Trustworthy Cyber-Physical Systems Design for Autonomous Vehicles

By Dr. Seungjin Oh

Professor of Electrical Engineering, Pohang University of Science and Technology (POSTECH), South Korea

1. Introduction

Additionally, FORCES captures strengths possessed by current state-of-the-art learning/AI techniques along with traditional control-efforts driven design. The first core contribution of this work is in presenting an approach for code generation-time fusion of both the learning- and control-based techniques into a combined loop, for the computation. This occurs in the context of a verified hybrid controller over the haPN model and the approach remains generally applicable. Consequently, the application of these advances results in production of much more flexible and robust implementations.

We leverage FORCES, a formal, model-based design technique for computation over such systems. FORCES extends the symbolic simulation capabilities of hybrid automaton Petri-Net (haPN) models for cyber-physical systems for incorporation of arbitrary mathematics-rooted computation models. As these are symbolic, hybrid solutions for pure mathematical computations, like polynomials, result, but these remain functional over a hybrid automaton modeling the associated underlying domain physics.

This work develops new diverse integrated techniques for creating trustworthy cyber-physical systems, with autonomous vehicles as the key driver. More specifically, the need to develop trustworthy approaches for data-driven cyber-physical systems arises as the world becomes increasingly harnessing AI and machine learning technologies to make real-time decisions.

Autonomous and connected vehicles are set to have a transformational impact on our transportation system, and with it potentially all sectors of the economy and society. These new systems, however, are being given a tremendous responsibility. The current traffic system is regulated and, in the main, governs different vehicles under a common framework.

However, the autonomous feature means substantial offloading to software and embedded system technology.

1.1. Background and Significance

Resilient autonomous driving requires a Safe-CPS that displays the best possible behavior in the presence of unpredictable influences that are usually referred to as uncertainties. Safe behavior requires multi-objective attention not only to safety concerning minimum and maximum bound constraints. The notion of safety often includes additional notions like estimation of incorrect sensor behavior, handling of sensor failure, and of all human impact on the scenario of use that is beyond the ordinary. There exist additional characteristics for the actions, most notably the idea of legality that requires the implicit derivation from the policy that derives decisions from sensor observations of which the underlying laws are obeyed.

Cyber-Physical Systems (CPS) are connecting computing devices, artifacts, and humans to the physical world. This is often realized by sensing physical observations through their communication to digital controllers. The controllers evaluate these observations and take decisions that are typically embodied by specific actions in the physical world, thus closing the loop between perception and action in the sense of intelligent behavior. The perception-decisions-action loop of a CPS is governed by decisions that are taken automatically in a digitally controlled cyber part so that the physical part can take action. This physical action becomes valuable in a concrete scenario of use, like autonomous driving in the scenario of a self-driving car. Benefits are user convenience because the vehicle can drive without human input, and additional safety if the automotive task that would otherwise be performed by a human driver is unsafe.

1.2. Research Objectives

However, safety integrity levels focus on threats to cyber-physical systems and mechanisms involved in protecting the physical systems from the threats. The objectives will mainly focus on subsystems that protect the vehicle systems from cyber threats. Successful completion of the proposed objectives will result in a safe and reliable highway autonomous vehicle system that can run in different weather conditions. The vehicle can plan and calculate its path and communicate with the surrounding environmental and vehicle system functionalities.

This proposed research study attempts to define a set of research objectives for the development of an SAE level 4 autonomous vehicle. The objectives are divided into levels that span both the research and prototyping stages. The proposed architecture uses a control system and a safety integrity level. The control system uses the vehicle systems, including control theory, route tracking, and approach.

1.3. Scope and Limitations

The project research provides artifacts for back-end (maintenance and training) and user-in-the-loop effects that enhance the understanding of an unsafe state or unsafe system condition. This phrase "unsafe system condition" is not specifically defined in the existing literature. Our research is aimed to bring this topic on the table and to align it with the existing work on other trustworthy CPS topics, since what our research provides an artifact and use data on so that we can mitigate the unsafe system condition or have awareness of the conditions.

Trustworthy issues for a CPS include security, safety, privacy, reliability, resiliency, and human learning and are ongoing conversations in the research and policy realms. We aim to constrain the vision of building trustworthy, secure by design CPS architectures and lower level subsystems for manual and autonomous vehicles. Our focus in this research is specifically on embedded software concerns in preliminary aircraft systems and autonomous UAS.

Context of frontloading is the usage of system development cycle knowledge available during architectural design to build functional properties into the system design. This research studies the traceability of safety and security goals to architectural elements and system architecture, where these architectural elements have implications to vehicle dynamics, software functions, and safety and mission critical subsystems. These safety and mission critical subsystems are treated as separate systems, and then mechanisms for identifying, mapping, and representing the safety and security goals of these systems are addressed in a mechanism to create more stringent frontloading opportunity.

The main focus of this research is on influencing an architectural pre-decision making mechanism for trustworthy CPS properties. This mechanism is also known as frontloading of system properties. The architectural structure of a system impacts various aspects of the system such as life cycle costs, size, functional requirements, system reliability, and safety.

Frontloading of various architectural properties can impact system design complexity, system components, early-life failures, and system safety and reliability.

