Systematic Assessment of Cyber-physical Security of Energy Management System for Connected and Automated Electric Vehicles

Lulu Guo, Bowen Yang, Jin Ye, Hong Chen, Fangyu Li, Wenzhan Song, Liang Du, and Le Guan

***Abstract*—In this paper, a systematic assessment of cyber-physical security on the energy management system for connected and automated electric vehicles is proposed, which, to our knowledge, has not been attempted before. The generalized methodology of impact analysis of cyber-attacks is developed, including novel evaluation metrics from the perspectives of steady-state and transient performance of the energy management system and innovative index-based resilience and security criteria. Specifically, we propose a security criterion in terms of dynamic performance, comfortability, and energy, which are the most critical metrics to evaluate the performance of an electronic control unit (ECU). If an attack does not impact these metrics, it perhaps can be negligible. Based on the statistical results and the proposed evaluation metrics, the impact of cyber-attacks on ECU is analyzed comprehensively. The conclusions can serve as guidelines for attack detection, diagnosis, and countermeasures.**

***Index Terms*—cyber-physical system, cyber-security, automated and connected electric vehicles, impact analysis.**

I. Introduction

With the significant increase in the traffic, road, and environmental information enabled by vehicle-to-infrastructure/cloud/vehicle communications, the connected and automated vehicle (CAV) technology can significantly enhance the driving safety, comfort, and energy efficiency [1]. However, since a large number of embedded ECUs are integrated into networks, it also brings cyber-security concerns. As demonstrated by recent examples [2]–[4], the vehicles are vulnerable to cyber-attacks, allowing an attacker to circumvent the vehicle control systems, which would lead to severe consequences such as disabling brakes, turning off headlights, and taking over steering [4]–[6]. For example, cyber-attacks on anti-lock braking systems in [7] demonstrate that a malicious attacker can modify the feedback measurements through wheel speed sensors and cause life-threatening situations. Spoofing attacks on the global positioning system (GPS) may result in course deviation in an autonomous vehicle [8]. Some cyber-attacks through direct (by connecting with onboard diagnostics (OBD-II) port) and remote (through wireless channels like Bluetooth) access have also been reported in the literature [4], [5], [9], [10]. Furthermore, cyber-attacks in connected and automated vehicles (CAVs) through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are discussed in [11], [12] and have received increased attention in real-life scenarios in the last two years [13].

In particular, due to the connection with battery charging infrastructure, more centralized control architecture, and higher electrification, the cyber-physical security in connected and automated electric vehicles (CAEVs) is receiving much more attention compared to an internal combustion engine (ICE) vehicle. For example, the connectivity between CAEVs, charging stations and smart grid may expose the CAEVs to the cyber-attacks. Compared to conventional cyber approaches for ICE vehicles, for instance, that focus on a vehicle's entry points [5], [9], cyber-physical security monitoring can serve as a second line of protection because an abnormal system measurement is a clear indicator for potential cyber-attacks. However, cyber-physical security on CAEVs is still in its infancy. Due to the lack of security monitoring, they are prone to a wide range of cyber-attacks ranging from conventional eaves-dropping and denial of service (DOS) attacks to man-in-the-middle (MiTM) attacks that degrade the vehicle's performance [14]. The consequences can be catastrophic as they have the ability to cause physical damage to vehicles, people, and the infrastructure (the grid). There have been some preliminary works on cyber-security of battery management systems [15]–[17]. However, to our knowledge, there are no existing works for vulnerability assessment, cyber-threat detection, and threat-resilient control of core control units for CAEVs driven by multiple electric machines. This paper presents a systematic vulnerability assessment of a four-wheel drive CAEV due to a variety of cyber-attacks. In the following, the literature and challenge of vehicle cybersecurity are reviewed, and then the works and contributions are described.

A. Literature Review and Challenge of Vehicle Cybersecurity

The growing range of cyber-security risks shown above has been promoting the development of vehicle cyber-security techniques for both theoretical and application aspects. The

Manuscript received XXX, 2019; revised XXX, 2019; accepted XXX, 2020; online XXX, 2020. This work was supported in part by the National Science Foundation under Grant ECCS-1946057 and in part by Southern Company. (*Corresponding author: Jin Ye.)*

L. Guo, B. Yang, J. Ye, and W. Song are with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602, USA (e-mail: lulu.guo@uga.edu, bowen.yang@uga.edu, jin.ye@uga.edu, wsong@uga.edu).

H. Chen is with the Clean Energy Automotive Engineering Center, Tongji University, Shanghai 201804, China. She is also with the Department of Control Science and Engineering, Jilin University, Changchun 130025, China (e-mail: chenhong2019@tongji.edu.cn).

F. Li is with the Department of Electrical and Computer Engineering, Kennesaw State University, Marietta, GA 30060, USA (e-mail: fli6@kennesaw.edu).

L. Du is with the Department of Electrical and Computer Engineering, Temple University, Philadelphia, PA 19122, USA (e-mail:ldu@temple.edu).

L. Guan is with the Department of Computer Science, University of Georgia, Athens, GA 30602, USA (e-mail:leguan@uga.edu).

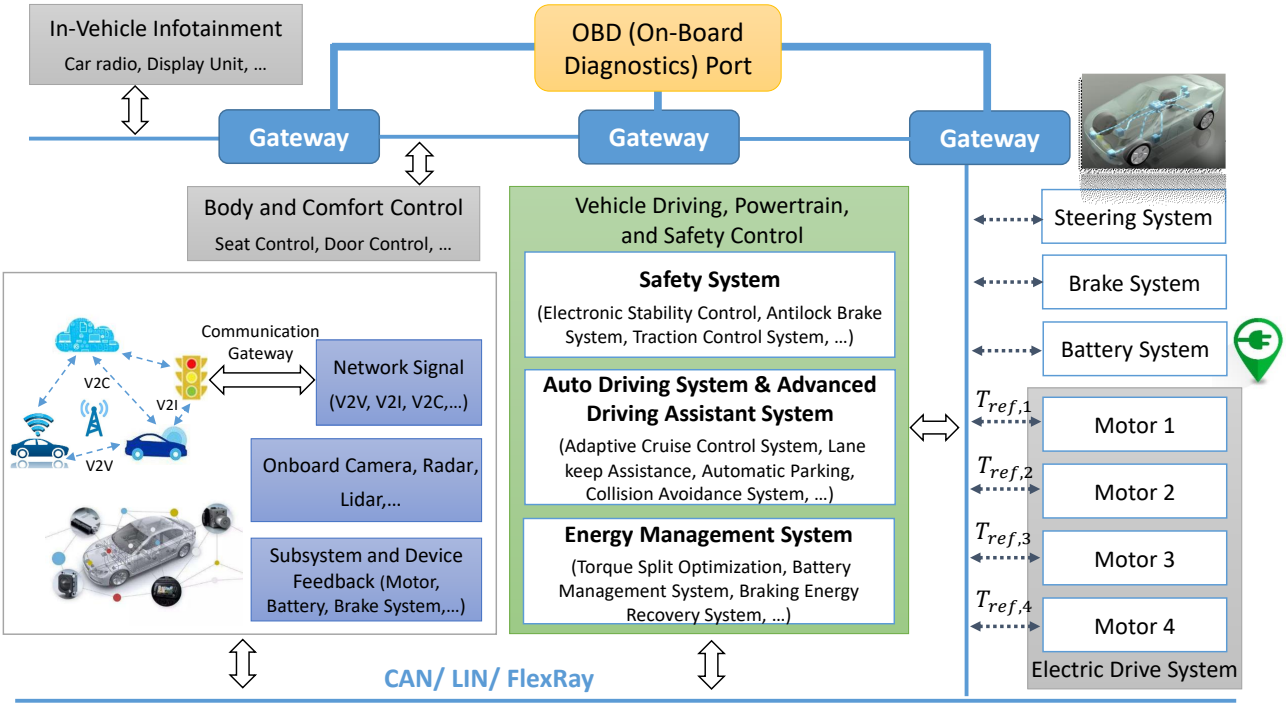

Fig. 1: System diagram of a four-wheel drive CAEV.

efforts can be categorized into two schemes. The first scheme focuses on the ability to prevent malicious attacks. For instance, throughout the vehicle development cycle, automakers can define core performance requirements of subsystems to automotive parts suppliers, and then the subsystems are designed by considering its security within the software. To prevent malicious attacks through direct contact with the OBD-II port, the communication protocol of the OBD-II is kept secret to the public. Several critical practices, like secure hardware, secure software updates, penetration testing, and code reviews, are also widely used by the automotive industry [10]. Besides, approaches concerning information security during driving, such as message authentication and encryption, the firewall between external networks and vehicle devices are also taken into consideration [10]. Although these conventional vehicle cybersecurity and information-security approaches can be used to prevent attacks, they alone cannot guarantee the security of the whole system. Therefore, cyber-physical security from the control perspective that concentrates on improving the resilience of the automotive control system to attack should be addressed, including impact analysis [18], [19], attack detection and diagnosis [3], and resilient control [2].

