ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY
A MAGYAR TUDOMÁNY ÜNNEPE
Az MTA programsorozata
Engineering Symposium at Bánki
(ESB 2024)

Limitations of ISO26262 in Addressing Nonlinear Dynamics in Highly Automated Driving Systems

[1]Samir Rasulov, [2]Péter Bakucz, [3]Judit Lukács

[1] Obuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary, rasulov.samir@phd.uni-obuda.hu
[2] Obuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Budapest, Hungary, bakucz.peter@bgk.uni-obuda.hu
[3] Obuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Budapest, Hungary, lukacs.judit@bgk.uni-obuda.hu

Abstract

Ensuring the functional safety of highly automated driving (HAD) systems introduces challenges that extend beyond the scope of existing standards. ISO26262, the leading framework for automotive electrical and electronic (E/E) systems, rests on assumptions of determinism, linearity, and modular fault containment. However, HAD systems inherently exhibit emergent phenomena, bifurcations, sensitivity to initial conditions, nonlinear dynamics, and temporal instability. These characteristics undermine the predictability and modular reasoning that ISO26262 depends on, rendering traditional safety analysis methods such as FMEA, FTA, and V&V insufficient. This study explores the fundamental limitations of ISO26262 when applied to nonlinear dynamic systems. By drawing on concepts from low-dimensional attractor analysis and chaos theory, it demonstrates how small perturbations, even in the absence of component failures, can lead to significant and unpredictable system-level risks. The findings highlight an urgent need to rethink safety frameworks to better address the dynamic and emergent behavior of HAD systems.

Keywords: functional safety, ISO26262, highly automated driving, nonlinear systems

1. Introduction

Ensuring the functional safety of highly autonomous driving (HAD) systems has become apparent as a crucial concern as vehicle autonomy increases. The ISO26262 standard, which offers a thorough framework for recognizing, evaluating, and reducing functional safety risks in electrical and electronic (E/E) systems, is widely used by the automotive industry [1]. Nonetheless, the underlying assumptions upon which ISO26262 is based assume deterministic behavior, linearity, and modularity of the system [2]. The intricate, adaptive, and frequently chaotic dynamics that define highly automated driving systems defy these presumptions [3].

Because of feedback-driven decision-making, multi-sensor fusion, and real-time environmental interactions, nonlinear behavior is characteristic of HAD systems [4]. These systems may exhibit emergent behaviors that cannot be linked to failures of individual components and are sensitive to beginning conditions [5]. Such dynamics are complicated for traditional hazard analysis techniques like FMEA (Failure Mode and Effects Analysis), FARA (Hazard Analysis and Risk Assessment), and FTA (Fault Tree Analysis), which are essential to ISO26262 Parts 3, 4, and 9. They rely on

cause-and-effect relationships and make the assumption that the architecture of the system can anticipate and contain safety-critical faults [6], [7], [8].

Moreover, the supporting procedures of ISO26262 (Part 8) impose further limitations. Verification and validation (V&V) activities assume the ability to specify expected system behavior under all operating conditions [5], [9]. This assumption is contradicted by nonlinear systems, where even minor adjustments can result in wildly divergent outcomes. Because previous successful performance under stable conditions does not imply safety in dynamic or uncommon event situations, the ”proven-in-use” of the standard defense is also undermined. Even tool qualifying procedures are ineffective when applied to models that attempt to simulate chaotic scenarios [2].

The constraints of existing methods for assessing the reliability of HAD systems are investigated in this study, with an emphasis on the suitability of ISO26262 for nonlinear dynamics. Low-dimensional attractors and chaos theory concepts are utilized to better comprehend the complex, emergent behaviors found in these systems, behaviors that current functional safety requirements are not well-suited to handle, rather than to suggest a completely new safety framework. In this paper, we contend that the ability of ISO26262 to handle the safety issues of nonlinear systems is fundamentally constrained. There is an urgent need to identify the shortcomings of conventional safety frameworks and to critically reevaluate the definition, testing, and assurance of functional safety as the automobile industry moves toward more autonomous vehicles [2], [3], [5].

2. Functional Safety Overview

Functional safety in the automotive industry refers to the absence of unnecessary risk resulting from hazards caused by malfunctioning electrical and electronic (E/E) systems [1]. Road vehicle functional safety is governed by ISO26262, which is considered a global standard. It provides a framework for managing safety-related risks at every phase of the life cycle of an automotive system, from design to decommissioning [10].

