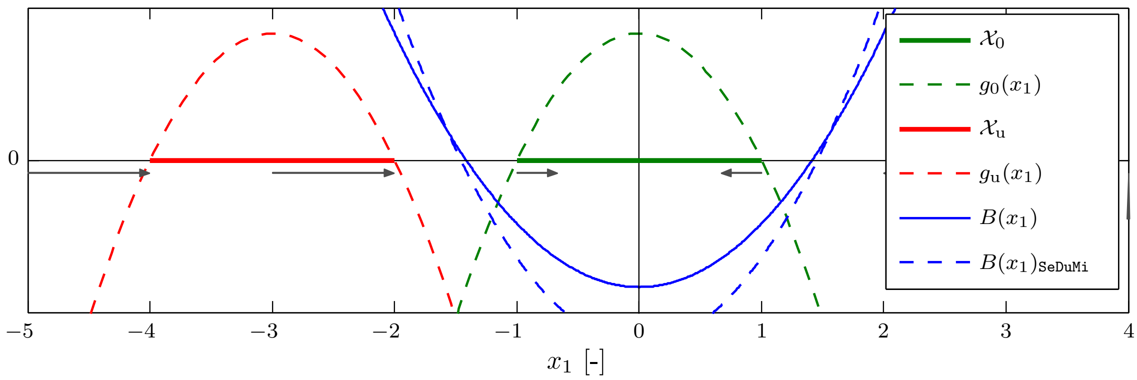


Figure K.1: *The solid green and red lines illustrate the safe and unsafe sets. The dashed polynomials illustrate the safe and unsafe polynomials, which are positive in the respective sets. The vector field of the system is given by grey arrows. The barrier certificate calculated by hand is given in solid blue. The barrier certificate calculated using the LMI solver* ***`SeDuMi`*** *is given in dashed blue.*

The barrier certificate can be found using the description of the barrier certificate from Example 2,

$$B(x_1)_{\mathrm{SeDuMi}} = x_1^2 c_1 + x_1 c_2 + c_3 = 0.6844 x_1^2 - 1.4521.$$

In Figure K.1 the barrier certificate found using the feasible solution to the LMI is illustrated. The barrier certificate found by hand in Section 9.5 is shown as reference. The `MATLAB` script used to solve the LMI using `SeDuMi` can be found on the enclosed DVD.

L Aerodynamic Approximations

In this appendix, polynomial approximations of the aerodynamic tables with reduced complexity are illustrated. In order to obtain a lower degree of the polynomial approximations, the wind span for which the approximations are valid has been reduced to $v_{\mathrm{w}} = [15\ \mathrm{m/s}\ ;\ 25\ \mathrm{m/s}]$. In Figure L.1 and L.2 the 4$^{\mathrm{th}}$ degree polynomial approximations are compared to the original lookup tables.

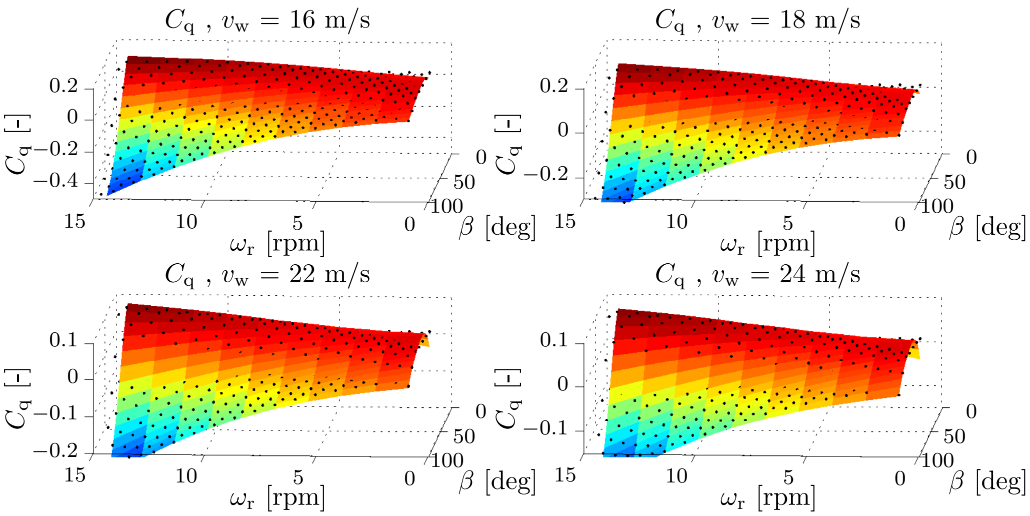


Figure L.1: *Polynomial approximation of the C_{q} lookup table. The surface illustrates the polynomial approximation to the lookup table given as black dots. The approximations are illustrated for 4 fixed values of the wind speed v_{w}.*

