MITSUBISHI ELECTRIC RESEARCH LABORATORIES
https://www.merl.com

MPC with Integrated Evasive Maneuvers for Failure-safe Automated Driving

Skibik, Terrence; Vinod, Abraham P.; Weiss, Avishai; Di Cairano, Stefano

TR2023-055 June 01, 2023

Abstract

Automated vehicles may encounter non-nominal situations called failure scenarios, due for instance to errors in perception or environment prediction. In some failure scenarios, a risk area must suddenly be avoided, possibly at the price of no longer satisfying all the constraints enforced in nominal driving conditions. We propose a design for a failure-safe controller that operates the vehicle according to the specifications in nominal conditions, while ensuring that, should a known failure occur, an evasive maneuver can be performed that avoids the risk area and satisfies a possibly relaxed set of driving constraints. We design evasive maneuver controllers parametrized in their reference, and we leverage set based methods to determine the region where such controllers satisfy the constraints and avoid the risk area. Membership in such a region during nominal operation is achieved by imposing additional constraints on the controller for nominal driving. We demonstrate the approach in simulations in a few different scenarios.

American Control Conference (ACC) 2023

Mitsubishi Electric Research Laboratories, Inc.
201 Broadway, Cambridge, Massachusetts 02139

MPC with Integrated Evasive Maneuvers for Failure-safe Automated Driving

Terrence Skibik, Abraham P. Vinod, Avishai Weiss, Stefano Di Cairano

***Abstract*— Automated vehicles may encounter non-nominal situations called failure scenarios, due for instance to errors in perception or environment prediction. In some failure scenarios, a risk area must suddenly be avoided, possibly at the price of no longer satisfying all the constraints enforced in nominal driving conditions. We propose a design for a failure-safe controller that operates the vehicle according to the specifications in nominal conditions, while ensuring that, should a known failure occur, an evasive maneuver can be performed that avoids the risk area and satisfies a possibly relaxed set of driving constraints. We design evasive maneuver controllers parametrized in their reference, and we leverage set based methods to determine the region where such controllers satisfy the constraints and avoid the risk area. Membership in such a region during nominal operation is achieved by imposing additional constraints on the controller for nominal driving. We demonstrate the approach in simulations in a few different scenarios.**

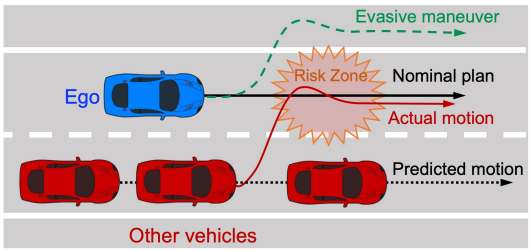

Fig. 1. Failure scenario requiring evasive maneuver: the ego vehicle computes a nominal plan based on a predicted motion of the other vehicles maintains their lanes. The actual motion of one of the other vehicles cuts in front of the ego vehicle, in a way that could lead to a collision. An evasive maneuver avoids entering the risk zone, where collision may occur, at the price of an aggressive sway maneuver that drives on the shoulder.

I. Introduction

As operations of automated vehicles expand to general conditions, they will encounter situations that are not nominal [1]. Some situations, which we will call "failure scenarios" or simply "failures", may be caused by mechanical or electronic malfunctions, or, much more commonly, from failures in understanding the environment, such as missing, misclassifying or wrongly predicting surrounding agents.

In the failure scenarios the automated vehicle must maintain safety, such as avoiding a dangerous zone, i.e., an exclusion zone, that may be impossible while retaining the specifications for nominal driving. Figure 1 shows an example where the ego vehicle computes a *nominal plan* based on a *predicted motion* of the other vehicles. However, the *actual motion* of one of the other vehicles aggressively cuts in front of the ego, which would lead to a risk of collision should the nominal plan be followed. In this case, the ego initiates an evasive maneuver that avoids entering the *risk zone* where a collision may occur, at the price of being more aggressive than in normal driving and of violating the nominal traffic rules by driving on the shoulder.

A single controller could be designed for performing both nominal and evasive maneuvers. However, it is hard to ensure that the evasive maneuver behavior is only enacted in the presence of failures. A different approach is to design a control system that integrates a nominal controller with one or more failure-handling controllers, the former providing nominal behavior that satisfies all the rules, and the latter providing evasive maneuvers when a failure is detected. In this approach, when a failure is detected, the autonomous vehicle must be in a condition that allows the evasive maneuver to avoid the risk zone, while satisfying a set of, possibly relaxed, constraints. The detection of failure is usually addressed by the perception system. Our focus is on determining conditions such that the evasive maneuver succeed, and then designing a nominal controller that guarantees such conditions and makes the evasive maneuver readily available, should a failure be detected.

Here, we address such problem by: (i) designing evasive maneuver controllers based on appropriate models, with maneuver parameters as decision variables; (ii) determining the set where the evasive maneuver controller satisfies the maneuver constraints on vehicle and the traffic rules, and avoids the risk zone; (iii) enforcing membership in such set as constraints on the nominal controller, that also determines the evasive maneuver parameters.

Set-based methods have been investigated for several operations in automated driving, such as decision making, motion planning, safety verification, and robust control, see, e.g., [2]–[7] and the references therein. Motion planning with failsafe trajectory is proposed in [8] for decoupled and integrator-like longitudinal and lateral dynamics, where failsafe maneuvers are not subject to any additional vehicle constraints or traffic rules. The method proposed here draws from our recent works in abort-safe control design [9], [10] for spacecraft rendezvous [11]. Compared to such works, we parametrize the evasive maneuvers by their target, i.e., reference, which allows for a degree of freedom in the maneuver, as opposed to the passive safe abort in [9], that has no

T. Skibik is with Dept. Electrical Engineering, University of Colorado, Boulder Terrence.Skibik@colorado.edu, and was an intern at MERL during this work.

A. Vinod, A. Weiss, S. Di Cairano are with Mitsubishi Electric Research Laboratories, Cambridge, MA. {vinod,weiss,dicairano}@ieee.org

actuation after failure, and the active safe abort in [10], that allows actuation but cannot enforce state constraints other than exclusion zone avoidance. The chosen parameterization enables the computation of the sets where constraints are satisfied and where the risk zone is avoided in an augmented state-parameter space as in reference governors [12].