2. Fundamentals of Cyber-Physical Systems

Each physical system is subject to a variety of environmental conditions, called disturbances. The elevator cab of a building system, for example, is exposed to multiple disturbances including wind, temperature, and vibration, all besides humans. Taken together, the ABCs form an event sequence, and the event sequence further defines the regional and provincial system states. Only when a set of ABC events is reported occurring over time, would the elevator system transition from one regional state to another, and this report of times between channel event reports with transition rule form the context. The passage of time then states "near", "during", or "after". These definitions lend themselves to a great degree of formalization by leveraging constructs like event, regional, provincial, state, and context logic, first introduced by Shehory et al. in 1997. With these terms formally defined, we can now quantify the physical and cyber systems and deduce relationships among their subsystems.

A premier challenge preventing making CPSs trustworthy today is that the design of both cyber and physical systems has its roots in silos with distinct methodologies engineered for properties important to each discipline only. Consider, for example, that the cyber (or software) community might understand how to model and enforce timing, founded from its roots in real-time systems, but may never need to do so, at least to the level of accuracy of physical degrees. To resolve this issue, we begin by formalizing the definitions of cyber and physical. Cyber refers to those systems which are engineered to control external physical actions, such as activation of actuators to safely position the elevator cab. Computational models characterize cyber systems; within cyber, software encompasses all implementation designs.

2.1. Definition and Characteristics

With this backdrop, we investigate how to design an autonomous vehicle system protocol that meets end-to-end safety guarantees in the context of simultaneous cyber- and physical-attacks by the adversary, at least some of which may be mutually reinforcing as we will demonstrate. Our work builds on a novel concept, Trustworthy Cyber-Physical Systems (TP-CPS), as does the work for real-time traffic control and operation using vulnerability metrics

and provides constructs, plans, and financial incentives to help private companies invest in reducing vulnerability. However, the contribution of this paper is the first to analyze a problem where the consequences may be dire physical outcomes and consider physical systems that can be attacked at the root level via cyber sensors.

The autonomous vehicle (AV) is a cyber-physical system (CPS) capable of moving in physical space and interacting with its environment (the physical world), using a variety of sensors and actuators. This is in the context of continuous technological progress. Cybersecurity is increasingly an important consideration for all vital systems, more so for AVs. Done with malicious intent, compromised AVs can inconvenience, harm, or even kill humans. The vehicles are entrusted to make decisions at a micro-scale, evidence supporting macro-scale safety guarantees such as those promised by safety model concepts such as "Certified Safe" or "Safety Cases".

2.2. Key Components

2.2. Key Components We intend to design, in particular, the following key components of awareness, perception, and decision support: 2a. An awareness system. An awareness system is an AI module that monitors the environment, perceiving events, states, and changes to detect evolving situations. It is in charge of maintaining and possibly updating a machine-friendly, partial, and approximate model of the physical surroundings from sensorial data, with relevance to specific goals. 2b. A multifaceted perception system. It is a combination of symbolics and sub- and holistic-quantitative aspects. So, it is not only in charge of perceiving external inputs but also updating a machine-learning-based internal model of the vehicle. The perception system aesthetics will be a function of the physical envelope of a vehicle, including internal causal-based representations. The actual envelope of the holistic model should be made to remain within both the physical envelope, at a distance, and the informational limits of the sensors. The multifaceted perception system will be involved in perceiving external inputs while updating an internal model of the vehicle.

Awareness, perception, and decision aspects are essential for the design and operation of Cyber-Physical Systems, such as assisting autonomous vehicles. For awareness, models of external entities and decision systems that interpret raw observations into knowledge are needed. An awareness system is an AI module that monitors the environment, perceiving events, states, and changes to detect evolving situations. Situation awareness requires radar,

LIDAR, cameras, and lidar/ultrasonic sensor fusion. In order to handle multiple objects, a complex environment model is needed. It will understand the surrounding environment in terms of horizontal and vertical track positions, track list, track type, and target list. Our design will also help local, self-contained control units. A multi-object tracking setup also helps the central awareness.

2.3. Interactions and Integration

Designing public API guarantees plays an important role in facilitating interaction between components developed in different organizations and following different development standards. Here, formal verification can play an important role, particularly about lower design levels and for the interfacing among vehicle component blocks, strongly focusing on contractual violations and being mentioned as the most preferable approach for the design of early integration points in which the component or interface developed by one organization is available to other organizations that will develop interaction mechanisms, like buses, and other enabling technologies. These activities are really important in the automotive field, in which most of the vehicle components are developed and integrated by the contract, with the tier 1 suppliers and their subcontractors.

A significant aspect in vehicle control design and development is the integration of various control system blocks with sensing and actuation that are part of other systems, like automotive, batteries, infotainment, etc. These systems may have different development cycles, be developed by different teams or sub-teams, in different organizations. An additional requirement is set by functional safety standards, with the call for isolation mechanisms that limit the propagation of errors and prevent generated hazard risks. The trend in the automotive development is into the aggregation of functionalities in the vehicle, followed by a strong process re-engineering and aggregation of software modules in large and possibly regular/periodic releases that need close support and management of third-party and sub-contractor integration activities.

3. Autonomous Vehicles Technology Overview

To enable high levels of autonomy, it requires the integration of technologies invented primarily to serve diverse markets (e.g., robotics, control networks, security). Furthermore, the integration of physical systems with novel cyber elements introduces innovative

requirements on the design process, especially when large uncertainties about performance and errors can adversely affect AV safety. The design of AV falls under the purview of Cyber-Physical Systems (CPS), demanding the presence of high safety elements, including security requirements, throughout the solution space. Proving AV safety and its compliance with its intended safety requirements will require impractical levels of practical experimentation. More reliable contracts will minimize inconsistencies in the safety arguments made available to the third-party consumers. AV technology is coupled with a higher level of vulnerability to safety hazards and security failures, requiring novel solutions for the design construction. This chapter delves deeply into the AV-CPS safety and security issues and expects that it will become a frequent conversation topic among those interested in this sector.