The standard is founded on a top-down, risk-based paradigm. The process begins with the Hazard Analysis and Risk Assessment (HARA) in Part 3, which determines potential risks and allocates Automobile Safety Integrity Levels (ASILs) based on severity, controllability, and exposure [11]. Higher ASILs necessitate stricter safety precautions [6]. Following HARA, system-level development is covered in Part 4, where safety objectives are divided into functional and technical safety criteria and dispersed among system components [7].

The phases of hardware and software development are covered in Parts 5 and 6, focusing on traceability, modularity, and adherence to established safety standards [12], [13]. Throughout the development process, verification and validation (V&V) procedures are used to ensure that all components of the system work as intended and that the system as a whole satisfies its safety goals [9], [10].

Safety analyses like Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) are covered in Part 9. These methods use fault propagation models and causal chains to pinpoint critical failure points and assess how errors could jeopardize safety objectives [8].

Tool qualification, change management, configuration management, and proven-in-use arguments are examples of supporting procedures in Part 8. These govern design evolution, guarantee tool safety, and permit reuse of previously verified components based on performance data from the past [9].

Although ISO26262 offers a comprehensive framework for controlling functional safety in traditional automotive systems, it is mainly based on the assumptions of component-level fault isolation, linearity, and predictability. These assumptions do not apply to nonlinear systems, particularly those dominated by chaotic dynamics, as the following section will demonstrate. In

these systems, minor perturbations can result in substantial behavioral alterations at the system level that are difficult to predict or evaluate using ISO26262 approaches.

3. Nonlinear Dynamics in Automated Driving

Environmental conditions for highly autonomous driving (HAD) systems are dynamic, uncertain, and frequently unstable. A characteristic of complex systems, HAD systems usually display nonlinear dynamics, unlike conventional automotive systems that can be represented using linear equations and deterministic reactions. The formation of attractors and bifurcations in system behavior, nonlinear feedback loops, and sensitivity to beginning circumstances are some manifestations of these [4], [14].

A system that does not have a direct proportionality between its input and output is said to be nonlinear. In these kinds of systems, minor adjustments to the input or starting circumstances can have radically different results; this is commonly known as the ”butterfly effect.” As Trogatz explains, if Lorenz started his simulations from two slightly different initial conditions, the resulting behaviors would be totally different [15]. It is very challenging to forecast future system states using deterministic simulations or conventional linear models because of this sensitivity. Bifurcations, or abrupt shifts in system behavior brought on by slow parameter changes, also make stability analysis and safety validation more difficult [16].

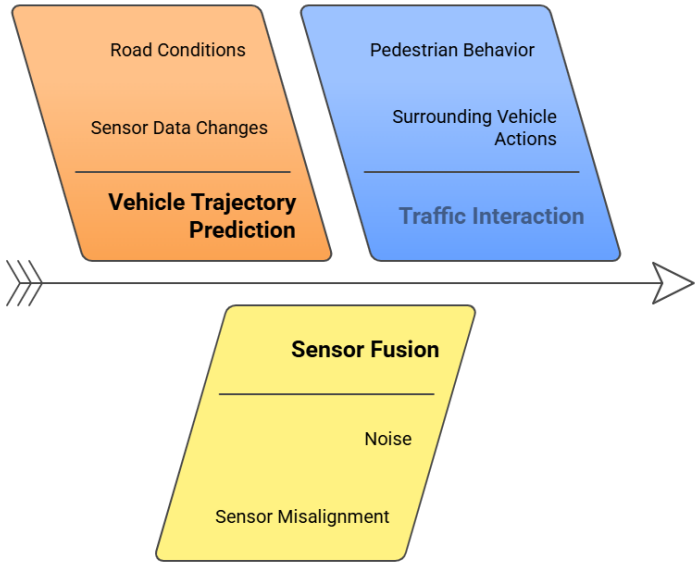

Figure 1. Challenging nonlinear features in HAD applications based on [2], [4], and [17]

Specifically, we employ low-dimensional attractor reconstruction, a method from chaos theory, to analyze these phenomena. We can determine the fundamental structure of the behavior of the system, whether it is chaotic, periodic, or stable, by simulating its dynamics in a reduced-dimensional phase space. These characteristics enable us to describe the system based on the overall change in its state over time rather than on specific flaws.