The nominal controller, implemented by model predictive control (MPC) [13], determines the maneuver reference to satisfy membership in both sets. MPC with integrated reference manipulation has been developed in the past to achieve recursive feasibility, see, e.g., [14], while here MPC determines the maneuver reference to enlarge the area where the evasive maneuver succeeds. A related construction for exclusion zone constraints appeared [15], that only aims at providing a method to modifying an existing control signal to ensure safety, instead of an integrated failure-safe controller.

In what follows, in Section II we introduce the models for nominal and evasive maneuvers, and formalize the problem. In Section III we describe the computation of the sets where the evasive maneuvers succeed. In Section IV we describe the implementation of the failure-safe vehicle controller, such that the existence of an evasive maneuver is guaranteed. We validate the approach in simulations in Section V, and conclusions are drawn in Section VI.

Notation: $\mathbb{Z}$, $\mathbb{Z}_{0+}$, and $\mathbb{Z}_+$ are the sets of integers, nonnegative integer and positive integers, and we denote intervals as $\mathbb{Z}_{[a,b)} = \{z \in \mathbb{Z} : a \leq z < b\}$. For a set $\mathcal{X}$, its complement is $\mathcal{X}^c$. For a matrix X and a vector x, $[X]_i$, $[x]_i$ denote the i^{th} row and i^{th} component, respectively. For vectors x, y, the stacking is $(x, y) = [x'\ y']'$, and inequalities between them are intended componentwise. We denote all-zero and all-one matrices/vectors by 0, 1, when dimensions are evident from the context. For a discrete-time signal $x \in \mathbb{R}^n$, $x(t)$ is the value a sampling instant t and $x_{k|t}$ denotes the predicted value of x k steps ahead of t, based on data at sample t.

II. Modeling and Problem Definition

First, we describe the models and constraints for nominal driving and evasive maneuvers, and then we formalize the failure-safe control problem.

A. Nominal driving

Under normal conditions, the automated driving system is expected to operate non-aggressively, in order to maximize the comfort and trust of the passengers. Thus, a kinematic motion model that ignores tires and traction forces is in general sufficient for motion planning and control [16]–[18],

$$\dot{p}_x = v\cos(\psi) \tag{1a}$$
$$\dot{p}_y = v\sin(\psi) \tag{1b}$$
$$\dot{\psi} = \frac{v}{L_a}\tan(\delta) \tag{1c}$$
$$\dot{v} = a \tag{1d}$$
$$\dot{\delta} = \sigma \tag{1e}$$

where $p = (p_x, p_y)$ is the position in the global frame, v is the vehicle velocity, ψ is the heading angle in the global frame, L_a is the wheelbase, a is the acceleration, δ is the steering angle, σ is the steering angular rate.

During normal driving the vehicle must satisfy constraints on its motion and on traffic rules. We consider constraints on acceleration, steering, and steering rate, that impose a comfortable driving behavior and that keep the vehicle operating in a region where the kinematic model (1) is a reliable motion model, e.g., tire sideslip effects are negligible,

$$\begin{aligned} &a_{\min}^{(m)} \leq a \leq a_{\max}^{(m)}, \quad \delta_{\min}^{(m)} \leq \delta \leq \delta_{\max}^{(m)}, \\ &\sigma_{\min}^{(m)} \leq \sigma \leq \sigma_{\max}^{(m)}, \end{aligned} \tag{2a}$$

where $m = 0$ for nominal driving. Road rules impose additional constraints, such as admissible position on the road with respect to the centerlane, velocity constraints, and safety distance from other vehicles,

$$\begin{aligned} &v_{\min}^{(m)} \leq v \leq v_{\max}^{(m)}, \quad \mathcal{D}(p, \mathcal{O}) \geq d_{\min}^{(m)}, \\ &w_{\min}^{(m)} \leq \mathcal{M}(\psi^r)(p - r) \leq w_{\max}^{(m)} \end{aligned} \tag{2b}$$

where $\mathcal{M}(\psi^r)(p-r)$ extracts the lateral distance from road heading ψ^r at a reference point r, $\mathcal{D}$ is a distance function, or an under-approximation, $\mathcal{O}$ is the closest obstacle position, and for nominal driving $m = 0$.

B. Evasive maneuvers against failures

Model (1) and vehicle and road constraints (2) where $m = 0$ are used for nominal motion planning and control. However, unforeseen events indicative of abnormal situations and hence called "failures", may occur, that require avoidance of possibly time-varying exclusion zones. Causes of such failures may be limited perception, such fast or an undetected vehicle or pedestrian appearing just ahead, or incorrect prediction of the environment, such as for a vehicle suddenly stopping or changing lane, a pedestrian unexpectedly crossing the street.

When a failure occurs, the system starts operating in a "failure mode". For each failure mode, $m \in \mathbb{Z}_{[1,M]}$, the exclusion zone $\mathcal{A}$ results in additional avoidance constraints

$$p(t) \notin \mathcal{A}^{(m)}(t), \tag{3a}$$

that must be satisfied only after the failure occurs. Satisfying (3) at all times, together with (2) for (1), may result in excessively conservative driving, or even infeasibility of the motion planning.

Instead of handling failures through nominal driving conditions, we design special evasive maneuvers where the set of constraints (2a), (2b) may be relaxed

$$\begin{aligned} &\eta_{\min}^{(m)} \leq \eta_{\min}^{(0)}, \quad \eta_{\max}^{(m)} \geq \eta_{\max}^{(0)}, \\ &m = 1, 2, \ldots, \quad \eta \in \{a, \delta, \sigma, v, w, d\}. \end{aligned} \tag{4}$$

