Certification for Autonomous Vehicles

James Martin, Namhoon Kim, Dhruv Mittal, and Micaiah Chisholm

Abstract

The landscape of certification in the auto industry reflects the necessity to keep consumers safe. Currently, certification of new vehicles depends on an ability to pass rigorous testing of components for durability and reliability in case of a crash. There currently exist no definitive standards that dictate best practices for software found in vehicles and responses to autonomous technology in vehicles are only just beginning to emerge. The National Highway Traffic Safety Administration in the United States has asserted itself at the vanguard of addressing new safety concerns that arise with the introduction of such new technologies. This paper discusses relevant modern standards that may pertain to autonomous vehicles and aims to highlight their shortcomings. Additionally, this paper explores the possibility of using existing standards in the avionics industry as a model for new standards in the automotive industry. Finally, this paper explains how techniques in formal methods could be used to alleviate some of the problems of testing complex systems.

I. Introduction

State of the art of certification in the automotive industry

Currently, the global automotive industry is subject to a series of safety standards to ensure the safety of consumers. In the United States, the National Highway Traffic Safety Administration (NHTSA) is responsible for establishing, maintaining, and enforcing these series of standards. Beginning in the 1970s following public outcry calling for universal seatbelt

requirements, the NHTSA began developing the Federal Motor Vehicle Safety Standards and Regulations (FMVSS). Nations across the world such as Canada, Australia, Korea, Japan, India, and the European Union have all developed analogous standards dedicated to keeping drivers safe and keeping industry best practices a part of the vehicle manufacturing process. The standards cover three desired attributes of vehicles:

1. Crash avoidance (100-series)
2. Crashworthiness (200-series)
3. Post-crash survivability (300-series)

Crash avoidance standards describe aspects of systems in the car such that the risk of a crash is minimized. For example, Standard No. 101 states that all "essential controls be located within reach of the driver when the driver is restrained by a lap belt and upper torso restraint," in addition to mandating all instruments be lit when the headlamps are on. These standards cover a range of physical parts from hood latches (No. 113) to brake hoses (No. 106), and all seek to reduce the possibility of mechanical failures.

Standards found in the crashworthiness section require specific interior parts to prevent injury in case of an impact. Standards covering head restraints, airbags, and seatbelts are found in this section.

Standards in the section covering post-crash survivability require structural integrity of safety-critical components of the vehicle such as gas tanks. These standards seek to mitigate risk of catastrophic events after crashes such as fires or explosions.

The FMVSS also outline other regulations not falling into the three mentioned categories. Standards numbered above 500 include a range of miscellaneous items such as fuel standards, manufacturer and vehicle identification requirements, and odometer disclosures. Autonomous

vehicles will have to adhere to these standards and must be subject to testing before reaching mass production.

Testing for compliance

In addition to the creation of standards such as the FMVSS, governments are responsible for enforcing compliance through testing of new vehicles. The NHTSA in the United States currently subjects new vehicles to a rigorous series of tests to keep manufacturers honest about following standards. Testing procedures are produced in great detail and are made publicly available on the NHTSA's website. Integrity tests for side and frontal impacts conducted by the NHTSA are often cited as testimonial for new car safety in advertisements. The NHTSA issues safety ratings on a five-star system, with the highest five star rating also highly coveted by advertisers. In this fashion, the existing standards and testing procedures set forth by the NHTSA have fostered a culture of striving for the highest levels of safety and consumer protection.

Shortcomings of current state of the art

However, despite protecting consumers, many holes exist in current standards when covering software found in vehicles. As vehicles become more connected to the Internet through entertainment and telemetric systems, they no longer exist as isolated systems. Higher degrees of networking correspond to higher risk of outside infiltration and potential damages. Previous studies performed at the University of California – San Diego have demonstrated the feasibility of installing malware on vehicle networks through multiple attack surfaces [1]. Technologies such as Bluetooth and addressable channels such as On-Star are two such examples of attack surfaces. Though these attacks require a great deal of reverse engineering, no standards in the