While these efforts provide some technical foundations, cyber-physical security challenges in CAEVs remains significant: (1) Most of the existing works are developed for connected and automated ICE vehicles rather than CAEVs. (2) Only safety-critical systems are addressed while long-term specification like efficiency performance (e.g., energy management system (EMS)) receives little attention. It is essential particularly for CAEVs because of the limited battery capacity and the 'range anxiety.' For instance, in [15], the authors provide a physics-driven approach to assess the vulnerability of EV batteries, and the results have shown that cyber-attacks can lead to faster deterioration in power capability and battery life. Furthermore, most of the existing literature is cyber-based methods and rely heavily on communication technology. There is little work on impact analysis on cyber-attacks. Although there have been some researches focusing on impact analysis of cyber threats on cyber-physical systems, e.g., electric systems and smart grids, they mainly focus on few metrics such as active (or reactive) power, system frequency, node voltage, and power angle. For example, in [20], the authors analyzed the data integrity attacks on automatic generation control loop for smart grids; in [21], the cybersecurity policies for flexible alternating current transmission devices are discussed; [22] presented the impact of integrity attacks on electric market operations; [23] used reachability methods in graph theory to assess the risks and vulnerabilities of two-area power systems. For a complicated control system in a CAEV, such as safety system (electronic stability control, antilock brake, etc.), auto driving system (adaptive cruise control system, lane keep assistance, etc.), and EMS (torque split optimization, battery management system, etc.), more detailed models and metrics should be considered to evaluate the system comprehensively. For example, the upper autonomous controller or human driver requires a fast and accurate dynamic response, reasonable power output, low torque ripple, as well as minimizing energy consumption in various drive cycles. These performances should be particularly addressed for control systems in CAEVs while these approaches for electric systems and smart grids are unfeasible. In summary, it is essential to emphasize the cyber-security challenge of the ECUs in CAEVs, and novel methodologies of vulnerability assessment should be developed.

B. Works and Contributions

In this paper, we propose a systematic vulnerability assessment of CAEVs, and the main contributions are as follows:

- A framework of impact analysis of cyber-physical security on core control systems in CAEVs, such as electronic stability control, antilock brake system that focuses on driving safety, advanced driver assistance system, and energy management system is presented.
- For the vulnerability assessment of the EMS in a CAEV, we design a model predictive control (MPC) based system that optimizes both the instantaneous driving velocity and torque allocation to reduce energy consumption, which is considered as one of the applications of EMS. Based on the system, we develop innovative index-based evaluation metrics in terms of dynamic performance, comfortability, energy, security, and resilience. If an attack does not impact these metrics, it perhaps can be negligible.
- The impact of cyber-attacks are analyzed under specific and statistical results, and the vulnerability of the vehicle to each attach type is discussed based on the evaluation metrics and security criteria. The conclusions can serve as guidelines for attack detection and countermeasures.

The paper is organized as follows. Section II provides an introduction of the system architecture and the framework of impact analysis on vulnerability. In section III, an EMS is designed by using the vehicle dynamics, motor and battery modeling, and problem formulation. Section IV describes the mathematical modeling of cyber-attacks and how these attacks can infect the system. Section V presents index-based evaluation metrics, and in section VI, simulation results and impact analysis of different cyber-attacks are presented. Finally, conclusions are given in section VII.

II. System Architecture and Framework of Impact Analysis on Vulnerability

As illustrated in Fig. 1, a four-wheel drive CAEV is controlled by a system-level ECU, which can be distributed into three parts according to their different functions: safety system, EMS, and auto or auxiliary drive system. It should be noted that besides the energy management that solely refers to energy allocation with given driving demands (e.g., torque split in vehicles with multi-power sources [24]), the 'EMS' in the paper is a broad term that includes many efficiency-motivated control systems, for instance, energy-efficient velocity profile optimization, battery management system, and braking energy recovery system, as shown in Fig. 1. These control systems are developed based on the extraneous intelligent information from V2X and onboard sensors and provide control commands to the lower systems, including steering system, electric drive system, battery, and brake system. Meanwhile, all of the signals are transmitted by high-speed Control Area Network (CAN) buses, Local Interconnect Network (LIN), and Flexray communication. In this paper, we assume that the attacker can re-flash and rewrite all of the signals on the automotive network. Then, the impact of the inaccurate sensing and perception of the terminal performance objectives can be analyzed. Generally speaking, the safety system focuses on automotive motion safety by adding extra steering or controlling the brake forces to ensure longitudinal and yaw stability. This scenario often occurs at emergency brake and steering and poor drive conditions like slippery road surface. The inputs are gathered from the chassis sensors like motor and wheel speeds, accelerate and brake pedals, steering angle, and feedback signals relating to yaw stability. Accordingly, the objectives can be defined as the vehicle yaw angle, yaw rate, and tracking error when tracking the desired path and velocity trajectory. The auto-drive system (or advanced driver assistance system) is designed from the perspective of drive strategy that can help or replace the human driver to control the car, whose signal inputs and outputs are the same with the EMS, together with the steering reference. Then the objective is the distance gap between the host and surrounding vehicles, tracking errors of the desired speed, acceleration, and its rate, tracking error of the path trajectory, and the drive decision.

Different from the above two parts, EMS is normally designed by optimizing the brake, torques, and battery to maximize the traveling range and battery health, which focuses on the longitudinal drive scenario. Because the cyber-attacks mainly affect the energy efficiency with the same dynamic features, once the attack occurs at the EMS, the driver can hardly notice this kind of abnormal drive conditions. For instance, several stealthy attacks that aim at deteriorating the power capability of battery packs are discussed in [15]. Therefore, compared to the safety and auto-drive systems, assessing the cyber-physical security of EMS is of significance. The inputs of an EMS are relevant to the energy efficiency of core devices like motor, battery and power electronics, vehicle dynamics, traffic and road information by V2X, and local information from onboard sensors. Once these signals are attacked, the vehicle would suffer from low efficiency and high-velocity tracking error. The performance metrics that need to be observed for impact analysis can be set as the overall energy consumption, powertrain efficiency, velocity tracking error under different drive cycles. Therefore, in the following sections, as a case study, we develop an EMS for CAEVs with four in-wheel motors, and then the impact of various cyber-attacks on EMS will be analyzed systematically.

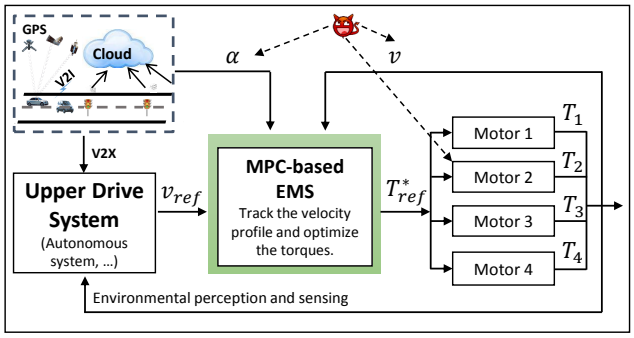

Fig. 2: System diagram of the designed MPC-based EMS.

III. Vehicle Modeling and EMS Design

The vehicle under investigation is a four-wheel drive EV, which can be modeled as a battery, electric drive system

TABLE I: Vehicle Parameters

Symbol	Description	Value [Unit]
m	Vehicle mass	1600 [kg]
ρ_a	Air density	1.205 [kg/m^3]
g	Gravitational constant	9.8 [m/s^2]
C_D	Air resistance coefficient	0.306
f	Rolling resistance coefficient	0.011
A_f	Vehicle face area	2.2 [m^2]
r_w	Dynamic tire radius	0.32 [m]
C_{bat}	nominal battery capacity	120 [Ah]

(motor and inverter), an upper drive control system (e.g. a human driver, autonomous drive system, adaptive cruise control), and a centralized controller. The speed reference is provided by the upper drive control system, and the centralized controller focuses on the speed track by optimizing the torque requirements of the four motors in consideration of battery energy consumption. By default, in the following sections of the paper, we mark this specific centralized controller as EMS. Then, each motor aims to track its torque reference given by EMS. Notice that the core performances about lateral safety like yaw stability are simplified to control constraints. Fig. 2 shows the control diagram of the EMS, which also presents the potential cyber-attack positions and signals. The vehicle parameters are shown in Table I.

A. Vehicle Dynamics

The vehicle longitudinal dynamics is generally derived by the Newton's second law of motion. Suppose the prediction horizon is discretized into N_p steps on the constant Δt-axis, then the longitudinal vehicle dynamics over the time horizon $k \in [1, N_p]$ are formulated as [25]:

$$s(k+1) = s(k) + v(k)\Delta t, \tag{1a}$$

$$v(k+1) = v(k) + \Delta t[T_{total}(k)/r_w - G(k)]/m, \tag{1b}$$

with $G(k) = F_w(k) + F_g(k) + F_r(k)$, and

$$T_{total}(k) = \sum_{i=1}^{4} T_{ref,i}(k), \tag{2}$$

where k represents the kth time instance, s and v represent the traveling distance and vehicle speed, respectively, and $s(1) = s_0$, $v(1) = v_0$; T_{total} is the total torque reference; r_w is the dynamic tire radius; F_w, F_g, and F_r denote the aerodynamic drag, grading resistance, and tire rolling resistance, respectively, and are determined by

$$F_w(k) = \frac{1}{2}\rho_a A_f C_D v^2(k), \tag{3a}$$

$$F_g(k) = mg\sin(\alpha(k)),\ F_r(k) = mgf\cos(\alpha(k)). \tag{3b}$$

Here α is the road slope, which varies with traveling distance. The definition and values that are necessary to parameterize these equations are given in Table I.

