A Safe and Robust Control System Architecture for Virtual Coupling

Mario Terlizzi, Davide Liuzza and Luigi Glielmo

Abstract— **The continuous increase in demand for railway transportation is pressing for finding new solutions to increase capacity accordingly. Nowadays, the capacity of high-speed railway lines is saturated, and solutions that allow for an increase are being studied. In this context, the implementation of technology such as Virtual Coupling (VC) is emerging as a promising prospect to address these challenges and improve the overall operational efficiency of the railway system. In this article, we introduce a control system architecture enabling the transition from European Railway Traffic Management System Level 3 to VC and managing VC operation. The proposed architecture addresses parameter uncertainty within train models and the variability in data communication, which is often unreliable and affected by delays and packet drops. We establish a robust control framework for safety and reliability despite these challenges. We incorporate a safety control barrier function to certify safety guarantees and prioritize operational safety. The architecture is designed with the possibility of implementing various control laws, safety rules and estimators block still guaranteeing performances. To validate our work, a railway simulation tool for VC scenarios is developed, demonstrating its effectiveness and foundational role in advancing railway safety.**

I. Introduction

The railway network is a complex and interconnected system that comprises a multitude of critical components, such as track circuits, switches, signals, and many others. All these elements work together to ensure the safe and efficient operation of the entire network. At the core of a railway infrastructure there are two systems: the Interlocking System (IS) and Radio Block Centre (RBC).

The IS plays a crucial role in guaranteeing the efficient and safe operation of the railway network by continuously overseeing and managing the status of all its elements. It ensures their proper functioning and communication. Through real-time monitoring of track circuits, switches, and various railway components, the IS has the capability to issue commands to signal switches and other essential elements, thereby maintaining optimal railway functionality.

The second important element of the railway network is the RBC which serves as the interface between the IS and the on-board trains. In Europe, it is based on European Railway Traffic Management System (ERTMS) a standardized and interoperable train control and command system for railways [1]. In its pursuit of ensuring the secure spacing of trains, the RBC leverages real-time insights into the current state of the railway network. This comprehensive understanding is derived from the data received both from the IS and the dynamic information regarding the positions and velocities of actively circulating trains. The goal of the RBC is to manage and optimize the safe distances between trains, thereby contributing to the overall safety and efficiency of railway operations. In this work, the RBC will be considered the actor which is in charge to initiate a VC operation between trains.

The current communication technology present on the railway infrastructure is Vehicle-to-Infrastructure (V2I), namely, the communication between the RBC and trains. The existing standard V2I is an integral component of the railway communication infrastructure, relying on the GSM-R network. Nowadays, the emergence of the 5G network-based railway communication technology, known as Future Railway Communication and Management System [2], it is a viable Vehicle-to-Vehicle (V2V) technology which is gradually gaining prominence due to its advanced capabilities in data transfer, reliability and low-latency characteristics, ensuring swift and real-time data exchange among trains within the network.

The growing popularity of trains as a mode of transportation presents a challenge of overburdening the railway system's capacity. As a result, enhancing infrastructure utilization and increasing capacity are two crucial objectives that railways are currently striving to achieve. These goals are being tackled by Shift2Rail [3], an initiative focused on developing innovative technologies and solutions to enhance the efficiency, safety, and sustainability of the railway system.

In the following, we will introduce two ERTMS technology standards, upon which the work is based: ERTMS Level 3 (L3) and VC which are depicted in Figure 1.

By transitioning from fixed to virtual block systems, L3 reduces dependence on trackside signals and infrastructure, relying instead on advanced onboard systems and continuous communication. This shift not only enhances line capacity but also reduces operational costs by optimizing train headways and minimizing the need for trackside maintenance; furthermore, it allows trains to move dynamically within a virtual continuously updated block which is contingent upon the position of the preceding train [4].

Nowadays, the technology for VC is still in the conception stage, and research is underway to determine the best way to

Mario Terlizzi is with RFI S.p.A., Rete Ferroviaria Italiana S.p.A, Rome, Italy.

Davide Liuzza is with DING, Dipartimento di Ingegneria, University of Sannio, Benevento, Italy.

Luigi Glielmo is with DIETI, Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione, University of Naples Federico II, Naples, Italy. *E-mail*: m.terlizzi@rfi.it, davide.liuzza@unisannio.it, luigi.glielmo@unina.it.

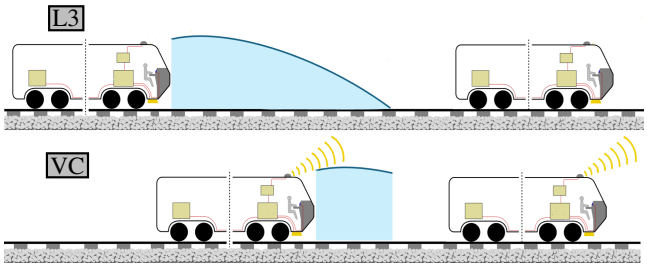

Fig. 1: Comparison scenarios between L3 and VC. The blue area beneath the curve represents the absolute braking distance required to stop the train.

implement it [5]. The control field is particularly interested in finding a solution that can provide the necessary speed, reliability, and safety to support real-time communication between trains. In addition to these technical considerations, research in the control field is also underway to determine the best way to implement VC from an operational perspective [6]. This involves studying the impact of the new technology on train operations and identifying the best practices for integrating the technology into the existing railway network [7].

In conclusion, VC presents a notable advantage in reducing railway delays, particularly in departure times. This innovative system holds the potential to decrease departure delays by optimizing train coordination and spacing. Promoting a more synchronized and efficient operation, VC emerges as a valuable solution to increase the capacity and enhances punctuality across the railway network.

A. Related Works

A fair amount of work exists on the topic of VC and in particular regarding the control techniques developed [8]. The main technologies mentioned include: consensus-based control [9], constraint following control [10], [11], sliding mode control [12], [13], Model Predictive Control (MPC), and Machine Learning (ML)-based control. Emphasis will be given to the last two types, as they prove to be the most promising in this field; specifically, the latter is the type upon which the control system presented in this paper is based.

The integration of ML into control algorithms has gained significant attention in the context of railway systems, particularly concerning virtual coupling [14]. In [15], the use of Reinforcement Learning (RL) is proposed to obtain an optimal policy for IoT-based Virtually Coupled Train Sets (VCTS). The proposed approach combines RL and artificial potential field to achieve global optimal policy and increase efficiency. Simulation results demonstrate the effectiveness of the proposed RL-based cooperative control approach for IoT-based VCTS. In [16], a Deep Deterministic Gradient Policy (DDPG) controller is proposed for VC control in uncertain autonomous trains convoys. The proposed controller tracks the reference behavior imposed by the RBC and maintains the desired inter-train distance with respect to the preceding train. The bottleneck of this innovative ML-based control type lies in the foundations of its theory. Currently, in the railway domain, it is not yet possible to certify an ML-based controller according to railway safety standards.

ADD ROBUSTEZZA AND COMUNICAZIONE ENFATIZZAZ RISPETTO AI PAPER CITATI The approaches most closely related to our solution are the works in [17] and [18]. In [17], a novel train control system utilizing virtual coupling is introduced. This system employs a decentralized model predictive control framework to optimize the control of both leading and following trains in a convoy. Comparative analyses, particularly against the moving block system, reveal improved performance, demonstrating the virtual coupling's efficacy in reducing headway and ensuring safe train separation. A linear MPC optimizing goals like track spacing, velocity, and comfort is implemented in [18]. Constraints, including line speed, collision avoidance, and traction/braking, are considered. In this work, although safety constraints are considered inside the controller, no certification of safety is demonstrated. Compared with these two contributions, our control scheme takes into account the intrinsic characteristics of the communication channel and assumes a heterogeneous platoon with parameters uncertainty. In both [17] and [18], the authors propose decentralized linear MPCs to realize the VC and assume the two trains can communicate in a reliable sampled framework. In our framework we also consider (nonlinear) MPCs but we do not focus on this aspect in details. Rather, in this paper we propose a hybrid/switching control architecture able to robustly satisfy safety constraints and reducing unnecessary follower train brakings, also considering not reliable communication between trains. Our framework is able to cope with diverse (MPC based) controller choices, both for the leader and the follower.

Details on our contribution are provided next.

B. Contribution

In this article, we introduce a control system architecture allowing the transition from L3 to VC and manage VC operations.

Specifically, the VC is a condition under which two trains are spaced not less than a safety distance d and, in principle, try to be spaced as close as possible to d. However, in the solution we propose the distance between the two trains may vary during the trains journey according to the operating conditions (but always keeping the prescribed minimum safety distance d).

The contributions of our work is articulated through the following key points:

1) Our architecture addresses the twofold challenge of parameter uncertainty within train system models and the throughput variability in data packet

communication channel characteristics. We establish a robust control system framework that is specifically engineered to accommodate these variabilities, always ensuring safety and reliable performance.

2) For ensuring safety, we incorporate into the design of our control architecture a safety control barrier function. This allows to certify safety guarantees and prioritize operational safety.
3) The control architecture allows to implement very general control laws (we provide a switched controller but other choices are possible), guaranteeing not only safety, but also avoiding as much as possible follower emergency braking when no information are received from the leader.
4) To validate the applicability and safety of our control system, we have developed a specialized railway simulation tool for VC. This tool enables testing and evaluation of the control system across various scenarios. The demonstration of the system's effectiveness in these tests not only proves its operational viability but also solidifies its foundational role in advancing railway safety.

The paper is organized as follows: Section II provides an initial overview of the problem and the proposed control system architecture, the principal blocks implemented are reported. Section III introduces safe sets and control barrier functions, ensuring system safety through robust and safety-compliant controllers, which maintain the system within safe operational conditions despite uncertainties. Section IV models the train's longitudinal dynamics defining the uncertain system parameters and ensuring safety with a robustification technique. Section V introduces braking and emergency controller definitions, used to ensure robust safety compliance for the train system. Section VI provides a detailed description of the control system architecture for trains operating under VC. It thoroughly examines the primary components and their interactions, offering insights into the design and functionality of each block within the system. This section highlights the innovative approaches used to manage the complexities of VC, ensuring efficient and safe train operations. Section VII presents the different operational scenario simulations and results. Finally, Section VIII includes the conclusions and future works.

II. Addressed problem and proposed control architecture

In this section we provide a preliminary description of the problem addressed in the paper and the proposed control architecture. Specifically, we consider asynchronous communication between the leader and the follower over an unreliable communication channel. Leader sends packets about its planned trajectory (more precisely it will be a robust information about the planned trajectory). Such packets might be received with delay (or not received at all) by the follower.

The problem to be addressed is the one of controlling the trains according to a "virtual coupling" (VC) scheme. Specifically, the follower train should move in a coordinated way with the leader, keeping a safety distance of at least d (which is a provided control parameter). The aim of the VC is to reduce the spacing between the trains on the railway and so increase its capacity. Often, when referring to VC in the literature, the distance between the trains is imposed to be exactly d.

In our control architecture, instead, the inter-trains distance might vary (but never being below d) according to the operating condition. Implicitly, the control architecture will control the inter-train distance guaranteeing safety and avoiding unnecessary train braking. This will be achieved through several control blocks simultaneously working. All these blocks run on the follower side.

Specifically:

- The leader robust lower proxy (RLP) predictor block is responsible of predicting the evolution of a system (namely the RLP) that provides a lower bound of the true leader trajectory subjected to an hypothetical emergency braking (that is, the maximum allowed deceleration). This block will be reset at follower packets receptions with the updated state of the leader.
- The safety control block is fed with the output of the leader RLP predictor and the actual state of the follower. It continuously monitor for the overall system safety via a suitable control barrier function. Such monitoring runs on predicted information even if no updates are received from the leader. If conditions are detected such that safety might be a risk, an emergency braking is imposed to the follower, overlapping any other possible control. The emergency braking is kept until safety conditions are restored (including new leader updates). The safety control block guarantees safety in a certified manner and robustly with respect to follower and leader parameters uncertainties.
- The cruise virtual coupling control block manages the follower during the normal cruise (i.e., when no safety issues are raised). It implements a predictive controller over a receding horizon while keeping the position of the follower at a certain (time-varying) distance from the leader. This distance is such that, if no updates are received, the follower can still move with its planned velocity for a given tunable amount of time before possibly trigger an emergency braking. This feature allows to implicitly regulate the inter-train distance according to the characteristics of the communication channel, enlarging or squeezing this dwell time in presence of less or more reliable communication (respectively).
- The delay estimator block continuously calculates the communication delay between the leader and follower by analyzing packet arrival times. This real-time estimation allows the control system to adjust reference

trajectories based on current delay conditions, ensuring smooth coordination despite channel variability. The block interacts with the cruise virtual coupling block to maintain system safety and minimize the impact of communication delays on overall performance.

It is worth mentioning that the proposed architecture does not prescribe a specific controller. Rather, it provides an environment enabling several possible controller choices, leaving the specific design to the developer. Therefore, while in this paper we propose a switching controller over three possible operational modes (with more or less aggressive maneuvers according to the inter-train distance), several other choices are possible. Also, our framework seamless allows the implementation of any additional safety criteria or the integration of other modules/features, such as an online estimation of the channel quality and characteristic delay, so as to adjust in real-time the dwell time in the cruise virtual coupling control block.

III. Background

A. Dynamical system and Barrier Function

Here we introduce the concept of safe set and barrier function. We keep our illustration rather informal and we only provide those concepts which will be useful in the rest of the paper. For this reason we do not always follow a "standard" notation and cast this background for the specific problem in hand. Further details can be found in several papers and books in the literature, see for example [19] and references therein.

Le us consider a dynamical system described by

$$\dot{x}(t) = f(x(t), u(t)), \tag{1a}$$

$$\mathscr{C}(x(t), u(t)) \leq 0 \tag{1b}$$

$$x_0 = x(t_0). \tag{1c}$$

where $t \in \mathbb{R}_+$ is the time, $x \in \mathbb{R}^n$ is the state of the system, $u \in \mathbb{R}^m$ the control input, $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ the (smooth) dynamical function and $\mathscr{C} : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^l$ provides static constraints.

Let us consider a safe set $\mathscr{S} \subseteq \mathbb{R}^n$, that is a set of the state space where we aim to confine the state of the system.

