doi: 10.82124/CEAS-GNC-2026-024 CEAS-GNC-2026-024

Fault Tolerant Control Barrier Functions

ir. Q.E.J. van Hilten PhD Candidate - Control & Operations, Delft University of Technology, Delft, The Netherlands. Q.E.J.vanHilten@tudelft.nl

Dr. ir. T. Li Postdoctoral Researcher - Control & Operations, Delft University of Technology, Delft, The Netherlands. T.Li-4@tudelft.nl

Dr. ir. C.C. de Visser Associate Professor - Control & Operations, Delft University of Technology, Delft, The Netherlands. C.C.deVisser@tudelft.nl

ABSTRACT

In this article, a novel Control Barrier Function (CBF) named the fault tolerant Control Barrier Function (ftCBF) is introduced. The ftCBF is able to keep a vehicle within a predefined safe set with changing control bounds and changing system dynamics. The ftCBF is shown to be feasible in fault tolerant control applications, as opposed to existing CBF methods. This novel constraint is tested on a double integrator system, and on a non-linear Dubin's Car system with changing system dynamics and changing control bounds. In the simulations it is shown that the ftCBF is able to keep the vehicle in the safe set with failure events occurring at any place in the timeline. The ftCBF contains design parameters that allow a trade-off between safety and performance.

Keywords: Fault Tolerant Control, Control Barrier Functions, Nonlinear Control

1 Introduction

Control Barrier Functions (CBFs) are a powerful tool in the control theory community that provide a systematic way to ensure safety in dynamical systems. CBFs enable the design of control laws that guarantee the system trajectories remain within predefined sets, which is also called set invariance[1]. CBFs have many applications in the field of robotics (e.g. Agrawal et al.[2]) and are able to be used in conjunction with other control techniques, such as Model Predictive Control (MPC) [3], to provide robust and safe control strategies for dynamical systems. For this research the definition of a CBF given in A.D. Ames et al. [4] will be used.

State of the art CBF methods[5][6][7] do not provide a way to ensure set invariance with changing system dynamics and changing control bounds, as the constraints provided by these methods do not provide constraints that are explicit in the control bounds and changing system parameters.

The main result of this research is the development of a new CBF method that is able to maintain set invariance in case of changing control bounds and changing system dynamics, and is thus able to guarantee safety during a failure event. This novel CBF constraint has been applied to both a linear and a non-linear system, and is generally applicable to any control affine system.

This article will first go over the necessary background that is needed to understand this article in Section 2. Section 3 will introduce the novel CBF method and show its workings on a relatively simple linear systems. Section 4 will show the application of the ftCBF on a non-linear system. Finally this article will be concluded in Section 5.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

2 Background

2.1 General Definitions

Definition 1 (Class κ_∞ function[8])**.** *A continuous function $\alpha : [0, \infty) \rightarrow [0, \infty)$, that is strictly increasing, and is such that $\alpha(0) = 0$ and $\lim_{r\rightarrow\infty} \alpha(r) = \infty$.*

Definition 2 (Extended class κ_∞ function [4])**.** *A class κ_∞ function for which the domain is extended to the entire real line $\mathbb{R} = (-\infty, \infty)$.*

Definition 3 (Lipschitz continuity)**.** *A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is Lipschitz continuous if there exists a positive real number L such that the equation below holds:*

$$|f(x) - f(y)| \leq L|x - y| \tag{1}$$

Definition 4 (Interval of existence[4])**.** *The interval for which a differential equation has a unique solution $x(t)$ on $I(x_0) = [t_0, \tau_{max})$.*

Definition 5 (Forward completeness[9])**.** *A system is said to be forward complete if the interval of existence is equal to $I(x_0) = [t_0, \infty)$.*

Definition 6 (Invariance and safety[4])**.** *Considering a system with feedback controller $u = k(x)$*

$$\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})k(\mathbf{x}) \tag{2}$$

a set C is forward invariant if for every $x_0 \in C$, $x(t) \in C$ for $x(t_0) = x_0$ and $\forall t \in I(x_0)$, where $I(x_0)$ is the interval of existence $I(x_0) = [t_0, \tau_{max})$ such that $x(t)$ is a unique solution for (2) on $I(x_0)$. The set C provides safety for its related system, if set C is forward invariant.

Definition 7 (Relative Degree[7])**.** *The relative degree of a function is the amount of times a function $d : \mathbb{R}^n \rightarrow \mathbb{R}$ has to be differentiated with respect to (3) along its dynamics in order for the input $\mathbf{u}$ of the system (3) to explicitly show up in the derivative. Provided that the function d can be differentiated sufficiently many times.*

2.2 Control Barrier Functions

2.2.1 Control Barrier Function

Definition 8 (Control Barrier Function[4])**.** *Consider a general control affine system of the form*

$$\dot{\mathbf{x}} = f(\mathbf{x}) + g(\mathbf{x})\mathbf{u} \tag{3}$$

with $\mathbf{x} \in X \subset \mathbb{R}^n$ and $\mathbf{u} \in U \subset \mathbb{R}^m$. Then consider a set C_1 defined by a continuously differentiable function $\psi_0 : \mathbb{R}^n \rightarrow \mathbb{R}$:

$$C_1 := \{\mathbf{x} \in \mathbb{R}^n | \psi_0(\mathbf{x}) \geq 0\} \tag{4}$$

The function ψ_0 is a Control Barrier Function (CBF), if there exists an extended class κ_∞ function α_1 for which the following holds for all $x \in X \subset \mathbb{R}^n$:

$$\sup_{u\in U}[\mathcal{L}_f\psi_0(\mathbf{x}) + \mathcal{L}_g\psi_0(\mathbf{x})\mathbf{u} + \alpha_1(\psi_0(\mathbf{x}))] \geq 0 \tag{5}$$

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

In the above equation (5) the symbols $\mathcal{L}_f$ and $\mathcal{L}_g$ denote the Lie derivatives of the function ψ_0 along the vector fields f and g respectively.

Theorem 1 (from [4])**.** *Let C_1 be defined as in (4), if ψ_0 is a Control Barrier Function and $\frac{\partial \psi_0}{\partial \mathbf{x}} \neq 0$ for all $\mathbf{x} \in \partial C_1$, then any lipschitz continuous controller that satisfies (5), renders the set C_1 invariant and thus safe (by Definition 6).*

2.2.2 Higher Order Control Barrier Functions

When the relative degree of the system is higher than one, (5) will not contain the input $\mathbf{u}$ explicitly as the term $\mathcal{L}_g \psi_0(\mathbf{x})$ will be zero by Definition 7. To still come up with a constraint explicit in the input, the Higher Order Control Barrier Function (HOCBF)[6] can be used.

