

# Joint design of stochastically safe setpoints and controllers for nonlinear constrained systems by means of optimization

J. Gillis <sup>\*,\*</sup> G. Horn <sup>\*\*</sup> M. Diehl <sup>\*\*\*</sup>

<sup>\*</sup> *KU Leuven, Electrical Engineering Department (ESAT-STADIUS),  
Belgium (e-mail: joris.gillis@esat.kuleuven.be).*

<sup>\*\*</sup> *KU Leuven, Electrical Engineering Department (ESAT-STADIUS),  
Belgium (e-mail: greg.horn@esat.kuleuven.be).*

<sup>\*\*\*</sup> *KU Leuven, Electrical Engineering Department (ESAT-STADIUS),  
Belgium (e-mail: moritz.diehl@esat.kuleuven.be).*

---

**Abstract:** Implementing complex control schemes for a mechanically fragile and expensive system can be a risky undertaking. We can reduce the operational risks by a) identifying regions of state-space where the system is far from critical system bounds and exhibits natural stability, and b) designing a backup controller that keeps the system from crashing if we venture beyond those regions. We propose to maximize the safety-margin of the system's operational bounds, using a stochastic interpretation of the algebraic Lyapunov equation. This technique allows us to find optimally safe open-loop stable setpoints of the system. Next, we propose to add the parameters of a linear output feedback controller as optimization variables, such that setpoint and controller are jointly designed to yield the safest operational regimes. We demonstrate these methods on the application of rotational launch of tethered airplanes for power-generation.

*Keywords:* optimal control; robust control; output feedback; Lyapunov equation; steady-states; renewable energy systems

---

## 1. INTRODUCTION

Some physical systems require a controller which is carefully balanced between performance and constraints, such as complex system dynamics and damage-avoiding constraints. An example of such a system can be found in the field of airborne wind energy (AWE). To the effect of demonstrating rotational startup for AWE systems, the Leuven/Freiburg Highwind group is putting into service a large second generation carousel (Geebelen et al., 2012), a device which tows around an airplane on a tether of adjustable length. Nonlinear model predictive control (NMPC) is the enabling technology here.

Before hitting the start button of this new experimental setup and towing around a sensor-packed airplane in gusty conditions, it makes sense to study the open-loop behavior and map out control settings which correspond to steady-state solutions that are a safe distance away from violating critical bounds, such as the height of the airplane above the ground. Also, it is desirable to have a simple controller that can take over when more complex schemes fail during prototyping.

This paper formulates an answer to both these research questions using techniques from the field of robustness and stability optimization, Zhou et al. (1996). In Section 2, we introduce a rigorous vocabulary to talk about operational safety, propose a method to optimize operational safety

---

<sup>\*</sup> J. Gillis is a Doctoral Fellow of the Fund for Scientific Research – Flanders (F.W.O.) in Belgium.

open-loop in an approximate fashion, and we extend the method for a simple superimposed controller. Section 3 highlights two implementation details: the elimination of a subset of decision variables, and the treatment of systems with invariants. Section 4 treats the AWE application which inspired the presented research. Discussion and conclusion sections follow at the end.

## 2. METHODS

The key idea of the proposed method is to scale up a safety-margin around a set of likely system states as much as possible, without leaving the region where system operation is safe. This idea and its formulation will be developed in the following subsection, followed by an extension for the incorporation of output feedback. In this section, we will treat systems described by ordinary differential equations (ODE). A generalization for systems with invariants is given in Section 3, and in Section 4, a class of differential-algebraic equations (DAE) is treated.

### 2.1 Optimally safe setpoints

Consider the continuous time dynamic system

$$\dot{x} = f(x, u), \quad (1)$$

with states  $x \in \mathbf{R}^n$ , control inputs  $u \in \mathbf{R}^m$  and  $f$  continuously differentiable. Neglecting modeling error and external disturbances for a moment, we define the system to have a *asymptotically safe setpoint*  $(x^*, u^*)$  if it holds that:

- (1) Control bounds are respected:  $u^* \in \mathbb{U} \subset \mathbf{R}^m$ .
- (2)  $x^*$  is in the interior of the operational set  $\mathbb{X}$ .
- (3) The point is a stationary point i.e.  $f(x^*, u^*) = 0$  holds.
- (4) The undisturbed system is asymptotically stable at this point:  $\alpha(\frac{\partial f}{\partial x}) < 0$ , where  $\alpha$  is the spectral abscissa i.e. the maximum of real parts of the eigenvalues.