B. Motor and Battery Model

In general, the battery dynamics in most EMSs of hybrid electric vehicles and battery electric vehicles are simplified to an equivalent resistance model, for instance [26]–[28], and at the kth time instance, expressed as

$$I_{bat}(k) = \frac{V_{oc}(k) - \sqrt{V_{oc}^2(k) - 4P_{bat}(k)R_b(k)}}{2R_b(k)}. \tag{4}$$

Here P_{bat} represents the battery output or input power; I_{bat} is the battery current; V_{oc} and R_b are the battery open-circuit voltage and internal resistance, respectively, and vary with the state of charge (SOC), which can be determined by

$$SOC(k+1) = SOC(k) - \frac{I_{bat}(k)}{C_{bat}}\Delta t, \tag{5}$$

where C_{bat} denotes the nominal capacity. The battery power in the above equation is normally calculated by the mechanical power and the efficiency, as

$$P_{bat}(k) = \sum_{i=1}^{4} \omega_i(k)T_i(k)\eta_i^{\nu}(\omega_i(k), T_i(k)), \tag{6}$$

where ω_i and T_i are the speed and torque of the ith motor; η_i shows the power efficiency of the ith motor, which is normally expressed as a map developed based on experimental data; ν indicates the working state of the electric drive system: $\nu = -1$ when the electric machine works as a motor, and $\nu = 1$ when the electric machine works as a generator. Note that the term ω_i (r/min) is relevant to the vehicle speed ([m/s]) when neglecting the tire slip rate, and formulated as $\omega_i(k) = 30v(k)/(\pi r_w)$, wherein, the difference between the four wheel speeds are ignored. In addition, because the EMS aims at a higher-level torque optimization compared to the electric drive control in the motor, the real-time output torque from the ith motor $T_i(k)$ in (6) is considered as $T_i(k) \approx T_{ref,i}(k)$ for simplification.

C. Energy Management System

As one of the most promising energy Management strategies, MPC-based approaches have been extensively studied theoretically and applied in different vehicle topologies, ranging from hybrid electric vehicles to battery electric vehicles [29]–[32]. In this subsection, we develop an MPC-based EMS for vulnerability assessment of the vehicle. Built on the above modeling and discussions, the MPC-based EMS is designed by solving an optimal control problem that find the optimal $u = [T_{ref,i}(1), T_{ref,i}(2), ..., T_{ref,i}(N_p - 1)](i = 1, 2, 3, 4)$, such that

$$\min_{u\in\mathcal{U}} \mathcal{J} = \sum_{k=1}^{N_p}[\zeta_1(v(k) - v_{ref}(k))^2 + \zeta_2 V_{oc}(k)I_{bat}(k)], \tag{7}$$

subject to nonlinear and time-varying system (1)-(6), where ζ_1 and ζ_2 are weighting factors that emphasize dynamic performance and energy efficiency, respectively (in the paper, we set $\zeta_1 = 1$ and $\zeta_2 = 0.9 \times 10^{-4}$); $\mathcal{U}$ is the closed set of admissible controls for every timing k, and expressed as

$$T_{ref,\min} \le T_{ref,i} \le T_{ref,max},\ i = 1, 2, 3, 4. \tag{8}$$

Moreover, to avoid the impact of different drive torques on yaw stability, the problem is simplified by the following relationship

between these torque references:

$$T_{ref,1} = T_{ref,2},\ T_{ref,3} = T_{ref,4}. \tag{9}$$

The optimal control problem can be solved by well-developed algorithms such as sequential quadratic programming [33], [34], interior point methods [35], [36], and some fast algorithms based on Pontryagin's minimum principle like C/GMRES (Continuation and Generalized Minimum Residual) [37] and two-point boundary value problem [25]. Because the work mainly focuses on the performance rather than real-time control property, the proposed MPC problem is solved by MATLAB toolbox. Finally, the first control command $[T^*_{ref,1}(1), ..., T^*_{ref,4}(1)]$ is applied to the lower system, and at the next time instance $k+1$, a receding horizon control is realized.

TABLE II: Attack Modeling and Case Definition

Case Definition		Targets (Case)		
		α	v	T_m^{atk}
$\bar{y} = \gamma^{atk} y$	$\gamma^{atk} = 0.7$ [Type 1]	1	2	3
	$\gamma^{atk} = 1.3$ [Type 2]	4	5	6
$\bar{y} = y + \delta^{atk}$	$\delta^{atk} = \delta_1^{atk}$ [Type 3]	7	8	9
	$\delta^{atk} = \delta_2^{atk}$ [Type 4]	10	11	12
	$\delta^{atk} = \delta_3^{atk}$ [Type 5]	13	14	15
	$\delta^{atk} = \delta_4^{atk}$ [Type 6]	16	17	18
DOS Attack	$\mathcal{T}_{atk} = \mathscr{T}_{atk}$ [Type 7]	19	20	21
Replay Attack	$\bar{y} \in \mathbf{Y}$ [Type 8]	22	23	24
T_m^{atk}	$T_m^{atk} = T_{m,\min}^{atk}$ [Type 9]–Case 25			
	$T_m^{atk} = T_{m,max}^{atk}$ [Type 10]–Case 26			

TABLE III: Coordinated Attacks

Coordinated Attacks [Type 11]	Case No.
Attacks (1 & 2) or (2 & 3)	27, 28
Attacks (4 & 2) or (2 & 6)	29, 30
Attacks (10 & 11) or (11 & 12)	31, 32
Attacks (13 & 11) or (11 & 15)	33, 34

While the major goal of the EMS is to improve energy efficiency, it considers other objectives, as shown in (7). The first cost function is to track the required velocity reference from the upper drive system, which is related to dynamic performance, such as safety and drivability (velocity track error) and comfortability (torque ripple); the second one refers to energy consumption or efficiency. The torque reference of the motor is then decided via optimization both of dynamic performance (safety and comfortability) and energy. Once the energy management system is attacked such as through maliciously modifying the parameters, the torque reference of the motors that are obtained by solving the optimization problem will be maliciously modified, leading to unexpected or incorrect changes in the speed profile or the torque production of the vehicle. This could later cause performance degradation of vehicles in terms of safety, comfortability, and energy. Therefore, in the paper, our goal is to systematically analyze the impact of cyber-attacks on the overall performance of an EMS. To quantify this impact, we propose a number of innovative performance metrics, including its tracking performance, comfortability, energy, safety, and resilience.

IV. Attack Modeling

The EMS system in Fig. 2 shows the most dominating signals that might be attacked in different typical data tunnels, including the road slop α provided by the V2X communication and vehicle speed v obtained through the wheel speed sensors. For the physics-based impact analysis of the cyber-attacks on the above feedback signals, it is critical to establish the mathematical modeling of the attacks. Up to date, three categories can be summarized in most published literature: denial of service (DOS) attacks, replay attacks, and deception attacks. DOS attacks normally attempt to make the system resources unavailable, by which the corresponding signal is considered to be a constant value. Assume that the time horizon under attack is noted as $[t_{atk}, t_{atk} + \mathcal{T}_{atk}]$, then the feedback signal used by the controller is

$$\bar{y} = \begin{cases} y(t_{atk}), & \text{if } t \in [t_{atk}, t_{atk} + \mathcal{T}_{atk}] \\ y(t), & \text{else.} \end{cases} \tag{10}$$

In replay attacks, the measurements are repeated or delayed, as $\bar{y} \in \mathbf{Y}$, where $\mathbf{Y}$ is the set of past information. With regard to deception attacks, we define two common expressions, as

$$\bar{y} = y + \delta^{atk},\ \bar{y} = \gamma^{atk} y, \tag{11}$$

where $\delta^{atk} \in \Delta^{atk}$ and $\gamma^{atk} \in \Gamma^{atk}$ denote the unknown signals due to the malicious modification of the signals. Normally the extra terms are bounded by compact sets Δ^{atk} and Γ^{atk}, which are determined by the physical limits because of the hard clippings in the EMS (to ensure reasonable range of states). Notice that δ^{atk} can be white noise (δ_1^{atk}), periodic function (δ_2^{atk}), periodic pulse injection δ_3^{atk}, and constant value $\delta_4^{atk} \equiv \mathcal{C}$, wherein, δ_2^{atk} and δ_3^{atk} are expressed as

$$\delta_2^{atk} = Ae^{-t/\tau_0} \sin(2\pi f t), \tag{12}$$

$$\delta_3^{atk} = \begin{cases} K,\ k_\delta T_s \leqslant t < DT_s + k_\delta T_s \\ 0,\ DT_s + k_\delta T_s \leqslant t < (k_\delta + 1)T_s. \end{cases} \tag{13}$$

In the above equations, A, τ_0, and f represent the oscillation amplitude, decaying coefficient, and oscillation frequency, respectively; k_δ is an integer; and D, T_s, K are the duty cycle, signal period and attack amplitude, respectively.