Definition 1 (CBF) Let us consider a dynamical system (1) and a safe set $\mathscr{S} \subseteq \mathbb{R}^n$. A control barrier function on $\mathscr{S}$ is any continuous function $b(x) : \mathbb{R}^n \to \mathbb{R}$ such that

$$b(x) \leq 0 \iff x \in \mathscr{S}. \tag{2}$$

Notice that some authors in the literature reverse the sign of the inequality in the above definition; this, obviously, is only a convention that does not alter its meaning. Also, in the literature a further hypothesis on $b(x)$ is being continuously differentiable. In our paper we do not ask for this requirement and we will consider $b(x)$ continuous only.

Control barrier function are particularly useful in control theory when there is the need of certifying system safety. Specifically, we give the following definition.

Definition 2 Let us consider a dynamical system (1) and an initial condition x_0 such that $b(x_0) \leq 0$ and a control input $u(t)$, with $t \in [t_0, +\infty)$.

The trajectory $x(t) = \phi(t, t_0, x_0, u)$ is said to be safe if $b(x(t)) \leq 0$ for all $t \in [t_0, +\infty)$. If $x(t)$ is safe, $u(t)$ is said a safe control trajectory.

Definition 3 Let us consider a feedback controller $u = K(x)$ for system (1) and, with some abuse of notation, let $\phi(t, t_0; x_0, K(\cdot))$ denote the closed-loop state $x(t)$. It is said a safe controller for set $\mathscr{S}$ if for any x_0 such that $b(x_0) \leq 0$, the trajectory $x(t) = \phi(t, t_0, x_0, K(\cdot))$ is safe.

Roughly speaking, the above definition means that $K(\cdot)$ is safe if, for any safe initial condition, it keeps the system in the safe set forward in time.

A further (stronger) definition for a feedback controller is provided in what follows.

Definition 4 Let us consider a feedback controller $u = K(x)$ for system (1) and let $x(t) = \phi(t, t_0, x_0, K(\cdot))$ be the system solution. The controller is said safety compliant for set $\mathscr{S}$ if

i. $K(\cdot)$ is safe;
ii. for any x_0 such that $b(x_0) > 0$, the function $b(x(t))$ with $t \in [t_0, \bar{t}]$ is monotonically decreasing (not necessarily strictly) for any $\bar{t}$ such that $b(x(\bar{t})) > 0$.

Roughly speaking, the above definition qualifies any controller able to keep safety when the system starts in the safe set and able not to "increase" the unsafety (that is, the value of $b(x(\cdot))$ for any unsafe initial condition.

With respect to Definition 4, let us call $\mathscr{T} \subseteq [t_0, +\infty)$ the set of the time instants where $b(x(t))$ is strictly monotone, that is $b(x(t_1)) > b(x(t_2))$ for any $t_1, t_2 \in \mathscr{T}$ with $t_1 < t_2$. The following result holds.

Theorem III.1 Let us consider a smooth dynamical system (1), a smooth feedback controller $K(x)$ and a continuous control barrier function $b(x)$ defined for the safe set $\mathscr{S}$. Suppose that the controller is safety compliant and the trajectory $x(t) = \phi(t, t_0, x_0, K(\cdot))$ is bounded for any valid initial condition $x_0 \in \mathbb{R}^n$ (that is, satisfying constraints (1b)). Also, suppose $\mathscr{T}$ unbounded. Then, the limit set $\omega(x_0) \subseteq \mathscr{S}$ for all x_0, [20].

Proof. We need to prove the results only for those $x_0 \notin \mathscr{S}$, since for $x_0 \in \mathscr{S}$ the result trivially comes from Definition 4. First of all, consider a sequence of time instants $t_k \in \mathscr{T}$, with $\lim_{k \to +\infty} t_k = +\infty$ (this can be done since $\mathscr{T}$ is supposed to be unbounded). The proof will be conducted with a contradiction argument. Let us suppose $\lim_{k \to +\infty} b(x(t_k)) = \bar{b}$, with $\bar{b} > 0$. Let us call $b^{-1}(\bar{b}) : \{x \in \mathbb{R}^n : b(x) = \bar{b}\}$. We obviously have $b^{-1}(\bar{b}) \cap \mathscr{S} = \emptyset$. Let us consider the limit set $\omega(x_0)$ (note that such set is not empty since $x(t)$ is bounded, see [20]). We trivially have $\omega(x_0) \subseteq b^{-1}(\bar{b})$.

Let us consider a point $\tilde{x} \in \omega(x_0)$, a finite time span $\tau > 0$ and an index sequence h such that $t < t_h \leq t + \tau$. By the smoothness of $f(\cdot)$ and $K(\cdot)$, the function $\phi(t + \tau, t, \tilde{x}, K(\cdot))$ is continuous with respect to the variable $\tilde{x}$ for any initial time t and evolution length τ. Calling $\tilde{b} = b(\phi(t + \tau, t, \tilde{x}, K(\cdot)))$,

we have $\tilde{b} < \bar{b}$. Let us choose a $\varepsilon < \bar{b} - \tilde{b}$. Then, by continuity we have that there exists a $\delta > 0$ such that any $\hat{x}$ such that $\|\tilde{x} - \hat{x}\| < \delta$ implies

$$\|b(\phi(t+\tau, t, \tilde{x}, K(\cdot))) - b(\phi(t+\tau, t, \hat{x}, K(\cdot)))\| < \varepsilon.$$

A direct consequence of the above inequality is that $b(\phi(t+\tau, t, \hat{x}, K(\cdot)) < \tilde{b}$ which implies that $\tilde{x}$ cannot belong to $\omega(x_0)$. Since this reasoning can be conducted for any point in $\omega(x_0)$, we have that the latter set is empty, leading to a contradiction. The reasoning can be repeated for any $\tilde{b} > 0$ implying that $\omega(x_0) \in \mathscr{S}$.

□

Let us now consider a variation of system (1), namely

$$\dot{x}(t) = f(x(t), u(t), p), \tag{3a}$$
$$\mathscr{C}(x(t), u(t), p) \leq 0, \tag{3b}$$
$$x_0 = x(t_0), \tag{3c}$$
$$u = K(x), \tag{3d}$$

where we explicitly pointed out the dependency of the system on a parameter vector $p \in \mathscr{P} \subset \mathbb{R}^q$, with $\mathscr{P}$ bounded set.

Obviously, system (3) solution depends on the value of p, that is $x(t) = \phi(t, t_0, x_0, K(\cdot), p)$. It could be the case (as in our manuscript) that the value of parameter p is not know. For this reason, we provide the following definitions.

Definition 5 Let us consider a feedback controller $u = K(x)$ for system (3). The controller is said robustly safe if, for any x_0 such that $b(x_0) \leq 0$, the trajectory $x(t) = \phi(t, t_0, x_0, K(\cdot), p)$ is safe for any $p \in \mathscr{P}$.

Definition 6 Let us consider a feedback controller $u = K(x)$ for system (3). The controller is said robustly safety compliant if it is safety compliant for any $p \in \mathscr{P}$.

The following theorem holds.

Theorem III.2 Let us consider the dynamical system (3) smooth for any $p \in \mathscr{P}$, a smooth feedback controller $K(\cdot)$ and a continuous control barrier function $b(\cdot)$ defined for the safe set $\mathscr{S}$. Suppose that the controller is robustly safety compliant and the trajectory $x(t) = \phi(t, t_0, x_0, K(\cdot), p)$ is bounded for any $p \in \mathscr{P}$ and any valid initial condition $x_0 \in \mathbb{R}^n$. Then, the limit set $\omega(x_0, p) \subseteq \mathscr{S}$ for all x_0.

Proof. The proof is a direct consequence of Theorem III.1 applied at any dynamical system model and any parameter value p. □

Finally, we provide the following definition.

Definition 7 Let us consider a (possibly parameter dependent) dynamical system in the general form (3) and suppose $\mathscr{S}' \subseteq \mathbb{R}^n$ is its safe set. Suppose also to consider another set $\mathscr{S}$ such that $\mathscr{S} \subseteq \mathscr{S}'$ and a CBF $b(x)$ on $\mathscr{S}$ (that is, considering $\mathscr{S}$ as safe set). We will say that $b(x)$ protects $\mathscr{S}'$.

Lemma III.3 Let us consider a dynamical system (3) and sets $\mathscr{S} \subseteq \mathscr{S}' \subseteq \mathbb{R}^n$, with $\mathscr{S}'$ safe set for the system. Consider a CBF $b(x)$ protecting $\mathscr{S}'$ and a feedback controller $u = K(x)$. The following points hold:

i. If $K(\cdot)$ is a safe controller for $\mathscr{S}$, it is also a safe controller for $\mathscr{S}'$;
ii. If $K(\cdot)$ is a safety compliant controller for $\mathscr{S}$, it is also a safety compliant controller for $\mathscr{S}'$.

Proof. The proof trivially derives from the inclusion relation between set $\mathscr{S}$ and $\mathscr{S}'$. □

B. Setting

In this paper, similarly to what done in [17], we consider two consecutive trains on the same line, the leader (denoted with superscript L) and the follower (denoted with superscript F) (the extension to more than two trains is not addressed in the paper, although the proposed framework allows for that, which is left as a future work).

Both leader and follower have a dynamical model (whose details are provided later) summarized as

$$\dot{x}^i(t) = f^i(x^i(t), u^i(t), p^i), \tag{4a}$$
$$\mathscr{C}^i(x^i(t), u^i(t), p^i) \leq 0, \tag{4b}$$
$$x_0^i = x^i(t_0), \tag{4c}$$

with $x^i \in \mathbb{R}^{n_i}$, $u^i \in \mathbb{R}^{m_i}$, $p^i \in \mathscr{P}^i \subset \mathbb{R}^{q_i}$, $\mathscr{C}^i(\cdot) \in \mathbb{R}^{l_i}$, with $i \in \{\mathrm{L}, \mathrm{F}\}$.

The controllers of the two trains have generic expressions K^{L} and K^{F}.

Notice that, via stacking $x = [x^{\mathrm{L}^T}, x^{\mathrm{F}^T}]^T$, $u = [u^{\mathrm{L}^T}, u^{\mathrm{F}^T}]^T$, $p = [p^{\mathrm{L}^T}, p^{\mathrm{F}^T}]^T$, $x_0 = [x_0^{\mathrm{L}^T}, x_0^{\mathrm{F}^T}]^T$, $f = [f^{\mathrm{L}^T}, f^{\mathrm{F}^T}]^T$, $\mathscr{C} = [\mathscr{C}^{\mathrm{L}^T}, \mathscr{C}^{\mathrm{F}^T}]^T$ and setting $n = n_{\mathrm{L}} + n_{\mathrm{F}}$, $m = m_{\mathrm{L}} + m_{\mathrm{F}}$, $l = l_{\mathrm{L}} + l_{\mathrm{F}}$ and $q = q_{\mathrm{L}} + q_{\mathrm{F}}$ the overall dynamical system is formally represented by (3), with controller $K = [K^{\mathrm{L}^T}, K^{\mathrm{F}^T}]^T$.

Both controller K^{L} and K^{F} will be applied over a receding horizon (more details about these controllers will be provided later). The overall horizon for the leader is called H.

C. Channel Communication

In this study, we consider the train communication under ERTMS technology, which utilizes an event-triggered transmission protocol. This approach entails the transmission of signals or messages in response to specific operational events or conditions. We specifically consider the challenges posed by communication delays and packet losses within the V2V context. In this regard, here we abstract how the communication happens on the physical layer and its implementation mechanisms (either via a direct communication between leader and follower or via the railway infrastructure) and focus on all its control related aspects.

Specifically, the leader transmits its information, from the current value up to a horizon H. Transmissions happen at instants $\{t_{\kappa^{\mathrm{L}}}\}_{\kappa^{\mathrm{L}}=0}^{+\infty}$ via sending the tuple $\big(t_{\kappa^{\mathrm{L}}}, x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}), \underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})\big)$, where $t_{\kappa^{\mathrm{L}}}$ is the trigger instant, $x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$ the state of the leader and $\underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}) = \underline{x}^{\mathrm{L}}(t)_{t \in [t_{\kappa^{\mathrm{L}}}, t_{\kappa^{\mathrm{L}}}+H]}$ the whole robustly predicted state of the leader (due to its

own control trajectory) up to horizon H. More details on such robust state estimation trajectory and in which sense it can be considered robust will be provided later.

The leader transmission instants $\{t_{\kappa^{\mathrm{L}}}\}_{\kappa^{\mathrm{L}}=0}^{+\infty}$ might be generated periodically or asynchronously (due to some event-triggered logic of the leader controller). In the current ERTMS, transmissions happen synchronously on a fixed period base. Therefore, for validating our algorithm we used in Section VII a fixed sampling time transmission. However, the whole framework we are going to develop can perfectly work with non periodic transmissions.

The follower receives the leader data packets at instants $\{t_{\kappa^{\mathrm{LF}}}\}_{\kappa^{\mathrm{LF}}=0}^{+\infty}$.

Notice that, due to packet losses and delays in the communication or stochastic processing time, leader packets are not received synchronously by the follower (or not received at all), in other words

$$\{t_{\kappa^{\mathrm{L}}}\}_{\kappa^{\mathrm{L}}=0}^{+\infty} \neq \{t_{\kappa^{\mathrm{LF}}}\}_{\kappa^{\mathrm{LF}}=0}^{+\infty}.$$

The following functions are defined to represent the last trigger time for the leader and follower, respectively, enabling a precise analysis of data transmission timing:

$$\ell_{\kappa^{\mathrm{L}}}(t) = \max_{t_{\kappa^{\mathrm{L}}} \leq t} \{t_{\kappa^{\mathrm{L}}}\}_{\kappa^{\mathrm{L}}=0}^{+\infty},$$
$$\ell_{\kappa^{\mathrm{LF}}}(t) = \max_{t_{\kappa^{\mathrm{LF}}} \leq t} \{t_{\kappa^{\mathrm{LF}}}\}_{\kappa^{\mathrm{LF}}=0}^{+\infty}.$$

Suppose the leader transmits a packet at time $t_{\kappa^{\mathrm{L}}}$, and let $\tau(t_{\kappa^{\mathrm{L}}}) \in \mathbb{R}^+ \cup \{+\infty\}$ denote the elapsed time of follower reception of such packet, that is the follower receives the packet at $t_{\kappa^{\mathrm{L}}} + \tau(t_{\kappa^{\mathrm{L}}})$.