This viewpoint highlights a key drawback in the use of ISO 26262: its incapacity to identify or measure dependability in systems where faults are emergent characteristics resulting from the internal dynamics of the system rather than isolated malfunctions. The traditional presumptions of

traceability, modularity, and predictability that support contemporary functional safety approaches are called into question by such behavior.

4. Why Functional Safety Fails Here

The foundation of ISO26262 is the idea that system behavior is traceable, quantifiable, and predictable. By spotting possible flaws, evaluating their risk, and putting mitigation plans based on predictable results into action, safety is guaranteed in this situation. However, in nonlinear systems, like highly automated driving, where minor deviations can have disproportionately enormous and unforeseen repercussions, this linear and modular approach proves to be fundamentally insufficient.

Under these circumstances, several provisions of ISO26262 become problematic:

4.1 Sensitivity to Initial Conditions

Nonlinear systems, particularly chaotic processes, are extremely sensitive to early conditions, which means even slight variations in initial states can result in wildly disparate system behaviors. This characteristic explicitly contradicts the predictability assumption incorporated into ISO26262.

For example, according to ISO26262-3:2018 (Clause 6.4.3), dangers must be categorized according to their severity, exposure, and controllability — that is, if the impact of a hazard can be reliably foreseen [6]. Similarly, repeatable test results are assumed by software unit and integration tests (ISO26262-6:2018, Clauses 9.4 and 10.4) [13].

However, in chaotic systems, this assumption collapses. Tiny deviations in system state or environmental inputs can lead to fundamentally different operational trajectories, even when starting from nearly identical initial conditions [15, 16]. As a consequence, deterministic testing and verification strategies are not sufficient to ensure comprehensive safety.

Additionally, tools must generate consistent outputs in accordance with Clause 11.4.5 in Part 8 (Tool Qualification) [9]. In contrast, in a nonlinear dynamic context, even minor arithmetic rounding errors during computation can cause significant divergences in system behavior over time [15, 16]. This renders model-based simulations and verification procedures highly unreliable for certifying the safety of systems dominated by chaotic dynamics, highlighting a critical gap in current functional safety standards.

4.2 Emergent Behavior

Emergent behavior occurs in nonlinear systems, particularly those that involve feedback and adaptation. That means the overall system displays traits or results that cannot be attributed to any one component; instead, these behaviors are the consequence of interactions between components, internal states, and environmental inputs, producing frequent, unexpected, and challenging outcomes using conventional safety engineering techniques [5].

This presents a significant obstacle for ISO26262, which is based on the concepts of fault containment and modular decomposition. A good illustration can be Clause 6.4.1 of ISO26262-4:2018, which specifies that technical safety criteria must be assigned to specific system components. This method makes the assumption that the system will be safe overall if every module satisfies its safety requirements [7].

Nevertheless, even when each component precisely complies with its designated safety standards when operating in isolation, the complex interactions among components in emergent dynamic systems might result in harmful behaviors at the system level. These undesirable behaviors result from the unforeseen ways that components affect one another in dynamic, real-world situations rather than from the failure of a single module. The system may enter dangerous states

that were not anticipated during modular verification or identified by component-level validation alone due to a combination of small timing errors, feedback loops, or environmental triggers that are harmless at the component level. Therefore, in the presence of nonlinear emergent events, the modular decomposition approach stated by ISO26262 is no longer sufficient to ensure overall system safety [5].

Comparably, Clause 6.4.4.4 of Part 4 mandates that the system design be analyzed using methods such as FMEA and FTA. These techniques are predicated on the idea that failures have a known root cause and spread linearly and traceably [7]. This restriction also applies to Part 3, namely the Concept Phase. Clause 6.4.2.2 of ISO26262-3:2018 specifies dangers regarding the malfunctioning behavior of the items, suggesting a clear correlation between system hazard and component failure [6]. Nonetheless, in reality of nonlinearity, emergent risks could arise without any component failure at all, rendering them undetectable to the analysis framework of the standard.

The idea that isolated components may be validated to ensure safety is simply not valid in emergent behavior-governed systems. Rather, the entire system needs to be examined, including the erratic interactions and nonlinear feedback loops that only show up when the system is fully integrated or operating.