Self-driving vehicles, also known as autonomous vehicles (AVs), are vehicles capable of functioning with limited or no human intervention. The full automation of AVs is considered by both the public and the automotive industry as a significant landmark, with several potential life-changing applications. In fully automated AVs, the operative responsibility of the driver is shifted to the vehicle, where the driving tasks and decisions are carried out by an autonomous system that includes numerous sensors within the vehicle and computational infrastructure on-board. These sensors acquire information on the AV operational environment such as the speed of vehicles in its vicinity, information on changes in lane, direction, velocity, and environmental conditions, notably weather and traffic signals. The computational infrastructure and the software slices were assessed according to the autonomous-driving capabilities.

3.1. Evolution and Current State

The planning module proposes a strategic route and a tactical trajectory for the vehicle by taking into account the vehicle specifications and the environment constraints (like regulation rules, priority for specific tasks or users, and communication requirements between vehicles). The actuation module is responsible for controlling the vehicle by moving its wheels and changing its speed, brake, and direction. This module depends on the vehicle actuators and sensors, more specifically on the steering, throttle, brakes, gearboxes, and related mechanisms, including the engine, if we are still considering conventional gasoline or diesel fuel engines. The control module is responsible for ensuring that the actuation module executes its

instructions in a safe and comfortable way, so the vehicle moves in the planned trajectory as close as possible, while obeying the dynamic and kinematic vehicle models.

One way to understand and evaluate the current research efforts and the diversity of problems related to CPS design for autonomous vehicles is to analyze the architecture and systems design of vehicles, especially on the aspects of software and sensing and actuation capabilities. From a high abstraction level, one can consider that the systems of an autonomous vehicle comprise the perception, planning, actuation, and control modules. The perception module is responsible for collecting the most possible real-time information about the environment, which may have different nature and in different forms, like objects, static obstacles, drivable paths, traffic signals, or other vehicles. The most usual sources are video cameras, ultrasonic range finders, LiDAR, RADAR, and/or GPS. Each of these sensor types has its unique constraints concerning the operating range, noise, and latency.

3.2. Key Technologies and Sensors

To this end, the Marshland-Rouen vehicle implements the function of advanced driver assistance systems (ADAS) but concludes to autonomous driving level-2. The steering wheel, accelerator/brake pedals, and seat position sensors are designed to supervise and implement the drive of the ADAS function of autonomous driving level-2.

The low-cost IMU sensor in the vehicle, the inertial navigation, high-precision LIDAR, and constant blind-area GNSS/BD driver assistance system can ensure Marshland-Rouen drives perfectly in the city and on highways. The vehicle environmental perception will generate large, complex, and variable data while driving in different ecological conditions, and the cloud service center will process and dispose of the data, enhancing the environmental perception of the vehicle. The intelligent message and spa voice messaging are adopted for the vehicle to cooperate with other pedestrians, vehicles, infrastructure, and cloud service center stakeholders. Smart sensors will realize the data exchange between vehicles and smart infrastructure to meet the demand for high-performance vehicle data transmission in scenarios such as road safety, assistance in emergencies, safe maneuvering at intersections, and increase the attribute management accuracy and efficient management operation.

The Marshland-Rouen vehicle uses LIDAR for the high-precision 3D real-time mapping of the driving environment, ensuring the all-time and all-weather safety of the vehicle motion. The

CMOS camera and the computer vision technique are used for lane recognition, thereby replacing white lines as road signs, and pedestrian recognition, so the vehicle can cooperate with pedestrians and cyclists through the image interface. GNSS/BD INS positioning is used to provide auxiliary positioning for the vehicle of low positioning accuracy and to use the multi-sensor information fusion technology to solve the positioning problem under the condition of high probability constant blind area.

The key technologies for the sensors and functions of the Marshland-Rouen vehicle are shown in Table 1, as well as a sketch of the functions and behaviors related to the mainstream development trends and the relations of the V2X, V2I, and V2P systems, shown in Figure 1. The vehicle motion control is based on the vehicle dynamics, which requires a complete model of the vehicle, together with models of the driver and the environment.

3.3. Challenges and Opportunities

The affected results of digital attacks or existing embedded problems must be unprecedented when transferred from a conventional linear time-driving system to the new autonomous vehicle, i.e. the affected results must be better than with human drivers. Then, several additional challenges in the validation of design for cybersecurity and potential attacks were identified. The challenges in integrating different subunits for AV are complex, such as heterogeneous equipment; dozens of advanced electronic controllers are constantly present in the vehicle. Conventional automotive electronics have been exposed to compromised field devices with non-negligible energy and communication capabilities, thanks to the widespread introduction of the FlexRay and CAN buses. The integration of these sub-technologies is a high-stakes process and the test of their integration results is complex rumors. There is also a need to consider the adverse effects of the collecting devices affecting these error messages.

Several key challenges still need to be addressed for safe, trustworthy, and resilient AV operation, such as the usability and security of increasingly complex systems in integrating different components, addressing errors and faults generated by these components, both physical and cyber attacks. The integration of these AV pieces is an evolving process, and the verification of those integration results is a persistent challenge. In addition to the verification challenge, the evaluation of the effectiveness of the automotive and cybersecurity attack surface is an evolving process as developers continue adding new features and overcoming problems. The threat landscape is also evolving, and as software, hardware, and infrastructure

continue to evolve and digitalization continues to expand, the attack surface of the cyber/physical or mixed-signal components will also increase.