To come up with a constraint that is explicit in $\mathbf{u}$, first (5) is made to define a new set

$$C_2 := \{\mathbf{x} \in \mathbb{R}^n | \psi_1 \geq 0\} \tag{6}$$

where ψ_1 is defined below:

$$\psi_1 := [\mathcal{L}_f \psi_0(\mathbf{x}) + \alpha_1(\psi_0(\mathbf{x}))] \tag{7}$$

In order for ψ_1 to be a control barrier function for the set C_2 it should by Definition 8 adhere to

$$\sup_{u \in U} [\mathcal{L}_f \psi_1(\mathbf{x}) + \mathcal{L}_g \psi_1(\mathbf{x}) \mathbf{u} + \alpha_2(\psi_1(\mathbf{x}))] \geq 0 \tag{8}$$

for all $x \in X \subset \mathbb{R}^n$, where α_2 in the above equation is again an extended class κ_∞ function (Definition 2) that may or may not be distinct from α_1. The set C_2 is invariant, if there exists a Lipschitz continuous controller that satisfies (8) and $\frac{\partial \psi_1}{\partial x} \neq 0$ for all $x \in \partial C_2$ (Theorem 1) . The invariance of the set C_2 leads to the invariance of set C_1, because the invariance of C_2 by the definition of C_2 (6) means that $\psi_1 \geq 0$, which is by the definition of ψ_1 (7) the same as satisfying (5), and thus in turn provides set invariance for C_1 provided that $\frac{\partial \psi_0}{\partial x} \neq 0$ for all $\mathbf{x} \in \partial C_1$.

If the constraint (8) still does not contain the input explicitly (i.e. $\mathcal{L}_g \psi_1(\mathbf{x}) = 0$), the above approach can be repeated until it does and the following will then be achieved with a relative degree of m:

$$\begin{aligned} \psi_0 &:= b(\mathbf{x}) \\ \psi_1 &:= \dot{\psi}_0 + \alpha_1(\psi_0) \\ &\vdots \\ \psi_m &:= \dot{\psi}_{m-1} + \alpha_m(\psi_{m-1}) \geq 0 \end{aligned} \tag{9}$$

When $\mathbf{x}_0 \in C_1 \cap \cdots \cap C_m$ and $\psi_m \geq 0$ holds for $\forall t \in I(x_0)$, the trajectories of the system (3) will remain in the set C_1 (Theorem 2). In (9), ψ_m is actually not a CBF, but is used for ease of communication and denotes the constraint which is explicit in the input and is used to provide set invariance of the original predefined safe set C_1 (4). In (9) the directional derivatives are replaced by the full derivatives (e.g. in $\mathcal{L}_f \psi_0(\mathbf{x}) + \mathcal{L}_g \psi_0(\mathbf{x}) \mathbf{u} = \dot{\psi}_0$) for ease of communication. The function $b(\mathbf{x})$ in (9) denotes an arbitrary continuously differentiable function of $\mathbf{x}$ that defines the safe set C_1 in (4).

The more formal definition of the HOCBF and the corresponding theorem can be seen below, but first the formal definition of the sets C_i for $i \in \{1, \ldots, m\}$ are given in (10).

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

$$
\begin{aligned}
C_1 &:= \{\mathbf{x} \in \mathbb{R}^n | \psi_0 \geq 0\} \\
C_2 &:= \{\mathbf{x} \in \mathbb{R}^n | \psi_1 \geq 0\} \\
&\vdots \\
C_m &:= \{\mathbf{x} \in \mathbb{R}^n | \psi_{m-1} \geq 0\}
\end{aligned} \tag{10}
$$

Definition 9 (Higher order control barrier function[6])**.** *Let $C_i, i \in \{1, \ldots, m\}$ be defined in (10) and $\psi_i, i \in \{1, \ldots, m\}$ be defined in (9). A function $b : \mathbb{R}^n \times I(x_0) \rightarrow \mathbb{R}$ is a higher order control barrier function of relative degree m for system (3) if there exist extended κ_∞ functions $\alpha_1, \ldots, \alpha_m$ such that $\psi_m \geq 0$ (9) holds for all $\forall t \in I(x_0)$ and for $\forall \mathbf{x} \in C_1 \cap \cdots \cap C_m$.*

Theorem 2 (from [6])**.** *Given a HOCBF (from Definition 9) with the sets $C_i, i \in \{1, \ldots, m\}$ (defined in (10)), if $x_0 \in C_1 \cap \cdots \cap C_m$, then any Lipschitz continuous controller $u(t) \in U$ that satisfies $\psi_m \geq 0$ (from (9)) for all $t \in I(x_0)$, renders the set $C_1 \cap \cdots \cap C_m$ forwards invariant for system (3).*

3 Fault Tolerant Control Barrier Functions

The Fault Tolerant Control Barrier Function (ftCBF) is a novel type of control barrier function and is the main contribution of this research. It guarantees set invariance for a predefined safe set C_1 in (4) for a system (3) that has changing control bounds and changing system dynamics. This makes it well suited for fault tolerant control, as a type of failure can be anticipated by describing how the failure would change the control bounds and system dynamics, in what will be hereafter called failure functions, describing these changes. The ftCBF can then with those failure functions provide invariance of the predefined safe set C_1 in (4).

First to explain the general concept, consider a system (3), with $\psi_m := \dot{\psi}_{m-1} + \alpha_m(\psi_{m-1}) \geq 0$ from (9) being the constraint that needs to be satisfied in order to guarantee safety for the system. Then a control function $u^*(t)$, within the changing control bounds $u_{min}(t) \leq u^*(t) \leq u_{max}(t)$, can be defined as a recovery function of the system that eventually at a time t^* is able to stop a system from moving closer to the boundary of the predefined safe set C_1 (4) for $\forall x_0 \in S \subset X$. Where S is the set for which the recovery function is defined. The recovery function is made to be a function of the system states $\mathbf{x}(t)$ and the changing system parameters $\lambda \in \Lambda \subset \mathbb{R}^p$, which includes the changing control boundaries $u_{min}(t)$ and $u_{max}(t)$. As the failure functions describe the changes of λ, the recovery function will also be defined for anticipated failure events. The formal definition of a recovery function, as well as the theorem that states when the set $C_1 \cap \cdots \cap C_m \cap \mathcal{S}$ will be invariant can be found below.

Definition 10 (Recovery function)**.** *The recovery function is defined as a Lipschitz continuous function $u^*(x, \lambda) : \mathbb{R}^n \times \mathbb{R}^p \rightarrow \mathbb{R}^m$ within the changing control bounds $u_{\min}(t) \leq u^*(t) \leq u_{\max}(t)$, such that for all initial states $x_0 \in S \subset \mathcal{X}$, there exists $t^* \in I(x_0)$ for which $\dot{\psi}_m(x(t)) \geq 0, \forall t \geq t^*$.*

Theorem 3. *If there exists a recovery function (Definition 10) for a system (3) with a HOCBF ψ_0 and a corresponding HOCBF constraint $\psi_m \geq 0$, such that*

$$
\min_{t \in I(x_0) | t_0 \leq t \leq t^*} \psi_m(u^*(\mathbf{x}(t), \lambda(t)), \mathbf{x}(t), \lambda(t)) \geq 0 \tag{11}
$$

and $\mathbf{x}_0 \in C_1 \cap \cdots \cap C_m \cap \mathcal{S}$, then the set $C_1 \cap \cdots \cap C_m \cap \mathcal{S}$ is forward invariant.