Thus, in the evasive maneuvers some of the nominal comfort ranges or road rules may be violated, which seems like a reasonable price to pay to avoid a catastrophic outcome in a failure scenario. Due to their different objectives, the evasive maneuvers may also be computed based on different motion models. Indeed, evasive maneuvers must be computed

quickly, thus it may be convenient to use linear models. Here we consider separately evasive maneuvers based on sway, i.e., lateral motion, and braking, i.e., longitudinal motion. For sway maneuver we use the dynamic bicycle model with respect to the centerlane with constant longitudinal velocity [19]

$$\begin{aligned}
\ddot{y}^e &= -\frac{C_f + C_r}{m_v v_x}\dot{y}^e + \frac{C_f + C_r}{m_v}\psi^e + \frac{-C_f\ell_f + C_r\ell_r}{m_v v_x}\dot{\psi}^e \\
&\quad + \frac{C_f}{m_v}\delta - \left(\frac{C_f\ell_f - C_r\ell_r}{m_v v_x} + v_x\right)\dot{\psi}^r \\
\ddot{\psi}^e &= -\frac{C_f\ell_f - C_r\ell_r}{m_v v_x}\dot{y}^e + \frac{C_f\ell_f - C_r\ell_r}{I_z}\psi^e - \frac{C_f\ell_f^2 + C_r\ell_r^2}{I_z v_x}\dot{\psi}^e \\
&\quad + \frac{C_f\ell_f}{I_z}\delta - \frac{C_f\ell_f^2 + C_r\ell_r^2}{I_z v_x}\dot{\psi}^r \\
\dot{v}_x &= 0 \\
\dot{d} &= v_x,
\end{aligned} \tag{5a}$$

where y^e is the lateral error with respect to road centerlane, ψ^e is the heading error with respect to road direction, $\dot{\psi}^r = v_x^2/R^r$ is the desired yaw rate, R^r is the turn radius, C_f, C_ν are the total front and rear cornering stiffnesses, v_x is the longitudinal velocity, d is the distance along the road, m_v is the vehicle mass, I_z is the moment of inertia along the vertical axes, and ℓ_f, ℓ_r are the front and rear axle distances from the center of mass. The sway maneuver sets v_x to a known value and keeps it constant. Assuming also the road radius R^r known in advance and constant, (5a) gives a linear model with $x^{(m)} = [y^e\ \dot{y}^e\ \psi^e\ \dot{\psi}^e\ d^e]'$, with parameters v_x and $\dot{\psi}^r$, which can be added to the state vector to model different (constant) conditions.

For braking maneuvers, we use a longitudinal vehicle motion model with constant lateral position and yaw

$$\begin{aligned}
\dot{d} &= v_x \\
\dot{v}_x &= -\frac{F_b}{m_v} \\
\dot{y}^e &= 0 \\
\dot{\psi} &= 0
\end{aligned} \tag{5b}$$

where F_b is the braking force from the braking system. Since the vehicle is not turning, the yaw can be ignored, and (5b) results in a linear model with $x^{(m)} = [d\ v_x\ y^e]'$.

C. Control architecture and problem definition

An overview schematic of the system considered here is shown in Figure 2. Based on the *ego vehicle* state and the surrounding *environment*, the *failure scenarios selector* in the *failure supervisor* determines the possible failure scenarios that the vehicle may encounter in the current conditions. The *failure-safe controller* determines a *nominal maneuver* and an *evasive maneuver* for each of the possible M_t failure scenarios. The *failure detector* determines whether the vehicle is operating nominally or it is in one of the failure scenarios. This is used by *a command selector* to determine what command is to be executed: if no failures are detected, the nominal maneuver is executed, resulting in comfortable drive and satisfaction of the nominal traffic rules, otherwise the evasive maneuver is executed, which may be more aggressive and possibly violate some of the nominal traffic rules, but avoids the exclusion zone.

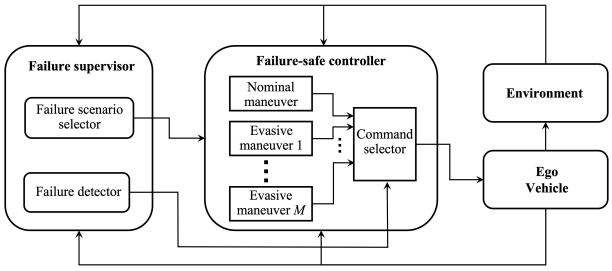

Fig. 2. Schematic of the failure-safe control architecture. The failure supervisor includes a failure scenarios selector that determines the possible failure scenarios and a failure detector that determines whether a failure scenario occurred. The failure-safe controller determines a nominal maneuver and evasive maneuvers for each of the possible M failure scenarios. The command selector determines what command is sent to the ego vehicle based on the failure detector.

In this paper we focus on the design of the failure-safe controller, while leaving the failure supervisor, which is primarily related to the perception system, to different works. Let $u_t = \kappa^{(0)}(x_t^{(0)}, r_t^{(0)})$ be a nominal controller for the nominal model (1), where $x^{(0)}$ is the nominal motion model state and $r^{(0)}$ are reference values, i.e., targets, and let the corresponding closed loop be $x_{t+1}^{(0)} = f_c^{(0)}(x_t^{(0)}, r_t^{(0)})$. Let $u_t = \kappa^{(m)}(x_t^{(m)}, \nu_t^{(m)})$, $m \in \mathbb{Z}_{[1,M]}$, be M evasive maneuver controllers, for evasive maneuver models such as (5) where $x^{(m)}$ is the evasive motion model state and $\nu^{(m)}$ is a maneuver parameter, and let $x_{t+1}^{(m)} = f_c^{(m)}(x_t^{(m)}, \nu_t^{(m)})$ be the closed-loop motion of the evasive maneuver. The objective of this paper is as follows.

Problem 1: Given a safety horizon $N \in \mathbb{Z}_+$, design $\kappa^{(m)}$, $m \in \mathbb{Z}_{[0,M]}$ such that under nominal operation $x_{t+1}^{(0)} = f_c^{(0)}(x_t^{(0)}, r_t^{(0)})$ satisfies (2) for $m = 0$ and, if failure $m \neq 0$ occurs at any $x_t^{(0)}$ of the closed-loop trajectory, there exist $\left(\nu_\tau^{(m)}\right)_{\tau=t}^{t+N-1}$ such that $x_{\tau+1}^{(m)} = f_c^{(m)}(x_\tau^{(m)}, \nu_\tau^{(m)})$ satisfies (2) and (3) for all $\tau \in \mathbb{Z}_{[t,t+N]}$. ■

III. Evasive maneuver controller Construction

For the evasive maneuver controllers we determine a structure and the set of the states and parameters for which the controller achieves the behavior solving Problem 1. Since we aim at keeping the calculations simple, to ensure fast reaction time, we consider linear feedforward-plus-feedback controllers

$$\kappa^{(m)}(x^{(m)}, \nu^{(m)}) = K^{(m)}x^{(m)} + G^{(m)}\nu^{(m)}, m \in \mathbb{Z}_{[1,M]}. \tag{6}$$

For a linear model of the evasive motion $x_{t+1}^{(m)} = A^{(m)}x_t^{(m)} + B^{(m)}u_t^{(m)}$, such as those in (5), with a control law in the form of (6) and an auxiliary constant reference dynamics, the closed-loop evasive maneuver motion model

is

$$x^{(m)}_{k+1|t} = (A^{(m)}+B^{(m)}K^{(m)})x^{(m)}_{k|t} + B^{(m)}G^{(m)}\nu^{(m)}_{k|t} \quad (7a)$$

$$\nu^{(m)}_{k+1|t} = \nu^{(m)}_{k|t} \quad (7b)$$

$$p^{(m)}_{k|t} = C^{(m)}x^{(m)}_{k|t} \quad (7c)$$

where (7c) is the position in the maneuver reference frame.