4. Trustworthiness in Cyber-Physical Systems

As such, a set of satisfactory properties is necessary for AVs, i.e., the AV final output must be obtained from a trustworthy input, and the failure of CPS components will not endanger the safety of the entire system. To guarantee the trustworthiness and safety of CPS architectures, we propose several considerations for AV design with the guidance of the software development process concept, composed by the framework of the relative part, knowledge flow management, and development processes. Additionally, in this manner of discussing these issues, we aim to identify not only the mechanisms that enable observable and predictable behavior of AVs but also the large number of unsolved issues and interesting directions that AV designers and operation researchers might address.

Given the increasing complexity, connectivity, and mode diversification of cyber-physical systems (CPS) and the widespread applications of autonomous vehicles (AVs), multiple disciplines are merging into the era of driverless cars. However, the consequence of integrative infrastructure is that new attacks, vulnerabilities, and risks emerge from such a fusion. These problems may cause unprecedented dangers such as accidents, privacy leakages, and data theft. Therefore, once the safety and trust of the AV ecosystem are compromised, it will directly affect the entire intelligent transportation ecosystem. Hence, how to design AVs to ensure that CPS architectures are trustworthy, reliable, and maintainable is a critical topic for unmanned vehicle developers.

4.1. Definition and Importance

A trustworthy CPS is a CPS that is perceived by its stakeholders as providing strong guarantees for properties demanded by its applications. A trustworthy CPS can enjoy an increased level of confidence from its evaluators in those properties, which is crucial for its mission and safety. This is essential to guarantee that the behavior of the system still matches the description of its original design. In this context, a trustworthy embedded system engineering process addresses several distinct stages. The advanced technology in software and cybersecurity for CPS devotes meaningful stakeholders' interactions and tailored trustworthy symptom recurrence control structures, and exploits unique properties of the

designed CPSs. As a result of interactions and evolutionary functioning, the requirements for building CPSs become increasingly challenging.

A cyber-physical system (CPS) is a computing system that manages, monitors, and controls a physical system, and enables direct or indirect interaction with humans. CPSs evolve through close coordination between computation and physical processes and their tight integration. Consequently, they emerge and change throughout the system's lifetime due to their inherent dynamics. In this context, an autonomous CPS is a CPS that can act on its own, independently of its software system and human operators. To a greater or lesser extent, most CPSs are autonomous. A system engineer should thus habitually enforce system behaviors to differentiate between successful and unsuccessful coordination and integration of the computational entities.

4.2. Security and Safety Considerations

Considerations should include modularity distinguishing safety-certified components from non-safety-critical components, defense-in-depth seeking to limit paths vulnerable to threats, and secure-by-design principles protecting each component. Security assessment practices guide AV stakeholder collaborative information risk evaluation for AV use cases, while software and hardware assurance activities seek to demonstrate software and electronics are protected against threats and faults that are work products of distinct life cycle processes. Relevant safety and security standards, such as SAE J3061, ISO 26262, NCLAÜ, IEC 62443 etc., suggest countermeasures that systematically or dynamically identify, prevent, or respond to threats. Supporting Federal guidance for the design, development and testing of automated safety technologies in the U.S. must be identified and applied.

During the design phase of an autonomous vehicle, a set of security solutions should focus on protecting vehicle systems from being compromised, and possible unexpected hazards or risks must be accounted for. Techniques to fault detect and recover from hardware and software failures must be accounted for in the design. The integration of security mechanisms in a standard-compliant manner at the design phase ensures item families can be widely and publicly adopted, ultimately leading to improved public safety – as CTI is developing technical consensus for emergent technologies backed and enforced by existing voluntary industry standards.

4.3. Reliability and Resilience

The traditional and practical approaches to reliability and resilience, premised on failsafe design, disallowing any failure to put vehicle occupants in danger, has risked overly simple systems defined in overly simplistic ways so that they are so limited in the functionality they can perform that they are effectively not autonomous. This has almost been the case in air and ground vehicles where deterministic, physics-based approaches are applied. Such determinism often limits the autonomous system in noise and unmodeled dynamics rejection and its adaptation to new situations, which is at odds with the main expectation that these systems have to be able to provide in a changing environment. These issues surely cannot be addressed by standard human-machine interaction approaches or traditional control considerations.

Autonomous vehicles should be protected from the catastrophic effects of component failures and attacks on hardware and software because they must be available to perform their functions at all times and under all conditions. Autonomous systems reliability and resilience engineering combines dependability technology and related subjects with self-adaptation concepts in order to maintain safety while exploiting autonomous systems' intrinsic context-dependent and goal-focused capabilities. The design and development of autonomous vehicles must be driven by the imperative of providing highly reliable function, safety, and security, despite the vulnerability to malfunctions and malicious attacks, and technical complexity associated with autonomous decision and control.

5. Design Principles for Trustworthy Cyber-Physical Systems

These design principles are given as informal, prescriptive statements that it is hoped may guide the development of new principles and formal models for trustworthy cyber-physical systems. These principles are motivated by the goal of increasing the trust that users place in the command languages that they employ in cyber-physical interaction scenarios. Despite appealing to a qualitative definition of trust that may differ for different actors and contexts, these principles generally apply across a broad range of cyber-physical settings, as they correspond to generally desirable properties of command languages. These principles can be employed in an ex ante manner when the cyber-physical relationships among a system are being drafted and also in an ex post manner to assess the trustworthiness of an existing system relative to some set of user needs.

1. Make control effects of actions explicit in cyber-physical command languages. 2. Make cyber-physical command languages aspectually complete. 3. Provide implicit expectations for potentially dangerous actions.