FMVSS in the United States cover procedures or best practices for addressing these concerns in vehicle software. Responses from manufacturers to these concerns have been mixed. The staff of Senator Edward J. Markey (D-Massachusetts) submitted a report claiming that "only two [out of sixteen surveyed] automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time" [2]. Markey's report received responses from BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedez-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen Audi, and Volvo. Aston Martin, Lamborghini, and Tesla were also contacted but did not provide a response. Furthermore, attacks on vehicles and the subsequent lack of response from automakers have garnered media attention from the likes of CNN and Wired Magazine [3][4]. The fairly dismissive response from automakers indicates that government regulators need to provide a set of standards and industry best practices of producing auto-specific software.

II. Standards for Autonomous Vehicles

In addition to maintaining current standards, the NHTSA in the United States has also composed a document detailing steps needed to ensure autonomous vehicles safely enter the consumer market. The document states that the "NHTSA intends to regularly review and update [the] document as necessary to provide additional clarity, reflect new findings, and outline any regulatory activity that the agency may pursue with respect to automated vehicles" [5]. Hence, this document produced by the NHTSA is the single, most thorough piece of literature published to date that seeks to address how autonomous vehicles will be standardized and regulated.

The primary motivation behind the statement is the NHTSA's recognition of the potential of autonomous vehicles to significantly reduce the number of deaths and injuries from crashes.

Because of this potential, the NHTSA boasts its involvement in three streams of technology and development.

The first is research into demonstrating vehicle-to-vehicle (V2V) communication technology, which "offers substantial crash avoidance possibilities;" the second is technology pertaining to in-vehicle warnings and/or limited automated control of safety functions; and the third is the development of self-driving vehicles [5].

In reaction to development in these three areas, the NHTSA has developed a scale of levels 0-4 to classify a vehicle's amount of autonomy [5]. Level 4 vehicles are capable of performing all safety-critical driving functions, including monitoring roadway conditions, for an entire trip without the driver providing any input or control. Electronic stability control is an example of a Level 1 technology that has been mandated in all new vehicles since Model Year 2011. The NHTSA hopes to incrementally enforce inclusion of these technologies with higher levels of autonomy.

In its preliminary statement, the NHTSA acknowledged the need for research into safe reliability and cybersecurity of control systems. Additionally, the NHTSA has tasked itself with supporting the development of any potential technical requirements for automated vehicle systems [5]. By taking a proactive approach, government regulators are well on their way to ensuring incremental progress continues in a smooth manner. The issuing of this statement also suggests that the NHTSA is aware of the lackadaisical response from auto manufacturers and wishes to drive innovation on safe terms.

Recommendations from the NHTSA

In reaction to developments in autonomous vehicle technologies and to states enacting legislation authorizing operation of autonomous vehicles, the NHTSA concluded their statement with a series of recommendations. The administration agrees that states are well suited to address licensing, driver training, and determining safe operating conditions of specific types of vehicles but does not recommend that states permit operation of self-driving vehicles for purposes other than testing. The reasoning behind this recommendation stems from the NHTSA's conclusion that true Level 4 technology does not yet exist and because technical specifications for Level 3 automated systems are "still in flux" [5]. Due to the unstable nature of this growing technology, the NHTSA wishes to ensure driver safety by limiting the operation of autonomous vehicles to testing. However, the NHTSA also stated that it recognizes premature regulation can run the risk of preventing the evolution toward increasingly better vehicle safety technologies [5].

Finally, due to pressure from states needing guidance on how to proceed with regulating autonomous vehicles, the NHTSA offered a series of recommendations on a range of topics. Included were:

1. Recommendation for licensing drivers to operate self-driving vehicles for testing;
2. Recommendations for state regulations governing testing of self-driving vehicles;
3. Recommended basic principles for testing of self-driving vehicles;
4. Regulations governing the operation of self-driving vehicles for purposes other than Testing.

Each section included a thorough framework for establishing regulation ensuring driver safety. These steps taken by the NHTSA have set a precedent for advancing technologies related to autonomous vehicles and have laid the groundwork for establishing laws governing such

technologies when they are made available. Though these technologies face computational and social obstacles, they are nonetheless poised to spark a revolution in travel and safety.