Besides the above attacks on feedback signals, the lower electric drive system might also show misbehavior in tracking the torque requirement caused by cyber-attacks or certain physical attacks. Without loss of generality, we suppose the mth ($m \in \{1, 2, 3, 4\}$) motor is attacked and fails to track its torque reference. Then, the actual output torque is set to a random value T_m^{atk} limited by the bonds:

$$T_{m,\min}^{atk} \leq T_m^{atk} \leq T_{m,max}^{atk}, \tag{14}$$

where $T_{m,\min}^{atk}$ and $T_{m,max}^{atk}$ represent the lower and upper boundary of the misbehavior, respectively. Note that the attacked motor cannot be split from the wheel due to the physical construction, then too large misbehavior boundary

may cause severe drive safety and lateral instability problem, which can be perceived by the driver or detected by the monitor immediately. In this case, the human driver would compulsively close the autonomous system and take over the car for safety. Therefore, in the perspective of stealthy attacks on energy, $T^{atk}_{m,\min}$ and $T^{atk}_{m,max}$ are defined by $|T^{atk}_m - T^*_{ref,n}| \leq \Delta T_{lim}$, where n denotes the nth motor on the same side, for instance, $[m = 1, n = 2]$, $[m = 3, n = 4]$, ΔT_{lim} is the tolerance torque difference between the two adjacent motors, and $\Delta T_{lim} = 100$Nm.

Built on the above attack modeling, Fig. 3 shows how these attacks impact the vehicle system. To fully observe the vulnerability of the designed EMS and the whole vehicle performance, we conducted various simulations under different attacks and targets. The specific expression are shown in Table II, wherein, in δ^{atk}_2 we set $f = 2$, $\tau_0 = 0.5$, $A = 1.2$ for α, $A = 4$ for v and $A = 100$ for T^{atk}_m; in δ^{atk}_3, $D = 0.1$, $T_s = 0.2$s, $K = 1$ for α, $K = 5$ for v, and $K = 50$ for T^{atk}_m; in δ^{atk}_4, we set $\mathcal{C} = 1$ for α, $\mathcal{C} = 10$ for v, and $\mathcal{C} = 100$ for T^{atk}_m. In addition, to observe the impact of complicated attack types, in Table III we design several coordinated cyber-attacks based the individual cases, wherein $(1\ \&\ 2)$ means that the attacks Cases 1 and 2 defined in Table II are simultaneously imposed on the system. Consider that the metric values of cyber-attacks on v are much larger than others, then each of the coordinated cyber-attacks covers one threat on v, for instance, Case 2 and Case 11, which can serve as a baseline for comparison. It should be noted that all of the time horizon under attack (marked as $\mathscr{T}_{atk} = 1$s) are the same for comparison between these cases. Consider the level of modification has a significant influence on the results despite the same cyber-attack. It is expected that the higher level of modification to the signal measurements, the higher damage it would cause. Hence, for a fair comparison between the attack types and cases, all of the intensity of attacks are the same, the maximum magnitude of which is $\pm 30\%$ of the original value.

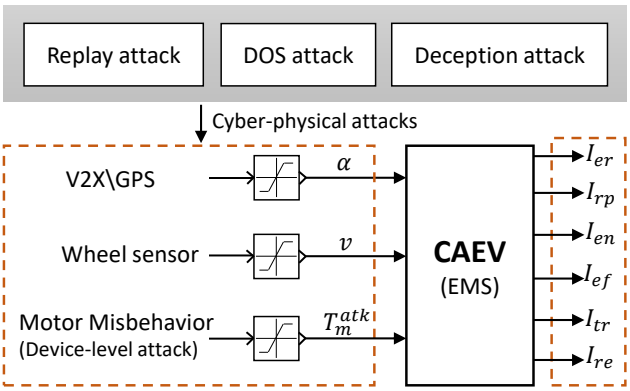

Fig. 3: Diagram of inputs, cyber-attacks and evaluation metrics.

V. Evaluation Metrics

A. Evaluation Metrics for System Performance

For vulnerability assessment of the EMS, we develop novel evaluation metrics from the perspectives of steady-state and transient performance of velocity tracking and energy optimization. All quantitative metrics are calculated by using the previous measurements, states, and control inputs in a fixed sliding window $[t_0 - \mathscr{T}_{obv}, t_0]$ (suppose the current time is t_0). Then, the indices can be developed.

1) Velocity Tracking Error and Ripple: As described above, the EMS is designed to track the velocity profile from the upper drive system. Therefore, the core indexes that indicate the system performance are the velocity tracking error and ripple, which can be defined by the maximum deviation $\mathcal{I}_{er}$ [m/s] and the integral value $\mathcal{I}_{rp}$ [m] over the sliding window:

$$\mathcal{I}_{er} = \max_{t\in[t_0-\mathscr{T}_{obv},t_0]} |v(t) - v_{ref}(t)|, \tag{15}$$

$$\mathcal{I}_{rp} = \int_{t_0-\mathscr{T}_{obv}}^{t_0} |v(t) - v_{ref}(t)|dt. \tag{16}$$

The two indexes reflect the basic dynamic performance, and large values can directly damage system function and lead to severe consequences particularly for urban scenarios.

2) Energy consumption and powertrain efficiency: Unlike the above two metrics, the next indexes focus on the energy consumption and powertrain efficiency, which are considered as stealthy impacts because they are long-term consequences, for instance, reduction in the traveling range. In mathematical expressions, the two metrics are formulated as

$$\mathcal{I}_{en} = \int_{t_0-\mathscr{T}_{obv}}^{t_0} V_{oc}(t)I_{bat}(t)dt, \tag{17}$$

$$\mathcal{I}'_{ef}(t) = \begin{cases} P_m(t)/(V_{oc}(t)I_{bat}(t)), & \text{if } P_m(t) \geq 0 \\ V_{oc}(t)I_{bat}(t)/P_m(t), & \text{else.} \end{cases} \tag{18}$$

where $\mathcal{I}_{en}$ [Wh] denotes the total energy consumption; $\mathcal{I}'_{ef}$ represents the energy efficiency; $P_m(t) = \sum_{i=1}^4 T_i(t)\omega_i(t)$ represents the total mechanical power. In addition, the average value of $\mathcal{I}'_{ef}$ over the sliding widow $[t_0 - \mathscr{T}_{obv}, t_0]$ is marked as $\mathcal{I}_{ef}$ to reflect the average energy efficiency.

3) Comfortability: Generally speaking, the smoothness of the vehicle's acceleration is one of the primary factors affecting driving comfortability, and an unsmooth profile may lead to feeling discomfort [38], which is mainly caused by the harmonic contributions of the motor torques according to the longitudinal vehicle dynamics in (1). Due to the problematic acquisition to the acceleration signal, we use the torque ripple during the time horizon $[t_0 - \mathscr{T}_{obv}, t_0]$ to derive the driving comfortability index $\mathcal{I}_{tr}$ [Nm]. Moreover, high torque ripple may cause abnormal tire slip ratio, which would also affect the driveability. Then, the metric reflecting the comfortability is given by

$$\mathcal{I}_{tr} = \frac{1}{\mathscr{T}_{obv}} \sum_{i=1}^{4} \int_{t_0-\mathscr{T}_{obv}}^{t_0} |T_i(t) - T_{i,ave}|dt, \tag{19}$$

where $T_{i,ave}$ represents the average torque value of ith motor.

B. Evaluation Metrics for System Security and Resilience

Then, we consider the security and resilience of the system and propose innovative index-based criteria.

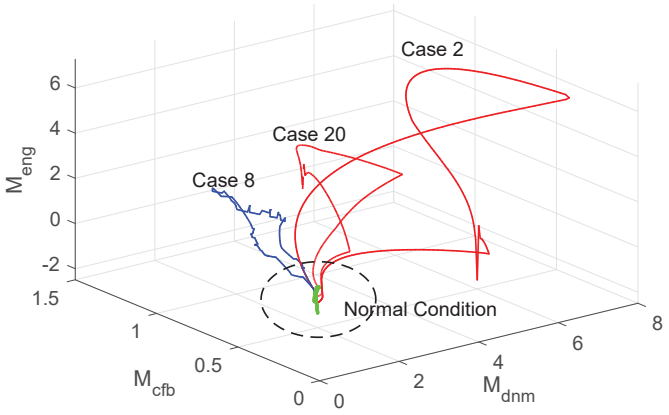

Fig. 4: Index-based phase portrait.

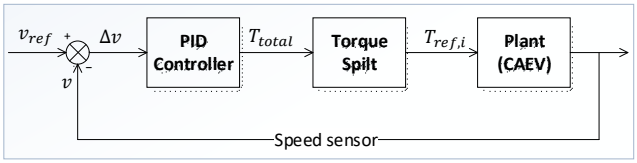

Fig. 5: Diagram of the PID-rule-based controller, where $K_p = 1.2$, $K_i = 0.05$, $K_d = 0.01$.