We will further assume that the operational set is defined by means of a collection of scalar operational bounds

$$\mathbb{X} = \{x | h_i(x) \leq 0\}. \quad (2)$$

Furthermore, we will assume that the linearized system dynamics matrix  $A = \frac{\partial f}{\partial x}$  is invertible on  $\mathbb{X} \times \mathbb{U}$  such that for a given  $u$ , the steady state equation  $f(x, u) = 0$  implicitly defines a locally unique steady-state function  $x = S(u)$  with a particular domain. We restrict our analysis to one such  $S$ . Also, we assume further that the linearized system is controllable.

It follows from the above conditions that we can always construct an open region in state-space around a safe setpoint  $(x^*, u^*)$  which is invariant under forward propagation of system dynamics and which lies entirely inside the operational set. Next, we will extend the notion of this safe region to a stochastically excited system.

Allowing for disturbances  $w \in \mathbb{R}^p$ , we consider the system

$$\dot{x} = f(x, u, w). \quad (3)$$

For a given fixed control input  $u^*$  and a stationary stochastic realization of  $w$ , the disturbed system will never reach the true steady state  $x^* = S(u^*)$ , but will remain in a region close to it if the system is asymptotically stable and the disturbances are sufficiently small. The deviation  $\hat{x}$  of the state  $x$  from  $x^*$  will then behave as a stochastic process as well.

We define the point  $(x^*, u^*)$  to be *stochastically safe* with confidence level  $0 < \bar{p} \leq 1$  for the disturbed system if it holds that:

- (1) The point is *asymptotically safe* for the corresponding undisturbed system.
- (2) For each operational bound  $h_i(x) \leq 0$ , the probability of the stochastic realization of  $h_i(x)$  satisfying its bound is at least  $\bar{p}$ .

If we assume zero-mean Gaussian white noise with covariance  $\Sigma_w$  as realization of  $w$ , then the covariance of the deviation of states w.r.t. to a safe steady-state point,  $\Sigma_{\hat{x}} \equiv P$  is given in linear approximation as the discrete Lyapunov equation as elaborated on in Houska (2007); Zhou et al. (1996):

$$\underbrace{AP + PA^T}_{\text{sink}} + \underbrace{D\Sigma_w D^T}_{\text{source}} = 0, \quad (4)$$

with  $A = \frac{\partial f}{\partial x}(x, u, 0)$ ,  $D = \frac{\partial f}{\partial w}(x, u, 0)$  and  $P$  a positive-definite symmetric matrix. This equation captures how the uncertainty injected through the source term (disturbances) finds a dynamic equilibrium with the sink term (strictly dissipative system dynamics). The equation is exact if  $f$  is linear in  $x$  and  $w$ .

In linear approximation of  $h_i(x)$ , we have that its (scalar) covariance is given by

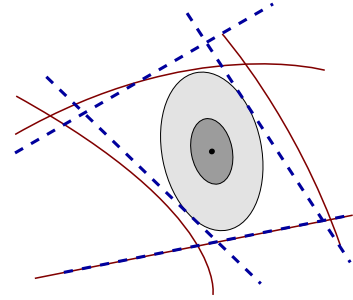


Fig. 1. State-space, state covariance and bounds

$$\Sigma_{h_i(x)} = \frac{\partial h_i}{\partial x} P \frac{\partial h_i}{\partial x}^T. \quad (5)$$

Under these approximations, we can guarantee that realizations of the perturbed state around the safe setpoint are within the operational set with safety margin  $0 < \gamma$ , by imposing the following bounds:

$$h_i(x^*) + \gamma \sqrt{\Sigma_{h_i}(x^*)} \leq 0, \quad (6)$$

with  $\gamma$  bearing a relationship with the confidence level through the cumulative normal distribution function  $\Phi$ :

$$\Phi(\gamma) = 1 - \bar{p}/2. \quad (7)$$

Our first contribution is the proposal to maximize the safety margin  $\gamma$  simultaneously with the search for a stochastically safe setpoint, yielding the *optimal stochastically safe* setpoint, in an optimal control problem formulation:

$$\underset{x, u, \gamma, P}{\text{minimize}} \quad -\gamma \quad (8a)$$

$$\text{subject to} \quad f(x, u, 0) = 0 \quad (8b)$$

$$u \in \mathbb{U} \quad (8c)$$

$$h_i + \gamma \sqrt{\frac{\partial h_i}{\partial x} P \frac{\partial h_i}{\partial x}^T} \leq 0 \quad (8d)$$

$$AP + PA^T + D\Sigma_w D^T = 0. \quad (8e)$$

For an illustrative summary of this method, we refer to Figure 1. Here, we have an illustration of state-space for a given control input  $u^*$ , with operational bounds  $h_i = 0$  depicted in solid lines, defining the operational set. The dot near its center is the stationary point  $x^* = S(u^*)$ . The dotted lines represent the approximate operational bounds, linearized in  $x^*$ . The inner ellipsoid is a representation of covariance  $P$ , with the eigenvectors defining the principal axes, and eigenvalues the squares of axis lengths.

The quantity  $\sqrt{\frac{\partial h_i}{\partial x} P \frac{\partial h_i}{\partial x}^T}$  corresponds to the maximum reach of the ellipsoid in the direction towards the linearized operational bound  $h_i$ . The outer ellipsoid is a scaled up version with factor  $\gamma$ . Note that two constraints on Equation (8d) are active here and none are violated; we can say that the point  $(x^*, u^*)$  is stochastically safe with safety margin  $\gamma$ . The goal of Method (8) is to scout the design space  $u$  for the setpoint with the largest safety margin  $\gamma$ . The other decision variables can be eliminated in principle.

Equation (8e) admits a positive-definite solution only when the spectral abscissa is smaller than zero. Hence, the requirement of asymptotic stability is implicitly captured

in this method. Moreover, we do not directly optimize for robust stability, as would be the case with an objective term  $\text{trace}(P)$  or when using the smoothed spectral abscissa (Vanbiervliet et al., 2009), but rather look at the *effect* of the interplay between disturbance and stability margin on several operational bounds. We optimize under the constraint of the effects not being too large.

### 2.2 Joint design of setpoint and control

The existence of an open-loop stochastically safe setpoint as defined in Method (8) of the previous section is not guaranteed. And when it exists, the corresponding safety margin might be insufficient. To diminish these problems, one can improve stability by embedding a controller into the dynamics. As an example, we propose to introduce simple output feedback control in the system with coefficients as new the decision variables. By adding additional degrees of freedom to the optimization problem we can only perform better or as good as Method (8).

Consider the linearization of System (3) around a candidate steady-point  $(x^*, u^*)$ :

$$\begin{aligned}\dot{\hat{x}} &= A\hat{x} + B\hat{u} + Dw \\ \hat{y} &= Y\hat{x} + v,\end{aligned}\quad (9)$$

with  $B = \frac{\partial f}{\partial u}(x^*, u^*, 0)$ ,  $Y = \frac{\partial y}{\partial x}(x^*)$ ,  $y(x) \in \mathbb{R}^s$  an observation function, and  $v$  a stochastic variable corresponding to measurement noise.

In the previous section, we had  $\hat{u} \equiv 0$ . Here, we couple  $\hat{y}$  back to  $\hat{u}$  with a linear feedback matrix  $K \in \mathbb{R}^{m \times s}$ :

$$\hat{u} = K(Y\hat{x} + v). \quad (10)$$

Adding this feedback into the dynamics of Method 8 leads to a method for jointly designing setpoint and control for optimal stochastic safety:

$$\underset{x, u, \gamma, P, K}{\text{minimize}} \quad -\gamma \quad (11a)$$

$$\text{subject to} \quad f(x, u, 0) = 0 \quad (11b)$$

$$q_j + \gamma \sqrt{\frac{\partial q_j}{\partial u} K Y P Y^T K^T \frac{\partial q_j}{\partial u}^T} \leq 0 \quad (11c)$$

$$h_i + \gamma \sqrt{\frac{\partial h_i}{\partial x} P \frac{\partial h_i}{\partial x}^T} \leq 0 \quad (11d)$$

$$\begin{aligned}(A + BK Y)P \\ + P(A + BK Y)^T \\ + D\Sigma_w D^T + BK\Sigma_v K^T B^T\end{aligned} = 0 \quad (11e)$$

where we have parametrized set  $\mathbb{U}$  by functions  $q_j$  as we did earlier for  $\mathbb{X}$ . Note that the introduction of output feedback on the system linearized around steady-state has direct influence on the state covariance  $P$  only, and on the safety margin as a direct consequence. The potential of output feedback to alter also the steady-state point – the *joint* design aspect – arises indirectly through the optimizer.