III. Industrial Standards for Automotive Systems

Electronic systems are increasingly replacing conventional mechanical or hydraulic systems in automotive application. This trend is accelerated by an evolution of technology and economic reasons. These electronic systems have been used to perform safety functions in automotive applications. However, there is a potential threat to life if a safety-critical application fails or malfunctions. Traditionally, such systems have been designed by practices established by a company or trained experts.

As systems become more complicated and modular, a standard framework for manufacturing is required to reduce production cost and effort. The introduction of standards in manufacturing provides benefits such as:

- A more scientific and numeric approach to specifying and designing safety systems is possible;
- The nature of the risk can be qualified and a system that protects against the risk can be designed [17].

Furthermore, the manufacturers can reduce development and production costs, which are great concerns for companies. It is extremely important that safety-critical systems must provide fail-safe operations in the presence of failures if the consequences of a failure might lead to loss of life.

IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

The International Electrotechnical Commission (IEC) led two studies, one on hardware and the other on software. In the early 1990s the two studies were merged, and a draft standard, IEC 1508, was announced in 1995. The draft suggests a risk-based approach in which the safety of a system should be based on an evaluation of possible risks. With feedback on the draft, the successor, IEC 61508 was approved as an international standard.

The standard consists of seven parts [18]. The first four parts are mandatory and the other parts provide information and guidance on the use of the first four parts. IEC 61508 is specified as follows:

Part 1, General Requirement, defines the activities to be performed at each stage of the lifecycle and the requirements for documentation, management, and safety assessment.

Part 2, Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems, defines the general requirements of Part 1 in the context of hardware.

Part 3, Software Requirements, defines the general requirements of Part 1 in the context of software.

Part 4, Definitions and Abbreviations, introduces definitions and abbreviations of the terms in the standard.

Part 5, Examples of Method for the Determination of Safety Integrity Levels, provides examples of risk-analysis and the determination of safety integrity levels (SILs).

Part 6, Guidelines on the Application of Parts 2 and 3

Part 7, Overview of Techniques and Measures, provides techniques and references of more detailed information.

The overall safety lifecycle consists of 16 phases. Phases 1 – 5 are analysis phases. Phases 1 and 2 consider the safety implications of the system level equipment under control (EUC). The risks and hazards are identified and analyzed in Phase 3, and in Phase 4 safety requirements for risk-reduction measures are specified. These requirements are translated into the design of safety functions in Phase 5. Phases 6 – 13 are realization phases. The planning of safety functions are considered in Phases 6 – 8 and these functions are realized in Phases 9 – 11. Phase 12 shows the installation and commissioning of the safety functions and Phase 13 shows the overall safety validation. Phases 14 – 16 are operation phases. These phases concern the operation of the safety functions. Phases 15 and 16 cover modification and retrofitting the system and decommissioning of the system, respectively.

The standard requires that hazard and risk assessment should be evaluated or estimated and offers guidance for many approaches. The analysis framework defines six likelihoods of occurrence and four consequences. The following tables show the categories of likelihoods of occurrence and consequences.