4.3 Bifurcations and Sudden Behavioral Shifts

Bifurcations, which are sudden and frequently dramatic changes in system behavior brought on by tiny, continuous alterations in input or internal parameters, are one of the characteristics that distinguish nonlinear systems [15]. Such bifurcations may result in sudden changes in operational modes, decision rules, or stability regimes when driving in a highly automated environment [18].

Faults are not always the cause of these immediate shifts. For example, the automatic system may transition from a standard lane-following mode to a defensive or emergency maneuver if any slight alteration is experienced in the estimated trajectory of a close vehicle. An abrupt fallback behavior, such as an emergency stop, might also result from a little delay in data fusion or a modest decline in sensor confidence. In each instance, bifurcation is characterized by a significant change in behavior while the system maintains its functionality [4].

ISO26262 fails to handle such a type of behavior. The foundation of the standard is the idea that system degradation occurs in a traceable and gentle manner with well-defined safe states and transitions. Clause 6.4.4.2 of ISO26262-4:2018, for example, highlights the necessity of defining safe states and the transitions between them [7]. However, the change from one behavior to another is not always linear or predictable in systems that are prone to bifurcation. It is possible for a system to switch between operating regimes, and established fault models or safety objectives are not able to address these transitions [19].

Additionally, software integration testing is covered in ISO26262-6:2018, Clause 10.4, which states the assumption that interactions between software units may be confirmed under known and controlled circumstances [13]. However, bifurcations frequently only happen when several subsystems engage in dynamic, real-time interaction. These transitions may be entirely missed in testing conducted under nominal or static settings [15, 18].

In addition, the idea of backup techniques as outlined in ISO26262 is compromised by bifurcation occurrences. According to the standard, fallback measures must be planned, intentional reactions to known flaws or dangers [7]. The fallback option may be unnecessary or dangerous in a nonlinear system, though, as a bifurcation could lead the system to enter a state that was never experienced during design or testing [15, 18].

4.4 Temporal and Rate Instability

In addition to exhibiting unexpected state changes, nonlinear systems can show unpredictable rates of change. The alteration of speed and timing of transitions between behaviors might not be anticipated either, so it is not just the end behavior of the system that becomes unknown. Even in the absence of external defects or component failures, phenomena like abrupt lane changes, rapid accelerations, rapid decelerations, or rapid loss of control can happen. The intrinsic nonlinear dynamics of the system and its sensitivity to minor perturbations lead directly to these erratic timing patterns [5, 20].

ISO26262-4:2018 (Clause 6.4.4.2) emphasizes the notion of safe states, where the timing constraints are also laid out for switching between operational modes. It makes the assumption that these changes take place within predictable time frames. As a result, it becomes possible to create safe backup plans like safe shutdowns or controlled emergency brakes [7]. These presumptions can be readily broken in highly automated driving (HAD) systems with chaotic and nonlinear dynamics. The system may progress toward a hazardous state more quickly than the safety measures were intended to handle due to slight actuation delays, sensing mistakes, or external disturbances [21, 22].

According to Strogatz (1994), nonlinear systems frequently show fast-slow alternations, in which abrupt regime transitions can result from comparatively minor parameter changes, rendering temporal evolution extremely non-uniform. A delay of even a single fraction of a second can cause a chaotic system to surpass a critical threshold, from which recovery becomes either exceedingly challenging or impossible. The reason is that the event happens too rapidly or unexpectedly, safety features that rely on preset reaction timings, like time-to-collision estimates, evasive maneuvers, or system degradations, might not react effectively in this situation [15].

Thus, temporal and rate instability present a fundamental challenge to the ISO26262 architecture. The assumption that system behaviors can be planned and validated with respect to predictable timing collapses in the face of nonlinear dynamics. This not only jeopardizes the effectiveness of hazard identification and risk mitigation strategies but also calls for new frameworks that can account for variable rates of change and emergent temporal patterns in HAD systems.

4.5 Summary of ISO26262 Limitations in Nonlinear Contexts

A comprehensive review of the structural assumptions included in specific ISO26262 clauses is given in Table 1, which also shows how these assumptions fail when they are applied to dynamic, nonlinear systems like highly automated driving. The analogy draws attention to the fundamental discrepancy between emergent, unexpected behavior found in nonlinear systems and deterministic safety logic.