The following principles for the design of trustworthy cyber-physical interaction mechanisms are proposed:

In this chapter, design principles for trustworthy cyber-physical systems are outlined. As systems such as autonomous vehicles interact more intimately with the physical world, more care must be taken in their design and implementation. These principles are strictly qualitative in nature, expressing a number of guidelines that designers can follow to increase the level of trust in the systems they build.

5.1. Modularity and Layered Architecture

The resultant design can be managed through a component-based system design approach. Components in this context are understood as contained conceptual entities that have attributes, roles, and interfaces. Components can play a major role in guiding the synthesis of a coherent system architecture organized in a plurality of layers (or levels, or strata) that depict the interplay of system components, the characteristics of the physical platform, and the operational environment. Such a layered system architecture enables a modular approach to the documentation, design, implementation, and integration of the functionality of vehicles with a much higher complexity than currently operating autonomous vehicles. Each layer can be documented in detail using separate components and interface descriptions. With clear separations between the layers, the link between high-level obstacles (or restrictions) and low-level functions can be maintained. Such a structured approach allows for separate development paths for vehicle components. In general, more abstract components, as defined in the higher system layers, should be widely usable and of stable design over the system operation time, covering most real world scenarios. The use of these components powered by adequate rules is necessary to provide a scalable vehicle design providing a defined level of operational safety. Under predictable navigational conditions, components that realize more detailed and highly optimized behaviors for the vehicle operation can be switched on. These highly specialized components can be used with predefined responsibilities for specific outputs only if the conditions are inside their predefined operational bounds. With this approach, the system becomes of lower inherent complexity and can be developed with less

effort, while the narrowness of the preconditions ensures a high level of reliability in the system operation. As for verification, responsibility of separate parts of the system versus coherent operation should be clearly defined and verified. Given a layered system architecture and a documentation that clearly delineates the interactions of the layers as well, this verification of the integrated system can be considered as the external interface test compared with the final framework that operates across all of the individual dynamic levels.

The high complexity of the systems being considered, as well as the design discipline, is expected to require a modular design approach. Modularization of system design is a systems engineering discipline that is based on the idea of making complexity manageable. In its most commonly understood form, a module is a high-fidelity representation of a part of a larger system. The module presents an interface whose inputs and outputs are explicitly defined and simple. The modules are interconnected to contribute to higher level functionality. While the internal complexity required to fulfill the specified interface of a module can be arbitrarily high, the interface itself should not be, so that a module can be designed and verified in separation from the rest of the overall system.

5.2. Redundancy and Diversity

While conventional E/E architectures use a multitude of microprocesses in order to accommodate functional safety requirements and/or implement security countermeasures, on the assumption that attackers can comprehend internal functional behaviors of devices, the presented research suggests a reevaluation of this assumption. As the sophistication of adversaries grows and looking forward to functional safety standard updates that recognize such threats, the classical fault-tolerant archetypes of redundancy and system response to provide mitigation can be applied to accomplish these specialized security countermeasure means as well.

One possible defense method against cyber vulnerabilities is the inherent properties of diversification of the solution. While hacking may exploit commonalities in the public interfaces and protocols in systems with similar themes, diversification in design and implementation details may provide a level of protection. In typical ECCPS implementations, software diversity may be used in security-critical components. This means deploying diverse, independently developed and/or generated components to perform the same security-critical functions.

5.3. Verification and Validation Techniques

CPS can be subjected to adversarial attacks. It is theoretically possible on real defects in the embedded controls or attacked via spoofing or other methods based on raw data from the vehicle's sensors, which capture the physical environment. For this reason, both monitors of the physical systems and access points to software components are, to the greatest extent possible, separated and protected by physical barriers. BD-AEVD proposes a concept of Activity-Driven verification for end-to-end verified and robust de-Saturation control system and uses Feature-Resilient Neural Network to make use of predictions processed by multiple independently trained NN, so as to detect evidence of possible adversarial attacks. Such a resilient model silos potential attacks and represents ensuring the maximum likelihood of correct predictions in a highly-different space, eventually producing probabilistic assessment independent of the current known adversarial techniques. The method does not require any threat model, any specific data, and can be used before an attack due to physical deception occurs.

Cost, safety, and legal reasons have naturally discouraged the overwhelming reliance on real-world data during the validation and verification of autonomous vehicle systems. Therefore, there is also the need to work out testing methods that do not rely on the huge, labeled real-world dataset. In "Bridging the Gap Between Robustness and Uncertainty," Hendry et al. proposed a method to test-and-train the difficult-to-satisfy transition adversarial examples. Freund et al. employed generative adversarial networks (GANs) to sample the hard-to-find inputs and enhance the fault detection models. Moreover, synthetic datasets, developed to be very close to real data, have also made training and verifying the autonomous vehicle system closer to the real world. Online methods relax testing requirements and exploit feedback that is available during operation, and then verify if critical safety properties may not be satisfied with the signal obtained from only a subset of sensors. These relaxed testing conditions greatly speed up the testing process. Assertions-based Model Checking is an online verification method for autonomous vehicles. Any key safety claim can be appended or designed into the autonomous vehicle safety system and cross-checked with both the vehicle perception model and the vehicle dynamics model. At runtime, the availability of ordinary sensors is used to check consistency with the proclaimed assertions, while the extension of model checkers allows the choice of specific surface areas and sky situations that guarantee the assertion(s).