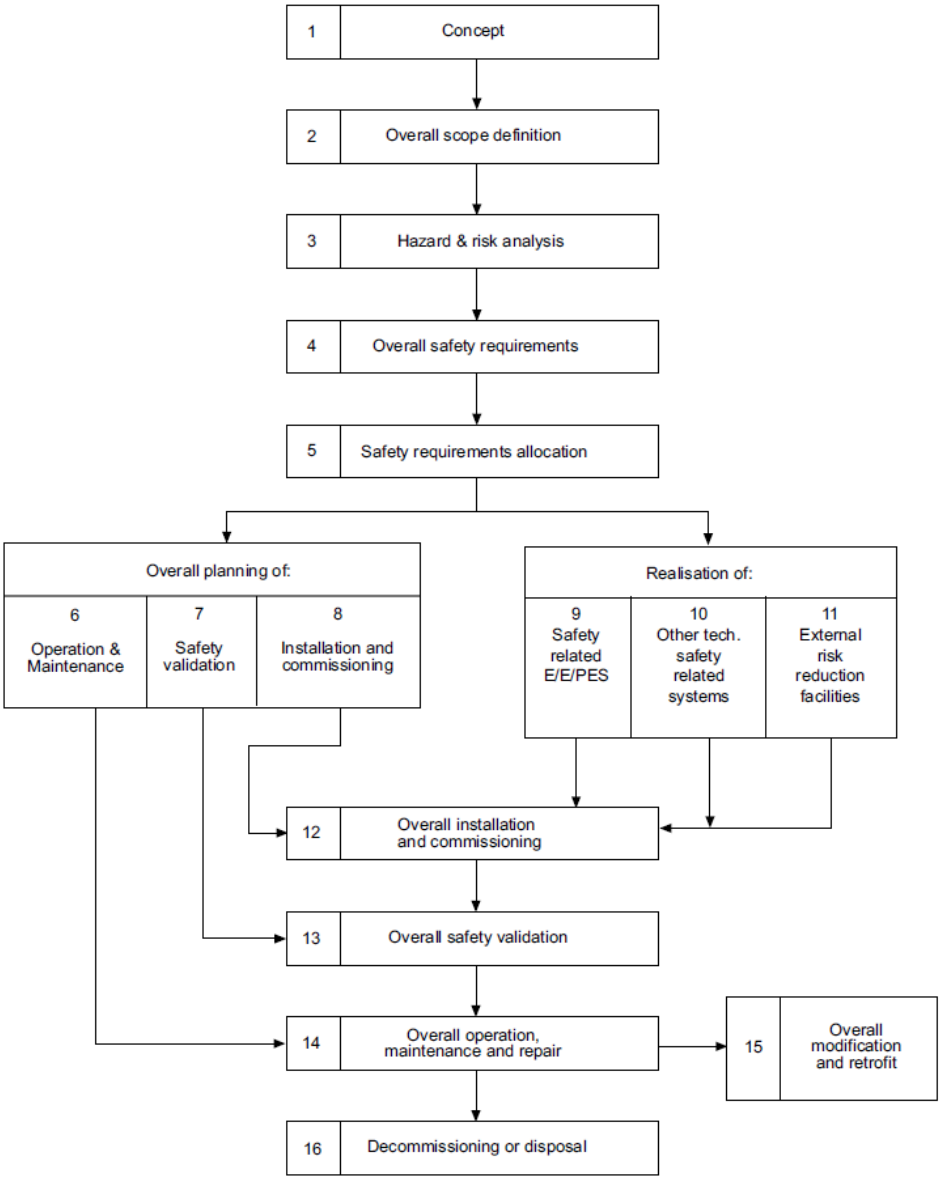


Figure 1. The overall safety lifecycle (Figure from IEC 61508-1 Figure 2) [17].

Table 1. Categories of likelihoods of occurrence

Category	Definition	Failure per year
Frequent	Many times in system lifecycle	$> 10^{-3}$
Probable	Several times in system lifecycle	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Table 2. Categories of consequences

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

With these two categories, we can produce risk class matrix as shown in Table 3. From this matrix, Class I risks are unacceptable in any circumstance. Class II risks are tolerable only if risk reduction is impracticable and Class II risks are also tolerable if the cost of risk reduction would exceed the improvement. Class IV risks are acceptable mainly due to the high improbability of their occurrence or of. To clarify, Class IV may include catastrophic consequences but an incredibly small likelihood of occurrence. However, a risk that is Class IV does not suggest that the failure of a component leads to multiple loss of life. It suggests that this component requires a high SIL that must be considered and addressed in the development process. A high SIL may be addressed with redundant systems or a redesign of the component.