Proof. By Theorem 2, the set $C_1 \cap \cdots \cap C_m$ is invariant if for $\mathbf{x}_0 \in C_1 \cap \cdots \cap C_m$, any lipschitz continuous controller $u(t)$ ensures that $\psi_m(u(t), \mathbf{x}(t), \lambda(t)) \geq 0$ (9) for $\forall t \in I(x_0)$. If for $u(t)$ the recovery function

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

$u^*(\mathbf{x}(t), \lambda(t))$ (Definition 10) is used, and the minimum value of $\psi_m(u^*(\mathbf{x}(t), \lambda(t)), \mathbf{x}(t), \lambda(t))$ is greater then zero for $t \in I(x_0)|t_0 \leq t \leq t^*$, the HOCBF constraint $\psi_m \geq 0$ (9) will be satisfied for $\forall t \in I(x_0)$, because for $t \in I(x_0)|t \geq t^*$ the derivative of the HOCBF constraint $\dot{\psi}_m \geq 0$ (by Definition 10), while the recovery function is used. However, because the recovery function u^* is only defined for $x_0 \in S$, only the intersection of the set $C_1 \cap \cdots \cap C_m$ and $\mathcal{S}$ is made invariant. □

Definition 11 (fault tolerant Control Barrier Function (ftCBF))**.** *A HOCBF $\psi_0 : \mathbb{R}^n \to \mathbb{R}$ is a ftCBF if there exists a recovery function u^* (Definition 10) such that (11) holds $\forall t \in I(x_0)$ and $\forall \mathbf{x} \in C_1 \cap \cdots \cap C_m \cap \mathcal{S}$.*

For the practical application of the ftCBF, the system is simulated offline for various different starting conditions (denoted with subscript $[\cdot]_s$), of the system states $\mathbf{x}_s$ and different starting system parameters λ_s through time to compute the minimum of the HOCBF constraint through time. This is done because the constraint can typically not be found analytically. The obtained constraint (12) which is a function of the starting parameters, is then interpolated in real time with current values for the system states and current system parameters substituted as starting values.

$$\min_{t \in I(x_s)|t_s \leq t \leq t^*} \psi_m(u^*(\mathbf{x}_s, \lambda_s, t), \mathbf{x}(t), \lambda(t)) \geq 0 \tag{12}$$

4 ftCBF Applications

4.1 Double Integrator System

For this example application the system described in (13) will be used, with a visualisation of the system given in Figure 1. The variable $z(t)$ describes the distance between an ego vehicle (which can be controlled) and a preceding vehicle. The variable $v(t)$ describes the velocity of the ego vehicle and v_p describes the constant velocity of the preceding vehicle in this example. $u(t)$ is the control input of the ego vehicle and controls the rate of change of the velocity of the ego vehicle.

The HOCBF of the system (13) that needs to be satisfied to guarantee set invariance then results in (14), with the class κ_∞ functions defined as $\alpha_1(\psi_0) := \psi_0$ and $\alpha_2(\psi_1) := \psi_1$, and safe set C_1 (4) defined by $\psi_0 := z(t) - l_p$. The constant l_p denotes the minimum safe distance between the preceding and ego vehicle. The function ψ_2 in (14) is the HOCBF constraint that should be satisfied in order to guarantee set invariance of C_1.

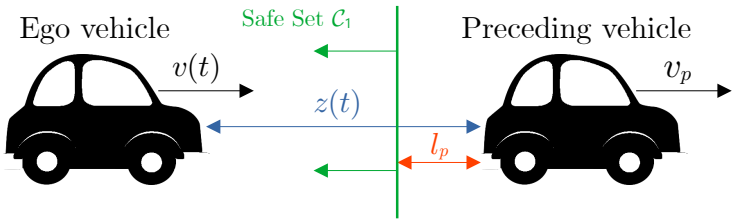

Fig. 1 This figure gives a visualisation of the simple double integrator system given in (13), with safe set C_1 (4), defined by $\psi_0 := z(t) - l_p \geq 0$.

$$\begin{aligned} \dot{z}(t) &= v_p - v(t) \\ \dot{v}(t) &= u(t) \end{aligned} \tag{13}$$

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

$$
\begin{aligned}
\psi_0 &:= z(t) - l_p \\
\psi_1 &:= (v_p - v(t)) + p_1(z(t) - l_p) \\
\psi_2(t) &= -u(t) + 2(v_p - v(t)) + (z(t) - l_p) \geq 0
\end{aligned} \tag{14}
$$

In this relatively simple system, a good recovery function would be the smallest input $u(t)$, which is by definition the lower control bound $u_{min}(t)$, and thus $u(t) = u_{min}(t)$. To simulate a failure in the control effectiveness, u_{min} is modelled to change over time during a failure by the following failure function

$$u_{min}(t) = u_{min_0} \cdot a^t \tag{15}$$

where a is a parameter between zero and one. The next step is to define a recovery function for the system (13), and as a candidate the lower bound of the control input $u_{\min}(t)$ is proposed. To prove that $u(t) = u_{min_0} \cdot a^t$ is a recovery function of the system (13), the derivative of (14) should be greater than zero after some time t^* (Definition 10). The derivative of (14) is given below.

$$\dot{\psi}_2 = -\dot{u}(t) - 2u(t) + (v_p - v(t)) \geq 0 \tag{16}$$

In above equation the derivative of the input is

$$\dot{u}(t) = u_{min_0} \cdot a^t ln(a) \tag{17}$$

and the velocity of the ego vehicle $v(t)$ can be written as

$$
\begin{aligned}
v(t) &= \int_0^t \dot{v}(\zeta) d\zeta + v_0 \\
&= \int_0^t u_{min_0} \cdot a^\zeta d\zeta + v_0 \\
&= u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)}) + v_0
\end{aligned} \tag{18}
$$

Then by substituting (15),(17) and (18) into (16), the following inequality will be obtained:

$$-u_{min_0}(a^t ln(a) + 2a^t + (\frac{a^t}{ln(a)} - \frac{1}{ln(a)})) \geq -(v_p - v_0) \tag{19}$$

The system (13) is forward complete (Definition 5), which makes the interval of existence $I(x_0)$ equal to the interval $[t_0, \infty)$, and thus to find the set $\mathcal{S} \subset X$ for which (15) is a recovery function (Definition 10), the limit of $t \to \infty$ can be taken of (19), which results in the following:

$$
\begin{aligned}
\lim_{t \to \infty} -u_{min_0}(a^t ln(a) + a^t + (\frac{a^t}{ln(a)} - \frac{1}{ln(a)})) &= \frac{u_{min_0}}{ln(a)} \\
\frac{u_{min_0}}{ln(a)} &\geq -(v_p - v_0)
\end{aligned} \tag{20}
$$