The increasing dependence on software complicates the verification and validation steps for autonomous vehicle systems. Besides the traditional validation and verification techniques for embedded software, such as static analysis and software-driven testing, there are also domain-specific validation and verification techniques for CPS. Testing CPS using real-world data has been a useful method. With a vast amount of real-world sensory data, deep learning-based testing methods, such as DRL-BUST and DeepTest, are developed to test CPS. In DRL-BUST, a DRL-powered black-box test selection approach creates a hybrid testing framework for system-level block and system integration verification. DeepTest employs an ensemble of deep neural network predictions as test oracles to automatically learn, generate, select, and perform test inputs on the target system.

6. Case Studies and Best Practices

To trust safety-critical data, it is crucial to consider the integrity of all the tools employed in their generation. Covariance matrix is also important. We are advocates of using strong methods to generate the initial estimate. Our AGV operates in an environment, therefore sometimes will fail. This is our software's ammunition in its software battle against environmental architectures which are detected. Supervisory Control and base CPS Architecture. Various critical soft and hard measures have been developed, and all these measures are verified by a generate-and-verify process at the designed 5th level 1 and 5th level 2 architectures variant. Remark in delivering safety-critical motor hardware, our software design innovations have significantly overwhelmed the confidence of car motor authorities. It is our intention to continue this strategy in our future Gen 2 systems. By reusing the software of a safe system, we do not imply that all software function is constant. New and traditional fault systems will disable.

The many automobile manufacturers and a growing majority of technology firms are rushing to become the dominant suppliers of advanced systems that control every aspect of a vehicle's motion, navigation, and environment management. Driverless cars would eliminate practically all accidents, not just most of them. The approach to energy, halted vehicle, and even road use efficiency which has been lost since our current system is on average 1-1.5 persons per vehicle. In this section, we present several case studies in the design of a trustworthy base Cyber-Physical System (CPS) for our AGV (a BMW X5 SAV), all of which

manner evidence trustworthiness. Data is never accepted simply to be honest; cause for honesty is required. There are at least 10 reasons not to trust data at all times.

6.1. Industry Examples

The Airbus A380, the largest commercial aircraft developed by Airbus, blends state-of-the-art technologies into an airplane that is the largest commercial jet in the world, seating 555 passengers in a three-class configuration. The airplane offers airline passengers the comfort of fewer problems and superior safety features. The airplane is the eighth all-digital design that provides less wiring, fewer equipment and software applications with fewer safety and reliability issues, and a more efficient operation and maintenance. The increased use of integrated digital technology is not only in improved architecture, design, development, and advanced technologies but also in the better use of internal aircraft systems. With better technology in the airplane infrastructure, system interchangeability, and less weight, system information and communications links with passengers and crew, the A380 is a flagship of the new generation of commercial aircraft as passengers become more demanding, flights longer, less space available for electrical systems, and the technological complexity of the aircraft systems.

The Boeing 787 Dreamliner (B787), the latest commercial aircraft developed by Boeing, is the first commercial aircraft to be designed with cyber-physical systems (CPS) to provide significant enhancements. The airplane introduces new wireless technologies by moving, storing, and processing data in the airplane to enhance airplane safety, automation, and aircraft system-wide coordination. In the B787 airplane, the networking system transfers data to the airplane and cockpit crew using multiple channels from separate locations on the airplane. Wireless and wired access points distribute information to the airplane's all-digital system using different locations and accesses, such as wired, wireless, passenger devices, and portable maintenance access. Megabit, gigabit, and terabit networking systems enable a layered topology that flows data in different flight modes using standard common components. Tiered networks provide deterministic tracking, reliability, and security through the use of smart search engines, emergency reset managers, and a user-defined watchdog.

We believe there are beneficial lessons to be learned from the Boeing 787 Dreamliner and the Airbus A380.

6.2. Success Stories and Lessons Learned

There have been quite a few success stories and we learned a lot through repeated practices with Draper in bringing security and resiliency to combat-zone UAVs. One good example was in securing the communications pipeline when bridging networks from UAVs to ground nodes and back. Draper has a unique technology in secure frequency and time hopping spread spectrum, which made it virtually impossible for adversaries to jam and eavesdrop on UAV communications, and this technology was either implanted on or retrofitted into security work we had done on programmable UAVs. We also had great success in improving the resilience of flight control algorithms to protect against cyber attacks by either spoofing GPS signals or corrupting sensor inputs into the UAV through a combination of component-based redundancy and an autonomic computing framework. In this framework, we developed automatic algorithms to recognize misbehaving components and reconfigure UAV control functionality to ensure that the flight plan was met and the vehicle under control, while at the same time rejecting compromised controls that could put the UAV into a vector that was unfavorable to the operation. Finally, during the design of counter-UAS defense as well as during our work with the Federal Aviation Administration (FAA), we learned a lot about operating UAVs in a crowded and competitive airspace, and about how to deconflict autonomous flight plans while efficiently performing flight control.

7. Future Trends and Research Directions

The TT CPSexF realization transforms the robust and dependable but mostly mature functionality, achieved at high financial and time cost, into the 'inherently' secure, repairable, safe and really sustainable design paradigm, desired for the future overall-systems for AVs.

- Development of the models with reliable prediction capabilities for a large class of the adverse states and events for various avionic/automotive solutions and the whole integrated CPSexF. - Multiparallel development of the novel advanced CPS technologies and specifications of such systems intrawork and the TT CPSexF actual realization, responding then as fast as possible to the requests from various stakeholders (intra-cyber and physical crisis management of AV incidents). - Development and deployment of the simple and intelligible models of the regulatory/integrational waiting buffer, where the systems developers can postulate their present (possibly failing to be desirable from the security perspective) solutions, while this differing from the best state-of-the-art and/or

(cross)manufacturer-solutions are being attracted and standardized by the industry and/or the public authorities. In this context, it is believed that the recent signing of the EU Declaration of Amsterdam on Cooperation in the Field of Connected and Automated Driving in the European Union can be evaluated as a long-awaited step in a positive direction.