1) Security of the System: Different from the theoretical concept of stability and robustness against uncertainties or disturbances, the security denotes whether the damage caused by the malicious behaviors or attacks are acceptable in terms of system performance and requirements. Then, the index-based boundaries are defined as

Proposition 1. *Based on the defined evaluation metrics $\mathcal{I}_\kappa$ ($\kappa = \{er, rp, en, ef, tr\}$), if a boundary $\mathbf{B}^\kappa$ could be found, which has the following properties: 1) the boundary $\mathbf{B}^\kappa$ is finite; 2) if $\mathcal{I}_\kappa \in \mathbf{B}^\kappa$, the damage caused by the attacks are acceptable. Then, the system is secure.*

It should be noted that the boundary is generally defined from the perspective of physical significance, and it is heuristic conclusion through massive simulations and experiments. To specifically derive this boundary, we reformulate the metrics $\mathcal{I}_\kappa$ from three aspects: dynamic performance, comfortability, and energy, as $\mathcal{M}_{dnm} = p_1\mathcal{I}_{er} + p_2\mathcal{I}_{rp} \geq 0$, $\mathcal{M}_{cfb} = p_3\mathcal{I}_{tr} \geq 0$ and $\mathcal{M}_{eng} = p_4\mathcal{I}_{en} - p_5\mathcal{I}_{ef}$, where $p_j \geq 0$ $(j = 1, 2, 3, 4, 5)$ is the weighting factor to match different physical meanings and units. Then, we can obtain a 3-D $(\mathcal{M}_{dnm} - \mathcal{M}_{cfb} - \mathcal{M}_{eng})$ phase portrait of the system over the sliding widow $[t_0 - \mathcal{T}_{obv}, t_0]$, in which the boundary is defined as a tetrahedron $\mathbf{B_1}$ or part of a spheroid $\mathbf{B_2}$ limited by $\mathcal{M}_{dnm,max}$, $\mathcal{M}_{cfb,max}$ and $\mathcal{M}_{eng,max}$. Then, the security can be defined qualitatively, as follows: Suppose a boundary $\hat{\mathbf{B}} \in \mathbb{R}^3$ determined by $\mathcal{M}_{dnm,max}$, $\mathcal{M}_{cfb,max}$ and $\mathcal{M}_{eng,max}$ is given; if the operating point belongs to $\hat{\mathbf{B}}$, then the system is considered secure and inversely insecure. As shown in Fig. 4, when in normal conditions, the region of operating points is near the origin. As the scale of the attack increases, the operating points spread out gradually until beyond the defined boundary. Therefore, the index can reflect the security of the system, which can also be one of the criteria in cyber-threat detection.

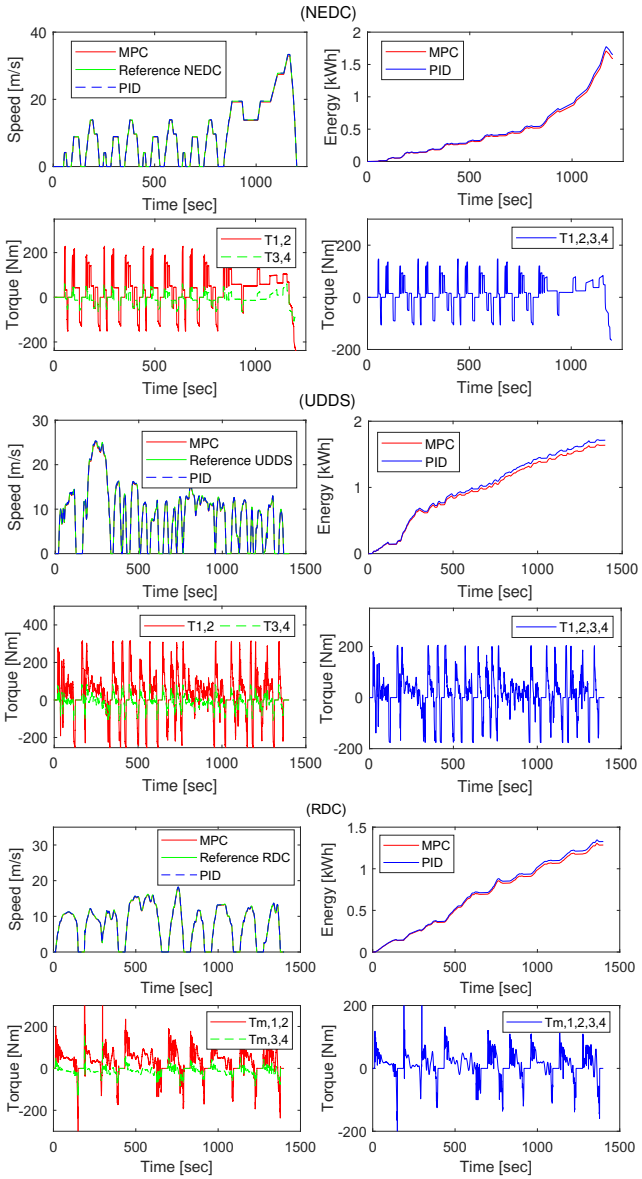

Fig. 6: Results in NEDC, UDDS, and RDC using the designed MPC and PID controllers.

Further, for quantitative analysis of the system security, based on the above boundary $\hat{\mathbf{B}} \in \mathbb{R}^3$, we define the metric reflecting the security level of the system under different cyber-physical threats and attack targets, as follows:

Proposition 2. *Assume the security boundary $\hat{\mathbf{B}} \in \mathbb{R}^3$ is defined as a tetrahedron in the three dimensional coordinate system $(\mathcal{M}_{dnm} - \mathcal{M}_{cfb} - \mathcal{M}_{eng})$, whose vertexes are $(\mathcal{M}_{dnm,max}, 0, 0)$, $(0, \mathcal{M}_{cfb,max}, 0)$, $(0, 0, \mathcal{M}_{eng,max})$, and the coordinate origin (0,0,0). At the current time t_0, the operating point in the three dimensional coordinate system is $(\mathcal{M}_{dnm}(t_0), \mathcal{M}_{cfb}(t_0), \mathcal{M}_{eng}(t_0))$. Then, the metric that quantitatively reflects the system security can be defined as*

$$\mathcal{I}_{se} = \frac{\mathcal{M}_{dnm}(t_0)\mathcal{M}_{cfb}(t_0)\mathcal{M}_{eng}(t_0)}{\mathcal{M}_{dnm,max}\mathcal{M}_{cfb,max}\mathcal{M}_{eng,max}}, \tag{20}$$

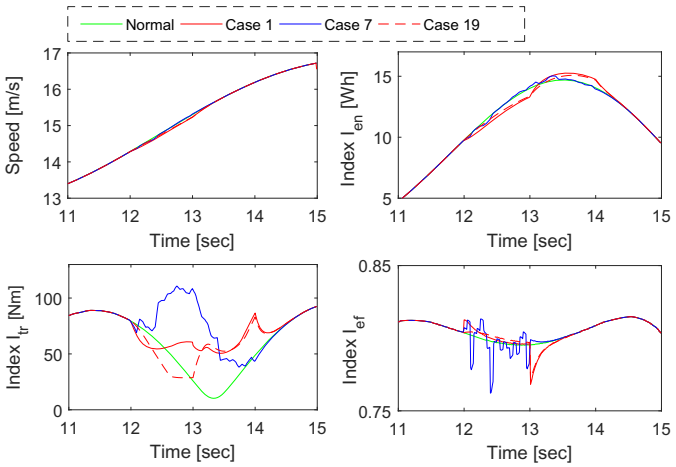

Fig. 7: Results of system dynamics and indexes in Cases 1, 7 and 19 ($[t_{atk}, t_{atk}+\mathcal{T}_{atk}]=[12,13]$s, $\mathcal{T}_{obv}=1$s).

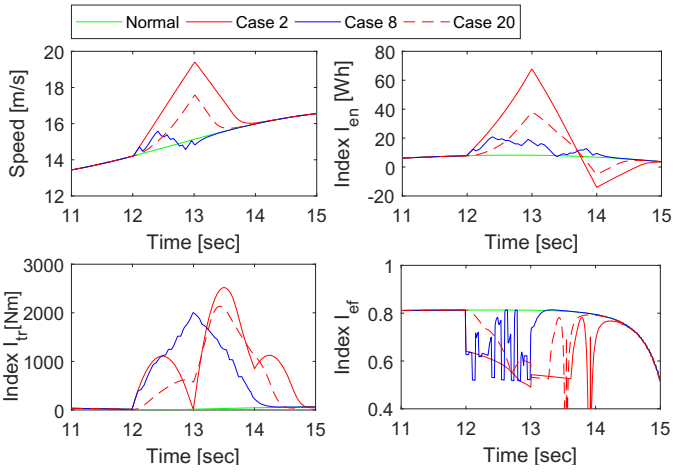

Fig. 8: Results of system dynamics and indexes in Cases 2, 8 and 20 ($[t_{atk}, t_{atk}+\mathcal{T}_{atk}]=[12,13]$s, $\mathcal{T}_{obv}=1$s).

which represents the security factor of the system.

According to the above definition, higher value of the $\mathcal{I}_{se}$ means greater damage to the system.