Table 3. Risk classes

	Consequences			
Likelihood	Catastrophic	Critical	Marginal	Negligble
Frequent	Class I	Class I	Class I	Class II
Probable	Class I	Class I	Class II	Class III
Occasional	Class I	Class II	Class III	Class III
Remote	Class II	Class III	Class III	Class IV
Improbable	Class III	Class III	Class IV	Class IV
Incredible	Class IV	Class IV	Class IV	Class IV

The more important the job, the more reliable it should be. The rate of unsafe failures is used as a metric for the safety integrity of a system, which is defined in Part 4 of IEC 61508. The standard identifies SILs with probabilities of failures. Parts 2 and 3 give guidance to attain SILs. The definition of high demand is more than one demand per year and the definition of low

demand is no more than one demand per year. SILs are intended to provide targets for developers.

Table 4. Safety integrity levels

SIL	Low demand	High demand
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

The software of safety-critical systems requires a unit test or modified condition/decision coverage (MCDC) test. Unit testing is a testing method for individual units of source code and evaluates the smallest testable part of an application. However, unit testing would not catch every error since it cannot evaluate every execution code path. Therefore, software with a high SIL requires more intensive testing. MCDC is a code coverage criterion that requires all the following conditions during testing:

- Each entry and exit point is invoked;
- Each decision tries every possible outcome;
- Each condition in a decision takes on every possible outcome;
- Each condition in a decision is shown to independently affect the outcome of the decision.

The design of a safety-critical system is more than specifying components that are approved at the required SIL. The designer should provide the probability of failure on demand that meets the required SIL.

ISO 26262: Road Vehicles – Functional Safety

The purpose of ISO 26262 is to provide a unifying safety standard for all automotive electrical and electronic systems [21]. The Draft International Standard (DIS) of ISO 26262 was published in June 2009 and the first edition was published in November 2011. The standard is applied to electrical and electric systems installed in "series production passenger cars" with a maximum gross weight of up to 3500kg. The standard addresses possible hazards caused by the malfunctioning behavior of electrical systems and provides regulations and recommendations throughout the development of the product from the conceptual to decommissioning. ISO 26262:

- Provides an automotive safety lifecycle and supports tailoring the necessary activities during the lifecycle;
- Provides an automotive specific risk-based approach to determine Automotive Safety Integrity Levels (ASILs);
- Uses ASILs for specifying the requirements for achieving an acceptable risk;
- Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety.

The ASIL is a crucial component of ISO 26262. The ASIL should be determined at the beginning of the development process. To estimate a risk, a combination of the probability of exposure, the possible controllability, and the possible severity is used. Table 5 shows the assessment of ASILs:

Table 5. The Assessment of ASILs

Exposure	
E0	Incredibly unlikely
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

Controllability	
C0	Controllable in general
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

Severity	
S0	No injuries
S1	Light to moderate injuries
S2	Severe to life-threatening injuries
S3	Life-threating to fatal injuries

ASIL D is defined as a combination of the highest probability of exposure (E4), the highest possible controllability (C3), and the highest severity (S3). Each single reduction in any one classification leads to a single level reduction in ASILs.

The qualification of hardware has two main objectives. The first one is to show how the part fits into the overall system and the other is to assess failure modes. Hardware parts require the evaluation of ASILs and are qualified by testing in a variety of environment and operational conditions. The hardware vendors have provided qualified microcontrollers and packages to facilitate the certification process.

The qualification of software involves activities such as defining functional requirements, determining resource usage, and predicting software behavior in failure and overload situations. The simplest way to certify is to use the qualified software during the development process.

IV. Legislation

The United Nations Economic Commission for Europe (UNECE) Homologations are unified technical regulations for vehicles and their components. Three safety-critical components

are presented, electronic stability control systems (ESC), steering systems, and braking systems. The World Forum for Harmonization of Vehicle Regulations (WP29) of the UNECE is responsible for a technical regulation for ESC. The regulation draft GTR-ESC-2008-06 was approved in 2008 [23]. As previously mentioned, the US National Highway Traffic Safety Administration and Canadian Transport Canada have mandated ESC for all vehicles manufactured from September 2011. The European Union also has mandated ESC for all new passenger cars and commercial vehicles from November 2011.