Future trends and research directions. In the context of the previous discussion, a number of directions for future research and developments can be anticipated, including in the framework of the TT CPSexF design for CPS for AVs:

7.1. Emerging Technologies

Autonomous parking, autonomous valet, and autonomous driving under special scenarios such as airport shuttle, last mile delivery, and auto driving competitions have benefited from the extensive deployment of autonomous driving in smart transportation systems. AI-based path planning and control methods can also optimize the energy efficiency of autonomous vehicles, and wireless edge AI can further improve the energy efficiency of vehicles. By working collaboratively with traffic flow management systems, including traffic signal controls, they enable the efficient provisioning of smart mobility services. Emerging HD map technologies provide high precision information for lane-level guidance, which is the prerequisite for lane-keeping and/or lateral control functions of today's L3 (conditional automation) production vehicles. It is utilized by reference generation modules that are at the core of many lane-keeping and lane-change control functions. Furthermore, the HD maps are also discussed within a safety analysis framework.

Besides the progress mentioned in the previous sections, a variety of state-of-the-art technologies enable autonomous driving applications. AI algorithms empower advances in both sensor data processing and vehicle control efficiency. For perception, deep learning plays a significant role in visual, radar, and lidar data processing. For decision-making and planning, advanced reinforcement learning approaches are also being actively studied. In addition, model-based and AI algorithms enable precise prediction of human-driven vehicle trajectories and further improve the performance of decision-making systems. Today, more and more decision-making and planning scenarios are being unfolded.

7.2. Regulatory Landscape

Furthermore, the committee set by the NHTSA was then put in charge to develop and provide specific suggestions and requirements signed by the NHTSA US Sec by 2014. The first step taken by the NHTSA will be to classify the advanced driving features in order to begin regulating it. Moreover, the NHTSA launched a Failure Analysis Research Report on Feb. 2, 2015, in which the NHTSA asked car manufacturers who have their vehicle being affected by a recall to notify the agency if their car is either a prototype or a vehicle equipped with self-driving technology.

In comparison to other industries, the safe deployment of CVs specifically raises ethical and societal concerns. Since CV state laws and regulations are very few, there is no legislative effort to prepare a stepping stone to safely deploy these vehicles. The National Highway Traffic Safety Administration (NHTSA), on the other hand, has recently recognized that the development of AV could alter the state and federal roles and that it would be difficult to deploy AV with the present regulatory framework unless the views of the US Department of Transportation (USDOT) rules are expanded.

7.3. Ethical and Social Implications

It is not in our plans to explore in detail the promises and risks, strengths and weaknesses, of existing ethical codes for autonomous cars. Such analysis endeavors by now count on a fully-developed array of scholarly literature, and readers interested in getting a quick bird's-eye view of this critical literature will be better served by making use of a recent systematic review. Instead, we would like to approach the challenges raised by the emergence of autonomous vehicles from an original philosophical perspective, namely that of New Cyberethics, the philosophical discipline located at the confluence of ethics and cybernetics. Being mindful of the sophisticated craftsmanship engendered by the approach that savvy engineers intend to put forth for the development of fully autonomous derived vehicles, we limit our discourse to a specific topic, namely the extent to which such vehicles can be expected to embody capabilities for passing or implementing moral decisions.

Ethical and societal consequences are yet two additional factors that are challenging the adoption of autonomous vehicles. The fact that cars will be driving on their own carries a demand for a specific type of radical philosophical approach, while it leads to technical and normative implications. Such a call for moral decisions, in its various specifications, has already been thoroughly explored by a number of researchers on different occasions. This

topic ranks very high on the agenda of research on autonomous vehicles, as witnessed by the frenzied production of ethical codes for autonomous cars. Car makers and trade associations have announced their commitments to ensuring that autonomous vehicles will behave in accordance with specific principles meant to ensure that they assign priority to human safety.

8. Conclusion and Recommendations

A simple example of expanding the VPH thinking to whole vehicle operation with applications beyond the flight envelope in time of troubled interactions is presented and discussed. However, this VPH effectiveness should not be easily dissolved to meet subverted bonus traffic deadline missions. The life-critical and costly capital of actual predictable operations should be carefully governed with technically proven objectives while deploying CPS-Hitchhiking and VPH. Our proposed CPS design and VPH need to be thoroughly investigated and tested in real-world vehicular applications. Only when the refined self-aware and voluntary VPH wear a CPS seal of trust and deterministic behavior can we be sure that those seeking opportunistic advantage won't bring forth a time of hitchhiking hyperinflation.

We have introduced foundations for trustworthy Cyber-Physical Systems (CPS) design with a unifying semantics that tightly couples the physical with operating functions. We bridged the gap between System-on-Chip (SoC), real-time control and Hybrid Systems technologies to distill time and robust information flow. Our foundational work enables systematic process of verifying operational CPS functionality without disturbing critical operating patterns. We then presented a CPS design that employs Virtual and Physical Hitchhiking (VPH) as a tolerance for adversarial timely disturbances. We validate the jeopardized islands VPH concept and its practical utility on the control side by exposing the dependence of nominal flight control under the simplified adverse setting of interest, and by practical experiments of it on a hobbyist quadrotor.