Table 1. Limitations of ISO26262 Clauses in Nonlinear Systems

ISO26262 Clause	Purpose / Assumption	Why It Fails in Nonlinear Systems
Part 3 – 6.4.3	Classify hazards by severity, exposure, and controllability	Assumes hazard effects can be foreseen, but small perturbations lead to unpredictable outcomes (chaos).
Part 4 – 6.4.1	Assign technical safety requirements to system components	Assumes modular decomposition, but emergent behavior arises from component interactions.
Part 4 – 6.4.4.2	Define safe states and their timed transitions	Assumes transitions occur within a predictable time, but rate instability breaks timing assumptions.
Part 4 – 6.4.4.4	Require system analysis using FMEA and FTA	Assumes linear fault propagation, but nonlinear systems fail without component-level faults.
Part 6 – 9.4, 10.4	Ensure deterministic software unit and integration testing	Assumes repeatable results, but system state diverges under identical inputs due to sensitivity to initial conditions.
Part 8 – 11.4.5	Require tool qualification for consistent output	Assumes model-based tools are stable, but minor numerical errors lead to divergent behavior in chaotic models.
Part 9 – Safety Analysis	Identify and mitigate fault propagation via FTA/FMEA	Based on cause-effect chains, nonlinear interactions bypass these fault pathways.

5. Summary

The structural limits of ISO 26262 as they relate to highly automated driving (HAD) systems with nonlinear dynamics were investigated in this study. Although ISO26262 offers a strict safety framework for traditional automotive systems, it is predicated on the ideas of modular fault containment, linear behavior, and determinism. These presumptions become problematic in nonlinear systems, when characteristics including temporal instability, bifurcations, emergent dynamics, and sensitivity to initial conditions compromise component-level safety assurances and predictability.

The study demonstrated how conventional methods like fault tree analysis (FTA), failure mode and effects analysis (FMEA), and deterministic software validation become unreliable when faced with chaotic interactions and system-level transitions that are impossible to capture through linear decomposition by analyzing particular clauses and safety procedures within ISO26262.

The findings underscore the urgent need to re-evaluate existing functional safety standards in light of the dynamic nature of HAD systems. Future safety frameworks must incorporate principles from chaos theory and nonlinear systems analysis to better account for emergent risks and unpredictable behavior that arise not from failures, but from complexity itself.

6. Future Work

The creation of supplementary safety evaluation techniques that go beyond linear cause-effect reasoning will be necessary to address the shortcomings of ISO26262 in the setting of nonlinear systems. Future studies should investigate how nonlinear dynamics tools like bifurcation theory and low-dimensional attractor analysis may be included in safety assurance pipelines. The detection of emergent dangers, latent instability, and erratic changes in system behavior may be aided by these tools.

Another interesting option is developing simulation and verification environments that explicitly mimic chaotic interactions and sensitivity to initial conditions. Beyond the presumptions of finite fault propagation, such platforms would enable safety engineers to examine system behavior across various dynamic inputs and failure scenarios.

Collaboration across disciplines will also be crucial. Both system design and the development of safety standards require consideration of insights from real-time systems engineering, complexity science, and control theory. The development of next-generation safety frameworks that are more suited to handle the dynamic reality of fully automated driving will be aided by this change.

Acknowledgments

Supported by the 2024-2.1.1 University Research Scholarship Program of the Ministry for Culture and Innovation from the Source of the National Research, Development and Innovation Fund.

7. References

[1] International Organization for Standardization, “ISO 26262-1:2018 – Road Vehicles – Functional Safety – Part 1: Vocabulary,” 2018, ISO Standard. [Online]. Available: https://www.iso.org/standard/68383.html

[2] Burton, S., Gauerhof, L., & Heinzemann, C. (2017). Making the case for safety of machine learning in highly automated driving. In Computer Safety, Reliability, and Security: SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings 36 (pp. 5-16). Springer International Publishing.