## 3. IMPLEMENTATION

Methods (8) and (11) are in principle directly suitable for solution with a derivative-based general-purpose non-linear programming (NLP) solver, if the derivatives can

be cheaply obtained through an automatic differentiation (AD) package. However, we introduce in this paper three important implementation techniques which improve convergence.

### 3.1 Elimination of covariance

It was observed in numerical experiments that, when started with a known asymptotically safe point as initial guess, both an implementation with an interior-point method ( IPOPT, Wächter and Biegler (2006) ) and a sequential quadratic program (SQP) method ( WORHP, Büskens and Wassel (2012) ), showed better global convergence behavior when  $P$  was eliminated as decision variable.

Indeed, Equation (8e) is linear in  $P$  and hence one can write the vector of its entries  $\mathcal{P} = \text{vec}(P)$  as the solution of a linear system  $\mathcal{A}\mathcal{P} = \mathcal{B}$  using

$$\begin{aligned}\mathcal{A} &= A \otimes \mathbf{1}^n + \mathbf{1}^n \otimes A \\ \mathcal{B} &= \text{vec}(D\Sigma_w D^T),\end{aligned}\quad (12)$$

with  $\otimes$  the Kronecker-product. The size of this linear system can be reduced from  $n$  to  $n(n+1)/2$  by taking symmetry of  $P$  into account. We omit a closed form expression for this reduced system here, but note that it is easily obtained in the AD tool we use. We further note that there exist dedicated algorithms with better complexity to solve the Lyapunov equation (Benner and Saak, 2013).

We implemented the methods in this paper in `python` with the help of the open-source AD tool `CasADi` (Andersson et al., 2012). The linear solve operation to obtain  $\mathcal{P}$  is an example of a node in the matrix-valued graphs that one can construct in `CasADi` to represent mathematical expressions and obtain derivatives through AD.

### 3.2 Treatment of invariants

Systems described with non-minimal coordinates come with a constraint  $C(x) = 0 \in \mathbb{R}^c$  on state-space that is invariant in time. Method (8) being an optimization method, one is easily tempted to just add this constraint alongside steady-state constraint (8b) and consider the job done. However, both constraints describe the same dynamics; they form a rank- $n$  constraint-Jacobian matrix of size  $(n+c) \times n$ . The resulting non-linear problem violates the linear independence constraint qualification (LICQ) required for many off-the-shelf gradient-based non-linear program solvers. In practice, this violation leads to stagnating progress during the iterations.

To resolve this, we borrow a technique from Sternberg et al. (2012), for treatment of invariants in an optimal control problem context. The technique uses projection and results in:

$$f(x, u) - J^\dagger C = 0, \quad (13)$$

with  $J = (\nabla C)^T \in \mathbb{R}^{r \times n}$  the constraint-Jacobian and  $J^\dagger = J^T(JJ^T)^{-1}$  its Moore-Penrose pseudoinverse. This simplifies into the steady-state condition  $f(x, u) = 0$  if  $C = 0$  holds. That the latter should hold becomes obvious by left multiplying Equation (13) with  $J$ :

$$\begin{aligned} Jf(x, u) &= C && \text{since } JJ^\dagger = \mathbf{1}, \\ \dot{C} &= C && \text{since } \frac{\partial C}{\partial x} \frac{dx}{dt} = \frac{dC}{dt}, \\ 0 &= C && \text{Time invariance is implied} \\ &&& \text{by the dynamic equations.} \end{aligned}$$

We obtain the following requirements for  $P$ :

$$P - V(P + AP + PA^T + D\Sigma_w D^T)V = 0, \quad (14)$$

with  $V = \mathbf{1} - J^\dagger J$ . Hence, we suggest the following adaption to Method (8), and similar for Method (11):

$$\underset{x, u, \gamma, P, Q}{\text{minimize}} \quad -\gamma \quad (15a)$$

$$\text{subject to} \quad f(x, u, 0) - J^\dagger C = 0 \quad (15b)$$

$$u \in \mathbb{U} \quad (15c)$$

$$h_i(x) + \gamma \sqrt{\frac{\partial h_i}{\partial x} P \frac{\partial h_i}{\partial x}} \leq 0 \quad (15d)$$

$$P - V(P + Q)V = 0 \quad (15e)$$

$$AP + PA^T + D\Sigma_w D^T = Q. \quad (15f)$$

Note that we can and should eliminate  $P$  and  $Q$  together from the problem by introducing a linear solve node as explained in the previous subsection.