8.1. Summary of Key Findings

The experiences in APS and AVs should be shared with a broad audience. We believe that the approach of TCF-pedigree secure software and conceptual shift from safety to security are the two high-impact ways to reach non-technical individuals and support this knowledge sharing. We also wish to share the key principles of AI infrastructure with both regulator and insurance stakeholders. These are transferable not only to other emerging digitalization

applications including the Industry Internet of Things (IIoT) but also to other emerging AI-enabled hazard detection, avoidance, and law-enforcement concepts like that of smart-cities police or disaster recovery and emergency first-responder robots.

In this talk, I presented key principles, such as machine learning-based foundation for the autonomous decision-making, testing and certification of machine learning-based Cyber-Physical Systems (CPS), finding and preventing the weakest link, and maintain readiness of a system that is constantly changing and probably learning after deployment. These principles were then integrated to develop a Trustworthy Computational Framework (TCF) capable of support deployment of next-generation autonomous vehicles for various complex mission operations including Automated Driving System (ADS). With the TCF, ADS developers are enabled to use flexible and modular artificial intelligence (AI) building blocks, integrate scalable, data-driven, traceable, and reliable AI solutions using machine learning, and be encouraged to involve multiple stakeholders in a joint verification and validation process of hybrid AI.

8.2. Practical Guidelines for Designers

Moreover, in the new era of information and communication-based cyberspace supporting increasingly autonomous systems, the data density of quickly accessible data is far beyond human comprehension without effective systems capable of data fusion to arrive at interpretation that is meaningful not only to the ever-faster autonomous decision-making processes necessary in advanced and autonomous vehicles for a safe and reliable driving experience but also to human observers in both normal operation and in the aftermath investigations of the few remaining hazardous events that could not be evaded or mitigated. Indeed, when we appropriate the major hallmarks for trustworthy systems developed by the SEI, we identify all four as having a major impact dependent upon the non-trivial complexity of the information that the designer must select, present, and judiciously allow non-expert users to individually or jointly fuse for a level of situational awareness appropriate.

Accordingly, as we move to the next generation of ever more dynamic complex products such as autonomous cars in which a vast (and growing) number of sensors and actuators communicate directly over cloud-based networks, the practical reality is that there are relatively few precedents on which to base a design. Indeed, the issue has, of course, also been central to all of the leading edge research associated with the development of the enabling

technologies for autonomous cars conducted under the Intelligent Automation Center of Carnegie Mellon University. Said research has highlighted many of the practical considerations encountered enabling a truly practical systems engineering framework for designers to rely upon. This framework has already been used in the validation and preliminary design associated with a number of the associated autonomous car related technologies and was used as an underlying basis of the scenario-based design approach developed for the pre-study of the new European funded Adaptive Systems Software Architecture project (ADAMANT).

Reference:

1. Prabhod, Kummaragunta Joel. "ANALYZING THE ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TECHNIQUES IN IMPROVING PRODUCTION SYSTEMS." *Science, Technology and Development* 10.7 (2021): 698-707.
2. Sadhu, Amith Kumar Reddy, and Ashok Kumar Reddy Sadhu. "Fortifying the Frontier: A Critical Examination of Best Practices, Emerging Trends, and Access Management Paradigms in Securing the Expanding Internet of Things (IoT) Network." *Journal of Science & Technology* 1.1 (2020): 171-195.
3. Tatineni, Sumanth, and Karthik Allam. "Implementing AI-Enhanced Continuous Testing in DevOps Pipelines: Strategies for Automated Test Generation, Execution, and Analysis." Blockchain Technology and Distributed Systems 2.1 (2022): 46-81.
4. Pulimamidi, Rahul. "Emerging Technological Trends for Enhancing Healthcare Access in Remote Areas." *Journal of Science & Technology* 2.4 (2021): 53-62.
5. Perumalsamy, Jegatheeswari, Chandrashekar Althati, and Lavanya Shanmugam. "Advanced AI and Machine Learning Techniques for Predictive Analytics in Annuity Products: Enhancing Risk Assessment and Pricing Accuracy." *Journal of Artificial Intelligence Research* 2.2 (2022): 51-82.
6. Devan, Munivel, Lavanya Shanmugam, and Chandrashekar Althati. "Overcoming Data Migration Challenges to Cloud Using AI and Machine Learning: Techniques, Tools, and Best Practices." *Australian Journal of Machine Learning Research & Applications* 1.2 (2021): 1-39.

7. Pelluru, Karthik. "Unveiling the Power of IT DataOps: Transforming Businesses across Industries." *Innovative Computer Sciences Journal* 8.1 (2022): 1-10.
8. Althati, Chandrashekar, Bhavani Krothapalli, and Bhargav Kumar Konidena. "Machine Learning Solutions for Data Migration to Cloud: Addressing Complexity, Security, and Performance." *Australian Journal of Machine Learning Research & Applications* 1.2 (2021): 38-79.
9. Sadhu, Ashok Kumar Reddy, and Amith Kumar Reddy. "A Comparative Analysis of Lightweight Cryptographic Protocols for Enhanced Communication Security in Resource-Constrained Internet of Things (IoT) Environments." *African Journal of Artificial Intelligence and Sustainable Development* 2.2 (2022): 121-142.
10. Tatineni, Sumanth, and Venkat Raviteja Boppana. "AI-Powered DevOps and MLOps Frameworks: Enhancing Collaboration, Automation, and Scalability in Machine Learning Pipelines." *Journal of Artificial Intelligence Research and Applications* 1.2 (2021): 58-88.