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

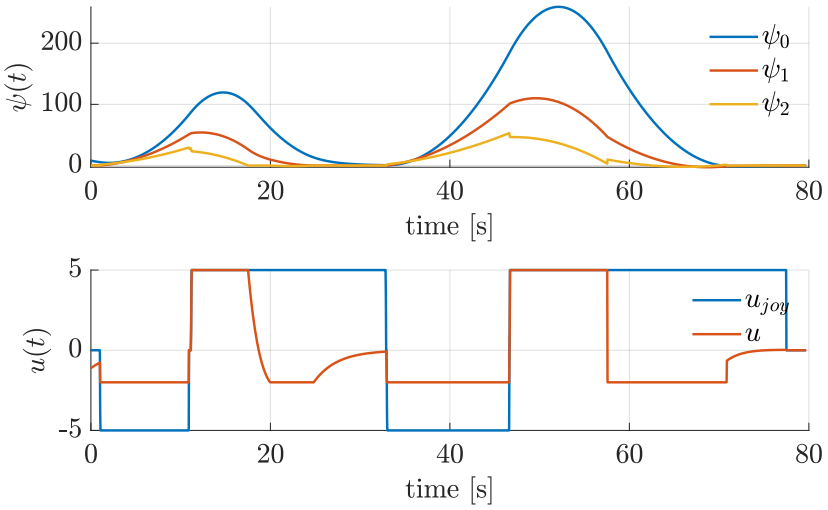

Fig. 2 In this figure the implementation of the ftCBF is shown. For this simulation a human controller was used to demonstrate the workings of the ftCBF. The function $\psi_0 := z(t) - l_p \geq 0$ describes the predefined safe set C_1 (4), and physically describes the distance between the ego vehicle and the preceding vehicle minus a safety constant l_p (as can also be seen in Figure 1). The CBF ψ_1 and the final constraint $\psi_2 \geq 0$ (14) are also shown. If $\psi_2 \geq 0$ both ψ_0 and ψ_1 are as a result also above zero (Definition 9), which guarantees that the safe set C_1 stays invariant. In this simulation the distance between both vehicles ($z(t) = \psi_0 + l_p$), was first increased by providing a negative controller input u_{joy} for about 10 seconds. After around 10 seconds, the controller input u_{joy} provided a positive input, which accelerated the ego vehicle towards the preceding vehicle, until around 18 seconds, where the ftCBF constraint first activates. After the successful recovery from the first maneuver, a second maneuver was performed (starting at around 35 seconds), that tried to accelerate longer towards the preceding vehicle. However, as can be seen the ftCBF ensures that the vehicle remains in the safe set C_1 ($\psi_0 \geq 0$ (4)) for both maneuvers, with control boundaries $-2 \leq u(t) \leq 5$. For this simulation the constant a in the failure function (15) was set to 1 for this example problem, thus u_{min} remained constant.

From the above equation it can be deduced that (15) is a recovery function (by Definition 10) for $v_0 \leq \frac{u_{min_0}}{ln(a)} + v_p$.

Then to provide set invariance for $\forall \mathbf{x}_0 \in C_1 \cap \cdots \cap C_m \cap \mathcal{S}$ by Theorem 3, (11) should be satisfied. Which for the system (13) and recovery function (15) would be

$$\min_{t \in I(x_0) | t_0 \leq t \leq t^*} -(u_{min_0} \cdot a^t) + 2(v_p - v_0 - u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)})) + (z_0 + \int_0^t \dot{z}(\zeta) d\zeta - l_p) \geq 0 \tag{21}$$

where in the above equation $z_0 + \int_0^t \dot{z}(\zeta) d\zeta = z(t)$.

A simulation of system (13) with the ftCBF constraint (21) can be seen in Figure 2. The parameters used for the simulation are given in Table 1, where it can be seen that $a = 1$. This is to keep the control bounds constant for simplicity in this example problem.

A more in depth application of the ftCBF on a non-linear system with changing system dynamics and changing control bounds will be shown in the next example application.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

Table 1 Simulation parameters ftCBF for Double Integrator System

p_0	z_0	v_0	l_p	v_p	a	u_{min}	u_{max}
0.4	10	11	2	8	1	-2	5

4.2 Dubin's Car

4.2.1 System Dynamics

The Dubin's Car system can be visualized as a car that has a constant velocity and has the ability to change direction.

In this variation of a Dubin's car system, the velocity will not be constant, but will be allowed to change as to demonstrate that the ftCBF is able to handle changing system dynamics as well as changing control bounds. Below the equations of motion of the system that will be used in this application are shown:

$$\begin{aligned} \dot{x} &= V(t)\cos(\theta(t)) \\ \dot{y} &= V(t)\sin(\theta(t)) \\ \dot{\theta} &= u(t) \end{aligned} \tag{22}$$

$$u_{min}(t) \leq u(t) \leq u_{max}(t) \tag{23}$$

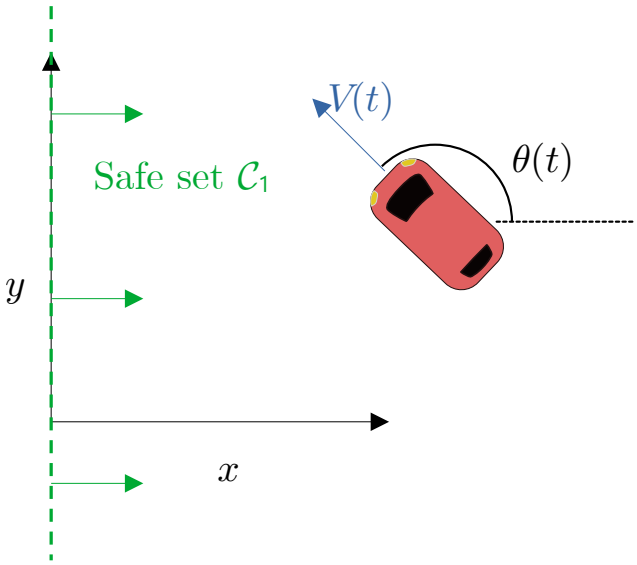

Fig. 3 This figure gives a visualisation of the Dubin's Car system (22), with safe set C_1 (4), where $\psi_0 := x(t) \geq 0$.

In the above equations $u(t)$ is the input that is able to change the angle θ at which the vehicle is driving. The speed will be a simple function of time:

$$V(t) = V_0 + \gamma t \tag{24}$$

where gamma is some positive design constant. A visualisation of the system (22), can be seen in Figure 3, where also a visualisation of the safe set C_1 (4) is given. The safe set for this application will be defined by $C_1 = \{\mathbf{x} | \psi_0 := \mathbf{x}(t) \geq 0\}$.

4.2.2 HOCBF & ftCBF constraints

For $\psi_0 := x(t)$ the system (22) will result in the the following HOCBF:

$$\begin{aligned} \psi_0 &:= x(t) \\ \psi_1 &= V(t)\cos(\theta(t)) + x(t) \\ \psi_2 &= \gamma\cos(\theta(t)) - V(t)\sin(\theta(t))u(t) + 2V(t)\cos(\theta(t)) + x(t) \geq 0 \end{aligned} \tag{25}$$

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

where $\alpha_1(\psi_0) := \psi_0$ and $\alpha_2(\psi_1) := \psi_1$.

For the system (22) a recovery function is defined below:

$$\begin{aligned} u^*(t) := u_{min}(t) = u_{min_0} \cdot a^t, \frac{\pi}{2} \leq \theta(t) \leq \pi \\ u^*(t) := u_{max}(t) = u_{max_0} \cdot a^t, \pi < \theta(t) \leq \frac{3\pi}{2} \\ u^*(t) := 0, -\pi/2 < \theta(t) < \pi/2 \end{aligned} \tag{26}$$

As the system behaves very similar in both domain $\frac{\pi}{2} \leq \theta(t) \leq \pi$ and the domain $\pi < \theta(t) \leq \frac{3\pi}{2}$ (only the direction of rotation will be different), only the domain $0 \leq \theta(t) \leq \pi$ will be considered for simplicity. Additionally, it should be noted that there is no Lipschitz discontinuity at $\theta = \pi$, since once the recovery controller is activated the system will always move away from $\theta = \pi$ in both directions. If the starting condition is at $\theta = \pi$, either $u_{\min}$ (clockwise rotation) or $u_{\max}$ (counter-clockwise rotation) could be chosen, but this example uses $u_{\min}$.