2) Resilience of the System: The resilience of the system reflects the ability of recovery after suffering from malicious attacks. Therefore, following the definition of security, another boundary in the 3-D phase portrait is defined as

Proposition 3. *If a boundary* $\mathbf{B}^{res}$ *could be found, which has the following properties: 1) the boundary* $\mathbf{B}^{res}$ *is finite; 2) if the operating point* $\{\mathcal{M}_{dnm}, \mathcal{M}_{cfb}, \mathcal{M}_{eng}\}$ *belongs to* $\mathbf{B}^{res}$*, the system can restore to its reasonable condition when the attack is withdrawn. Then, the system is resilient.*

When in real-life applications, not only the ability to recover but also the recovery time that reflects the transient performance needs to be concerned. Hence, the recovery time T^{σ}_{res} ($\sigma=\{\mathcal{M}_{dnm}, \mathcal{M}_{cfb}, \mathcal{M}_{eng}\}$, which indicates how soon the σth metric restores to its normal condition after the attack is withdrawn. Then, the index reflecting the resilience of the

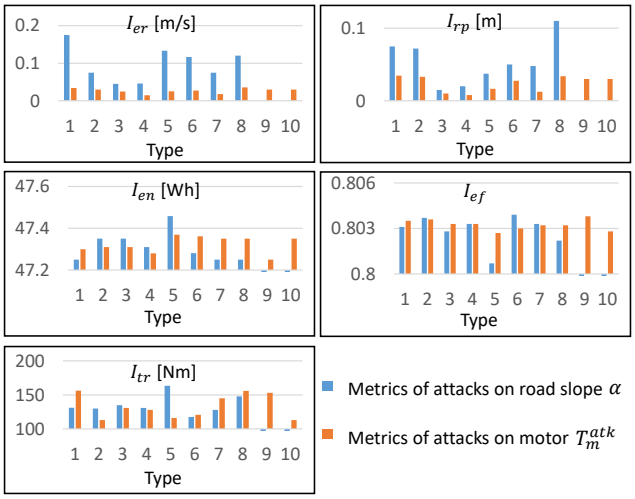

Fig. 9: Statistical graph of attacks on α and T_m^{atk}.

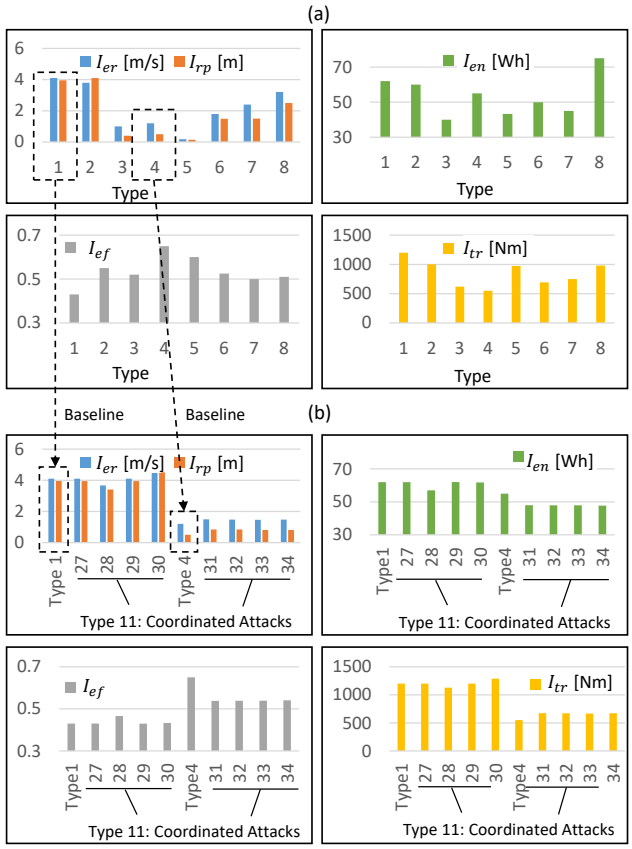

Fig. 10: Statistical graph of attacks on v in Tables II and III.

system is defined as the average form

$$\mathcal{I}_{re}=(T_{res}^{\mathcal{M}_{dnm}}+T_{res}^{\mathcal{M}_{cfb}}+T_{res}^{\mathcal{M}_{eng}})/3. \tag{21}$$

VI. Simulation and Cyber-attack Impact Analysis

In this section, we assess the vulnerabilities of CAEVs with the designed EMS due to cyber-attacks. The CAEV is built in MATLAB Simulink, and the attacks are defined in Table II. Three main works are presented here: 1) as the basis of vulnerability assessment, the MPC-based EMS is

evaluated by observing the dynamic performance without cyber-attacks, for instance, its stability, velocity tracking ability, and energy efficiency; 2) based on the defined evaluation metrics, innovative index-based resilience, and security criteria are proposed, which can be used for cyber-attack detection; 3) then the impact of the cyber-attacks are analyzed under specific and statistical results, which can serve as guidelines for attack detection and countermeasures.

A. Evaluation of the Control System

To evaluate the performance of the designed EMS, new European drive cycle (NEDC) and urban dynamometer drive schedule (UDDS) are chosen as the velocity references. Besides, we use one real inner-city cycle for the simulation, as shown in Fig. 6, which is extracted from a human driver in an arbitrary city route and marked as RDC (real drive cycle). A PID-rule-based controller is designed to compare with the normal performance of the MPC-based EMS. As shown in Fig. 5, in the PID-rule-based control system, the desired velocity reference is tracked by using a PID controller, as

$$a(t) = K_p \Delta v(t) + K_i \int_0^t \Delta v(\tau) d\tau + K_d \frac{d}{dt} \Delta v(t), \quad (22)$$

$$T_{total}(t) = a(t) T_{total,max}, \quad (23)$$

where $a(t)$ represents the acceleration pedal position of the vehicle; $T_{total,max}$ is the maximum total torque at the current time; $\Delta v(t) = v_{ref}(t) - v(t)$, where $v_{ref}(t)$ and $v(t)$ are the desired and actual speeds, respectively. Then, the torque reference of each motor is given by

$$T_{ref,i}(t) = T_{total}(t)/4, \ i = 1, 2, 3, 4. \quad (24)$$

The simulation results for comparison are presented in Fig. 6, including the velocity, torque, and energy consumption, from which we can see that both the two controllers can track the desired velocity profiles well. The energy consumption of the MPC in the chosen three drive cycles (NEDC, UDDS, and RDC) are 1.592kWh, 1.637kWh, and 1.285kWh, respectively; the corresponding values of the PID-based controller are 1.656kWh, 1.713kWh, and 1.327kWh, respectively. The primary benefit of the MPC-based EMS is lower energy consumption, and compared to the PID-rule-based controller, the energy efficiency is improved by 3.2-4.5%.

B. Impact Analysis of Cyber-attacks

1) Observation of Specific Cases: For the sake of detailed discussion and observation, the results of Cases 1, 7, 19 are shown in Fig. 7, and Cases 2, 8, 20 are given in Fig. 8. From these results, we can see that sensor data integrity attacks can heavily damage the system, and all of the metrics can reflect the impact. Although the system can recover after the attacks are withdrawn, the recovery time is also considerably long when considering real-life damage to physical devices. On the one hand, by comparing the results with the same attack, it is obvious that the speed v is of vital importance than the others, for both dynamic and energy performances. Therefore, when designing an EMS, much attention should be paid to ensure an accurate speed signal. The impact of attacks to α mainly focuses on energy efficiency and torque ripple of the motors, and the influence is much less significant. The reason lies in the value limitation (normally, the road slope is less than 5° for most roads). On the other hand, through the comparisons between different attacks on the same signal, we can see that the system dynamics vary with attack types.

TABLE IV: Results of $\mathcal{I}_{se}$ Under Different Attacks

Attack Type	Results of $\mathcal{I}_{se}$		
	α	v	T_m^{atk}
1	2.2843	1151.4375	0.7512
2	1.3341	864.0625	0.4964
3	0.5658	57.3531	0.3198
4	0.6030	87.6563	0.2051
5	1.9555	20.9938	0.3414
6	1.3629	200.0494	0.4657
7	1.0959	228.5156	0.3088
8	2.3711	807.9750	0.7571
9	–	–	0.6388
10	–	–	0.4736

TABLE V: Results of $\mathcal{I}_{se}$ Under Coordinated Attacks

Attack Type 11	Results of $\mathcal{I}_{se}$
(1 & 2) or (2 & 3)	1150.3355, 849.1247
(4 & 2) or (2 & 6)	1151.3954, 1380.3271
(10 & 11) or (11 & 12)	130.8404, 129.3212
(13 & 11) or (11 & 15)	125.9727, 126.8828

2) Statistical Results and Impact Analysis: Based on the massive results, the statistical graphs are given in Figs. 9-11. Consider the fact that the time horizon under attacks is $[t_{atk}, t_{atk} + \mathcal{T}_{atk}] = [12, 13]$s and the system can recover to its normal conditions within two seconds, as shown in Figs. 7-8. Then, we set the time horizon $[t_0 - \mathscr{T}_{obv}, t_0]$ as $t_0 = 15$s, $\mathscr{T}_{obv} = 4$s, which needs to cover the whole time horizon of attack and system recovery. It should be noted that if the chosen time horizon is wider, e.g., $t_0 = 20$s and $\mathscr{T}_{obv} = 10$s, then the proportion of normal conditions is larger, which would attenuate the impacts of cyber-attacks for those metrics defined in integrated form due to the larger base value, for instance, $\mathcal{I}_{rp}$, $\mathcal{I}_{en}$ and $\mathcal{I}_{tr}$. Then, the metrics $\mathcal{I}_{er,rp,en,ef,tr,re}(t_0)$ are used as the indexes to reflect the overall performance. Because the metric values of the attacks on v are much larger than others, the results of attacks on α and T_m^{atk} are given in Fig. 9, and other cases are shown in Fig. 10, including the singular and coordinated attacks on v. The recovery time of cyber-attacks are given in Fig. 11, and the results of the metric reflecting system security ($\mathcal{I}_{se}$) are summarized in Tables IV and V, wherein, we set $\mathcal{M}_{dnm,max} = 0.5$, $\mathcal{M}_{cfb,max} = 1.4$, $\mathcal{M}_{eng,max} = 1.6$, $p_1 = p_2 = 5$, $p_3 = 0.01$, $p_4 = 0.05$, and $p_5 = 1$. The normal results (with no cyber-attacks) are as follows: $I_{er}^{nom} \approx 0$, $I_{rp}^{nom} = 0.0016$m, $I_{en}^{nom} = 47.22$Wh, $I_{ef}^{nom} = 0.8042$, and $I_{tr}^{nom} = 107.83$Nm.