"X-by-wire" is an electronic system that seeks to replace mechanical or hydraulic systems such as steer-by-wire or brake-by-wire. The conventional steering system requires a mechanical link between the driver and the road surface. Steer-by-wire systems have no physical contact between the driver and the road, but an electric actuator that assists steering of a vehicle. The discrepancy between the law and the technical status has led to a creation of new laws. The UNECE approved the regulation ECE R79 for road vehicles [24]. Other regulations such as self-centering of the steering system remain valid.

Electric or hybrid vehicles are equipped with a new regenerative brake system. The manufacturer ensures that the new regenerative brake system does not affect the braking system. The ECE R13 is the regulation for brake systems for passenger cars and commercial vehicles. However, the EU Project, Highly Automated Vehicles for Intelligent Transport (HAVEIT), could not meet all technical requirement of ECE R13 due to the nature of the electro-mechanical braking systems. So, HAVEIT made proposals for updating ECE R13 [25].

V. Certifications in Avionics as a Model

Although certification standards do exist to regulate the automotive industry, it is common for these standards to discuss only requirements imposed on hardware. It seems that software standards such as AutoSAR [26] tend to exist only in tenuous alliances between companies and research institutions working towards common research goals.

It should then seem obvious for us to look towards the certification model used in avionic systems, where software has typically governed a higher proportion of safety-critical tasks than in automotive systems. Avionic systems gain additional relevance to our interest in autonomy when one considers that software-controlled autopilot has long had significant control of commercial aircraft. These software systems are trusted with hundreds of lives (over five-hundred, in the case of high capacity aircraft like the Airbus A380 or the Boeing 747).

While many companies are working on autonomous automotive systems, few do so under the explicit blessing of any government. This is a dramatic contrast to the avionics world, in which the United States Air Force (USAF) might be the leading research organization; it appears that majority of research in autonomous systems in avionics is conducted by either the Air Force Research Lab (AFRL) or by contractors such as Boeing or Lockheed-Martin. Thus, avionics research has a tendency to move hand-in-hand, if not outright drive, relevant governmental oversight and regulation.

One might naively look towards the army for similar guidance on the ground. However, research in autonomous or remotely controlled army vehicles tends to concern itself with off-road functionality in the complete absence of human passengers. While the technology may be similar, this doesn't translate to the same regulatory concerns we hope to address.

Current standards in avionics

Many of the major certification standards in avionics are developed by private organizations that serve as advisory bodies to the FAA. One such organization is the Society of Automotive Engineers (SAE International), a professional association for engineers in a number of industries. The SAE creates task forces of engineers to assemble regulatory standards based on industry best practices. SAE is responsible for ARP4764 [28] and ARP 4761 [9]. The Radio Technical Commission for Aeronautics (RTCA) is another private not-for-profit corporation that advises the FAA. The RTCA develops technical guidance for use by both government regulatory authorities as well as industry, and is responsible for DO-178 [27] and its numerous supplements.

ARP 4754: Guidelines for Development of Civil Aircraft and Systems concerns itself with the complete development lifecycle for "highly-integrated or complex systems" that implement aircraft-level functions – critical systems such as communications, navigation, monitoring, flight-control, and collision avoidance. The document is particularly interested in "systems whose safety cannot be shown solely by test and whose logic is difficult to comprehend without the aid of analytical tools," and dictates the usage of the safety analysis methods outlined in ARP 4761, as well as several RTCA standards dictating specific development methods for software, electronics, and other integrated components.

ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment outlines several method for conducting a safety assessment. The three major steps are the Functional Hazard Assessment (FHA), in which the possible failure conditions and severities are determined, the Preliminary System Safety Assessment (PSSA), in which the methods in which failures can arise are determined, and the System Safety Assessment (SSA), in which it is verified that all failure conditions fall within

acceptable probability bounds dictated by the assurance level they fall under (Table A). ARP4761 provides several tools to accomplish these steps, including Fault Tree Analysis, the Dependence Diagram, Markov Analysis, Failure Modes and Effect Analysis, and Common Causes Analysis.