To prove that

$$\begin{aligned} u^* = u_{min_0} \cdot a^t, \frac{\pi}{2} \leq \theta(t) \leq \pi \\ u^*(t) := 0, 0 \leq \theta(t) < \pi/2 \end{aligned} \tag{27}$$

is a recovery function for $0 \leq \theta(t) \leq \pi$, the derivative of ψ_2 in (25) must be greater or equal to zero after a time t^* (Definition 10). The derivative of ψ_2 (9) is given below

$$\begin{aligned} \dot{\psi_2} = -2\gamma \sin\theta(t)u(t) - V(t)\cos\theta(t)u^2(t) \\ -V(t)\sin\theta(t)\dot{u}(t) + 2\gamma\cos\theta(t) - 2V(t)\sin\theta(t)u(t) + V(t)\cos\theta(t) \end{aligned} \tag{28}$$

and for $0 \leq \theta(t) \leq \pi/2$ it can be shown that $\dot{\psi_2} \geq 0$, by substituting $u^* = 0$ (27) into (28).

$$\dot{\psi_2} = 2\gamma\cos\theta(t) + V(t)\cos\theta(t) \tag{29}$$

In the above equation γ and $V(t)$ are always positive or zero, and $\cos\theta(t)$ is also always positive or zero in the domain $0 \leq \theta(t) \leq \pi/2$, thus if the control function (27) is able to get the vehicle into the domain $0 \leq \theta(t) \leq \pi/2$, (27) is a recovery function as $\dot{\psi}_m \geq 0$ after a time t^*. The angle of the vehicle $\theta(t)$ can be made into a function of the control function u^* (27) as can be seen below

$$\begin{aligned} \theta(t) &= \theta_0 + \int_0^t \dot{\theta}(\zeta)d\zeta \\ &= \theta_0 + \int_0^t u(\zeta)d\zeta \\ &= \theta_0 + u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)}) \end{aligned} \tag{30}$$

When assuming a negative lower control bound, and if θ_0 is not in the domain $0 \leq \theta(t) \leq \pi/2$, the angle $\theta(t)$ will enter the domain $0 \leq \theta(t) \leq \pi/2$ at $\theta(t^*) = \frac{\pi}{2}$. Then by finding the limit of (30) for

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

t approaching infinity (assuming that the system (22) is forward complete (Definition 5)), and setting this limit smaller or equal to $\frac{\pi}{2}$, the set $\mathcal{S}$ can be found, for which (27) is defined as a recovery function (Definition 10).

$$\begin{aligned} \lim_{t\to\infty} \theta_0 + u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)}) &\leq \frac{\pi}{2} \\ \theta_0 - \frac{u_{min_0}}{ln(a)} &\leq \frac{\pi}{2} \end{aligned} \tag{31}$$

From the equation above it can thus be deduced that (27) is a recovery function (by Definition 10) for $\theta_0 \leq \frac{\pi}{2} + \frac{u_{min_0}}{ln(a)}$ (31).

Then to provide set invariance for $\forall x_0 \in C_1 \cap \cdots \cap C_m \cap \mathcal{S}$ by Theorem 3, (11) should be satisfied. Which for the system (22) and recovery function (27) would be

$$\begin{aligned} \min_{t\in I(x_0)|t_0\leq t\leq t^*} \gamma\cos\theta(t) - V(t)\sin\theta(t)(u_{min_0}\cdot a^t) \\ +2V(t)\cos\theta(t) + x(t) \geq 0 \end{aligned} \tag{32}$$

for which $x(t)$ can be described as

$$x(t) = x_0 + \int_0^t \dot{x}(\zeta)d\zeta \tag{33}$$

Substituting (33), (24) and (30) in (32) results in the equation below.

$$\begin{aligned} \min_{t\in I(x_0)|t_0\leq t\leq t^*} \gamma\cos(\theta_0 + u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)})) \\ -(V_0+\gamma t)(u_{min_0}\cdot a^t)\sin(\theta_0 + u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)})) \\ +2(V_0+\gamma t)\cos(\theta_0 + u_{min_0}(\frac{a^t}{ln(a)} - \frac{1}{ln(a)})) \\ +\int_0^t (V_0+\gamma\zeta)\cos(\theta_0 + u_{min_0}(\frac{a^\zeta}{ln(a)} - \frac{1}{ln(a)}))d\zeta \\ +x_0 \geq 0 \end{aligned} \tag{34}$$

For practical reasons the above ftCBF constraint is computed offline and then interpolated online during a simulation.

To make the computation a bit less computationally expensive and the constraint a bit more intuitive, x_0 in (34) is subtracted from both sides of the inequality sign and then both sides are multiplied with -1, which results in the following constraint

$$-\min_{t\in I(x_0)|t_0\leq t\leq t^*} (\psi_2(u^*) - x_0) \leq x_0 \tag{35}$$

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

which is easier to compute, as the constraint now does not have to be calculated offline for different starting conditions x_0, as the current value for $x(t)$ can be substituted for x_0 during the simulation to check if it satisfies the constraint. The new form of the constraint is also a bit more intuitive, as the value of the left hand side of (35) represents the required distance from the x-axis in order for (34) to be satisfied, and thus has a more physical meaning.

In Figure 4 and Figure 5 visualisations of the left hand side of the constraint (35) can be seen.

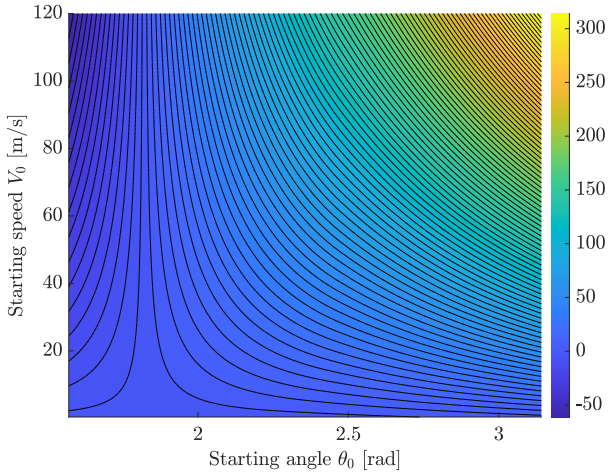

Fig. 4 This figure gives a slice of left hand side of the constraint of (35) for $u_{min_0} = -0.5$ [rad/s]. The color-bar on the right indicates the value of the left hand side of (35) and physically represents the required x-distance from the boundary the satisfy the constraint (35), which in turn is required to ensure safety for the system (22). For the computation of the constraint, $a = 0.9$ and $\gamma = 2$ were used. The lines that can be seen throughout the figure indicate different height levels of the function for visualisation purposes.