Here, we recall some basic results, see, e.g., [12], [20].

Definition 1: Given system $x_{t+1} = f(x_t)$, and set $\mathcal{S}$ the (1-step) backward reachable set of $\mathcal{S}$ through f is the set of states that are in $\mathcal{S}$ after one step through f, i.e., $\mathrm{Pre}_f(\mathcal{S}) = \{x : \ f(x) \in \mathcal{S}\}$. The N-steps backward reachable set is recursively defined as $\mathrm{Pre}^N_f(\mathcal{S}) = \mathrm{Pre}_f(\mathrm{Pre}^{N-1}_f(\mathcal{S}))$. □

Definition 2: Given system $x_{t+1} = f(x_t)$ subject to $y_t = h(x_t) \in \mathcal{S}$, the N-steps constraint admissible set is the set of initial states for which the evolution through f satisfies the constraints for at least N steps, $\mathcal{O}_N = \{x : \ x_{k+1} = f(x_k),\, x_0 = x,\, h(x_k) \in \mathcal{S},\, \forall k \in \mathbb{Z}_{[0,N]}\}$. □

Definition 3: A constraint admissible set is the limit of a sequence of N-steps admissible sets, $\mathcal{O}_\infty = \lim_{N\to\infty} \mathcal{O}_N$. A constraint admissible set is maximal if it contains all others constraint admissible sets. □

Result 1: Let f, h define an asymptotically stable, fully observable linear system, and $\mathcal{S}$ be a compact polytope. Then, the maximal constrained admissible set $\mathcal{O}_\infty$: (i) exists; (ii) is a finitely determined polytope, i.e., described by a finite number of constraints; (iii) is the fix point of the sequence $\mathcal{O}_0 = \mathcal{S}$, $\mathcal{O}_{k+1} = \mathcal{O}_k \cap \mathrm{Pre}_f(\mathcal{O}_k)$, which is reached in finite time $\bar{k}$, i.e, $\mathcal{O}_{\bar{k}+1} = \mathcal{O}_{\bar{k}}$. □

Next, we define the set where the evasive maneuver (7) for the failure scenario m satisfies (1), (2). The exclusion zone (3) is the region to be avoided from the time when the failure scenario m occurs,

$$\mathcal{A}^{(m)} = \{(p^{(m)}, \rho^{(m)}) : \ -\ell^{(m)}_{\min} \le (p^{(m)} - \rho^{(m)}) \le \ell^{(m)}_{\max}\}, \quad (8)$$

where $\rho^{(m)}$ is the position of the reference point of the exclusion zone in the reference frame of the evasive maneuver, and the vectors $\ell^{(m)}_{\min}$, $\ell^{(m)}_{\max}$ define the spatial extent. For allowing the exclusion zone to move with a known motion from the initial time when the failure occurs, e.g., a car cutting in front of the ego vehicle and proceeding at a slow speed, we model $\rho^{(m)}$ as the output of a known system,

$$\phi^{(m)}_{k+1|t} = \Phi^{(m)}\phi^{(m)}_{k|t}, \quad (9a)$$

$$\rho^{(m)}_{k|t} = \Theta^{(m)}\phi^{(m)}_{k|t}, \quad (9b)$$

where $\phi^{(m)}$ is the state and the initial value $\phi_{0|t}$ is known and describe the conditions when the fault initially occurs. Thus, for each failure scenario, the exclusion zone is defined by its spatial extent (8), its motion after the failure occured (9), and the initial state of (9) when the failure occurs $\phi_{0|t}$.

We combine (7), (9) in a dynamical system

$$\xi^{(m)}_{t+1} = A^{(m)}_\xi \xi_t, \quad \eta_t = C^{(m)}_\xi \xi^{(m)}_t, \quad (10)$$

$$A^{(m)}_\xi = \begin{bmatrix} A^{(m)}+B^{(m)}K^{(m)} & B^{(m)}F^{(m)} & 0 \\ 0 & I & 0 \\ 0 & 0 & \Phi^{(m)} \end{bmatrix}, C_\xi = \begin{bmatrix} C^{(m)} & 0 & -\Upsilon^{(m)} \end{bmatrix}$$

where $\xi^{(m)}_t = (x^{(m)}_t, \nu^{(m)}_t, \phi^{(m)}_t)$ is the state. The exclusion zone polytope

$$\mathcal{A}^{(m)}_\xi = \{(x^{(m)}, \nu^{(m)}, \phi^{(m)}) : \ H^{(m)}_x x^{(m)} + H^{(m)}_\phi \phi^{(m)} + H^{(m)}_\nu \nu \le H^{(m)}_b\}, \quad (11)$$

where we may add constraints to ensure boundedness based on (2) without removing any relevant part of the space. The set such that $\xi^{(m)}_k \in \mathcal{A}^{(m)}_\xi$ for $k \in \mathbb{Z}_{[0,N]}$ is

$$\mathcal{W}^{(m)}_k = \mathrm{Pre}^k_{A_\xi}(\mathcal{A}^{(m)}_\xi), \quad (12)$$

and the safe set where collisions are avoided for N steps is

$$\mathcal{F}^{(m)} = \left(\bigcup_{k=0}^{N} \mathcal{W}^{(m)}_k\right)^c. \quad (13)$$

which is in general non-convex. Then, the exclusion zone avoidance constraint is $(x^{(m)}_t, \nu^{(m)}_t, \phi^{(m)}_{0|t}) \in \mathcal{F}^{(m)}$.