[3] Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In Proceedings of the 47th Design Automation Conference (pp. 731-736). https://doi.org/10.1145/1837274.1837461

[4] Paden, B., Čáp, M., Yong, S. Z., Yershov, D., & Frazzoli, E. (2016). A survey of motion planning and control techniques for self-driving urban vehicles. IEEE Transactions on intelligent vehicles, 1(1), 33-55. https://doi.org/10.1109/TIV.2016.2578706

[5] Leveson, N. G. (2016). Engineering a safer world: Systems thinking applied to safety (p. 560). The MIT Press.

[6] International Organization for Standardization, “ISO 26262-3:2018 – Road Vehicles – Functional Safety – Part 3: Concept Phase,” 2018, iSO Standard. [Online]. Available: https://www.iso.org/standard/68385.html

[7] International Organization for Standardization, “ISO 26262-4:2018 – Road Vehicles – Functional Safety – Part 4: Product Development at the System Level,” 2018, iSO Standard. [Online]. Available: https://www.iso.org/standard/68386.html

[8] International Organization for Standardization, "ISO 26262-9:2018 – Road Vehicles – Functional Safety – Part 9: ASIL-Oriented and Safety-Oriented Analysis," 2018, ISO Standard. [Online]. Available: https://www.iso.org/standard/68391.html

[9] International Organization for Standardization, "ISO 26262-8:2018 – Road Vehicles – Functional Safety – Part 8: Supporting Processes," 2018, ISO Standard. [Online]. Available: https://www.iso.org/standard/68390.html

[10] Macher, G., Höller, A., Sporer, H., Armengaud, E., & Kreiner, C. (2015). A combined safety-hazards and security-threat analysis method for automotive systems. In Computer Safety, Reliability, and Security: SAFECOMP 2015 Workshops, ASSURE, DECSoS. ISSE, ReSA4CI, and SASSUR, Delft, The Netherlands, September 22, 2015, Proceedings 34 (pp. 237-250). Springer International Publishing.
https://doi.org/10.1007/978-3-319-24249-1_21

[11] Khastgir, S., Birrell, S., Dhadyalla, G., Sivencrona, H., & Jennings, P. (2017). Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems. Safety Science, 99, 166-177. https://doi.org/10.1016/j.ssci.2017.03.024

[12] International Organization for Standardization, "ISO 26262-5:2018 – Road Vehicles – Functional Safety – Part 5: Product Development at the Hardware Level," 2018, ISO Standard. [Online]. Available: https://www.iso.org/standard/68387.html

[13] International Organization for Standardization, "ISO 26262-6:2018 – Road Vehicles – Functional Safety – Part 6: Product Development at the Software Level," 2018, ISO Standard. [Online]. Available: https://www.iso.org/standard/68388.html

[14] Defoort, M., Floquet, T., Kokosy, A., & Perruquetti, W. (2008). Sliding-mode formation control for cooperative autonomous mobile robots. IEEE Transactions on Industrial Electronics, 55(11), 3944-3953.
https://doi.org/10.1109/TIE.2008.2002717

[15] Strogatz, S. H. (2024). Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. Chapman and Hall/CRC.

[16] Abarbanel, H. D., Brown, R., Sidorowich, J. J., & Tsimring, L. S. (1993). The analysis of observed chaotic data in physical systems. Reviews of modern physics, 65(4), 1331. https://doi.org/10.1103/RevModPhys.65.1331

[17] Rhinehart, N., McAllister, R., Kitani, K., & Levine, S. (2019). Precog: Prediction conditioned on goals in visual multi-agent settings. In Proceedings of the IEEE/CVF international conference on computer vision (pp. 2821-2830).

[18] Ott, E., Chaos in Dynamical Systems, 2nd ed. Cambridge, UK: Cambridge University Press, 2002.

[19] Koopman, P., & Wagner, M. (2017). Autonomous vehicle safety: An interdisciplinary challenge. IEEE Intelligent Transportation Systems Magazine, 9(1), 90-96. https://doi.org/10.1109/MITS.2016.2583491

[20] Slotine, J. J. E., & Li, W. (1991). Applied nonlinear control (Vol. 199, No. 1, p. 705). Englewood Cliffs, NJ: Prentice hall.

[21] Khalil, H. K., & Grizzle, J. W. (2002). Nonlinear systems (Vol. 3). Upper Saddle River, NJ: Prentice hall.

[22] Thrun, S. (2002). Probabilistic robotics. Communications of the ACM, 45(3), 52-57. https://doi.org/10.1145/504729.504754