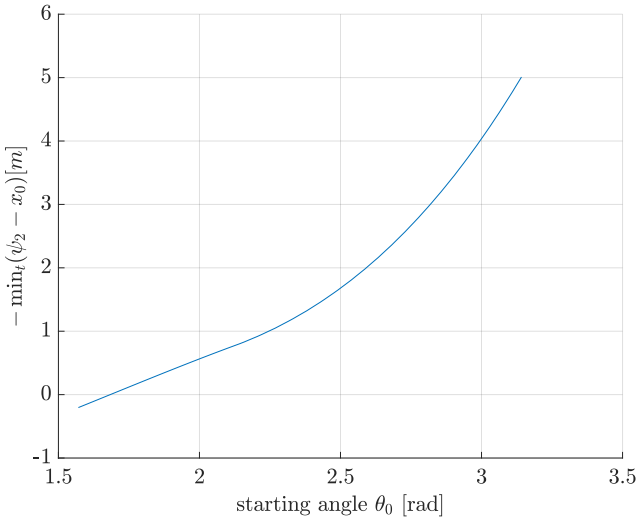

Fig. 5 This figure gives the function $-\min_{t\in I(x_0)|t_0\leq t\leq t^*}(\psi_2(u^*) - x_0)$ (left hand side of (35)) for $u_{min_s} = -0.5$ [rad/s] and $V_s = 0.5$ [m/s], and physically represents the required x-distance from the boundary to satisfy the constraint (35).

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

4.2.3 Simulation Setup

The simulation was set-up in Matlab and Simulink[10]. In Figure 6 the general layout of the setup that was used can be seen. The setup works with a joystick controller and gives input u_{joy} to the system if both the HOCBF and the ftCBF constraint are not active. If the ftCBF constraint is active the output that is given by the HOCBF constraint is overruled and the ftCBF provides the final input $u(t)$ to the system. The ftCBF thus has the highest hierarchy in the system, and always provides the input once it is activated, ensuring that the system will always remain in the safe set. The ftCBF constraint and the HOCBF constraint get state updates from the system. The HOCBF constraint is not necessary for safety, but in practice does provide a bit smoother behavior in approaching the boundary.

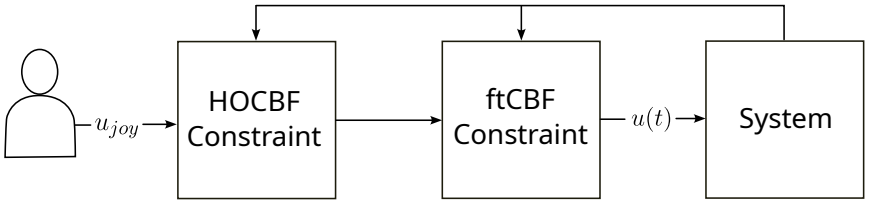

Fig. 6 General setup of the ftCBF implementation on the Dubin's Car system

The parameters that are used in the simulation will be displayed in Table 2.

Table 2 Simulation parameters ftCBF Dubin's Car

x_0	y_0	θ_0	u_{min_0}	u_{max_0}	V_c	γ	a
20	1	π	-0.5	0.5	0.5	2	0.9

4.3 Results

The main results of the simulation can be seen in Figure 8 and Figure 9, which uses xy-plots to show that the system (22) does not leave the safe set C_1 (4), defined by $\psi_0 := x(t) \geq 0$. The defined safe set and the top down view of the system used in Figure 8 and Figure 9, can be visualized in Figure 3 for more clarity. The effect of the induced failure on $V(t)$, $u_{min}(t)$ and $u_{max}(t)$, can be seen in Figure 7. The Figures 8 and 9 show that the ftCBF controller is capable of providing safety for a vehicle in the case of a failure as the vehicle does not leave the safe set C_1, defined by $\psi_0 := x(t) \geq 0$, during the simulation, regardless of when the failure occurs. This can be seen in Figure 8 where it shows a failure that happens well before the constraint would normally activate and in Figure 9 which shows an induced failure after the ftCBF constraint (35) has been activated.

The effect the ftCBF parameters γ and a on the maneuverability of the vehicle in nominal conditions (thus with no induced failure), is shown in Figure 10 and Figure 11. The effect of γ on the maneuverability is quite significant (Figure 10) as the ftCBF does not allow the system to go near to boundary $x = 0$ as much for higher values of γ. Therefore, a trade-off between safety and maneuverability has to be made as the higher the value for γ, the more prepared the system is for possible rapid changes in the system dynamics, but the less maneuverability it has. The effect of a on the maneuverability (Figure 11) in nominal conditions (thus without an induced failure) is not very significant in the range of $0.8 \leq a \leq 0.9$, as the boundary $x = 0$ is almost equally well approachable for $0.8 \leq a \leq 0.9$. It should be noted however that if the value of a becomes too small the recovery function (27) is not defined for all $0 \leq \theta \leq \pi$, as can be seen from (31). From (31) it can be deduced that if the recovery function is to be defined for all $0 \leq \theta \leq \pi$, then $e^{\frac{-0.5}{0.5\pi}} \leq a \leq 1$ for $u_{min_0} = -0.5$ and more generally $e^{\frac{u_{min_0}}{0.5\pi}} \leq a \leq 1$. However, if $0 \leq a \leq e^{\frac{u_{min_0}}{0.5\pi}}$ the vehicle can still be made safe (provided that $\theta_0 \leq \frac{\pi}{2} + \frac{u_{min_0}}{ln(a)}$), but the maneuverability will be significantly impaired as $\theta(t)$ cannot reach the whole domain $0 \leq \theta(t) \leq \pi$.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

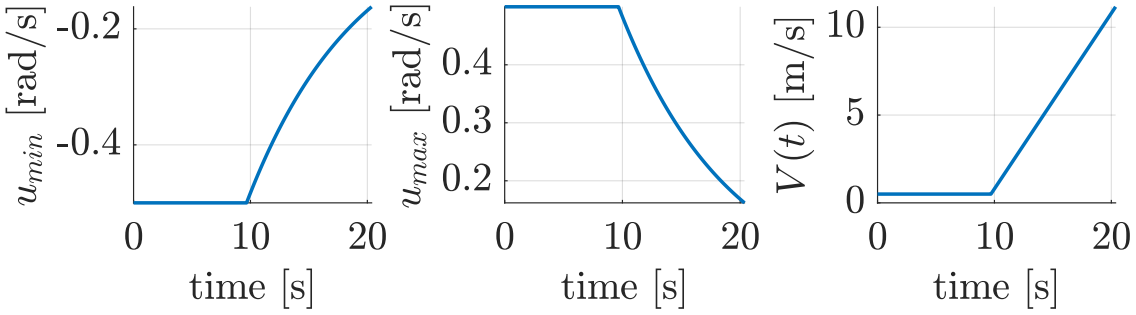

Fig. 7 This figure indicates what happens during an induced failure described by (24) and $u_{min}(t) = u_{min_0} \cdot a^t$. In the figure the failure is induced at around t=10. As can be seen the velocity $V(t)$ increases quickly and the control effectiveness decreases exponentially. The failure parameters used for this figure are $a = 0.9$ and $\gamma = 2$.