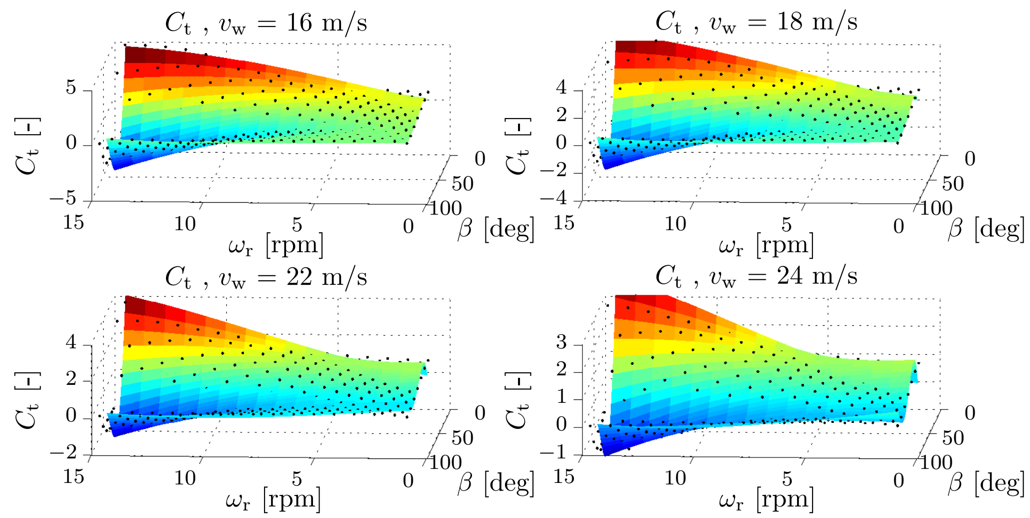


Figure L.2: *Polynomial approximation of the C_{t} lookup table. The surface illustrates the polynomial approximation to the lookup table given as black dots. The approximations are illustrated for 4 fixed values of the wind speed v_{w}.*

Safety Supervisor Simulation

M

In Figure M.1 a simulation of the safety supervisor designed in Chapter 11 is illustrated. The safety supervisor system is implemented on the NREL 5-MW wind turbine with the control system being active. The simulation show that the safety supervisor system does not shut down the wind turbine during normal operation (when no controller faults or extreme external events occur).