Besides the exclusion zone avoidance, the evasive maneuver must satisfy some vehicle and traffic rules constraints (2), where $m \neq 0$, although these may be relaxed with respect to those for nominal driving. Since the maneuver is parametrized through its reference, we compute the constraint admissible set of states and references for (7) subject to (2), and then lift it to the dimension of (10), resulting in

$$\mathcal{O}^{(m)}_\infty = \{(x^{(m)}, \nu^{(m)}, \phi^{(m)}) : x^{(m)}_0 = x^{(m)}, \ \nu^{(m)}_0 = r, \ \phi^{(m)}_{0|t} = \phi^{(m)} \implies (7) \text{ satisfies } (2), \forall t \in \mathbb{Z}_+\}. \quad (14)$$

In this work, we consider constraints (2) that for $m \neq 0$, when formulated with respect to (7) are linear inequalities. Thus, by Result 1, $\mathcal{O}^{(m)}_\infty$ is a polyhedron. According to Problem 1, in (15) it is enough to use $\mathcal{O}^{(m)}_N$, but here we use $\mathcal{O}^{(m)}_\infty$ since it may be beneficial to ensure constraint feasibility for longer horizons.

Based on (13), (14) we can characterize the region where the evasive maneuver (7) succeeds in avoiding the exclusion zone (3) and in satisfying the constraints (2).

Proposition 1: Consider failure scenario $m \in \mathbb{Z}_{[1,M]}$ with exclusion zone defined by (8), (9), $\phi^{(m)}_{0|t}$, all given for every $t \in \mathbb{Z}_{0+}$. For all x_t such that there exists $\nu^{(m)}_t$ for which

$$(x^{(m)}_t, \nu^{(m)}_t, \phi^{(m)}_{0|t}) \in \mathcal{F}^{(m)} \cap \mathcal{O}^{(m)}_\infty \quad (15)$$

evasive maneuver (7) satisfies (2), (3) for all $\tau \in \mathbb{Z}_{[t,t+N]}$.

Remark 1: If the entire maneuver input sequence were free, as in [10] that only require avoidance, the sets dimensions will grow with the safety horizon, so that the computations at design time become hard and those at runtime, slow. The approach of "eliminating" the inputs in the set computation [10] avoids such an issue, but avoidance and constraint satisfaction can no longer be enforced at the same time, because there is no guarantee that a single input can achieve both, i.e., we cannot intersect the sets as in (15). Parameterizing the evasive maneuver by a constant reference avoids the dimension to grow with N, and allows intersecting the sets as in (15), which guarantees both, exclusion zone avoidance and constraint satisfaction. □

Next, we discuss how the failure-safe controller ensures the feasibility of evasive maneuvers by imposing the nominal operation to satisfy the conditions of Proposition 1.

IV. Failure-safe Vehicle Control by MPC

Next, we design the failure-safe controller in Figure 2 that produces nominal maneuvers ensuring that should the failure be detected the evasive maneuver succeeds.

A. Failure-safe Model Predictive Control

We design a model predictive control (MPC) based on the nominal vehicle model (1) and nominal constraints (2), that ensures that the trajectory remains within the region where (15) is feasible. At every step t the supervisor shown in Figure 2 provides the subset $\mathcal{M}_t \subseteq \mathbb{Z}_{[1,M]}$ of the possible failure scenarios and the initial conditions for the exclusion zone motion (9), and the failure-safe controller solves the optimal control problem

$$\min_{U_t, \Upsilon_t} \; F(x^{(0)}_{N_p|t}, r^{(0)}_{N_p|t}) + \sum_{k=0}^{N_p-1} \Big(L(x^{(0)}_{k|t}, u_{k|t}, r^{(0)}_{k|t}) + \sum_{m\in\mathcal{M}_t} L^{(m)}_{\nu}(\nu^{(m)}_{k|t}) \Big) \quad (16a)$$

$$\text{s.t. } x^{(0)}_{k+1|t} = f^{(0)}(x^{(0)}_{k|t}, u_{k|t}) \quad (16b)$$

$$(x^{(0)}_{k|t}, u_{k|t}) \in \mathcal{C}^{(0)} \quad (16c)$$

$$x^{(m)}_{k|t} = h^{(m)}(x^{(0)}_{k|t}, u_{k|t}, r^{(0)}_{k|t}), \quad (16d)$$

$$(x^{(m)}_{k|t}, \nu^{(m)}_{k|t}, \phi^{(m)}_{k|t}) \in \mathcal{O}^{(m)}_{\infty} \cap \tilde{\mathcal{F}}^{(m)}_{k|t} \quad (16e)$$

$$x^{(0)}_{0|t} = x(t), \; \phi^{(m)}_{k|t} = \phi^{(m)}(t+k), \forall m \in \mathcal{M}_t \quad (16f)$$

where in (16a), N_p is the prediction horizon, usually $N_p \ll N$, F and L are the terminal and stage cost for nominal driving, $L^{(m)}_{\nu}$, $m \in \mathbb{Z}_{[1,M]}$, are costs associated to the evasive maneuvers parameters, $U_t = (u_{0|t} \dots u_{N_p-1|t})$, $\Upsilon_t = \{(\nu^{(m)}_{0|k} \dots \nu^{(m)}_{N_p|t})\}_{m\in\mathcal{M}_t}$, (16c) are the nominal constraints (2) for $m = 0$, (16e) imposes membership in the sets where the evasive maneuvers succeed and $\tilde{\mathcal{F}}^{(m)}_{k|t} \subseteq \mathcal{F}^{(m)}$, for all $k \in \mathbb{Z}_{[0,N_p-1]}$, $m \in \mathcal{M}_t$, (16d) constructs the state of the model of evasive maneuver m from the nominal state, input and reference $r_{t|k}$, $k \in \mathbb{Z}_{[0,N_p]}$, which contains road information, (16b) is the nominal driving dynamics[1](1), and (16f) initializes the prediction model and the exclusion zone motions at each prediction step. The initialization in (16f) defines the initial state of the exclusion zone when a failure occurs at different instants in the prediction horizon, while (9) describes the evolution of the exclusion zone after the failure occurs. Hence, $\phi(t+k)$, $k \in \mathbb{Z}_{[0,N-1]}$, are initialized by the failure scenario selector.