The sequence of $\{\tau(t_{\kappa^{\mathrm{L}}})\}_{\kappa^{\mathrm{L}}=0}^{+\infty}$ can be modeled as a random process as will be proposed in Section VII. Nevertheless, as it will be clearer later in the manuscript, our framework does not need a specific transmission packets delay model.

IV. Train Modeling

The model employed in this manuscript relies on the principles of longitudinal train dynamics. It treats the train as a singular point mass with one degree of freedom. Additionally, it incorporates aspects such as the propulsion and braking system, the effects of rolling and bearing resistances, air input, the influence of aerodynamic drag, as well as the consideration of grade and curving resistances [21]:

$$\begin{aligned} \dot{x}_1^i(t) &= x_2^i(t), \\ \dot{x}_2^i(t) &= \frac{1}{M^i}(-A^i - B^i x_2^i(t) - C^i (x_2^i(t))^2) - \mathrm{F}_e^i(t) + \frac{u^i(t)}{M^i}. \end{aligned} \tag{5}$$

We utilize the symbols $x_1^i(t)$ and $x_2^i(t)$ to represent the i-th train's position and velocity, respectively, with $i \in \{L, F\}$. By convention, we consider a reference frame at the head of each train (therefore the position is referred to as the train head). Also, we consider positive positions, with the origin at the beginning of the railway. Implicitly, both position and velocity will only be nonnegative (the trains cannot move backward during normal operations). The constraints $x_1^i(t) \leq 0$ and $x_2^i(t) \leq 0$ will be therefore implicitly included in compact term (4b).

The state vector is compactly written as $x^i(t) = (x_1^i(t), x_2^i(t))^T$. The variable $u^i(t)$ is the control driving or braking force; F_e^i denotes the external force originating from the track; M^i denotes the mass parameter, while A^i encompasses both rolling resistance and bearing resistance; B^i is a coefficient related to the flange friction, and C^i represents the aerodynamic coefficient. In this model, $\mathrm{F}_e^i(t)$ is the i-th external force

$$\mathrm{F}_e^i(t) = g\sigma(x_1^i(t)) + \frac{\gamma}{\rho(x_1^i(t))},$$

where $\gamma = 6 \cdot 10^6$ is a constant parameter. It encompasses two distinct terms: the first one is the gravity force resulting from the track's slope $\sigma(x_1^i(t))$ at point $x_1^i(t)$, with g representing the gravitational acceleration; the second term designates the curving resistance, with $\rho(x_1^i(t))$ representing the curve's radius.

Regarding the constraints on the state and input of the model, they are presented as follows

$$u^i(t) \in \left[-M^i a_{\mathrm{br}}^i,\, M^i a_{\mathrm{dr}}^i\right], \tag{6a}$$
$$u^i(t) \cdot x_2^i(t) \in \left[-P_{\mathrm{br}}^i,\, P_{\mathrm{dr}}^i\right], \tag{6b}$$
$$x_2^i(t) \in \left[0,\, \min\{V^{\max,i}, V^{\mathrm{line}}(x_1^i(t))\}\right], \tag{6c}$$
$$x_1^i(t) \in \mathbb{R}_+. \tag{6d}$$

All the above parameters are nonnegative and are constructional characteristics unique to each individual train and the railway. Specifically, a_{br}^i and a_{dr}^i correspond to the maximum braking and acceleration admitted, P_{br}^i and P_{dr}^i represent the minimum and maximum mechanical power, and $V^{\max,i}$ and V^{line} denotes the maximum attainable velocity for the train and railway speed limit at position x_1^i, respectively.

A. Robust Modeling

In the context of railway control, safety is of utmost importance and must be guaranteed even with parametric uncertainties.

In this paper, the following model parameters are supposed uncertain in a given range

$$\begin{gathered} a_{\mathrm{br}}^i \in [\underline{a}_{\mathrm{br}}^i, \overline{a}_{\mathrm{br}}^i],\ a_{\mathrm{dr}}^i \in [\underline{a}_{\mathrm{dr}}^i, \overline{a}_{\mathrm{dr}}^i],\ P_{\mathrm{br}}^i \in [\underline{P}_{\mathrm{br}}^i, \overline{P}_{\mathrm{br}}^i], \\ P_{\mathrm{dr}}^i \in [\underline{P}_{\mathrm{dr}}^i, \overline{P}_{\mathrm{dr}}^i],\ C^i \in [\underline{C}^i, \overline{C}^i], M^i \in [\underline{M}^i, \overline{M}^i], \\ A^i \in [\underline{A}^i, \overline{A}^i],\ B^i \in [\underline{B}^i, \overline{B}^i]. \end{gathered} \tag{7}$$

Compactly, we call $\mathscr{P}^i$ the Cartesian product of the above intervals. With such a choice, and taking into account (5) and (6), the train model can be compactly written as (4).

B. Robust Proxies

To derive a control architecture robust against any possible parameter choice of the two trains, the notions of Robust Lower Proxy (RLP) and Robust Upper Proxy (RUP) are introduced as simple (yet effective) robustification technique.

Definition 8 (RLP) A RLP for the system (4) is any dynamical system of the form

$$\dot{\underline{x}}^i(t) = \underline{f}^i(\underline{x}^i(t), u^i(t)), \tag{8}$$

with $\underline{x} \in \mathbb{R}^{n_i}$ and $u \in \mathbb{R}^{m_i}$ and such that its dynamical flow $\underline{\phi}^i\left(t, t_0, x_0^i, u^i\right)$ satisfies

$$\underline{\phi}^i\left(t, t_0, x_0^i, u^i\right) \leq \phi^i\left(t, t_0, x_0^i, u^i, p^i\right), \tag{9}$$

for all $x_0 \in \mathbb{R}^{n_i}$, for all $u_i \in \mathbb{R}^{m_i}$, for all $t \in [t_0, +\infty)$ and for all $p^i \in \mathscr{P}^i$ and where the inequality is meant component-wise.

Similarly, we provide the following definition.

Definition 9 (RUP) A RUP for the system (4) is any dynamical system of the form

$$\dot{\overline{x}}^i(t) = \overline{f}^i(\overline{x}^i(t), u^i(t)), \tag{10}$$

with $\overline{x} \in \mathbb{R}^{n_i}$ and $u \in \mathbb{R}^{m_i}$ and such that its dynamical flow $\overline{\phi}^i\left(t, t_0, x_0^i, u^i\right)$ satisfies

$$\overline{\phi}^i\left(t, t_0, x_0^i, u^i\right) \geq \phi^i\left(t, t_0, x_0^i, u^i, p^i\right) \tag{11}$$

for all $x_0 \in \mathbb{R}^{n_i}$, for all $u_i \in \mathbb{R}^{m_i}$, for all $t \in [t_0, +\infty)$ and for all $p^i \in \mathscr{P}^i$ and where the inequality is meant component-wise.

As evident from the two definitions, there might exist several proxies for (4). In this work, we will consider the following piece-wise smooth systems.

The following system has been chosen as RLP:

$$\begin{cases} \dot{\underline{x}}_1^i(t) = \underline{x}_2^i(t), & \text{if } u^i(t) < 0, \\ \dot{\underline{x}}_2^i(t) = \frac{1}{\underline{M}^i}\left(-\overline{A}^i - \overline{B}^i \underline{x}_2^i(t) - \overline{C}^i\left(\underline{x}_2^i(t_0)\right)^2\right) \\ \qquad\qquad -\overline{F}_e^i(\underline{x}_1^i(t_0)) + \frac{u^i(t)}{\underline{M}^i}, \\ \text{with } \overline{F}_e^i(\underline{x}_1^i(t_0)) = g\sigma_{\sup}\left(\underline{x}_1^i(t_0)\right) + \frac{\gamma}{\rho_{\inf}\left(\underline{x}_1^i(t_0)\right)}, \\ \dot{\underline{x}}_1^i(t) = \underline{x}_2^i(t), & \text{if } u^i(t) \geq 0, \\ \dot{\underline{x}}_2^i(t) = \frac{1}{\underline{M}^i}\left(-\overline{A}^i - \overline{B}^i \underline{x}_2^i(t) - \overline{C}^i\left(\underline{x}_2^i(t)\right)^2\right) \\ \qquad\qquad -\overline{\mathrm{F}}_e^i(\underline{x}_1^i(t_0)) + \frac{u^i(t)}{\overline{M}^i}, \\ \sigma_{\sup}\left(\underline{x}_1^i(t_0)\right) = \max\limits_{s \in [\underline{x}_1^i(t_0), s^{H,i}]} \sigma(s), \\ \rho_{\inf}\left(\underline{x}_1^i(t_0)\right) = \min\limits_{s \in [\underline{x}_1^i(t_0), s^{H,i}]} \rho(s). \end{cases} \tag{12}$$

Above, t_0 is a time instant upon which we consider the proxy time evolution and $s^{H,i}$ is a far enough ahead train position. Details on t_0 and $s^{H,i}$ will be provided later in the paper.

Similarly, we consider the following piece-wise system as RUP:

$$\begin{cases} \dot{\overline{x}}_1^i(t) = \overline{x}_2^i(t), & \text{if } u^i(t) < 0, \\ \dot{\overline{x}}_2^i(t) = -\frac{\underline{A}^i}{\overline{M}^i} - \underline{F}_e^i(\overline{x}_1^i(t_0)) + \frac{u^i(t)}{\overline{M}^i}, \\ \text{with } \underline{F}_e^i(\overline{x}_1^i(t_0)) = g\sigma_{\inf}\left(\overline{x}_1^i(t_0)\right) + \frac{\gamma}{\rho_{\sup}\left(\overline{x}_1^i t_0)\right)}, \\ \dot{\overline{x}}_1^i(t) = \overline{x}_2^i(t), & \text{if } u^i(t) \geq 0, \\ \dot{\overline{x}}_2^i(t) = \frac{1}{\overline{M}^i}\left(-\underline{A}^i - \underline{B}^i \overline{x}_2^i(t) - \underline{C}^i\left(\overline{x}_2^i(t)\right)^2\right) \\ -\underline{\mathrm{F}}_e^i(\overline{x}_1^i(t_0)) + \frac{u^i(t)}{\underline{M}^i}, \\ \sigma_{\inf}\left(\overline{x}_1^i(t_0)\right) = \min\limits_{s \in [\overline{x}_1^i(t_0), s^{H,i}]} \sigma(s), \\ \rho_{\sup}\left(\overline{x}_1^i(t_0)\right) = \max\limits_{s \in [\overline{x}_1^i(t_0), s^{H,i}]} \rho(s), \end{cases} \tag{13}$$

where again as before t_0 and $s^{H,i}$ are an initial time and a position ahead to be determined later.

The following lemma states the validity of our choice.

Lemma IV.1 Systems (12) and (13) are valid RLP and RUP for the train dynamics (5)-(7).

Proof. The proof is immediate since it suffices to consider the following differential equations

$$\dot{\tilde{x}}^i = \overline{f}\left(\tilde{x}^i, u^i\right) - f\left(\tilde{x}^i, u^i, p^i\right),$$
$$\dot{\hat{x}}^i = f\left(\hat{x}^i, u^i\right) - \underline{f}\left(\hat{x}^i, u^i, p^i\right).$$

Since all component terms are non-negative, this ensures the positivity of the systems.

□

V. Safety Guarantee

One of the objectives of the train control system we propose in this paper is to ensure that the two trains maintain a safety separation distance. In other words, the goal is to guarantee that the distance between the leader and follower never falls below the predefined safety threshold d. Remembering that the overall state is $x = [x^{\mathrm{L}^T}, x^{\mathrm{F}^T}]^T$, this is formally modeled through the safe set

$$\mathscr{S}'(x) = \{x : x_1^{\mathrm{L}} - x_1^{\mathrm{F}} \geq L^{\mathrm{L}} + d\}, \tag{14}$$

where L^{L} is the leader's length.

In order to ensure that the system solution always stays in $\mathscr{S}'(x)$, we consider for this paper another safe set $\mathscr{S}$ such that $\mathscr{S} \subseteq \mathscr{S}'$ and a protecting CBF for $\mathscr{S}'(x)$, as for Definition 7.

To do so, let us first define $\underline{\alpha}^i\left(x_2^i\right) = \min\left\{\underline{a}_{\mathrm{br}}^i, \frac{\underline{p}_{\mathrm{br}}^i}{M^i x_2^i}\right\}$. Also, considering an $\varepsilon < 1$ (the latter is a tuning parameter that can be chosen slightly less than one to reduce conservatism) let us compute a "large" deceleration of the follower

$$\underline{e}^{\mathrm{L}}\left(x_2^{\mathrm{L}}\right) = -\frac{1}{\underline{M}^{\mathrm{L}}}\left(-\overline{A}^{\mathrm{L}} - \overline{B}^{\mathrm{L}}(x_2^{\mathrm{L}}) - \overline{C}^{\mathrm{L}}\left(x_2^{\mathrm{L}}\right)^2\right) + \overline{F}_e^{\mathrm{L}}(x_2^{\mathrm{L}}) + \overline{a}_{\mathrm{br}}^{\mathrm{L}},$$

and a "small" deceleration of the follower

$$\overline{e}^{\mathrm{F}}(x^{\mathrm{F}}) = \frac{\underline{A}^{\mathrm{F}}}{\overline{M}^{\mathrm{F}}} + \underline{F}_e^{\mathrm{F}}(x_1^{\mathrm{F}}) + \varepsilon\underline{\alpha}^{\mathrm{F}}(x_2^{\mathrm{F}}).$$

We define the functions

$$b'(x) = L^{\mathrm{L}} + d - (x_1^{\mathrm{L}} - x_1^{\mathrm{F}}) - \frac{1}{2}\left(\frac{x_2^{\mathrm{L}2}}{\underline{e}^{\mathrm{L}}(x_2^{\mathrm{L}})} - \frac{x_2^{\mathrm{F}2}}{\overline{e}^{\mathrm{F}}(x_2^{\mathrm{F}})}\right), \quad (15a)$$

$$b''(x) = L^{\mathrm{L}} + d - (x_1^{\mathrm{L}} - x_1^{\mathrm{F}}), \quad (15b)$$

$$b(x) = \max\{b'(x), b''(x)\}. \quad (15c)$$

The safe set S corresponds to those states resulting in $b(x) \leq 0$, that is $S = \{x : b(x) \leq 0\}$ as defined in (2). The following lemma holds.