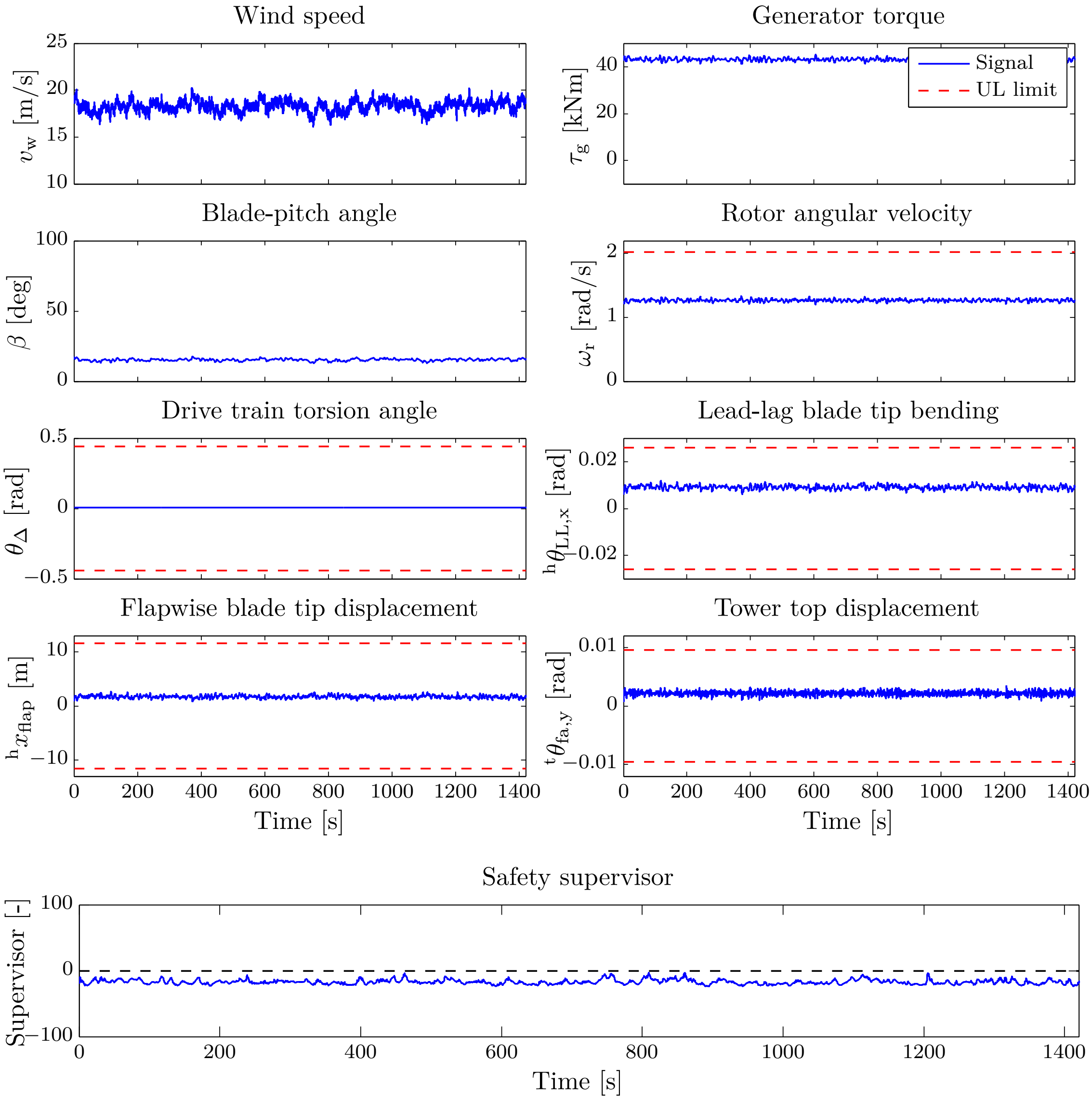


Figure M.1: *A simulation of the NREL 5-MW wind turbine during a time window of approximately 1500 s. During the simulation no errors occur. The simulation show that the safety supervisor system does not shut down the wind turbine during normal operation.*

Additional simulations can be found in Section 11.3 on Page 112.

N DVD

- `/thesis.pdf`: This thesis in digital form.
- `/References/`: Prints of internet sources from bibliography.
- `/Matlab_Wind_Turbine_Model/`: Wind turbine emergency shutdown procedure implemented in `SIMULINK`. Run `main.m` to get shutdown trajectory.
- `/Polynomial_Approximation/`: Calculates the polynomial approximation of the aerodynamic coefficient look-up tables. Run `fitpoly.m` to start.
- `/Subsystem_Barrier_Certificate/`: Finds the subsystem envelopes. Run `flapping_plot.m`, `bending_plot.m`, `tower_plot.m` and `rotor_plot.m` to show the respective envelopes (requires `YALMIP` and `SeDuMi`).
- `/Compositional_Barrier_Certificate/`: Finds the compositional envelope. Run `master_algorithm.m` to run algorithm (requires `YALMIP` and `SeDuMi`).
- `/SOS_Example/`: Calculates the SOS example from Appendix K using `SeDuMi`. Run `sos_example.m` to solve LMIs (requires `SeDuMi`).
- `/NREL_5MW_Separate_Safety/`: Subsystem safety supervisor implementation with `FAST` in `SIMULINK`. Use `NREL_5MW_Separate_Safety.mdl` to run simulation (requires `FAST`).
- `/NREL_5MW_Compositional_Safety/`: Compositional safety supervisor implementation with `FAST` in `SIMULINK`. Use `NREL_5MW_Compositional_Safety.mdl` to run simulation (requires `FAST`).
- `/Normal_Operation/`: Covariance data of normal operation and plot of normal operation clouds. Use `plot_clouds.m` to run.