By comparing the results of these metrics with the normal

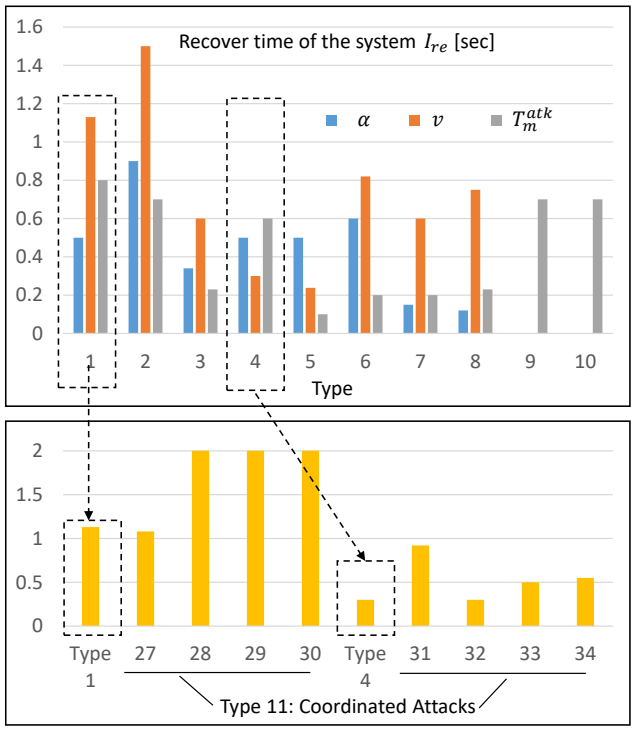

Fig. 11: Recovery time of different attacks.

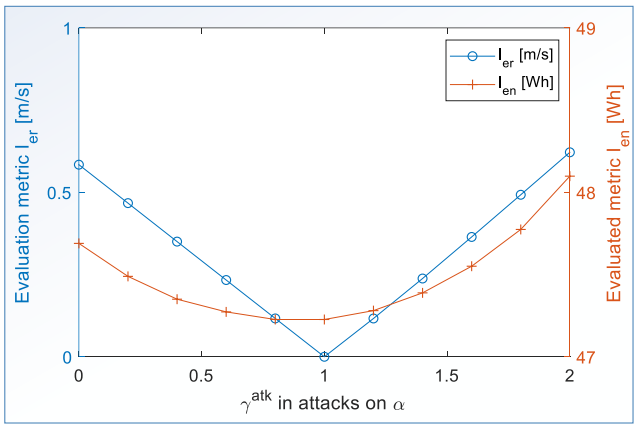

Fig. 12: Results under different parameters in Case 1.

values, we can conclude that they adequately reflect the performance variation to the cyber-attacks, which can be used to develop a cyber-threat detector. From the results in Table IV, we can see that the security factor significantly varies with the attack types and targets. Specifically, the results of most cyber-attacks on T_m^{atk} are less than 1, which means that the vulnerability of the system to cyber-threats on T_m^{atk} is lower, and in these cases, the system is considered secure. Unlike the attack target T_m^{atk}, in the attacks on the road slope α, there are several scenarios that the operating points are out of the security boundary with different severity. Moreover, as illustrated in Figs. 9-11, the evaluation metrics of the cyber-attacks on v are much higher than the security value, which indicates that the impact of cyber-attacks on speed is much more significant than other signals, regardless of the types. Therefore, while

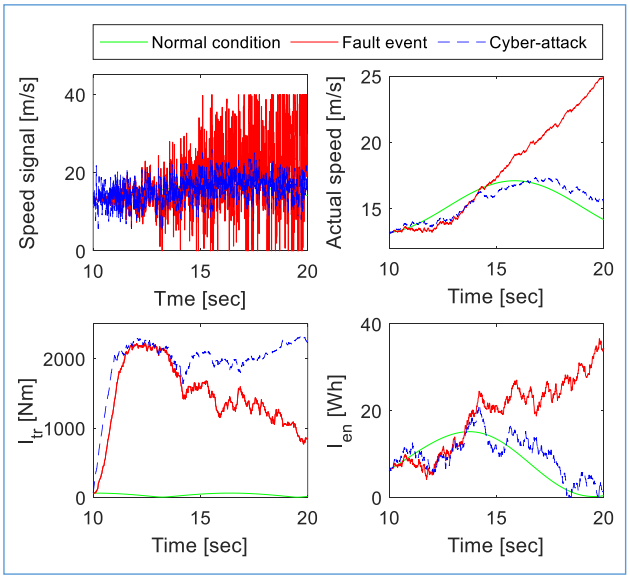

Fig. 13: Differentiation between malicious cyber-attack and fault event.

developing detection and high-assurance controller, the speed is the most important signal to be considered.

Moreover, in the results of Fig. 10, under the same attack intensity, types 1, 2, and 8 show larger damage to the system, especially on velocity tracking error and energy consumption. In other types of attack, although one threat cannot significantly influence all performance indexes, it may cause dramatic degradation of a specific metric, for instance, Type 4 and Type 5 in Fig. 10(a). Besides the attacks on v, the results in Fig. 9 illustrate that the difference of the impact between α and T_m^{atk} is mainly shown in velocity tracking error and energy consumption, and then these two metrics can serve as crucial monitor indexes for cyber-threat diagnosis. According to the recovery time in Fig. 11, we can see that once the threat is withdrawn, the system can recover to its normal condition within two seconds. Also, types 1 and 2 may result in longer recovery time, which corresponds to the results of other metrics. It's also worth pointing out that although in the results reported in the graphs the impact of α and T_m^{atk} is much lower than v, it does not imply that these cyber-attacks have little influence on the EMS because these attacks are designed under the same intensity (limited to $\pm 30\%$). Once this boundary is enlarged, the impact would be noticeable, as shown in Fig. 12.

Considering the coordinated attacks on v shown in Fig. 10(b), Fig. 11, and Table V, it is not always the case that coordinated attacks may cause more extensive damage to the system. For example, in Case 28, both the speed signal v and motor torque T_m^{atk} are reduced by 30%, and then, by using the erroneous v, the EMS tends to provide larger torque to the powertrain. If the attacker also reduces the motor torque, the impact of the incorrect speed measurement is attenuated, as is shown in the results of Case 28 and Type 1 in Fig. 10(b). It implies that if the attacker has no prior knowledge of the system, an arbitrary coordinated attack may not realize the expected results, which would need more resources for attacking. Moreover, we find

it difficult to distinguish between the coordinated attacks and singular sensor attack on v because of similar results, which means that the cyber-attacks on α or T_m^{atk} may be masked by the speed attack, which can lead to more significant results.

In order to observe the cost of developing and deploying such attacks, especially for those coordinated attack scenarios, we reformulate the evaluation metrics stated above, as

$$\mathcal{I}'_p = \frac{\mathcal{I}_p}{\mathcal{K}_{cost}}, \tag{25}$$

where, $p = \{er, rp, en, ef, tr, re\}$, and $\mathcal{K}_{cost}$ is derived by

$$\mathcal{K}_{cost} = \delta_\alpha N_{level,\alpha} + \delta_v N_{level,v} + \delta_t N_{level,T_m^{atk}} \tag{26}$$

to reflect the difficulty of deploying the attacks. In the above equation, $\delta_{\{\cdot\}}$ is the state of the specific signal measurement, and $\delta_{\{\cdot\}} = 0$ and $\delta_{\{\cdot\}} = 1$ respectively represent normal and attacked conditions; $N_{level,\{\cdot\}}$ denotes the access level of attacks on the corresponding target. In the first level, a malicious attacker only needs to obtain access to the network between the infrastructure and the host vehicle, which requires the minimum effort. For the cyber-attacks considered in this paper, it is apparent that the attacks on α are such a circumstance, and we set $N_{level,\alpha} = 1$. Subsequently, in the second level, the attackers need to gain communication access on the internal controller area network to modify the sensor measurements, which needs more effort and resources compared to the first level. For the attacks on v, as an illustrative example, we set $N_{level,v} = 2$. In the third level, the cyber-attacks can damage the lower electric drive system, which may be elaborated by the highly-skilled attackers to cause misbehavior in tracking the torque requirement, e.g., the attacks on T_m^{atk}, and we set $N_{level,T_m^{atk}} = 3$. Then, more targets or higher levels of the cyber-attacks will make larger $\mathcal{K}_{cost}$, leading to a lower relative impact to the system. By using this reformulated metrics, we can easily conclude that although the coordinated attacks defined in Table III may cause more extensive damage to the system, e.g., Cases 29 and 30, when considering the cost factor in (25), these coordinated attacks are not desirable for the attackers.