### 3.3 Enforcing $P$ positive definiteness

Rather than resorting to a sequential convex solver, we had success with a simpler method: to use a standard NLP solver, to start it with an initial guess for which  $P$  is positive definite, and to simply return a failure in line-search when a candidate  $P$  is proposed by the nonlinear solver that is not positive-definite.

## 4. APPLICATION

The experimental setup this method was designed for is illustrated in Figure 2. The goal is launching an airplane starting from standstill next to the carousel, and ending up injecting it into a power harvesting mode far away downwind. The tether is initially slowly rolled out as the airplane is towed around by a beam rotating around a vertical axis. For short tether lengths, the carousel's height prevents the airplane from touching the ground. For longer tether lengths, the airplane may well physically crash if the system is operated in uncarefully chosen setpoints or becomes unstable due to e.g. a faulty implementation of a controller. This section shows how safe steady-state points for this apparatus can be found for a range of tether lengths.

### 4.1 Modeling

The carousel model is given as a CasADi script encoding a fully implicit DAE described by Gros et al. (2013). Assuming perfect velocity control of the carousel, and after eliminating the pure integrator states introduced to make the control action smoother, we can summarize the model as

$$\begin{cases} g(x, \dot{x}, u, z) = 0 \\ C(x) = 0, \end{cases} \quad (16)$$

with

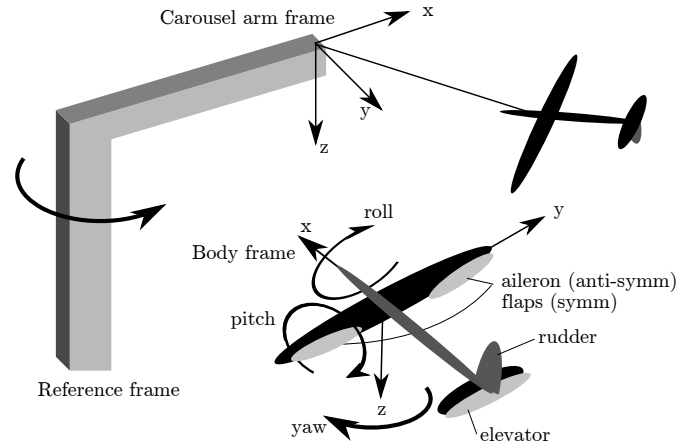


Fig. 2. Illustration of the carousel setup, which tows around an airplane, and illustration of the airplane in detail with its controls surfaces and rotational modes. Positive angular positions for control surfaces correspond to rotational modes along positive axes.

**states**  $x \in \mathbb{R}^{n=18}$  :

$x, y, z$	airplane position in carousel arm frame [m]
$e_{11}, e_{12}, e_{13}, e_{21}, e_{22}, e_{23}, e_{31}, e_{32}, e_{33}$	components of rotation matrix from carousel frame to airplane frame
$dx, dy, dz$	time derivatives of $(x, y, z)$
$w_x, w_y, w_z$	angular rates of airplane in its frame [m/s],

**controls**  $u \in \mathbb{R}^{m=6}$  :

aileron, rudder, elevator, flaps	angular position of aerodynamic control surfaces [rad]
$r$	tether length [m]
$d\delta$	carousel turn speed [rad/s],

**algebraic variables**  $z \in \mathbb{R}$  :

$nu$	tether tension normalized by tether length [N/m],
------	---

**invariants**  $C(x) \in \mathbb{R}^{r=8}$  :

6 orthonormality constraints on $e_{ij}$
consistency between $(x, y, z)$ and $r$ , and derivative of this,

and we augment this model with

**disturbances**  $w \in \mathbb{R}^{p=6}$  :

wind_x, wind_y, wind_z	wind velocity in the world frame [m/s], $\Sigma = 0.5^2$
dist_aileron, dist_elevator, dist_rudder, dist_flaps	biases on control surface positions [rad], $\Sigma = 0.01^2$ .