Probability (Quantitative)	1.0 1.0E-5	1.0E-5 1.0E-7	1.0E-7 1.0E-9	1.0E-9
Probability (Descriptive)	Probable	Improbable		Extremely Improbable
Failure Severity	Minor	Major	Severe Major	Catastrophic
Failure Effect	• Slight reduction in safety margins • Slight increase in crew workload • Some inconvenience to occupants	• Significant reduction in safety margins or functional capabilities • Significant increase in crew workload or conditions impairing crew efficiency • Some discomfort to occupants	• Large reduction in safety margins or functional capabilities • Significant increase in crew workload or conditions impairing crew efficiency • Some discomfort to occupants	• All failure conditions that prevent continued safe flight and landing
Development Assurance Level	Level D	Level C	Level B	Level A

Table A: Reproduced from [9], criticality levels and corresponding acceptable failure bounds that the SSA must comply with.

DO178: Software Considerations in Airborne Systems and Equipment Certification is of particular interest to us, as we are primarily interested in the process of certifying software. This standard utilizes assurance levels determined in the previous step of ARP4761 to guide objectives for planning and development based on safety requirements. DO178 sets up specific guidelines for software development, explicitly defining which languages, compilers, IDEs, version control systems, verification tools, and test environments can be used to develop safety critical avionics systems. The most recent revision of this standard, DO178C, actually decreases subjectivity across the software development and verification process over the previous version

DO178B. The true power of this standard can actually be found in its supplements, DO330-333, which cover considerations for each particular tool and technique. Of particular interest here is the final supplement, DO333: Formal Methods, which will be treated in a later section of this paper in greater detail. While significant research is being done in autonomous avionics systems, there do not appear to be standards that apply specifically to their development at this time.

Differing definitions of autonomy

A key point as we begin to examine autonomous avionics systems is the difference between the two most prevalent definitions of the term autonomy. The AFRL defines autonomy as "Systems that have a set of 'intelligence-based' capabilities that allow them to respond to situations in uncertain environments by choosing from a set of potential actions," while the FAA claims that "Autonomous operations refer to any system design that precludes any person from affecting the normal operations of the aircraft." It is important to note the military definition precludes what we would refer to as full autonomy – this is because of the Geneva conventions for the laws of war, which require that a human makes the decision to end the life of another human. Using their definition, the USAF has many aircraft with autonomous functionality in service at this time.

United States Air Force

The USAF looks to autonomous aircraft to dramatically reduce the manpower necessary for Unmanned Aerial Vehicle (UAV) missions. Here, autonomy enables a single remote operator to simultaneously control up to 4 UAVs. In the current state of the art, this is accomplished by a system of abstraction; rather than controlling every aspect of the UAV remotely, the operator is able to give high-level commands (e.g. "normal full coverage patrol," "go to this location and

report") or waypoint based instructions. As previously discussed, the human operator ultimately drives all decisions in this system. The USAF has also announced plans to slowly increase the level of autonomy present in their systems, but does not plan to remove the human component in the foreseeable future.

FAA roadmap for autonomy integration in commercial aerospace

The FAA, using the more familiar definition of autonomy that we have grown used to, details a number of necessary challenges that must be accounted for in a recent document [6]. The FAA Roadmap outlines the basics of their plan to "Accommodate, Integrate, and Evolve" new technologies into the National Airspace System (NAS). In the short-term accommodation step, they recognize that current "airworthiness regulations may not consider many of the unique aspects of [Unmanned Aircraft Systems] operations." UAS operations in the NAS are to be considered exclusively on a case-by-case basis as the technology has yet to mature to the point that generalizations can be made. Here, we see a focus on nascent technologies that the FAA hopes to promote. Of particular interest to us, Sense and Avoid (SAA) technology, through which all aircraft broadcast their position to all other aircraft as a means of collision avoidance protection.

As the technology continues to develop, the integration step will drive the evaluation of all relevant standards and certifications such that they discuss the necessary considerations for UAS operations. This stage will be characterized by a focus on new training and certification standards, research and technology development, and the goal of addressing privacy, security, and environmental implications of UAS operation. In the longer term (13-15 years), the evolution perspective will allow the FAA to drive development of UAS in a direction consistent with the evolution of the National Airspace System itself.