Lemma V.1 Function $b(x)$ in (15c) is a CBF protecting the set $\mathscr{S}'$ in (14).

Proof. The set $\mathscr{S}'$ corresponds to those states where $b''(x) \leq 0$. Due to (15c), $b(x) \leq 0 \Rightarrow b''(x) \leq 0$. □

Before showing further properties of the CBF $b(x)$, we first provide some definitions.

Let us first call $\mathscr{U}^i(x^i)$ the robust set of all the admissible control inputs at state x^i for system (4), that is

$$\mathscr{U}^i(x^i) = \left\{u^i \in \mathbb{R}^{m_i} : (4b), (6a), (6b) \text{ are satisfied } \forall p^i \in \mathscr{P}^i\right\}. \quad (16)$$

Together with the above, we call the robust set of all admissible braking control input at state x^i for system (4) the set

$$\underline{\mathscr{U}}^i(x^i) = \left\{u^i \in \mathscr{U}^i(x^i) : u^i \leq 0\right\}. \quad (17)$$

We are ready to provide the following definition.

Definition 10 (Braking Controller) We define a braking controller $u^i = K_{\mathrm{B}}^i(x^i)$ any feedback function such that

- $u^i \in \underline{\mathscr{U}}^i(x^i)$, if $x_2^i > 0$;
- $u^i = 0$, if $x_2^i = 0$.

Roughly speaking, a braking controller is any controller providing a nonpositive control input whenever the velocity is greater than zero and a null control input in case of null velocity[1]

Among the braking controller, the emergency controllers is a peculiar case, where the controller attains the highest allowed braking action.

Definition 11 (Emergency Controller) We define the emergency controller $u^i(t) = K_{\mathrm{E}}^i(x^i)$ a braking controller with

- $u^i = \min \underline{\mathscr{U}}^i(x^i)$, if $x_2^i > 0$;
- $u^i = 0$, if $x_2^i = 0$.

We are now ready for the following result.

Theorem V.2 Let us consider the trains system of form (4) with $i \in \{\mathrm{L}, \mathrm{F}\}$ in their stack form (3). Let us consider any valid (that is, outputting values satisfying the system constraints) leader controller K^{L}. Let us consider that $x_2^{\mathrm{F}}(t_0) > 0$ (the follower is not standing at the initial time t_0). Then, the controller $K = [K^{\mathrm{L}T}, K_E^{\mathrm{F}T}]^T$ is robustly safety compliant for $\mathscr{S}$ (and therefore also for $\mathscr{S}'$ according to Lemma III.3).

Proof. see AppendixA. □

[1]The case of null control input for null velocity could, in principle, be omitted since it is implicitly deducible by the positive constraint $x_2^i \geq 0$ of the system. Nevertheless, we prefer to keep it for the sake of clarity.

VI. Control system

In this section, we introduce the three blocks of the proposed control architecture which are depicted in 2: the leader RLP predictor, the safety control, the cruise virtual coupling and the delay estimator.

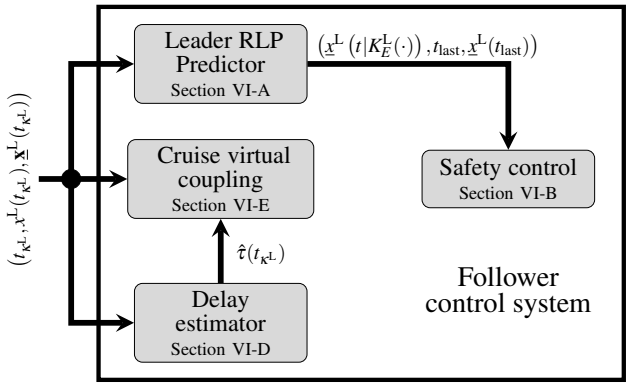

Fig. 2: Follower control system architecture for VC operation.

The Leader RLP predictor block is crucial for the follower train, as it processes data packets from the leader, received at irregular intervals. It continuously updates the follower's predictions of the leader's state, starting from the last received packet and projecting forward using the leader's dynamical model, supposing (for unknown future control inputs) the activation of an emergency brake. The overall safety is managed by the safety control block which continuously monitors the state of the follower and the predicted leader state. The block uses specific safety conditions to determine when to enforce the emergency controller on the follower train. When safety conditions are not met the emergency controller is activated to ensure the follower train maintains a safe distance from the leader. The Cruise virtual coupling block synchronizes the follower train with the leader, maintaining a safe distance using the predicted trajectory data. This block adjusts the follower's control strategy to match the leader's state, avoids unnecessary braking by keeping an appropriate gap based on communication delays, and employs a switched controller architecture to manage performances under varying conditions. This ensures efficient and safe operation of the follower train in response to the leader's movements. The last block, the delay estimator, is responsible for estimating the communication delay, which is expected to vary along the route. This estimator continuously monitors and analyzes the communication signals to accurately predict the latency, allowing the control system to adjust accordingly.We wish to emphasize that this block is not necessary, and a fixed delay estimation could be

assumed. The architecture we are going to develop is indeed very general and can be particularized for several design control choices including different possible delay estimators, different follower controllers, different safety rules. As it will be clearer later, the control system architecture we propose guarantees safety, robustness and some important performances on the emergency braking, leaving degrees of freedom to such control choices.

The following subsections will introduce the aforementioned control system blocks in detail.

A. Leader RLP predictor

As already reported in Section III-C, the follower receives at instants $\{t_{\kappa^{\mathrm{LF}}}\}_{\kappa^{\mathrm{LF}}=0}^{+\infty}$ the asynchronous data from the leader (transmission time, state at the transmission time and a robust prediction of the state trajectory).

Since the follower is not aware of what actual control input the leader is adopting in the time between consecutive message receptions, the follower does not know of the real leader state. It is worth mentioning that among the control input options available to the leader, the emergency control is the most important to be considered. Indeed, right after a communication at time $\ell_{\kappa^{\mathrm{L}}}(t)$, the leader might start an emergency breaking which could lead, if not adequately addressed, to safety hazards.

To avoid this, Algorithm 1 is run by the follower and executes a leader RLP predictor in presence of possible emergency breaking. Such prediction block will then be used in the next section for the safety control.

For consistency, we assume Algorithm 1 to be started the first time a follower receives its first packet, with initial conditions $t_{\mathrm{last}} = -\infty$, $\underline{x}^{\mathrm{L}}(t_{\mathrm{last}}) = +\infty$.

Algorithm 1 Leader RLP predictor. Outputs: $\underline{x}^{\mathrm{L}}(t|K_{\mathrm{E}}^{\mathrm{L}})$, t_{last}, $\underline{x}^{\mathrm{L}}(t_{\mathrm{last}})$.

loop
  Listen to possible transmission of information from the leader;
  if A packet $\left(t_{\kappa^{\mathrm{L}}}, x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}), \underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})\right)$ is received with $t_{\kappa^{\mathrm{L}}} > t_{\mathrm{last}}$ **then**
    $t_{\mathrm{last}} \leftarrow t_{\kappa^{\mathrm{L}}}$
    $\underline{x}^{\mathrm{L}}(t_{\mathrm{last}}) \leftarrow x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$
  end if
  Integrate the dynamical model $\dot{\underline{x}}^{\mathrm{L}}(t) = \underline{f}^{\mathrm{L}}(\underline{x}^{\mathrm{L}}(t), K_{\mathrm{E}}^{\mathrm{L}}(\underline{x}^{\mathrm{L}}(t)))$ from the initial time t_{last} and initial condition $\underline{x}^{\mathrm{L}}(t_{\mathrm{last}})$ up to current time (the resulting trajectory will be denoted with $\underline{x}^{\mathrm{L}}(t|K_{\mathrm{E}}^{\mathrm{L}})$);
end loop

As it is possible to see, Algorithm 1 is continuously run in background, integrating the leader RLP under an emergency controller, resetting the initial time and initial condition on an event triggered basis at the most recent received values. The outputs of the algorithm are the predicted leader RLP state subjected to the emergency controller and here denoted as $\underline{x}^{\mathrm{L}}(t|K_{\mathrm{E}}^{\mathrm{L}})$ at the current time t, and the time of the most recent information from the leader, together with its state, respectively t_{last}, and $\underline{x}^{\mathrm{L}}(t_{\mathrm{last}})$. These two latter information, together with $\underline{x}^{\mathrm{L}}(t|K_{\mathrm{E}}^{\mathrm{L}})$, might be useful for some safety enforcing condition as described in the next section.

Notice that Algorithm 1 does not use the robust leader predicted trajectory estimation $\underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$. Notice also that so far we did not describe yet how $\underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$ is computed. This will be done later since $\underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$ will be exploited in the cruise virtual coupling control block.

B. Safety control block

This block allows to constantly keep the system safe by monitoring the follower state $x^{\mathrm{F}}(t)$ and the leader RLP prediction from the corresponding block outputs described in Section VI-A. This block receives in input, together with $x^{\mathrm{F}}(t)$, the t_{last} and $\underline{x}^{\mathrm{L}}(t|K_{\mathrm{E}}^{\mathrm{L}})$ from the RLP predictor block. To ease the notation, we denote in this subsection $\underline{x}^{\mathrm{L}}(t|K_{\mathrm{E}}^{\mathrm{L}})$ as $\underline{x}^{\mathrm{L}}(t)$.

Specifically, considering $c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}}))$ any possible safety rule (further details on this will be provided later), the safety control block is implemented by Algorithm 2 which continuously runs in background.

Algorithm 2 Safety control

loop
  Continuously monitor $b(\underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}(t))$ and $c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}}))$, with $b(x)$ given in (15c);
  if $b(\underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}(t)) \geq 0$ **or** $c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}})) \geq 0$ **then**
    Enforce the emergency controller for the follower, that is $K_{\mathrm{E}}^{\mathrm{F}}$;
  else
    Do not enforce/stop enforcing the follower emergency controller $K_{\mathrm{E}}^{\mathrm{F}}$;
  end if
end loop

In practice, Algorithm 2 continuously monitor the train system safety condition and, in case it is violated (or at the boundary of its violation) enforce the follower emergency controller. When no safety violation is detected, the emergency controller is turned off.

This is formally stated in the next result.

Theorem VI.1 Consider the trains system of form (4) with $i \in \{\mathrm{L}, \mathrm{F}\}$ and the safe set $\mathscr{S}(x) = \{x : b(x) \leq 0\}$. If the system starts in a safe state, that is $[x^{\mathrm{L}^T}(t_0), x^{\mathrm{F}^T}(t_0)]^T \in \mathscr{S}$, then the safety control block of Algorithm 2 keeps the system safe forward in time, that is $[x^{\mathrm{L}^T}(t), x^{\mathrm{F}^T}(t)]^T \in \mathscr{S}$ for any $t \geq t_0$.

Proof. By hypothesis the system starts in the safe set. Being $\underline{x}^{\mathrm{L}}(t)$ and $x^{\mathrm{F}}(t)$ continuous time curves, safety is preserved until $b(\underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}(t)) = 0$ since $x^{\mathrm{L}}(t) \geq \underline{x}^{\mathrm{L}}(t)$ and, therefore, $b(x^{\mathrm{L}}(t), x^{\mathrm{F}}(t)^T) \leq b(\underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}(t))$. Since when

$b(\underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}(t)) = 0$ controller $K_{\mathrm{E}}^{\mathrm{F}}$ is activated, by Theorem V.2 safety is kept. □

Remark As it is possible to notice, the activation of $K_{\mathrm{E}}^{\mathrm{F}}$ due to the triggers generated by the violation of condition $c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}})) \geq 0$ does not play any role in the proof of Theorem VI.1. For this reason, rule $c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}}))$ can be omitted by trivially setting $c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}})) = -\infty$ without harming the system safety. Therefore, any other choice of $c(\cdot)$ is allowed. The reason why we decided to report rule $c(\cdot)$ is motivated by the peculiar application we are considering. In train control, extra/redundant safety conditions are often adopted, even though they do not look necessary from a strict mathematical analysis. Specifically, being this paper developed under the collaboration with personnel from the Italian railway company, the condition

$$c(x^{\mathrm{F}}(t), \underline{x}^{\mathrm{L}}(t), t_{\mathrm{last}}, \underline{x}^{\mathrm{L}}(t_{\mathrm{last}})) = t - t_{\mathrm{last}} - T^{\max}, \tag{18}$$

is adopted, where $T^{\max}$ is a maximum allowed time to wait for a new transmission update. As said, despite not necessary for keeping the system safe, the railway operator prefers to stop the follower train if no updates on the leader position are received after $T^{\max}$. Therefore, in this paper we will consider (18).

A good choice for $T^{\max}$ is having it bigger than the statistically relevant delay experienced by the communication channel. Its adoption turns to be useful in setting $s^{H,i}$ in (12) and (13), with the easy choice $s^{H,i} = x_1^i(t_0) + V_{\max}^i T^{\max}$.

Algorithm 2 implicitly provides a sequence of events in which the emergency braking is activated (and a sequence in which it is deactivated). We denote with $\{t_{\kappa^{\mathrm{E}}}\}_{\kappa^{\mathrm{E}}=0}^{+\infty}$ the sequence of time instants of emergency braking activation.

C. Cruise virtual coupling block: fixed controller

It is worth to observe that the safety condition in line 3 of Algorithm 2 might be restored either because the follower, while braking, is increasing its distance from $\underline{x}^{\mathrm{L}}(t)$ and/or because a new update of the leader position is received, thus resulting in new initialization update of the leader RLP predictor (line 7 of Algorithm 1.) This latter case is probably the most interesting in practice, since in normal (desirable) conditions, the leader train proceeds at constant or smoothly variable speed without incurring in aggressive braking. Similarly, the desired virtual coupling condition is that the follower proceeds at nearly the same velocity of the leader at a certain (obviously safe) distance from it.