A property of this model is that the state derivatives  $\dot{x}$  and algebraic variables  $z$  appear linearly in  $g$ . This allows us to obtain an explicit form for  $\dot{x}$  from which  $z$  is eliminated:

$$\begin{bmatrix} \dot{x} \\ z \end{bmatrix} = - \begin{bmatrix} \frac{\partial g}{\partial \dot{x}} & \frac{\partial g}{\partial z} \end{bmatrix}^{-1} g(0, x, 0, u) = \begin{bmatrix} f(x, u, p) \\ f_a(x, u, p) \end{bmatrix}. \quad (17)$$

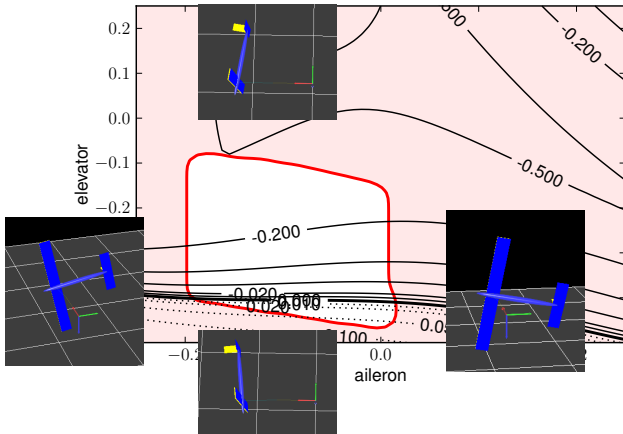


Fig. 3. Steady-state plot for a sweep along (aileron, elevator) with  $r = 1\text{m}$ ,  $d\delta = -4\text{rad/s}$ ,  $\text{rudder} = 0$ ,  $\text{flaps} = 0$ . Every point corresponds to a steady-state. Stability  $s$  is visible as thin contours, full for stable and dotted for unstable. In the shaded region, operational bounds are violated (smoothed for visual cleanliness). Superimposed on the edges of the graph are depictions of airplane configurations that hold near these edges.

The operational bounds defining our operational set  $\mathbb{X}$  are:

Angle of attack [deg]	$[-4.5, 8.5]$
Sideslip angle [deg]	$[-9, 9]$
Airplane position (z) [m]	$[-\infty, 1.5]$
Carousel motor torque [Nm]	$[-20, 20]$
Control surfaces angle [rad]	$[-0.20, 0.20]$
Lift coefficient [-]	$[-0.15, 1.5]$
Winch motor torque [Nm]	$[-78, 78]$
Tether tension [N]	$[0, 600]$
Airspeed. [m/s]	$[10, 65]$

#### 4.2 Steady state exploration

Before we demonstrate in the next section the main methods of this paper, we investigate in this section the set of asymptotically safe points. Given the function  $x = S(u)$  that maps from control inputs to steady-state solutions for our model, we sweep along two coordinates of  $u$  while keeping the remainder fixed to convey a rough idea of the six-dimensional geometry of the minimally safe set. A notable property we highlight is the stability metric

$$s = \alpha(Z^T \frac{\partial f}{\partial x} Z), \quad (18)$$

with  $Z$ , a normalized basis for the null-space of  $J$ , projecting away the zero eigenvalues that arise from the system invariants. In Figure 3, we observe a) that a rectangle of operational feasibility exists, and b) that **elevator** has far more possibility to affect stability than **aileron**. It makes intuitive sense to pick a setting for **elevator** near the top of this rectangle, but not too close to the edge, to be able to operate the system safely.

As the tether is rolled out quasi-statically, we notice from Figure 4a and 4b that regions of stability become unreachable due to violations of the operational bounds. Also, we observe that we should increase the **elevator** along with  $r$  to maintain operation feasibility. In Figure 4c, it appears there is a far-reaching peak of stability (up to