Based on the solution of (16), $U^*_t = (u^*_{0|k} \dots u^*_{N_p|t})$, $\Upsilon^*_t = \{(\nu^{(m),*}_{0|k} \dots \nu^{(m),*}_{N_p|t})\}_{m\in\mathcal{M}_t}$, the nominal controller and evasive controllers of Problem 1 are constructed as

$$\kappa^{(0)}\Big(x_t, \{r^{(0)}_{k|t}\}^N_{k=0}, \{\phi^{(m)}_t\}_{m\in\mathcal{M}_t}\Big) = u^*_{0|t} \quad (17a)$$

$$\kappa^{(m)}\Big(x_t, \{r^{(0)}_{k|t}\}^N_{k=0}, \{\phi^{(m)}_t\}_{m\in\mathcal{M}_t}\Big) = K^{(m)}x(t) + G^{(m)}\nu^{(m),*}_{0|t}, \; \forall m \in \mathcal{M}_t. \quad (17b)$$

In (16e), $\tilde{\mathcal{F}}^{(m)}_{k|t} \subseteq \mathcal{F}^{(m)}$ is a convex subset, which makes the computations in (16) simpler and may avoid additional approximations internal to the optimization routine. $\tilde{\mathcal{F}}^{(m)}_{k|t}$ can be constructed in multiple ways, see, e.g., [9], [20]. Next, we briefly describe the approach used here.

B. Avoidance Constraint Convexification

Convexification based on a single separating hyperplane [9] prevents the trajectory from entering regions surrounded by sets $\mathcal{W}^{(m)}_k$ on multiple sides. For automated driving applications, this may be limiting due to the shape of the sets $\mathcal{W}^{(m)}_k$, for instance for sway maneuvers. Thus, we convexify $\mathcal{F}^{(m)}$ around the trajectory from previous time step by projections, obtaining

$$\tilde{\mathcal{F}}^{(m)}_{k|t} = \{\xi : \Gamma^{(m)}_{k|t}\xi \le \gamma^{(m)}_{k|t} - \varepsilon 1\}, \quad (18)$$

where $\xi = (x^{(m),*}, \nu^{(m)}, \phi^{(m)})$, $\Gamma^{(m)}_{k|t}$ and $\gamma^{(m)}_{k|t}$ are a matrix and a vector with $N+1$ rows, and ε is an arbitrarily small positive constant. Let $\bar{\xi}^{(m)}_{k|t} = (x^{(m),*}_{k+1|t-1}, \nu^{(m),*}_{k+1|t-1}, \phi^{(m)}_{k|t})$, and its projection onto $\mathcal{W}^{(m)}_{j-1}$ be

$$\hat{\xi}^{(m)}_{k|t,j} = \mathrm{Proj}(\bar{\xi}^{(m)}_{k|t}, \mathcal{W}^{(m)}_{j-1}), \; j \in \mathbb{Z}_{[1,N+1]}. \quad (19)$$

Define the j^{th} row of $\Gamma^{(m)}_{k|t}$, and component of $\gamma^{(m)}_{k|t}$ by

$$[\Gamma^{(m)}_{k|t}]_j = \hat{\xi}^{(m)}_{k|t,j} - \bar{\xi}^{(m)}_{k|t}, \qquad [\gamma^{(m)}_{k|t}]_j = [\Gamma^{(m)}_{k|t}]_j \hat{\xi}^{(m)}_{k|t,j}.$$

Then, $-[\Gamma^{(m)}_{k|t}]'_j$ is in the normal cone of $\mathcal{W}_{j-1}$ at $\hat{\xi}^{(m)}_{k|t,j}$, and hence $\mathcal{H}^{(m)}_{j,k|t} = \{\xi : \; [\Gamma^{(m)}_{k|t}]_j\xi \le [\Gamma^{(m)}_{k|t}]_j\hat{\xi}^{(m)}_{k|t,j} - \varepsilon\}$ ensures $\mathcal{H}^{(m)}_{j,k|t} \subseteq (\mathcal{W}^{(m)}_{j-1})^c$ for all $\varepsilon > 0$. Thus, by De Morgan's law, $\tilde{\mathcal{F}}^{(m)}_{k|t} = \bigcap^N_{j=0} \mathcal{H}^{(m)}_{j,k|t} = \{\xi : \; \Gamma^{(m)}_{k|t}\xi \le \gamma^{(m)}_{k|t} - \varepsilon 1\} \subseteq \mathcal{F}^{(m)}$.

Remark 2: ε is introduced to obtain non-strict inequalities as required by solvers for (16). The main computations for (19) are the projections (19) that, when considering orthogonal projection on polyhedral sets $\mathcal{W}^{(m)}_j$, amount to $N+1$ small scale quadratic program for each $k \in \mathbb{Z}_{[0,N_p]}$.

Next we summarize (17) solves Problem 1.

Proposition 2: At time $t \in \mathbb{Z}_{0+}$, let $\mathcal{M}_t$, $x(t)$, $r_{t|k}$ and $\{\phi^{(m)}(t+k)\}^{N_p-1}_{k=0}$ for all $m \in \mathcal{M}_t$, $k \in \mathbb{Z}_{[0,N_p]}$ be given. When (16) has a feasible solution, if a failure $m \in \mathcal{M}_t$ occurs, the evasive maneuver (7), according to (17b) guarantees that the constraints (2) are satisfied and the exclusion zone is avoided (3). Otherwise, the nominal control based on (17a) ensures satisfaction of (2), for $m = 0$. ■

[1]Model (1) may be extended with auxiliary states for constructing the evasive maneuver states, e.g., previous states to compute 1-step changes.