The safety control block is designed to always preserve safety via enforcing the follower to brake in the worst possible condition, that is supposing that from the last transmission the leader starts a maximum braking. Since, as said, this condition in practice will be rare, a good choice for the follower distance from the leader during VC cruise is such that it could proceed at the same speed the leader has planned for a given amount of time $\bar{\tau}$ before the condition of line 3 of Algorithm 2 is met. In this way, at least a time $\bar{\tau}$ is wait before a follower emergency braking occurs. With the realistic hypothesis of having a statistical description of the communication delay process $\{\tau(t_{\kappa^{\mathrm{L}}})\}_{\kappa^{\mathrm{L}}=0}^{+\infty}$, choosing a $\bar{\tau}$ so as that $P(\tau(t_{\kappa^{\mathrm{L}}}) \leq \bar{\tau}) = \bar{p}$ with a $\bar{p} \in [0,1]$, ensures that $100\bar{p}$ percent of the times a leader state update is received before triggering any follower braking (which will proceed roughly maintaining the leader velocity).

In this section we formally describe a control block able to guarantee the behaviour described before and implement the VC between the two trains. To do so, let us first recall that the follower receives asynchronous packets $\left(t_{\kappa^{\mathrm{L}}}, x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}), \underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})\right)$ with $\underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$, as said, robust leader' state trajectory estimation up to horizon H. Specifically, the latter is computed via any valid MPC embedded on the leader over its nominal model. The computed control $\mathbf{u}^{\mathrm{L}}(t)$ for the time interval $[t_{\kappa^{\mathrm{L}}}, t_{\kappa^{\mathrm{L}}} + H)$ is then applied open loop to the leader RLP (initialized at state $x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$) to compute $\underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})$, which results in a robust estimated leader trajectory. In the framework we are going to propose, we consider the choice

$$\bar{\tau} < T^{\max} \ll H. \tag{19}$$

Let us consider again controller $\hat{K}^{\mathrm{L}}$ as defined in the proof of Theorem V.2 and $t_{\mathrm{st}}^{\mathrm{L},p}(t|\hat{K}^{\mathrm{L}})$ as defined in (41) (here for a generic time t). For brevity, from now on we will omit the dependency on the controller $\hat{K}^{\mathrm{L}}$ and we will write $t_{\mathrm{st}}^{\mathrm{L},p}(t)$. We define

$$v_{\bar{\tau}}^{\mathrm{L}}\left(t, \underline{x}^{\mathrm{L}}\right) = \begin{cases} 0, & \text{if } t_{\mathrm{st}}^{\mathrm{L},p}(t) \leq t + \bar{\tau}, \\ \underline{x}_2^{\mathrm{L}} - \underline{e}^{\mathrm{L}}\left(\underline{x}_2^{\mathrm{L}}\right)\bar{\tau}, & \text{if } t_{\mathrm{st}}^{\mathrm{L},p}(t) > t + \bar{\tau}, \end{cases} \tag{20}$$

and

$$s_{\bar{\tau}}^{\mathrm{L}}\left(t, \underline{x}^{\mathrm{L}}\right) = \begin{cases} \underline{x}_1^{\mathrm{L}} + \underline{x}_2^{\mathrm{L}}\left(t_{\mathrm{st}}^{\mathrm{L},p}(t) - t\right) & \text{if } t_{\mathrm{st}}^{\mathrm{L},p}(t) \leq t + \bar{\tau}, \\ \qquad - \frac{1}{2}\underline{e}^{\mathrm{L}}\left(\underline{x}_2^{\mathrm{L}}\right)\left(t_{\mathrm{st}}^{\mathrm{L},p}(t) - t\right)^2, & \\ \underline{x}_1^{\mathrm{L}} + \underline{x}_2^{\mathrm{L}}\bar{\tau} - \frac{1}{2}\underline{e}^{\mathrm{L}}\left(\underline{x}_2^{\mathrm{L}}\right)\bar{\tau}^2, & \text{if } t_{\mathrm{st}}^{\mathrm{L},p}(t) > t + \bar{\tau}. \end{cases} \tag{21}$$

Quantities (20) and (21) represent the velocity and the position of the leader RLP at time $t + \bar{\tau}$ under a braking with controller $\hat{K}^{\mathrm{L}}$ starting at time t from the leader state $x^{\mathrm{L}}(t)$ and a time duration $\bar{\tau}$.

We also define $V_{\bar{\tau}}^{\mathrm{line},*}(t, x_1^{\mathrm{F}}, \underline{x}^{\mathrm{L}}) = \min_{s \in \left[x_1^{\mathrm{F}}, s_{\bar{\tau}}^{\mathrm{L}}\left(t, \underline{x}^{\mathrm{L}}\right)\right]} V^{\mathrm{line}}(s)$ and

$$v_{\bar{\tau}}^{\max,\mathrm{F}}\left(t, x_1^{\mathrm{F}}, \underline{x}^{\mathrm{L}}\right) = \max\left\{V^{\max,\mathrm{F}}, V_{\bar{\tau}}^{\mathrm{line},*}(t, x_1^{\mathrm{F}}, \underline{x}^{\mathrm{L}})\right\}. \tag{22}$$

The term (22) is an upper bound on the maximum velocity the follower can assume along the railway interval $\left[x_1^{\mathrm{F}}, s_{\bar{\tau}}^{\mathrm{L}}\left(t, \underline{x}^{\mathrm{L}}\right)\right]$.

Furthermore, since the state trajectory of the leader RLP is available up to time $l_{\kappa^{\mathrm{L}}}(t) + H$, the follower can compute the leader's average velocity

$$v_{\mathrm{ave}}^{\mathrm{L}}(t) = \int_t^{t+\bar{\tau}} \underline{x}_2^{\mathrm{L}}(r)\, dr. \tag{23}$$

In view of the (20)-(23) we can define

$$\tilde{z}^{\mathrm{F},1}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)) = -\Bigg[L^d + d - \left(s^{\mathrm{L}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t)) - v^{\mathrm{L}}_{\mathrm{ave}}(t)\bar{\tau}\right) - \frac{1}{2}\left(\frac{v^{\mathrm{L}^2}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t))}{\underline{e}^{\mathrm{L}}(\underline{x}^{\mathrm{L}}_2(t))} - \frac{v^{\max,F^2}_{\bar{\tau}}\left(t,x^{\mathrm{F}}_1,\underline{x}^{\mathrm{L}}\right)}{\overline{e}^{\mathrm{F}}(x^{\mathrm{F}}(t))}\right)\Bigg]$$

$$\tilde{z}^{\mathrm{F},2}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)) = -\left[L^d + d - \left(s^{\mathrm{L}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t)) - v^{\mathrm{L}}_{\mathrm{ave}}(t)\bar{\tau}\right)\right],$$

$$\tilde{z}^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)) = \min\left\{\tilde{z}^{\mathrm{F},1}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)), \tilde{z}^{\mathrm{F},2}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t))\right\}, \tag{24}$$

and

$$\tilde{z}^{\mathrm{FL}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)) = \underline{x}^{\mathrm{L}} - \tilde{z}^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)). \tag{25}$$

The above (25) is therefore exploited in what follow to define

$$z^{\mathrm{FL}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t),t_0) = \begin{cases} \max_{t'\in[t_0,t]} \tilde{z}^{\mathrm{FL}}_{\bar{\tau}}(t',\underline{x}^{\mathrm{L}}(t'),x^{\mathrm{F}}_1(t')) & \textit{if } t-t_0 \le \bar{\tau}, \\ \max_{t'\in[t-\bar{\tau},t]} \tilde{z}^{\mathrm{FL}}_{\tau}(t',\underline{x}^{\mathrm{L}}(t'),x^{\mathrm{F}}_1(t')) & \textit{if } t-t_0 > \bar{\tau}, \end{cases} \tag{26}$$

where t_0 is a generic time that will be assigned later.

Finally, we define

$$z^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t),t_0) = \underline{x}^{\mathrm{L}}_1(t) - z^{\mathrm{FL}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t),t_0). \tag{27}$$

The above formulas allow to run Algorithm 3 which provides the reference trajectory $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})$ for the follower predictive controller. The algorithm is initialized with $t_{\mathrm{last}} = -\infty$ and $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})$ null trajectory.

Algorithm 3 $\bar{t}$ far reference generator. Output: $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})$.

1: **loop**
2: Listen to possible transmission of information from the leader;
3: **if** A packet $\left(t_{\kappa^{\mathrm{L}}}, x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}), \underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})\right)$ is received with $t_{\kappa^{\mathrm{L}}} > t_{\mathrm{last}}$ **then**
4: $t_{\mathrm{last}} \leftarrow t_{\kappa^{\mathrm{L}}}$
5: Compute

$$\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}}) = z^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t),t_{\mathrm{last}})_{t\in[t_{\mathrm{last}},t_{\mathrm{last}}+H-\bar{\tau})}, \tag{28}$$

with $z^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t),t_{\mathrm{last}})$ computed according to (27) with the help of (20)-(26).
6: **end if**
7: **end loop**

Let us denote with $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})[t]$ the value of trajectory $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})[t]$ at time t. The following theorem formalizes the role of reference $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})$.

Theorem VI.2 Consider the trains system of form (4) with $i \in \{L,F\}$ and the safe set $\mathscr{S}(x) = \{x : b(x) \le 0\}$, with $b(x)$ defined in (15c). Suppose the system starts in a safe state, that is $[x^{\mathrm{L}^T}(t_0), x^{\mathrm{F}^T}(t_0)]^T \in \mathscr{S}$. Consider the control architecture encompassing the safety control block (Algorithm 2) and the $\bar{\tau}$ far reference generator (Algorithm 3), with $\bar{\tau}$ satisfying (19). Then, any valid predictive controller $K^{\mathrm{F}}(x^{\mathrm{F}})$ able to enforce

$$x^{\mathrm{F}}_1(t) \le \mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})[t], \forall t \in [t_{\mathrm{last}}, t_{\mathrm{last}}+H-\bar{\tau}) \tag{29}$$

guarantees that at least a $\bar{\tau}$ is wait before an emergency braking is triggered, that is $t_{\kappa^{\mathrm{E}}+1} - t_{\kappa^{\mathrm{E}}} \ge \bar{\tau}$ for any κ^{E}.

Proof. To prove the result let us assume that the follower's controller plans a path forward such that, at any time t and for the time interval $[t, t+\bar{\tau}]$ it keeps an average velocity $v^{\mathrm{L}}_{\mathrm{ave}}(t)$ as in (23). We are therefore supposing that, roughly speaking, the follower controller is able to track the RLP leader average velocity computed over a $\bar{\tau}$ ahead interval. This hypothesis will not necessarily be met and, in general, it is not satisfied. Nevertheless, let us keep it as working hypothesis for now (we will then address later the case in which such hypothesis is not met). Saying this, even if the follower keeps $v^{\mathrm{L}}_{\mathrm{ave}}(t)$ as average velocity in $[t, t+\bar{\tau}]$ the instant velocity could vary. In particular, we can consider the worst case were the follower assumes, at time $t+\bar{\tau}$, the instant velocity of $v^{\max,\mathrm{F}}_{\bar{\tau}}(t,x^{\mathrm{F}}_1,\underline{x}^{\mathrm{L}})$ (that is, an upper bound computed at time t on the maximum velocity achievable by the follower). In view of this, $\tilde{z}^{\mathrm{F},1}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t))$ represents the position that the follower should have, at time t, such that when proceeding at the planned RLP leader average velocity and supposing the leader is instead activating an emergency braking, at time $t+\bar{\tau}$ and with the (worst) case of a follower velocity (we omit the dependency for the sake of brevity) $v^{\max,\mathrm{F}}_{\bar{\tau}}$ the barrier $b'(s^{\mathrm{L}}_{\bar{\tau}}, v^{\mathrm{L}}_{\bar{\tau}}, \tilde{z}^{\mathrm{F},1}_{\bar{\tau}} + v^{\mathrm{L}}_{\mathrm{ave}}\bar{\tau}, v^{\max,\mathrm{F}}_{\bar{\tau}}) = 0$. In the latter formula, we slight abuse the notation and explicitly point out (not in a stack vector form) the variables upon which $b'(\cdot)$ in (15a) depends. Specifically, $s^{\mathrm{L}}_{\bar{\tau}}\left(t,\underline{x}^{\mathrm{L}}\right)$ in (21) (for brevity, we omit the dependencies) is, as said, the position of the leader RLP at time $t+\bar{\tau}$ after a braking with controller $\hat{K}^{\mathrm{L}}$. Such a position is a lower bound for that achieved by the true leader after an emergency braking (notice that $\hat{K}^{\mathrm{L}}$ is more aggressive than K^{L}_E). Analogously, $v^{\mathrm{L}}_{\bar{\tau}}\left(t,\underline{x}^{\mathrm{L}}\right)$ in (20) is the achieved RLP velocity.

As for $\tilde{z}^{\mathrm{F},1}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t))$, the term $\tilde{z}^{\mathrm{F},2}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t))$ is the follower position such that $b''(s^{\mathrm{L}}_{\bar{\tau}}, v^{\mathrm{L}}_{\bar{\tau}}, \tilde{z}^{\mathrm{F},2}_{\bar{\tau}} + v^{\mathrm{L}}_{\mathrm{ave}}\bar{\tau}, v^{\max,\mathrm{F}}_{\bar{\tau}}) = 0$ at time $t+\bar{\tau}$, with $b''(\cdot)$ defined in (15b).

The term $\tilde{z}^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t))$ represents, in view of what stated above, the position the follower should have such that, proceeding at an average velocity $v^{\mathrm{L}}_{\mathrm{ave}}(t)$ for the time interval $[t, t+\bar{\tau}]$ and considering instead a leader emergency braking, the barrier $b(s^{\mathrm{L}}_{\bar{\tau}}, v^{\mathrm{L}}_{\bar{\tau}}, \tilde{z}^{\mathrm{F}}_{\bar{\tau}} + v^{\mathrm{L}}_{\mathrm{ave}}\bar{\tau}, v^{\max,\mathrm{F}}_{\bar{\tau}})$ will assume null value a time $t+\bar{\tau}$, with $b(\cdot)$ given in (15c).

Therefore, any controller of the follower able to guarantee

$$x^{\mathrm{F}}_1(t) \le \tilde{z}^{\mathrm{F}}_{\bar{\tau}}(t,\underline{x}^{\mathrm{L}}(t),x^{\mathrm{F}}_1(t)), \tag{30}$$

and an average velocity $v^{\mathrm{L}}_{\mathrm{ave}}(t)$ guarantees that the CBF is not intercepted before a time $t+\bar{\tau}$. Since this is valid for any time t, keeping the constraint (30) guarantees that, at any t_{last} upon which the RLP predictor of Algorithm 1 is reset, an emergency braking event does not happen before time $t+\bar{\tau}$.