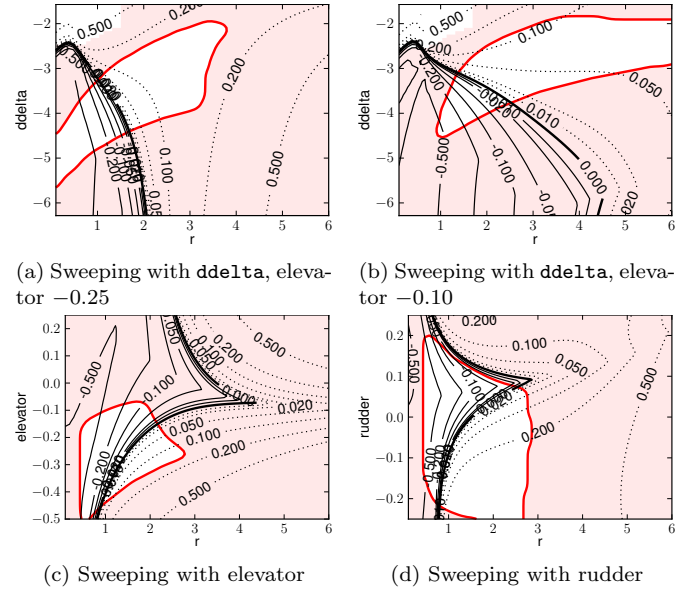


Fig. 4. Steady-state plots with increasing  $r$  on the x-axis. Stable region is at the left hand side.

$r = 4\text{m}$ ) that is impossible to attain with **elevator** alone. In Figure 4d, we notice that a similar peak is observed that does lie in the operationally feasible region attainable by using **rudder** action.

As we interpret these graphs, it becomes clear that a) we are considering both stability and feasibility to determine safe setpoints, a trade-off that is not easy to make intuitively, and b) we should combine authority in multiple inputs to find a path to bring us up safely to long tether lengths, something which is difficult to do by interpreting two-dimensional plots. Stochastic safety is our answer to the former difficulty, and this paper's main methods are an elegant – albeit approximate – solution to the latter.

#### 4.3 Safe setpoints

Before, manual inspection of slices of the asymptotically safe set led us to believe that we should not expect asymptotically safe points further than at  $r = 4\text{m}$ .

In this section, we sweep over  $r$  while optimizing for stochastic safety over the remaining controls. In Methods (8) and (11), we simply restrict all  $r$  coordinates in  $U$  to a single value and use hot-starting to efficiently carry out the sweep. For the closed-loop methods, we choose  $(y, z)$  as observations and (aileron, rudder) as feedback controls. Measurement noise  $\Sigma_v$  was discarded in this simulation.

Figure 5 presents the results for this application. Figure 5a shows we found asymptotically safe points well beyond the tether lengths we expected (up to 6m). Using linear output feedback, we get further still. For each tether length, we have in effect found the largest ellipsoid scaled up from state covariance with factor  $\gamma$  that still fits in the linearized operational set, as depicted in Figure 1. In Figure 5b, the optimizer picks  $\approx -0.28$  for **elevator** at  $r = 1\text{m}$  which lies at the center of the window of feasibility of Figure 3. Also, **elevator** is steadily increased; a correct prediction from the previous section. In Figure 5d, the controller is de-tuned with increasing  $r$ , mainly because control force

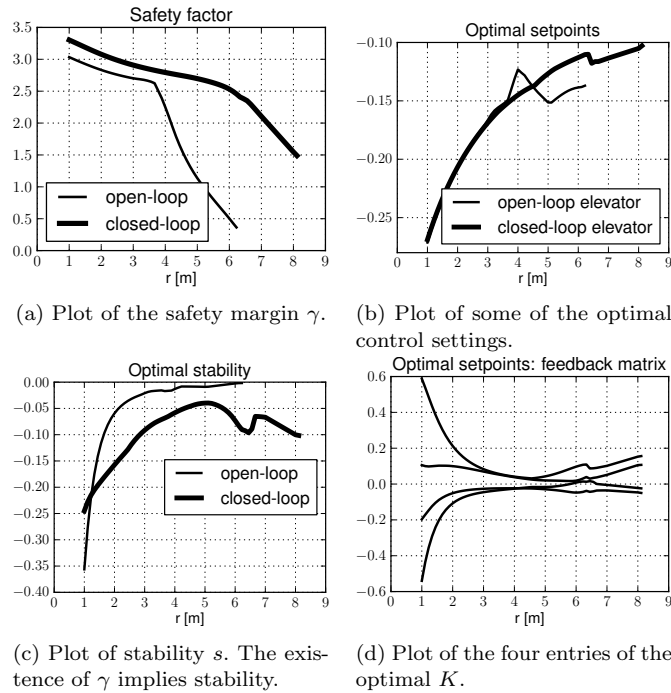


Fig. 5. Results of the search for optimal stochastic safety for a sweep along  $r$ .

rises with air speed for a fixed control surface angle. Using the methods of this paper we have successfully found safe regions in control-space to fall back to, when advanced controllers fail.