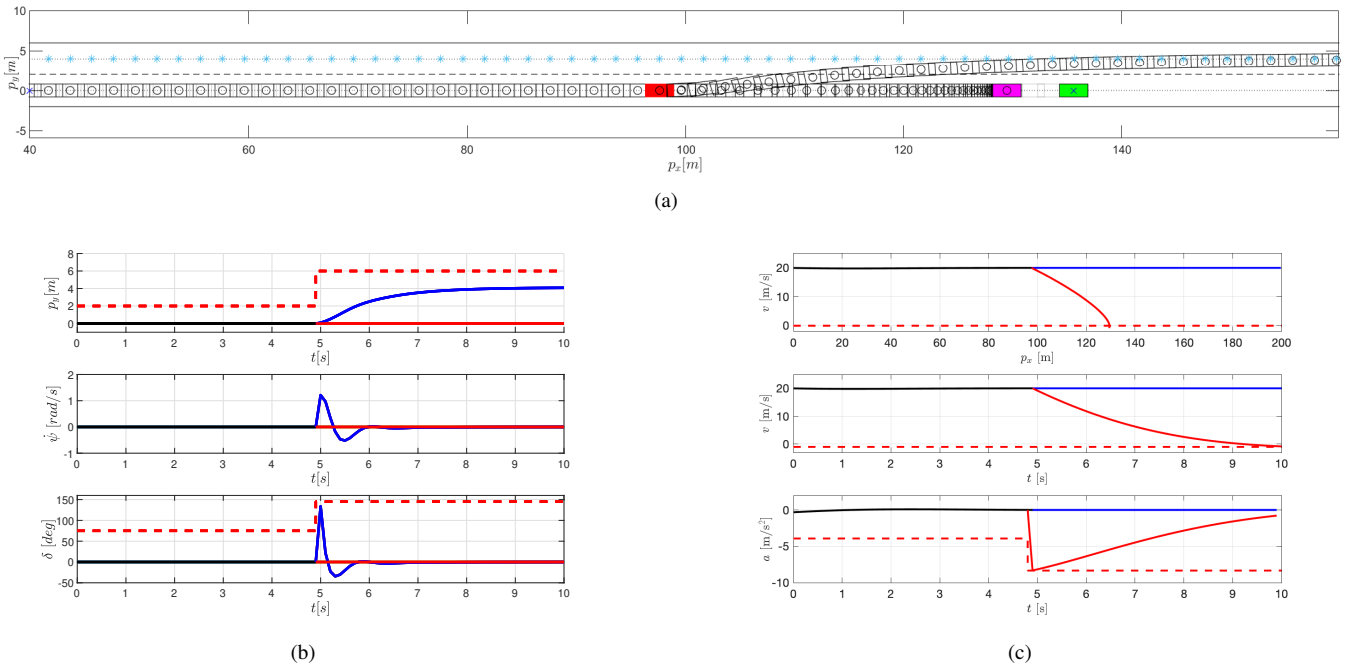

Fig. 3. Simulation of nominal driving and evasive maneuver, both sway and braking, in a failure scenario due to an obstacle (green) unexpectedly appearing 40m ahead of the ego vehicle. (a) Trajectories: ego vehicle position (black circles), ego vehicle position when failure occurs (red), final position of braking maneuver (purple), reference lateral position for sway maneuver (blue stars). (b) Lateral and (c) Longitudinal vehicle dynamics signals: nominal driving (black), evasive sway maneuver (blue), evasive braking maneuver (red), constraints of nominal and evasive maneuvers (dash red).

V. Case Studies

Next, we demonstrate the operation of the vehicle in some scenarios. The ego vehicle is traveling on a straight West-East road with two lanes, each 4m wide, with a target velocity of 20m/s. The nominal driving is operated by a nonlinear MPC based on the kinematic bicycle model (1) with sampling period $T_s = 0.1$s and prediction horizon $N_p = 10$ steps. The nominal driving is subject to constraints on steering angle, $\delta \in [-75, 75]$deg at the steering wheel, lateral position error with respect to the reference, which is the centerlane when keeping the lane, $y^e \in [-2, 2]$, acceleration $a \in [-0.4, 0.3]g$, and steering rate $\sigma \in [-50, 50]$deg/s. We consider one failure scenario, where an obstacle appears 40m in front of the ego vehicle, and is stopped. This results in an exclusion zone (8) that has extent 1.6m in width, 2.6m in length and that, according to (9), is initialized with position 40m in front of the vehicle at every time t, by $\phi_{0|t}$, and it is predicted not to move from such position, which is a challenging, and dangerous, failure scenario. Thus, until the failure occurs, the exclusion zone moves ahead with the vehicle.

We apply two evasive maneuvers with $N = 40$ safety steps, i.e., 4s: sway, based on dynamic bicycle model with respect to centerlane (5a), and braking, based on longitudinal model (5b). During evasive maneuvers, we consider relaxed constraints $\delta \in [-135, 135]$deg, $y^e \in [-2, 6]$, $\psi^e \in [-30, 30]$deg, acceleration $a \in [-0.85, 0.65]g$, and we leave the steering rate σ unconstrained. The controllers for the two evasive maneuvers are as in (6), where the feedback component is an LQR, and the feedforward component is gives unitary gain with respect to the reference lateral position $r_{y^e} \in [-2, 6]$m for sway, and reference stopping distance $r_d \in [0, 100]$m, for braking. All models use data from a real vehicle, a mid-size SUV, experimentally validated [19].

Figure 3 shows the behavior of the failure-safe controller when the failure scenario occurs at 5s in the simulation, for the two cases when sway and braking evasive maneuvers are enabled. Figure 3(a) shows that exclusion zone is avoided in both cases, and Figures 3(b), 3(c) show that the relaxed constraints for the evasive maneuver are satisfied. For the braking, we allow the velocity to be slightly negative, for the numerics in the set construction. In practice, as the velocity is almost zero, the vehicle stops due to friction and will not move backwards.

Figures 4, 5 show a more challenging case where the exclusion zone in the failure scenario has width $8m$. In this case the sway evasive maneuver would not be able to avoid the exclusion zone if the vehicle drives in the centerlane. As a result, the constraints (15) force the nominal driving MPC to offset the lateral position in the lane. This ensures that, when the failure occurs at $t = 3$s, the exclusion zone is avoided while still satisfying the constraints.

VI. Conclusions

We proposed a failure-safe controller that executes evasive maneuvers, which are less restricted than the ones in nominal driving, in presence of failures, e.g., due to not detecting or wrongly predicting another vehicle. The controller ensures avoidance of a risk area and satisfaction of maneuver constraints using reachable and invariant sets for the closed-loop evasive maneuvers parametrized by references. Such sets are

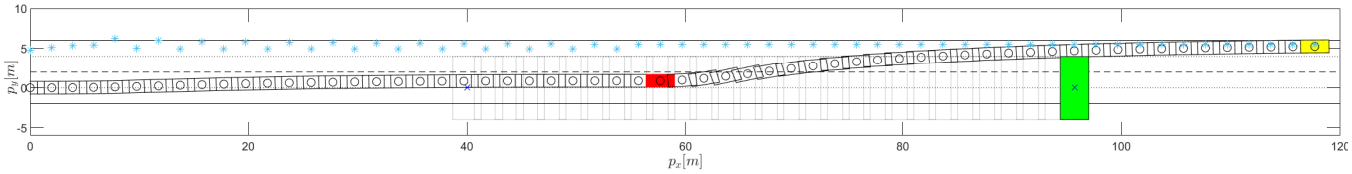

Fig. 4. Simulation of nominal driving and sway evasive maneuver in a failure scenario due to a *large* obstacle (green) unexpectedly appearing 40m ahead of the ego vehicle. Trajectories: ego vehicle position (black circles), ego vehicle position when failure occurs (red), final position of braking maneuver (purple), reference lateral position for sway maneuver (blue stars).