The reasoning conducted so far is based on the hypothesis that the follower controller is able not only to satisfy (30), but also to keep an average velocity $v^{\mathrm{L}}_{\mathrm{ave}}(t)$ for the time interval $[t, t+\bar{\tau}]$. This, in general, cannot be assumed. Nevertheless, it is immediate to notice that if the follower has an average velocity $\tilde{v}$ lower than $v^{\mathrm{L}}_{\mathrm{ave}}(t)$ the whole reasoning still holds. Indeed, the follower would reach, at time $t+\bar{\tau}$, a position $\tilde{x}^{\mathrm{F}}(t+\bar{\tau}) = x^{\mathrm{F}}(t) + \tilde{v}\bar{\tau}$ with $\tilde{x}^{\mathrm{F}}(t+\bar{\tau}) \leq x^{\mathrm{F}}(t) + v^{\mathrm{L}}_{\mathrm{ave}}(t)\bar{\tau}$ therefore attaining a more conservative barrier value $b(s^{\mathrm{L}}_{\bar{\tau}}, v^{\mathrm{L}}_{\bar{\tau}}, \tilde{x}^{\mathrm{F}}(t+\bar{\tau}), v^{\max,F}_{\bar{\tau}}) \leq b(s^{\mathrm{L}}_{\bar{\tau}}, v^{\mathrm{L}}_{\bar{\tau}}, \tilde{z}^{\mathrm{F}}_{\bar{\tau}} + v^{\mathrm{L}}_{\mathrm{ave}}\bar{\tau}, v^{\max,F}_{\bar{\tau}})$.

To cope instead with an average velocity greater than $v^{\mathrm{L}}_{\mathrm{ave}}(t)$, we first need to observe that this might happen when the leader-follower inter distance $\tilde{z}^{\mathrm{FL}}_{\bar{\tau}}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t))$ in (25) is decreasing. It might therefore happen then, when tracking $x^{\mathrm{F}}_1(t) \leq \tilde{z}^{\mathrm{F}}_{\bar{\tau}}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t))$, the follower average velocity might grow bigger than $v^{\mathrm{L}}_{\mathrm{ave}}(t)$, violating the hypothesis on which the theorem is valid. This aspect can be easily fixed by replacing constraint (30) with

$$x^{\mathrm{F}}_1(t) \leq z^{\mathrm{F}}_{\bar{\tau}}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}}), \tag{31}$$

with $z^{\mathrm{F}}_{\bar{\tau}}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}})$ defined in (27). □

D. Delay estimator block

Given the variability in channel communication along railway lines, it is advantageous to introduce a block that estimates the communication delay between the leader and follower. The leader transmits at synchronous sampling interval of ΔT^{ch} but, due to the unreliable network the follower receives data asynchronously. The sequence of delays $\{\tau(t_{\kappa^{\mathrm{L}}})\}^{+\infty}_{\kappa^{\mathrm{L}}=0}$ is influenced by various factors, e.g. stochastic properties of channel communication and hardware processing time. To this end, it has been treated as a random variable, is approximated with the following exponential probability distribution

$$\tau \sim f_{\mathrm{d}}(t; \lambda, T^{\min}) = \begin{cases} \lambda e^{-\lambda(t-T^{\min})} & t \geq T^{\min}, \\ 0 & \text{otherwise}, \end{cases} \tag{32}$$

where $T^{\min}$ is the minimum time of arrival and λ is the distribution's parameter. Moreover, the communication channel is modeled to be subject to packet loss, which follows a Bernoulli distribution $f_{\mathrm{l}} \sim \mathrm{Bernoulli}(p_{\mathrm{loss}})$. As a result, there is a possibility that the follower train may fail to receive the transmitted packets from the leader.

The estimated delay is computed in 4, where $N_{\hat{\tau}}$ represents the samples of past arrival times stored in a buffer.

This estimation is calculated each time a new packet from the leader arrives. Subsequently, the cruise virtual coupling block, as described in VI-E, sets $\bar{\tau} = \hat{\tau}(t_{\kappa^{\mathrm{L}}})$. This process allows for the generation of delay-dependent reference trajectories (33)-(35).

As already said, this block might be omitted since the proposed architecture guarantee safety and a minimum time before an emergency braking is triggered. However, the presence of a delay estimator allows to better chose such minimum time so as to reduce unnecessary braking. We also emphasize that, thanks to the generality of the proposed framework, several other possible choices can be adopted for the delay estimator, such as weighted mobile average or mean and variance estimation (ad higher order statistical moments).

Algorithm 4 Delay estimator. Output: $\hat{\tau}(t_{\kappa^{\mathrm{L}}})$.

loop
  Listen to possible transmission of information from the leader;
  if A packet $\left(t_{\kappa^{\mathrm{L}}}, x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}), \underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})\right)$ is received with $t_{\kappa^{\mathrm{L}}} > t_{\mathrm{last}}$ **then**
    Estimate $\hat{\lambda}$ and $\hat{T}^{\min}$
    Compute $\hat{\tau}(t_{\kappa^{\mathrm{L}}}) = F_{\mathrm{d}}(\bar{p}; \hat{\lambda}, \hat{T}^{\min})$
  end if
end loop

In Section VII, we will demonstrate the benefits of incorporating this block within the control architecture through simulations.

E. Cruise virtual coupling block: switched controller

Section VI-C does not explicitly state the expression of the predictive controller to be applied for the follower. Rather, it provides, through Algorithm 3 the trajectory constraint $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})$ generated at any updates event t_{last} which, if enforced by the predictive controller on the follower position, allows no to have any transmission before a $\bar{\tau}$ time interval is passed.

Since $\bar{\tau}$ is a design value, whose choice might follow a criterion as that depicted at the beginning of Section VI-C, it is in principle possible to consider several values of $\bar{\tau}$ so as to have several $\bar{\tau}$-distances levels and develop switched controllers.

In this section we propose a three-level predictive switched controller considering three $\tau_i = \omega_i \bar{\tau}$ values, with $i = \in \{1,2,3\}$, with $1 < \omega_1 < \omega_2 < \omega_3$ scaling parameters.

The whole reasoning conducted in Section VI-C can therefore be repeated substituting in the formulas $\bar{\tau}$ with τ_i.

The switched controller is therefore implemented in Algorithm 5, where synthetically we call $K^{\mathrm{F}}_i(x^{\mathrm{F}})$, with $i \in \{1,2,3\}$ the three controller modes.

The controller $K^{\mathrm{F}}_1(x^{\mathrm{F}}(t))$ is deployed in scenarios where the VC approaches the critical condition when the follower is reaching the safety barrier. The primary objective of this controller is to ensure safety by maximizing the distance from the safety boundary while also minimizing control effort. Its cost function is defined as follows

$$\begin{aligned} K^{\mathrm{F}}_1(x^{\mathrm{F}}(t)) = \arg\min_{u^{\mathrm{F}}(t)} \int_t^{t+H} & \Theta^u_1 \left(u^{\mathrm{F}}(r)\right)^2 \\ & + \Theta^s_1 \left(x^{\mathrm{F}}_1(r) - \mathbf{z}^{\mathrm{F}}_{\tau_2}(t_{\mathrm{last}})[r]\right)^2 dr, \\ \text{subject to} \quad & \text{Eqs. (6)}, \quad \text{with } i = \mathrm{F}. \end{aligned} \tag{36}$$

The controller $K^{\mathrm{F}}_2(x^{\mathrm{F}}(t))$ is tasked with supporting the VC under normal operating conditions. Its primary objective is to

Algorithm 5 $\bar{t}$ far reference generator. Output: $\mathbf{z}^{\mathrm{F}}_{\bar{\tau}}(t_{\mathrm{last}})$.

loop
  Listen to possible transmission of information from the leader;
  if A packet $\left(t_{\kappa^{\mathrm{L}}}, x^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}}), \underline{\mathbf{x}}^{\mathrm{L}}(t_{\kappa^{\mathrm{L}}})\right)$ is received with $t_{\kappa^{\mathrm{L}}} > t_{\mathrm{last}}$ **then**
    $t_{\mathrm{last}} \leftarrow t_{\kappa^{\mathrm{L}}}$
    Compute

$$\mathbf{z}^{\mathrm{F}}_{\tau_1}(t_{\mathrm{last}}) = z^{\mathrm{F}}_{\tau_1}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}})_{t\in[t_{\mathrm{last}}, t_{\mathrm{last}}+H-\tau_1)}, \quad (33)$$

$$\mathbf{z}^{\mathrm{F}}_{\tau_2}(t_{\mathrm{last}}) = z^{\mathrm{F}}_{\tau_2}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}})_{t\in[t_{\mathrm{last}}, t_{\mathrm{last}}+H-\tau_2)}, \quad (34)$$

$$\mathbf{z}^{\mathrm{F}}_{\tau_3}(t_{\mathrm{last}}) = z^{\mathrm{F}}_{\tau_3}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}})_{t\in[t_{\mathrm{last}}, t_{\mathrm{last}}+H-\tau_3)}. \quad (35)$$

    if $x^{\mathrm{F}}_1(t) \leq z^{\mathrm{F}}_{\tau_3}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}})$ **then**
      Select controller $K^{\mathrm{F}}_1(x^{\mathrm{F}}(t))$;
    else if $z^{\mathrm{F}}_{\tau_3}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}}) < x^{\mathrm{F}}_1(t) \leq z^{\mathrm{F}}_{\tau_1}(t, \underline{x}^{\mathrm{L}}(t), x^{\mathrm{F}}_1(t), t_{\mathrm{last}})$ **then**
      Select controller $K^{\mathrm{F}}_2(x^{\mathrm{F}}(t))$;
    else
      Select controller $K^{\mathrm{F}}_3(x^{\mathrm{F}}(t))$;
    end if
  end if
end loop

maintain the average velocity of the leader, ensuring smooth and efficient operation. This controller works to minimize deviations from the desired velocity and position, while also optimizing control effort. Its functional cost is defined as follows

$$\begin{aligned} K^{\mathrm{F}}_2(x^{\mathrm{F}}(t)) = \arg\min_{u(t)} \int_t^{t+H} & \Theta^s_2 (x^{\mathrm{F}}_1(r) - \mathbf{z}^{\mathrm{F}}_{\tau_2}(t_{\mathrm{last}})[r])^2 \\ & + \Theta^v_2 (x^{\mathrm{F}}_2(r) - \underline{\mathbf{x}}^{\mathrm{L}}_2(r))^2 + \Theta^u_2 (u^{\mathrm{F}}(r))^2 dr, \\ \text{subject to} \quad & Eqs.(6), \quad \text{with } i = \mathrm{F}. \end{aligned} \quad (37)$$

The controller $K^{\mathrm{F}}_3(x^{\mathrm{F}}(t))$, designated as the L3-VC transition controller, is specifically designed to minimize the distance between the two trains by employing an aggressive control strategy to catch up to the leader. This controller is activated at the onset of the VC operation, serving as the initial control mechanism to quickly establish the desired train spacing.. The optimization problem it aims to solve is outlined as follows

$$\begin{aligned} K^{\mathrm{F}}_3(x^{\mathrm{F}}(t)) = \arg\min_{u(t)} \int_t^{t+H} & \Theta^s_3 (x^{\mathrm{F}}_1(r) - \mathbf{z}^{\mathrm{F}}_{\tau_2}(t_{\mathrm{last}})[r])^2, \\ \text{subject to} \quad & Eqs.(6), \quad \text{with } i = \mathrm{F}. \end{aligned} \quad (38)$$

VII. Simulations

To verify the efficacy of our control system, we will utilize a specialized simulation tool named *RV4565*, a video of its functionalities is reported in [22]. This tool, developed with MATLAB enables detailed observation of train variables, including those influencing platoon systems, such as inter-train distance and velocity. All simulations were conducted on a laptop equipped with an Intel i7-10710U processor (6 cores at 4.7GHz) and 16GB of RAM, running the Windows operating system.

For the sake of readability, all parameters used in the simulations are listed in Appendix B. The controllers (36)-(38) presented in VI-E have been implemented as Nonlinear Model Predictive Controls (NMPCs) using the OpEn framework and the PANOC solver [23] with ΔT^{mpc} as discretization time.

The dynamic parameters of the trains were modeled after those of two Frecciarossa ETR1000 trains [24]. For the simulations, it was specifically assumed that the follower train is fully loaded, while the leader train is not. Figure 3 reports the data profile of the railway line used to conduct the simulation is the Italian Firenze-Bologna railway line. The maximum velocity of the railway line is assumed to be constant and is set to $83\frac{\mathrm{m}}{\mathrm{s}}$ which is the maximum permitted by the infrastructure along the entire route.

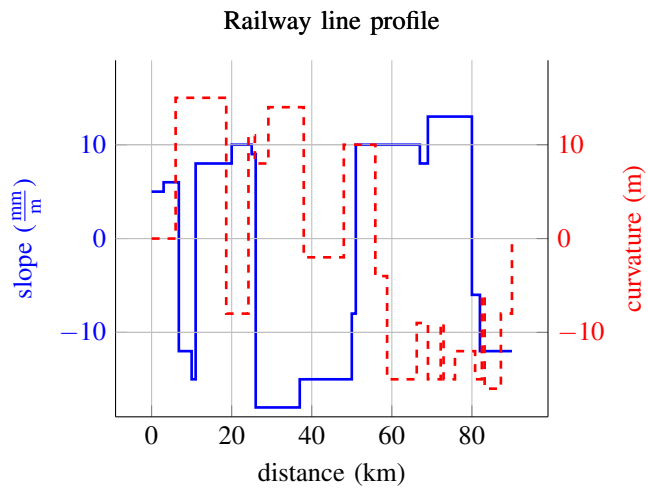

Fig. 3: Curvature(dashed line) and slope(continuos line) of Firenze-Bologna railway line.

A. Operational scenarios

Two different Operational Scenario (OS) have been considered to demonstrate the safety and advantages of the control system presented in this work.