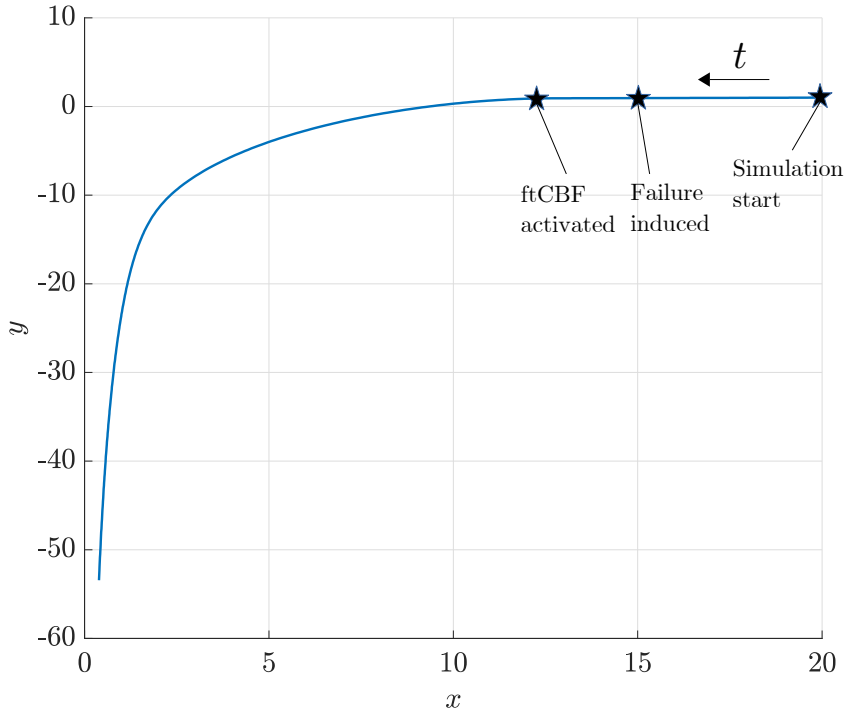

Fig. 8 This figure shows a xy-plot of the system (22). In the figure it can be seen that the ftCBF is able to keep the vehicle in the safe set C_1, defined by $\psi_0 := x(t) \geq 0$ (Figure 3), with a failure resulting in changed system dynamics and changed control bounds (as can be seen in Figure 7). In this simulation there was no joystick input given and the failure was induced before the ftCBF constraint (35) was activated. The parameters used for the simulation can be found in Table 2.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

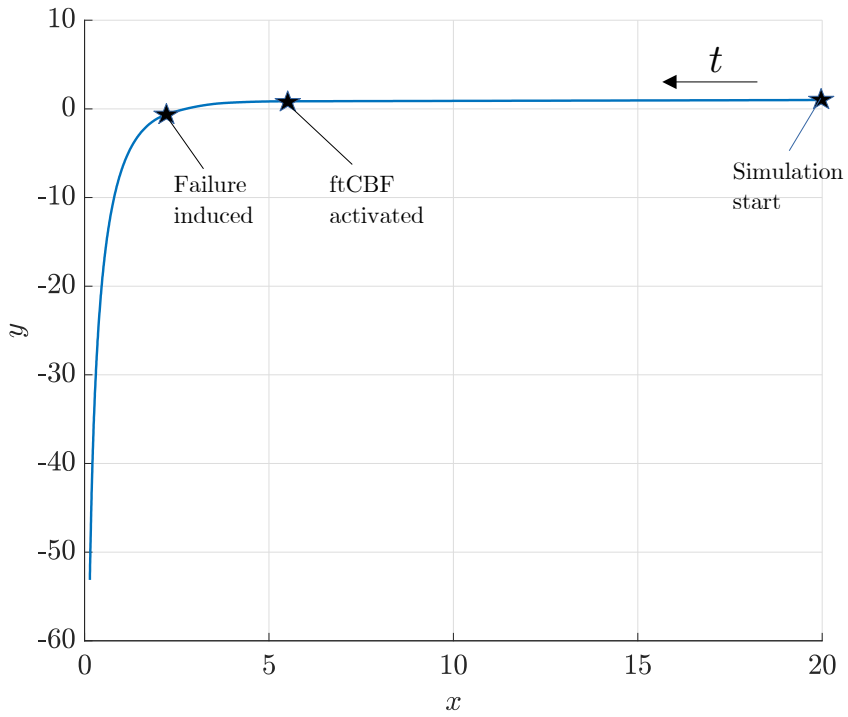

Fig. 9 This figure shows a xy-plot of the system (22). In this figure it can be seen that if the failure is induced after the ftCBF has been activated, the constraint is also able to make sure that the vehicle remains in the safe set C_1 (4), defined by $\psi_0 := x(t) \geq 0$ (Figure 3). In this simulation there was no joystick input given. The parameters used in the simulation can be found in Table 2.

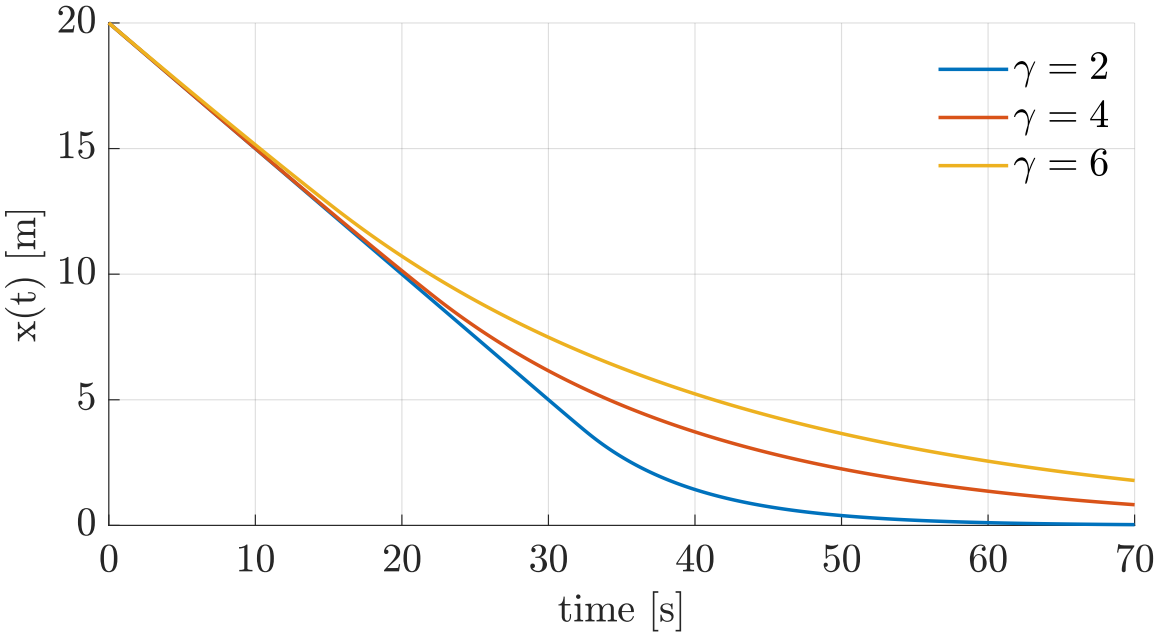

Fig. 10 This figure shows the effect of higher values of γ for (24) in the constraint (35) on vehicle maneuverability when no failure is induced. As can be seen, the faster the system dynamics are thought to be able to change (by setting a higher value for γ), the less maneuverability the vehicle has, as can be seen in the figure by the fact that the vehicle is not allowed to go near to boundary ($x = 0$) as much, as lower values of γ will allow. Setting the value for γ is thus a trade off between safety and maneuverability of the vehicle. For this figure no joystick input was given and $a = 0.9$ was used.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