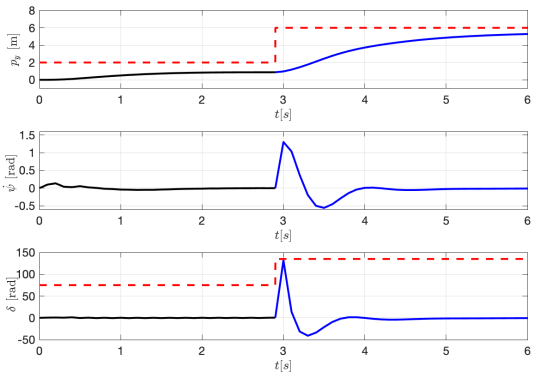

Fig. 5. Simulation of nominal driving and sway evasive maneuver in a failure scenario due to a *large* obstacle unexpectedly appearing 40m ahead of the ego vehicle. Lateral vehicle dynamics signals: nominal driving (black), evasive sway maneuver (blue), constraints of nominal and evasive maneuvers (dash red).

imposed as constraints in the nominal driving controller, and the maneuver references are additional decision variables.

In the future we will consider more expressive parametrizations of the evasive maneuvers, e.g., by leveraging with a structure similar to the extended command governor [12], more general formulations of the nominal driving controller to ensure feasibility of at least one evasive maneuver, and we will investigate recursive feasibility conditions. Other works will focus on the design of the failure supervisor that selects the possible failures for the current traffic conditions, and on detecting the failures.

REFERENCES

[1] A. Censi, K. Slutsky, T. Wongpiromsarn, D. Yershov, S. Pendleton, J. Fu, and E. Frazzoli, "Liability, ethics, and culture-aware behavior specification using rulebooks," in *Int. Conf. on Robotics and Automation*, 2019, pp. 8536–8542.

[2] M. Althoff and J. M. Dolan, "Online verification of automated road vehicles using reachability analysis," *IEEE Trans. Robotics*, vol. 30, no. 4, pp. 903–918, 2014.

[3] Y. Gao, A. Gray, H. E. Tseng, and F. Borrelli, "A tube-based robust nonlinear predictive control approach to semiautonomous ground vehicles," *Vehicle System Dynamics*, vol. 52, no. 6, pp. 802–823, 2014.

[4] K. Berntorp, R. Bai, K. F. Erliksson, C. Danielson, A. Weiss, and S. Di Cairano, "Positive invariant sets for safe integrated vehicle motion planning and control," *IEEE Trans. Intelligent Vehicles*, vol. 5, no. 1, pp. 112–126, 2019.

[5] H. Ahn, K. Berntorp, P. Inani, A. J. Ram, and S. Di Cairano, "Reachability-based decision-making for autonomous driving: Theory and experiments," *IEEE Trans. Control Systems Technology*, vol. 29, no. 5, pp. 1907–1921, 2020.

[6] B. Schurmann, M. Klischat, N. Kochdumper, and M. Althoff, "Formal safety net control using backward reachability analysis," *IEEE Trans. Automatic Control*, 2021.

[7] M. Koschi and M. Althoff, "Set-based prediction of traffic participants considering occlusions and traffic rules," *IEEE Trans. Intelligent Vehicles*, vol. 6, no. 2, pp. 249–265, 2020.

[8] C. Pek and M. Althoff, "Fail-safe motion planning for online verification of autonomous vehicles using convex optimization," *IEEE Trans. Robotics*, vol. 37, no. 3, pp. 798–814, 2020.

[9] D. Aguilar Marsillach, S. Di Cairano, and A. Weiss, "Abort-safe spacecraft rendezvous in case of partial thrust failure," in *IEEE Conf. Decision and Control*, 2020, pp. 1490–1495.

[10] ——, "Abort-safe spacecraft rendezvous in case of partial thrust failure," in *IEEE Conf. Decision and Control*, 2020, pp. 1490–1495.

[11] S. Di Cairano, H. Park, and I. Kolmanovsky, "Model predictive control approach for guidance of spacecraft rendezvous and proximity maneuvering," *Int. J. Robust and Nonlinear Control*, vol. 22, no. 12, pp. 1398–1427, 2012.

[12] E. Garone, S. Di Cairano, and I. Kolmanovsky, "Reference and command governors for systems with constraints: A survey on theory and applications," *Automatica*, vol. 75, pp. 306–328, 2017.

[13] J. B. Rawlings and D. Q. Mayne, *Model Predictive Control: Theory and Design*. Nob Hill Pub., 2009.

[14] D. Limón, I. Alvarado, T. Alamo, and E. F. Camacho, "Mpc for tracking piecewise constant references for constrained linear systems," *Automatica*, vol. 44, no. 9, pp. 2382–2387, 2008.

[15] N. Li, K. Han, A. Girard, H. E. Tseng, D. Filev, and I. Kolmanovsky, "Action governor for discrete-time linear systems with non-convex constraints," *IEEE Control Sys. Lett.*, vol. 5, no. 1, pp. 121–126, 2020.

[16] S. M. LaValle, *Planning algorithms*. Cambridge Univ. press, 2006.

[17] P. Polack, F. Altché, B. d'Andréa Novel, and A. de La Fortelle, "The kinematic bicycle model: A consistent model for planning feasible trajectories for autonomous vehicles?" in *IEEE Intelligent Vehicles Symp.*, 2017, pp. 812–818.

[18] K. Berntorp, T. Hoang, and S. Di Cairano, "Motion planning of autonomous road vehicles by particle filtering," *IEEE trans. intelligent vehicles*, vol. 4, no. 2, pp. 197–210, 2019.

[19] S. Di Cairano, U. Kalabić, and K. Berntorp, "Vehicle tracking control on piecewise-clothoidal trajectories by mpc with guaranteed error bounds," in *55th IEEE Conf Deci. Control*, 2016, pp. 709–714.

[20] F. Blanchini and S. Miani, *Set-theoretic methods in control*. Springer, 2008, vol. 78.