In the first scenario, called OS1, we examine the situation where the leader and follower initiate a VC operation starting from L3 at 6000m distance between them. Throughout the trajectory, the leader modifies its velocity to demonstrate the responsiveness and effectiveness of the proposed control architecture. At a designated point along the route, the leader stabilizes and maintains it constant. For the whole testing scenario the follower is able to safely approach the leader (despite its varying velocity) and successfully reach and establish the virtual coupling. This scenario emphasizes the capabilities of the control system in managing variable speeds and achieving precise coordination. At a certain point

in the journey, the leader suddenly initiates braking, gradually reducing its speed until it comes to a complete stop. This situation tests the responsiveness and safety of the follower's control system, assessing its ability to efficiently respond to the sudden braking of the leader.

The third case presents a scenario similar to OS2, where the leader and the follower are traveling in VC operation. Initially, the leader maintains a steady and constant speed, and the follower keeps a safety distance. This case explores a situation where communication between the leader and the follower becomes degraded, increasing the delay in channel communication. Following this initial degradation, the communication eventually fails to arrive on time. This communication delay introduces significant challenges, testing the robustness and resilience of the follower's control system. The follower must rely on its last received data and onboard sensors to ensure safety and maintain proper operation despite the lack of timely updates from the leader. This scenario underscores the importance of having robust fallback mechanisms and adaptive control strategies to handle unexpected communication failures.

B. Results

In scenario OS1, the simulations results reported in Figure **??**, the leader and follower start with an initial separation of 6000 m when the virtual coupling operation begins. Throughout the route, the leader performs braking and acceleration maneuvers to demonstrate the follower's switched controller's capability to effectively manage and respond to these variations using controllers K_1^{F}, K_2^{F} and K_3^{F}. To note that at 310 s, the follower switches to the K_3^F controller, which is the most restrictive.By the end of the simulation, the interdistance between the leader and follower reduces to approximately 1750 m, with both maintaining nearly the same velocity of 60 $\frac{\mathrm{m}}{\mathrm{s}}$. Importantly, safety is ensured throughout the scenario, as the safety barrier remains non-negative at all times.Furthermore, reference trajectories within a specific time window illustrate how the follower's position affects the switching of the virtual cruise controller. This detailed observation highlights the system's capability to manage dynamic interactions and maintain safety during virtual coupling operations.

Figure **??** depicts the simulations results for scenario OS2, it is essential for showcasing the effectiveness of our control system architecture, especially under extreme conditions where the leader suddenly brakes to a complete stop. Initially, both the safety distance and inter-vehicle distance remain stable at 1750m, reflecting the leader's constant speed. However, at 150s, the leader begins to brake, resulting in a significant decrease in the safety distance. By 150s, the emergency controller $K_{\mathrm{E}}^{\mathrm{F}}$ is activated due to the condition $b(x) \geq 0$. Once activated, the follower re-enters the safe region and for the remainder of the train's movement, the virtual cruise control system engages the three controllers K_1^{F}, K_2^{F} and K_3^{F}, ensuring the train stops at a distance greater than d.

The last scenario OS3, reported in in Figure **??**, highlights two key features of our control system: its robustness against variability in communication channel characteristics and its ability to safely manage potential connection losses between the leader and follower. As in the previous scenario, the two trains are initially assumed to be in VC, maintaining a distance of 1750m. Around 75s, the communication channel undergoes a change (specifically, the variable T^{min} increases to $\overline{T}^{min}$, as detailed in Appendix B). The delay estimator block continuously estimates the delay and sends it to the cruise virtual coupling block, which computes the reference trajectories $\mathbf{z}_{\tau_1}^{\mathrm{F}}(t)$, $\mathbf{z}_{\tau_2}^{\mathrm{F}}(t)$, and $\mathbf{z}_{\tau_3}^{\mathrm{F}}(t)$. These trajectories tend to have lower values, prompting the controller to switch to a more restrictive mode. This adjustment allows the follower train, in the event of increased delays, to maintain a greater distance from the leader. The communication loss occurs at 215s. As observed, the safety barrier increases due to the leader RLP predictor block integrating the distance covered by the leader, assuming it is braking at maximum capacity. Once the condition $(x) \geq 0$ is met, the follower initiates an emergency brake using the controller $K_{\mathrm{E}}^{\mathrm{F}}$.

To demonstrate the real-time capabilities of the control system architecture described in our work, Table I presents the statistical computational times of the controller. The values obtained indicate that the system can be effectively utilized in railway applications, where the controller's frequency rate is typically around 100ms.

TABLE I: Computation time controller.

Parameter	Value
mean	0.70ms
standard deviation	1.01ms
max time	20.18ms

VIII. Conclusion and Future Work

In this study, we have presented a comprehensive control system architecture to facilitate the transition from ETCS Level 3 to Virtual Coupling operations in railway systems. Our proposed system effectively manages the dynamic interaction between trains, ensuring safety and enhancing operational efficiency. Through different operational scenarios considered into the simulations, we have demonstrated that the control architecture can maintain a safe distance between trains, even under conditions of communication delay and packet loss.

The key contributions of our work include the development of a robust control framework that accommodates variabilities in train system parameters and communication throughput. By incorporating a safety control barrier function, we ensure operational safety while minimizing unnecessary emergency braking. Our simulations, conducted using a specialized railway simulation tool, validate the efficacy of our control system and underscore its foundational role in advancing railway safety.

Future work will focus on extending the architecture to handle multiple trains in a platoon and exploring the integration of AI-based controllers to further enhance system performance. Additionally, further studies are needed to address the certification of ML-based controllers in the railway domain, ensuring they meet stringent safety standards. Our ongoing research aims to refine the control algorithms and validate the system through field trials, paving the way for the widespread adoption of Virtual Coupling in modern railway networks.

Acknowledgement

We sincerely thank Rete Ferroviaria Italiana for their support through knowledge transfer and background insights, significantly contributing to the advancement of our work.

Appendix

A. Proof of Theorem V.2

Proof. To prove the result, let us first consider two special choices for the leader and follower controller, namely:

$$\hat{K}^{\mathrm{L}}(x^{\mathrm{L}}) = \begin{cases} \overline{a}^{\mathrm{L}}_{\mathrm{br}}, & \text{if } x^{\mathrm{L}}_2 > 0, \\ 0, & \text{if } x^{\mathrm{L}}_2 = 0, \end{cases}$$

$$\hat{K}^{\mathrm{F}}(x^{\mathrm{F}}) = \begin{cases} \varepsilon \underline{\alpha}^{\mathrm{F}}(x^{\mathrm{F}}_2), & \text{if } x^{\mathrm{F}}_2 > 0, \\ 0, & \text{if } x^{\mathrm{F}}_2 = 0, \end{cases}$$

with, as said, $\varepsilon < 1$ (a good choice is slightly less than one).

Now, let us suppose to apply from the initial time t_0 controllers $\hat{K}^{\mathrm{L}}$ and $\hat{K}^{\mathrm{F}}$ at the leader's RLP and at the follower's RUP, respectively.

Also, let us suppose for the moment that at the considered initial time t_0 the leader is not standing, i.e. $x^{\mathrm{L}}_2(t_0) > 0$ (this hypothesis will be removed later).

Notice that the assumption $x^{\mathrm{F}}_2(t_0) > 0$ in the theorem statement and the technical one $x^{\mathrm{L}}_2(t_0) > 0$ we just added temporarily are only meant to allow these two controllers to provide non zero input, since, in case a train is still, the set $\mathscr{U}^i(x^i) = \{0\}$ is the only available controller satisfying (5), forse questa va messa al posto della (6).

With such a choice, it is immediate to verify that the leader RLP dynamics are

$$\dot{\underline{x}}^{\mathrm{L}}_1 = \underline{x}^{\mathrm{L}}_2 \tag{39a}$$

$$\dot{\underline{x}}^{\mathrm{L}}_2 = -\underline{e}^{\mathrm{L}}\left(x^{\mathrm{L}}_2(t_0)\right), \tag{39b}$$

$$\underline{x}^{\mathrm{L}}(t_0) = x^{\mathrm{L}}(t_0), \tag{39c}$$

while the follower RUP dynamics are

$$\dot{\overline{x}}^{\mathrm{F}}_1 = \overline{x}^{\mathrm{F}}_2 \tag{40a}$$

$$\dot{\overline{x}}^{\mathrm{F}}_2 = -\overline{e}^{\mathrm{F}}\left(x^{\mathrm{F}}(t_0)\right), \tag{40b}$$

$$\overline{x}^{\mathrm{F}}(t_0) = x^{\mathrm{F}}(t_0). \tag{40c}$$

Let us define $t^{\mathrm{L},p}_{\mathrm{st}}(t_0|\hat{K}^{\mathrm{L}}) = \min\{t \in [t_0, +\infty) : \underline{x}^{\mathrm{L}}_2(t) = 0\}$ the stopping time of the leader RLP subjected to controller $\hat{K}^{\mathrm{L}}$ applied from time t_0 and, similarly, let us define $t^{\mathrm{F},p}_{\mathrm{st}}(t_0|\hat{K}^{\mathrm{F}}) = \min\{t \in [t_0, +\infty) : \overline{x}^{\mathrm{F}}_2(t) = 0\}$ the stopping time of the follower RUP subjected to $\hat{K}^{\mathrm{F}}$ from t_0.

From the dynamics (39) and (40), we have

$$t^{\mathrm{L},p}_{\mathrm{st}}(t_0|\hat{K}^{\mathrm{L}}) = \frac{x^{\mathrm{L}}_2(t_0)}{\underline{e}^{\mathrm{L}}\left(x^{\mathrm{L}}_2(t_0)\right)} + t_0 \tag{41}$$

at position

$$\underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}}) = x^{\mathrm{L}}_1(t_0) + \frac{1}{2}\frac{x^{\mathrm{L}}_2(t_0)^2}{\underline{e}^{\mathrm{L}}\left(x^{\mathrm{L}}_2(t_0)\right)}, \tag{42}$$

while the follower's RUP stops at time $t^{\mathrm{F},p}_{\mathrm{st}}(t_0|\hat{K}^{\mathrm{F}}) = \frac{x^{\mathrm{F}}_2(t_0)}{\overline{e}^{\mathrm{F}}\left(x^{\mathrm{F}}(t_0)\right)} + t_0$ at position

$$\overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}}) = x^{\mathrm{F}}_1(t_0) + \frac{1}{2}\frac{x^{\mathrm{F}}_2(t_0)^2}{\overline{e}^{\mathrm{F}}\left(x^{\mathrm{F}}(t_0)\right)}. \tag{43}$$

The position difference of the two trains proxies when they are both stopped is, therefore,

$$\begin{aligned} \underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}}) - \overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}}) = & x^{\mathrm{L}}_1(t_0) - x^{\mathrm{F}}_1(t_0) \\ & + \frac{1}{2}\left(\frac{x^{\mathrm{L}}_2(t_0)^2}{\underline{e}^{\mathrm{L}}\left(x^{\mathrm{L}}_2(t_0)\right)} - \frac{x^{\mathrm{F}}_2(t_0)^2}{\overline{e}^{\mathrm{F}}\left(x^{\mathrm{F}}_2(t_0)\right)}\right). \end{aligned} \tag{44}$$

It is worth noticing that when the proxies are stopped, being $\mathscr{U}^{\mathrm{L}}(\underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}})) = \{0\}$ and $\mathscr{U}^{\mathrm{F}}(\overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}})) = \{0\}$, we have that $\underline{x}^{\mathrm{L}}_1(t) = \underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}})$ at any $t \geq t^{\mathrm{L},p}_{\mathrm{st}}$ and, similarly, $\overline{x}^{\mathrm{F}}_1(t) = \overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}})$ at any time $t \geq t^{\mathrm{F},p}_{\mathrm{st}}$.

When comparing (44) with $b'(x)$ in (15a), it is immediate to notice that

$$b'([\underline{x}^{\mathrm{L}^T}(t_0), \overline{x}^{\mathrm{F}^T}(t_0)]^T) = L^{\mathrm{L}} + d - \left(\underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}}) - \overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}})\right). \tag{45}$$

From the above equation we have that, when evaluated at $x = [\underline{x}^{\mathrm{L}^T}(t_0), \overline{x}^{\mathrm{F}^T}(t_0)]^T$, $b'(x)$ can be interpreted as the difference between the minimum required inter-trains distance $L^{\mathrm{L}} + d$ and the proxy leader-follower distance achieved when considering that, at a generic initial time instant t_0, the two proxies engage controllers $\hat{K}^{\mathrm{L}}$ and $\hat{K}^{\mathrm{F}}$, respectively, until they stop. Notice also that, in view of this interpretation, the following equality holds[2]

$$b'(\underline{x}^{\mathrm{L}}(t), \overline{x}^{\mathrm{F}}(t)) = b'(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0)), \tag{46}$$

at any time instant $t > t_0$ with $\underline{x}^{\mathrm{L}}(t) = \underline{\phi}^{\mathrm{L}}(t, t_0, x^{\mathrm{L}}(t_0), \hat{K}^{\mathrm{L}})$ and $\overline{x}^{\mathrm{F}}(t) = \overline{\phi}^{\mathrm{F}}(t, t_0, x^{\mathrm{F}}(t_0), \hat{K}^{\mathrm{F}})$, that is evaluated on the dynamical flow of the two proxies subjected to the controllers $\hat{K}^{\mathrm{L}}$ and $\hat{K}^{\mathrm{F}}$.

For shorting the notation, let us rewrite $\underline{x}^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}})$ to denote the RLP trajectory of the leader under controller $\hat{K}^{\mathrm{L}}$ and initial condition $x^{\mathrm{L}}(t_0)$ and, similarly $\overline{x}^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})$ to denote the RUP trajectory of the follower under controller $\hat{K}^{\mathrm{F}}$ and initial condition $x^{\mathrm{F}}(t_0)$.

[2]To ease the notation we will write $b'(\underline{x}^{\mathrm{L}}(t), \overline{x}^{\mathrm{F}}(t))$ instead of $b'([\underline{x}^{\mathrm{L}^T}(t), \overline{x}^{\mathrm{F}^T}(t)]^T)$ (and similarly mutatis mutandis for the other terms on which $b(\cdot)$ is evaluated).