## 5. DISCUSSION

Our particular application was about backup control, for which nothing but system's integrity is of importance. For other applications, the proposed methods in this paper can benefit from adding extra performance metrics into the objective.

The methods presented here are exact for systems that are linear in  $x$  and  $w$  and operational constraints linear in  $x$ . To some extent, linearization error can be seen as a disturbance acting on the system, something the method can deal with if quantified.

Incorporating state-of-the art Lyapunov solving algorithms into the AD context is the subject of further study, while the extension of the method to limit cycles is straightforward (Sternberg et al., 2012; Gillis and Diehl, 2013).

## 6. CONCLUSION

In this paper, we introduced notions of marginal and stochastic safety. We argued that the latter was a useful criterion to find setpoints for disturbed physical systems with hard constraints that must be met. Next, we developed a method to optimize the stochastic safety margin. After highlighting some implementation details, we demonstrated the techniques on the application that was the inspiration for the research, safe rotational start-up for power-generating tethered airplanes, for which we extended the known region of safe operation significantly.

## ACKNOWLEDGEMENTS

This research was supported by Research Council KUL: PFV/10/002 Optimization in Engineering Center OPTEC, GOA/10/09 MaNet and GOA/10/11 Global real-time optimal control of autonomous robots and mechatronic systems. Flemish Government: IOF / KP / SCORES4CHEM, FWO: PhD/postdoc grants and projects: G.0320.08 (convex MPC), G.0377.09 (Mechatronics MPC); IWT: PhD Grants, projects: SBO LeCoPro; Belgian Federal Science Policy Office: IUAP P7 (DYSCO, Dynamical systems, control and optimization, 2012-2017); FP7-SADCO (MC ITN-264735), ERC ST HIGHWIND (259 166), Eurostars SMART, ACCM.

## REFERENCES

- Andersson, J., Åkesson, J., and Diehl, M. (2012). CasADi – A symbolic package for automatic differentiation and optimal control. In S. Forth, P. Hovland, E. Phipps, J. Utke, and A. Walther (eds.), *Recent Advances in Algorithmic Differentiation*, Lecture Notes in Computational Science and Engineering. Springer, Berlin.
- Benner, P. and Saak, J. (2013). Numerical solution of large and sparse continuous time algebraic matrix riccati and lyapunov equations: a state of the art survey. *GAMM Mitteilungen*, 36(1), 32–52.
- Büskens, C. and Wassel, D. (2012). *Modeling and Optimization in Space Engineering*, chapter The ESA NLP Solver WORHP. Springer Verlag.
- Geebelen, K., Ahmad, H., Vukov, M., Gros, S., Swevers, J., and Diehl, M. (2012). An experimental test set-up for launch/recovery of an Airborne Wind Energy (AWE) system. In *Proceedings of the 2012 American Control Conference*.
- Gillis, J. and Diehl, M. (2013). A Positive Definiteness Preserving Discretization Method for nonlinear Lyapunov Differential Equations. In *Proceedings of the 52nd IEEE Conference on Decision and Control*.
- Gros, S., Zanon, M., and Diehl, M. (2013). A Relaxation Strategy for the Optimization of Airborne Wind Energy Systems. In *European Control Conference*.
- Houska, B. (2007). *Robustness and Stability Optimization of Open-Loop Controlled Power Generating Kites*. Master's thesis, University of Heidelberg.
- Sternberg, J., Gros, S., Houska, B., and Diehl, M. (2012). Approximate Robust Optimal Control of Periodic Systems with Invariants and High-Index Differential Algebraic Systems. In *In Proceedings of the 7th IFAC Symposium on Robust Control Design*, 678–683.
- Vanbiervliet, J., Vandereycken, B., Michiels, W., Vandewalle, S., and Diehl, M. (2009). The smoothed spectral abscissa for robust stability optimization. *SIAM Journal on Optimization*, 20(1), 156–171.
- Wächter, A. and Biegler, L. (2006). On the Implementation of a Primal-Dual Interior Point Filter Line Search Algorithm for Large-Scale Nonlinear Programming. *Mathematical Programming*, 106(1), 25–57.
- Zhou, K., Doyle, J., and Glover, K. (1996). *Robust and optimal control*. Prentice Hall, Englewood Cliffs, NJ.