3) Differentiation between malicious cyber-attacks and fault events: To differentiate between malicious cyber-attacks and fault events, we consider one of the early-stage failures of v. The fault event is emulated by using white noise with increasing power, considering the continuous physical process. For comparison, the cyber-attacks are designed under white noise with a fixed power. Without loss of generality, we suppose the start time of both the failure and cyber-attacks are $t_{failure,0} = t_{atk,0} = 10$s, and then the results are shown in Fig. 13. We can observe that the metrics of both the cyber-attack and the fault event on speed sensors are significantly increased once the threats are activated. In the early state of the fault event (before 14s), it is indeed that distinguishing between the cyber-attack and a fault event is quite a challenge due to the same expressions of threats But if we assume that there is always a transitional stage before complete failure, then compared to an instantaneous and fixed-energy cyber-attack, the rate of change of an evaluation metric would be lower, which may be used to make a difference between the two threats. In the later stage of the fault event, with the increasing power of the white noise, the tracking error increases quickly, which eventually leads to instability of the system. Although the actual speed and the energy efficiency in the fault event are much larger than the cyber-attack, the metric that reflects torque ripple is lower, which indicates that in the case of distinguishing between the cyber-attack and fault event, this metric may be unfeasible.

VII. Conclusion

This paper provided a general guidance for vulnerability assessment of core control systems for CAEVs, with which the impact of cyber-attacks on different critical systems and signals, as well as the interaction between these subsystems can be analyzed comprehensively. As a case study, we have developed an MPC-based EMS for CAEVs with four in-wheel motors and presented a systematic vulnerability assessment on cyber-threats. Then, innovative index-based evaluation metrics in terms of dynamic performance, comfortability, energy, and system security and resilience are established to evaluate the critical performance. Following, we give a few remarks on practical applications and future works. In the paper, we have demonstrated that an attacker can degenerate the overall performance of the vehicle through data integrity attacks, e.g., higher velocity tracking error and torque ripples, lower energy efficiency, and even instability. For the developed MPC-based EMS, the results have shown that all of the evaluation metrics, including the proposed indices of recovery time and resilience, can reflect the impact of various cyber-attacks. Then, by using these metrics, one can develop data-based or model-based detection and diagnosis approaches in practical applications. Also, the statistical results can help to identify the critical signals, so that they pay more attention to it when designing a system. For example, use encryption, observer, multiple signals, or interaction with other control systems that can provide an estimated value, to improve the reliability of the critical feedback measurements.

It should be noted that besides the detailed impact analysis of cyber-threats on EMS, this paper provides a general framework of vulnerability assessment of a control system in the ECU (from the control perspective). For other systems, e.g., safety system and advanced driver assistance systems in Fig. 1, one needs to conduct a detailed impact analysis by using the potential signal inputs and objectives stated in Section II (under a variety of cyber-physical attacks according to specific demands). Particularly, for those learning-based systems, e.g., a pedestrian detection system in deep learning approaches in rough weather, although vulnerability assessment can be addressed by designing various cyber-physical attacks and evaluation metrics as described in the paper, because of the unique algorithm structure compared to traditional control methodologies, further research is needed.

References

[1] J. K. Naufal, J. B. Camargo, L. F. Vismari, J. R. de Almeida, C. Molina, R. I. R. González, R. Inam, and E. Fersman, "A^2 CPS: A vehicle-centric safety conceptual framework for autonomous transport systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 6, pp. 1925–1939, 2017.

[2] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Control Systems Magazine*, vol. 37, no. 2, pp. 66–81, 2017.

[3] P. Guo, H. Kim, L. Guan, M. Zhu, and P. Liu, "Vcids: Collaborative intrusion detection of sensor and actuator attacks on connected vehicles," in *2017 International Conference on Security and Privacy in Communication Systems*. Springer, 2017, pp. 377–396.

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *2011 USENIX Security Symposium*. San Francisco, 2011, pp. 447–462.

[6] C. Valasek and C. Miller, "Adventures in automotive networks and control units," *Technical White Paper, IOActive*, 2014.

[7] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *2013 International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2013, pp. 55–72.

[8] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *2011 ACM Symposium on Computer and communications security*. ACM, 2011, pp. 75–86.

[9] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 10–21, 2014.

[10] D. Wise, "Vehicle cybersecurity dot and industry have efforts under way, but dot needs to define its role in responding to a real-world attack," *Gao Reports. US Government Accountability Office*, 2016.

[11] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk assessment for cooperative automated driving," in *2016 ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, 2016, pp. 47–58.

[12] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transport reviews*, vol. 39, no. 1, pp. 103–128, 2019.

[13] "Cyber cttacks in connected cars: what tesla did differently to win. https://blog.appknox.com/cyber-attacks-in-connected-cars/."

[14] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of internet of electric vehicles," in *2018 IEEE Conference on Wireless Communications and Networking*. IEEE, 2018, pp. 1–6.

[15] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," *arXiv preprint arXiv:1711.04822*, 2017.

[16] S. Chakraborty, M. A. Al Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu, "Automotive cyber–physical systems: A tutorial introduction," *IEEE Design & Test*, vol. 33, no. 4, pp. 92–108, 2016.

[17] R. Hull, "Nissan disables leaf electric car app after revelation that hackers can switch on the heater to drain the battery," *Thisismoney, Feb*, vol. 26, 2016.

[18] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (cacc)," in *2017 IEEE Conference on Vehicular Networking*. IEEE, 2017, pp. 45–52.

[19] P. Johannessen, F. Törner, and J. Torin, "Actuator based hazard analysis for safety critical systems," in *2004 International Conference on Computer Safety, Reliability, and Security*. Springer, 2004, pp. 130–141.

[20] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on scada control system," in *IEEE PES general meeting*. IEEE, 2010, pp. 1–6.

[21] L. R. Phillips, B. Tejani, J. Margulies, J. L. Hills, B. T. Richardson, M. J. Baca, and L. Weiland, "Analysis of operations and cyber security policies for a system of cooperating flexible alternating current transmission system (facts) devices." Sandia National Laboratories, Tech. Rep., 2005.

[22] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[23] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proceedings of the 2010 American control conference*. IEEE, 2010, pp. 962–967.

[24] H. Wang, Y. Huang, A. Khajepour, H. He, and D. Cao, "A novel energy management for hybrid off-road vehicles without future driving cycles as a priori," *Energy*, vol. 133, pp. 929–940, 2017.

[25] H. Chen, L. Guo, H. Ding, Y. Li, and B. Gao, "Real-time predictive cruise control for eco-driving taking into account traffic constraints," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 8, pp. 2858–2868, 2019.

[26] L. Tang, G. Rizzoni, and S. Onori, "Energy management strategy for HEVs including battery life optimization," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 3, pp. 211–222, 2015.

[27] L. Guo, B. Gao, Q. Liu, J. Tang, and H. Chen, "On-line optimal control of the gearshift command for multispeed electric vehicles," *IEEE/ASME Transactions on Mechatronics*, vol. 22, no. 4, pp. 1519–1530, 2017.

[28] H. Borhan, A. Vahidi, A. M. Phillips, M. L. Kuang, I. V. Kolmanovsky, and S. Di Cairano, "MPC-based energy management of a power-split hybrid electric vehicle," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 3, pp. 593–603, 2012.

[29] Z. Jia, J. Jiang, H. Lin, and L. Cheng, "A real-time MPC-based energy management of hybrid energy storage system in urban rail vehicles," *Energy Procedia*, vol. 152, pp. 526–531, 2018.

[30] S. East and M. Cannon, "An admm algorithm for MPC-based energy management in hybrid electric vehicles with nonlinear losses," in *2018 IEEE Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 2641–2646.

[31] L. Qiu, L. Qian, H. Zomorodi, and P. Pisu, "Global optimal energy management control strategies for connected four-wheel-drive hybrid electric vehicles," *IET Intelligent Transport Systems*, vol. 11, no. 5, pp. 264–272, 2017.

[32] M. Wahba and S. Brennan, "MPC-based energy management of a parallel hybrid electric vehicle using terrain information," in *ASME 2015 Dynamic Systems and Control Conference*. American Society of Mechanical Engineers Digital Collection, 2015.

[33] S.-P. Han, "Superlinearly convergent variable metric algorithms for general nonlinear programming problems," *Mathematical Programming*, vol. 11, no. 1, pp. 263–282, 1976.

[34] M. J. Powell, "Algorithms for nonlinear constraints that use lagrangian functions," *Mathematical programming*, vol. 14, no. 1, pp. 224–248, 1978.

[35] N. Karmarkar, "A new polynomial-time algorithm for linear programming," in *1984 ACM Symposium on Theory of computing*. ACM, 1984, pp. 302–311.

[36] S. Mehrotra, "On the implementation of a primal-dual interior point method," *SIAM Journal on optimization*, vol. 2, no. 4, pp. 575–601, 1992.

[37] T. Ohtsuka, "A continuation/gmres method for fast computation of nonlinear receding horizon control," *Automatica*, vol. 40, no. 4, pp. 563–574, 2004.

[38] L. Castellazzi, A. Tonoli, N. Amati, A. Piu, and E. Galliera, "Vehicle driveability: dynamic analysis of powertrain system components," SAE Technical Paper, Tech. Rep., 2016.