Analogously (and still considering the initial conditions $x^{\mathrm{L}}(t_0)$ and $x^{\mathrm{F}}(t_0)$), let us denote with $x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}})$ and $x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})$ the trajectory of the leader and the follower under the controllers $\hat{K}^{\mathrm{L}}$ and $\hat{K}^{\mathrm{F}}$, respectively. By the properties of RLP and RUP (Definition 8 and Definition 9) the following inequalities hold

$$x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}) \geq \underline{x}^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), \tag{47a}$$

$$x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}}) \leq \overline{x}^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}}), \tag{47b}$$

for any $t > t_0$.

Notice also that, so far, we considered the technical assumption that the initial velocity of the leader is not null, so as to apply the controller $\hat{K}^{\mathrm{L}}$. Nevertheless, inequality (47a) still holds (with the equality relation) also in case the leader has null initial velocity. In that case, being the null input the only allowed, we have $\hat{K}^{\mathrm{L}}(\underline{x}_L) = 0$.

From (47a) and (47b) we have

$$b'(x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})]) \leq b'(\underline{x}^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), \overline{x}^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})), \qquad \forall t > t_0. \tag{48}$$

Furthermore, noticing that $t^F_{\mathrm{st}} \leq t^{\mathrm{F},p}_{\mathrm{st}}$, for the above formula it holds

$$b'(x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})) < b'(\underline{x}^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), \overline{x}^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})), \ \forall t_0 \geq t \geq t^F_{\mathrm{st}}.$$

Combining (48) with (46), we obtain

$$b'(x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})) \leq b'(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0))), \qquad \forall t > t_0. \tag{49}$$

Being t and t_0 two generic instants, inequality (49) shows that $b'(x)$ is monotonically decreasing on the trains system under the control provided by $\hat{K}^{\mathrm{L}}$ and $\hat{K}^{\mathrm{F}}$.

To show that the special controller $\hat{K}^{\mathrm{L}}$ $\hat{K}^{\mathrm{F}}$ is robustly safety compliant we need to analyze the evolution of $b(x)$ along the system trajectory also when $b(x)$ attains its maximum on $b''(x)$. To do so, let us consider the case that $b(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0)) = b''(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0))$ which, equivalently, reads as

$$b'(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0)) < b''(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0)). \tag{50}$$

Let us again consider the evolution of the two proxies $\underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}})$ and $\overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}})$. By considering (44) and (45), from (50) it follows that

$$\underline{x}^{\mathrm{L}}_1(t^{\mathrm{L},p}_{\mathrm{st}}) - \overline{x}^{\mathrm{F}}_1(t^{\mathrm{F},p}_{\mathrm{st}}) > x^{\mathrm{L}}_1(t_0) - x^{\mathrm{F}}_1(t_0). \tag{51}$$

Therefore, from the above equation, the case (50) yields an inter proxies distance when both are stopped greater than the initial one. Furthermore, by considering the position error dynamics, from (39) and (40) we have

$$\begin{aligned} &\dot{\underline{x}}^{\mathrm{L}}_1(t) - \dot{\overline{x}}^{\mathrm{F}}_1(t) = \\ &x^{\mathrm{L}}_2(t_0) - x^{\mathrm{F}}_2(t_0) - \left(\underline{e}^{\mathrm{L}}\left(x^{\mathrm{L}}_2(t_0)\right) - \overline{e}^{\mathrm{F}}\left(x^{\mathrm{F}}_2(t_0)\right)\right)(t - t_0). \end{aligned} \tag{52}$$

It is immediate to observe from (52) that the proxies distance is monotone and, by considering (51) we have that $\dot{\underline{x}}^{\mathrm{L}}_1(t) - \dot{\overline{x}}^{\mathrm{F}}_1(t) > 0$ for any $t < \max\{t^{\mathrm{L},p}_{\mathrm{st}}, t^{\mathrm{F},p}_{\mathrm{st}}\}$, while remaining constant otherwise. Therefore, it is monotone increasing. This leads to

$$b''(x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})) < b''(\underline{x}^{\mathrm{L}}(t_0), \overline{x}^{\mathrm{F}}(t_0)). \tag{53}$$

Combining (49) and (53) we prove the monotonicity of $b(x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}}))$ and, hence, that the special controller we considered it robustly safety compliant.

To prove that the controller $K = [K^{\mathrm{L}^T}, K^{\mathrm{F}^T}_E]^T$ is robustly safe compliant, let us denote with $x^{\mathrm{L}}(t|K^{\mathrm{L}})$ the trajectory of the leader under any controller K^{L} and with $x^{\mathrm{F}}(t|K^{\mathrm{F}}_{\mathrm{E}})$ the trajectory of the follower under the emergency controller $K^{\mathrm{F}}_{\mathrm{E}}$. By again considering the properties of RLP and RUP and the definition of emergency controller (Definition 11) the following inequalities hold

$$x^{\mathrm{L}}(t|K^{\mathrm{L}}) \geq x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), \tag{54}$$

$$x^{\mathrm{F}}(t|K^{\mathrm{F}}_{\mathrm{E}}) \leq x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}}), \tag{55}$$

for any $t > t_0$.

Hence, $x^{\mathrm{L}}(t|K^{\mathrm{L}}) - x^{\mathrm{F}}(t|K^{\mathrm{F}}_{\mathrm{E}}) \geq x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}) - x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})$ and, therefore,

$$b([x^{\mathrm{L}}(t|K^{\mathrm{L}}), x^{\mathrm{F}}(t|K^{\mathrm{F}}_{\mathrm{E}})]^T) \leq b([x^{\mathrm{L}}(t|\hat{K}^{\mathrm{L}}), x^{\mathrm{F}}(t|\hat{K}^{\mathrm{F}})]^T) \qquad \forall t > t_0.$$

□

B. Simulation parameters

The data used during the simulation for the train models, the controller parameters, and those characterizing the communication channel are:

Train Models			
Parameter	**Value**	**Parameter**	**Value**
M^{L}(kg)	$4.9 \cdot 10^5$	M^{F}(kg)	$5.1 \cdot 10^5$
γ	10^6	L^{L}(m)	202
A^{L}(N)	27.30	A^{F}(N)	26.15
$B^{\mathrm{L}}(\frac{\mathrm{Nm}}{\mathrm{s}})$	9.5	$B^{\mathrm{F}}(\frac{\mathrm{Nm}}{\mathrm{s}})$	8.36
$C^{\mathrm{L}}(\frac{\mathrm{Nm}^2}{\mathrm{s}^2})$	2.05	$C^{\mathrm{F}}(\frac{\mathrm{Nm}^2}{\mathrm{s}^2})$	1.92
$a^{\mathrm{L}}_{\mathrm{br}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	-0.65	$a^{\mathrm{F}}_{\mathrm{br}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	-0.65
$a^{\mathrm{L}}_{\mathrm{dr}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	1	$a^{\mathrm{F}}_{\mathrm{dr}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	1
$P^{\mathrm{L}}_{\mathrm{br}}$(W)	$-30.82 \cdot 10^4$	$P^{\mathrm{F}}_{\mathrm{br}}$(W)	$-30.82 \cdot 10^4$
$P^{\mathrm{L}}_{\mathrm{dr}}$(W)	$30.82 \cdot 10^4$	$P^{\mathrm{F}}_{\mathrm{dr}}$(W)	$30.82 \cdot 10^4$
Robust Parameters			
Parameter	**Value**	**Parameter**	**Value**
$\underline{M}$(kg)	$4.5 \cdot 10^5$	$\overline{M}$(kg)	$5.5 \cdot 10^5$
$\underline{A}$(N)	25.11	$\overline{A}$(N)	28.24
$\underline{B}(\frac{\mathrm{Nm}}{\mathrm{s}})$	8.02	$\overline{B}(\frac{\mathrm{Nm}}{\mathrm{s}})$	10.12
$\underline{C}(\frac{\mathrm{Nm}^2}{\mathrm{s}^2})$	1.88	$\overline{C}(\frac{\mathrm{Nm}^2}{\mathrm{s}^2})$	2.11
$\underline{a}_{\mathrm{br}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	-0.70	$\overline{a}_{\mathrm{br}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	-0.59
$\underline{a}_{\mathrm{dr}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	0.92	$\overline{a}_{\mathrm{dr}}(\frac{\mathrm{m}}{\mathrm{s}^2})$	1.08
$\underline{P}_{\mathrm{br}}$(W)	$-33.28 \cdot 10^4$	$\overline{P}_{\mathrm{br}}$(W)	$-30 \cdot 10^4$
$\underline{P}_{\mathrm{dr}}$(W)	$30 \cdot 10^4$	$\overline{P}_{\mathrm{dr}}$(W)	$33.28 \cdot 10^4$
Controller Parameters			
Parameter	**Value**	**Parameter**	**Value**
H(s)	12	ΔT^{mpc}(s)	0.06
ω_1	1	ω_2	3
ω_3	6	$T^{\max}$(s)	8
Θ^s_1	2	Θ^v_1	0.225
Θ^u_1	$1 \cdot 10^{-2}$	Θ^s_2	$2 \cdot 10^{-2}$
Θ^v_2	10	Θ^u_2	$5 \cdot 10^{-2}$
Θ^s_3	1	Θ^u_3	$4 \cdot 10^{-3}$
d(m)	1000		
Channel Communication			
Parameter	**Value**	**Parameter**	**Value**
λ	0.3	$T^{\min}$(s)	0.7
p	0.98	$\overline{T}^{\min}$(s)	2
$\Delta T^{\mathrm{ch}}(s)$	1.02	p_{loss}	0.01

REFERENCES

[1] W. Y. O. Peri Smith, Arnab Majumdar, "An overview of lessons learnt from ertms implementation in european railways," *Journal of Rail Transport Planning & Management*, vol. 2, no. 4, pp. 79–87, 2012.

[2] E. T. S. Institute, "Future rail mobile communication system (frmcs); study on system architecture," tech. rep., ETSI, 2020.

[3] . Shift2Rail Joint Undertaking, "Multi-annual action plan," tech. rep., Shift2Rail, 2020.

[4] I. of railway signal engineers, "Ertms level 3: the game-changer," tech. rep., IRSE, 2017.

[5] F. Flammini, S. Marrone, R. Nardone, A. Petrillo, S. Santini, and V. Vittorini, "Towards railway virtual coupling," in *2018 IEEE International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles & International Transportation Electrification Conference (ESARS-ITEC)*, pp. 1–6, 2018.

[6] C. Di Meo, M. Di Vaio, F. Flammini, R. Nardone, S. Santini, and V. Vittorini, "Ertms/etcs virtual coupling: Proof of concept and numerical analysis," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 6, pp. 2545–2556, 2020.

[7] I. of railway signal engineers, "Ertms level 4, train convoys or virtual coupling," tech. rep., IRSE, 2016.

[8] Q. Wu, X. Ge, Q.-L. Han, and Y. Liu, "Railway virtual coupling: A survey of emerging control techniques," *IEEE Transactions on Intelligent Vehicles*, 2023.

[9] Q. Wu, X. Ge, Q.-L. Han, B. Wang, H. Wu, C. Cole, and M. Spiryagin, "Dynamics and control simulation of railway virtual coupling," *Vehicle System Dynamics*, vol. 61, no. 9, pp. 2292–2316, 2023.

[10] X. Zhang, D. Yang, W. Zhang, and J. Huang, "Optimal robust constraints-following control for rail vehicle virtual coupling," *Journal of Vibration and Control*, vol. 29, no. 5-6, pp. 1352–1365, 2023.

[11] B. Wang, D. Yang, X. Zhang, and X. Jia, "Constraint-force driven control design for rail vehicle virtual coupling," *Journal of Vibration and Control*, vol. 28, no. 5-6, pp. 551–563, 2022.

[12] J. Park, B.-H. Lee, and Y. Eun, "Virtual coupling of railway vehicles: Gap reference for merge and separation, robust control, and position measurement," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1085–1096, 2022.

[13] Y. Liu, D. Ou, Y. Yang, and D. Dong, "A method for maintaining virtually coupled states of train convoys," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 237, no. 2, pp. 243–252, 2023.

[14] G. Basile, E. Napoletano, A. Petrillo, and S. Santini, "Roadmap and challenges for reinforcement learning control in railway virtual coupling," *Discover Artificial Intelligence*, vol. 2, no. 1, p. 27, 2022.

[15] H. Wang, Q. Zhao, S. Lin, D. Cui, C. Luo, L. Zhu, X. Wang, and T. Tang, "A reinforcement learning empowered cooperative control approach for iiot-based virtually coupled train sets," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4935–4945, 2021.

[16] G. Basile, D. G. Lui, A. Petrillo, and S. Santini, "Deep deterministic policy gradient-based virtual coupling control for high-speed train convoys," in *2022 IEEE International Conference on Networking, Sensing and Control (ICNSC)*, pp. 1–6, 2022.

[17] J. Felez, Y. Kim, and F. Borrelli, "A model predictive control approach for virtual coupling in railways," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 7, pp. 2728–2739, 2019.

[18] Z. Wu, C. Gao, and T. Tang, "A virtually coupled metro train platoon control approach based on model predictive control," *IEEE Access*, vol. 9, pp. 56354–56363, 2021.

[19] W. Xiao, C. G. Cassandras, and C. Belta, *Safe Autonomy with Control Barrier Functions: Theory and Applications*. Springer, 2023.

[20] H. K. Khalil, *Control of nonlinear systems*. Prentice Hall, New York, NY, 2002.

[21] Q. Wu, M. Spiryagin, and C. Cole, "Longitudinal train dynamics: an overview," *Vehicle System Dynamics*, vol. 54, no. 12, pp. 1688–1714, 2016.

[22] M. Terlizzi, "Railway tool transition level virtual coupling, `https://www.youtube.com/watch?v=6Jr4a_wj9z8&t=1s`," aug 2024. YouTube video.

[23] P. Sopasakis, E. Fresk, and P. Patrinos, "OpEn: Code generation for embedded nonconvex optimization," in *IFAC World Congress*, (Berlin, Germany), 2020.

[24] A. Frilli, E. Meli, D. Nocciolini, L. Pugi, A. Rindi, B. Romani, M. Ceraolo, and G. Lutzemberger, "The tesys rail project: Innovative models to enhance the energy sustainability of railway systems," *International Journal of Railway Technology*, vol. 6, pp. 1–28, 12 2017.