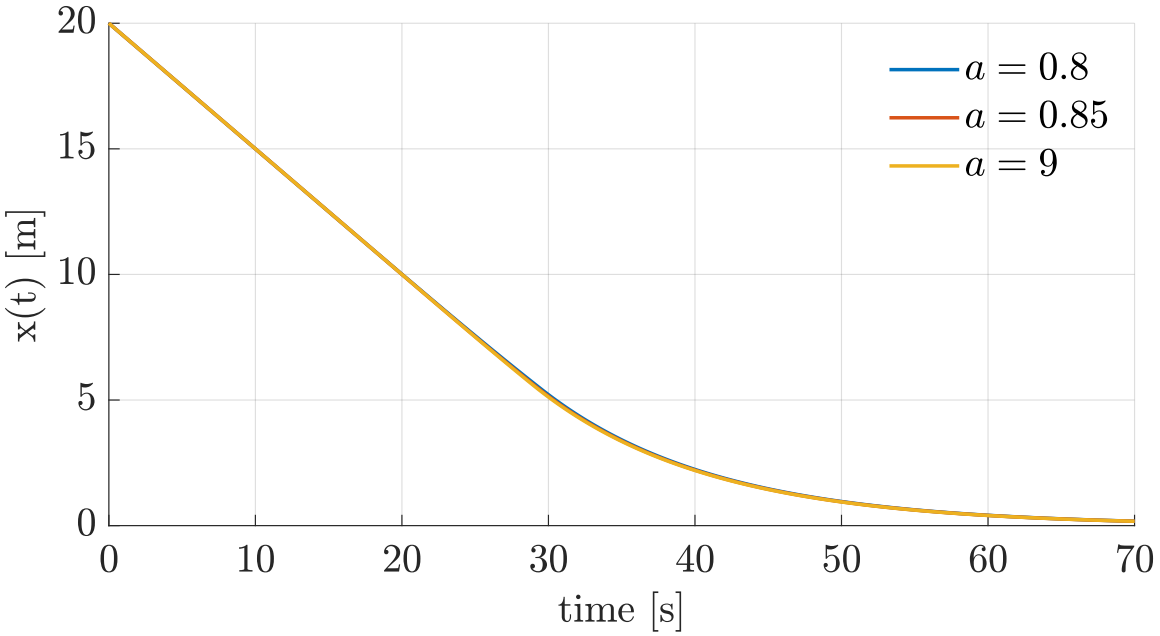

Fig. 11 This figure shows the effect of the value of a used in the failure function $u_{min}(t) = u_{min_0} \cdot a^t$, on the maneuverability of the vehicle. As can be seen in this figure, the changes in a do not effect the maneuverability of the vehicle in nominal conditions (where no failures are induced), thus it seems that a lower value of a would be most suitable, as this would mitigate more aggressive failures. However, a value of a that is lower then $a \leq e^{\frac{u_{min_0}}{0.5\pi}}$ (deduced from (31)), will result in the recovery function (27) to be not defined for all $\theta(t)$ on the domain $0 \leq \theta(t)\pi$, which will have a large impact on the maneuverability of the vehicle.

4.3.1 Discussion

The results have shown that the ftCBF constraint is able to keep systems within their safe set, even when a failure is induced.

As can be seen in Figure 10, choosing higher values for γ has an effect on maneuverability, thus a trade-off can be made between safety and performance, where higher values of γ are more in favour of safety, and lower values of γ are more favourable for performance.

Another point that should be mentioned, is that the computational time required to calculate the constraint will go up exponentially for higher dimensional systems. For the Dubin's Car model only three dimensions had to be considered for the constraint, however for more complex systems like for instance full state drone models, the amount of states required are much higher than three, which would very likely require very long computational times. This phenomenon, called curse of dimensionality, also occurs in the related field of Reachability[11], for which reachable sets are solved from the Hamilton Jacobi PDE's with the level-set methods[12].

5 Conclusion

This paper has presented a new type of control barrier function called the fault tolerant Control Barrier Function (ftCBF), that is able to keep a system within its safe set C_1 (4), with a failure event occurring at any time during the simulation.

The failure function, used in the ftCBF, has design parameters that should be tuned according to a trade-off between safety and performance of the system.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.

For future work it is recommended to incorporate measurement noise and system dynamic parameters uncertainties within the ftCBF, to further increase the safety critical behavior of the ftCBF. Further work should also be done on mitigating the curse of dimensionality, such that the ftCBF could also be used practically for higher dimensional systems.

References

[1] F. Blanchini. Set invariance in control. *Automatica*, 35:1747–1767, 11 1999. ISSN: 0005-1098. doi: 10.1016/S0005-1098(99)00113-2.

[2] Ayush Agrawal and Koushil Sreenath. Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation. In *Robotics: Science and Systems*, volume 13. Cambridge, MA, USA, 2017.

[3] Jun Zeng, Bike Zhang, and Koushil Sreenath. Safety-critical model predictive control with discrete-time control barrier function. *Proceedings of the American Control Conference*, 2021-May:3882–3889, 5 2021. ISSN: 07431619. doi: 10.23919/ACC50511.2021.9483029.

[4] Aaron D. Ames, Samuel Coogan, Magnus Egerstedt, Gennaro Notomista, Koushil Sreenath, and Paulo Tabuada. Control barrier functions: Theory and applications. *2019 18th European Control Conference, ECC 2019*, pages 3420–3431, 6 2019. doi: 10.23919/ECC.2019.8796030.

[5] Quan Nguyen and Koushil Sreenath. Exponential control barrier functions for enforcing high relative-degree safety-critical constraints; exponential control barrier functions for enforcing high relative-degree safety-critical constraints. *American Control Conference*, 2016. doi: 10.1109/ACC.2016.7524935.

[6] Wei Xiao and Calin Belta. Control barrier functions for systems with high relative degree. volume 2019-December, pages 474–479. Institute of Electrical and Electronics Engineers Inc., 12 2019. ISBN: 9781728113982. doi: 10.1109/CDC40024.2019.9029455.

[7] Wei Xiao, Calin Belta, and Christos G. Cassandras. Adaptive control barrier functions. *IEEE Transactions on Automatic Control*, 67:2267–2281, 5 2022. ISSN: 15582523. doi: 10.1109/TAC.2021.3074895.

[8] Hassan K Khalil. *Nonlinear systems; 3rd ed.* Prentice-Hall, Upper Saddle River, NJ, 2002.

[9] David Angeli and Eduardo D. Sontag. Forward completeness, unboundedness observability, and their lyapunov characterizations. *Systems Control Letters*, 38:209–217, 12 1999. ISSN: 0167-6911. doi: 10.1016/S0167-6911(99)00055-9.

[10] MATLAB. *version R2021a*. The MathWorks Inc., Natick, Massachusetts, 2021.

[11] John Lygeros. On reachability and minimum cost optimal control. *Automatica*, 40:917–927, 6 2004. ISSN: 0005-1098. doi: 10.1016/J.AUTOMATICA.2004.01.012.

[12] Ian M. Mitchell. The flexible, extensible and efficient toolbox of level set methods. *Journal of Scientific Computing*, 35:300–329, 6 2008. ISSN: 08857474. doi: 10.1007/S10915-007-9174-4/METRICS.

Except where otherwise noted, content of this paper is licensed under a Creative Commons Attribution 4.0 International License.

The reproduction and distribution with attribution of the entire paper or of individual pages, in electronic or printed form, including any material under non-CC-BY 4.0 licenses is hereby granted by the authors and respective copyright owners.