Unfortunately, the FAA has also established that ground demonstrations of autonomous airfield navigation are necessary before the integration step can begin. As such, it will be necessary to solve the problem of autonomous automotive systems before we begin to see fully autonomous aircraft.

VI. Concluding Remarks on Standards in the Avionics Industry

There are several factors that explain the rapid development and advancement of both autonomy technology and the certification processes in avionics when compared to automotive systems. Avionics systems are often much simpler with regard to safety certifications. An autonomous aircraft today would never have to deal with many of the challenges that prevent the growth of autonomy in cars. Challenges such as pedestrian detection or navigation of constantly changing traffic conditions are a complete non-factor as the skies of today are significantly emptier than the roads. Along a similar vein, computer vision techniques are not particularly necessary to autonomous aircraft. Radar is sufficient as a mid-to-long-range detection tool and commercial aircraft rarely come within visual distance of one another.

We must also consider the target demographic: aircraft are operated primarily by professionals and not by general consumers. This advantage allows for the rapid development observed in the USAF, as every pilot will be well aware of the systems in the machine they are piloting and should have the training to deal with any mishaps.

Finally, there is little interest in reducing the cost of avionic systems, as the relative pricing of an aircraft far outweighs the cost of any autonomous systems. At first glance, one might wonder what impact the price of the product has to do with efforts in certification. It is important to consider that aircraft are developed and produced in significantly smaller quantities than cars and that the development cycle for a single aircraft stretches across several years. As

such, we must question whether the stringent development process imposed by the standards discussed here can be made to fit the processes of automotive development.

Still, there are lessons to be learned from the successes in the avionics industries. The SAE and RTCA standards discussed in this paper present a proven model for analysis and certification of software in safety-critical systems that could easily be extended to the automotive industry. While additional work will certainly be necessary to account for the prevalence of probabilistic computer vision technologies in SSA methods, the avionics model already includes at least one technique for dealing with systems of random behavior and ambiguous dependence. It seems that the avionics model, while not a perfect fit for the problems we hope to address, can be adapted into a strong foundation for regulation and certification of automotive technologies.

VII. Formal Methods in Certification

Traditionally, verification of safety critical system behavior has been approached with black box testing, or observing different inputs and outputs of a system without analyzing internal behavior. Black box testing becomes less practical, however, as hardware systems and software become more complex. The addition of new features within safety critical systems introduces new sources of interference between components and adds the potential for more bugs that affect smaller percentages of runtime scenarios. Testers must analyze system behavior in a sufficient number of scenarios to make safety claims regarding the behavior of systems in any scenario. However, as the number of scenarios increases, what qualifies as a “sufficient” number of tests becomes intractable.

To handle this problem, verification has slowly shifted towards formal logic techniques for verification. In some cases, these simplify the process for exhaustive state simulating. In

other cases, they remove the need to analyze states individually. To give the reader an idea of how formal methods are influencing certification, we describe examples of formal method use in avionics certification and verification, as well as proposed formal method techniques in a broader range of safety critical systems.

Formal methods in avionics certification

To understand how formal methods can be integrated into certification processes, we consider case studies for formal methods used to meet DO-178C requirements for a flight guidance system (FGS). These case studies were presented in a two hundred page report provided by NASA [10]. The three studies in the report show how three categories of formal methods were used to certify three different components of the FGS system. Here, we will describe the common concerns for certification that occur in all of these case studies. More case-specific information regarding the formal methods used and the exact properties verified can be found in the full NASA report.

FGS overview

Figure 2 provides the structure of the flight guidance system in question. The system consists of two concurrently running channels (for redundancy backup) labeled FGS_R and FGS_L. Each channel receives data regarding the plane's state (elevation, heading, etc.) from a separate AHRS (attitude heading reference system), FMS (flight management system), and other sources. From this data, each channel uses a separate set of "Control Laws" that examine the current and desired state of flight, and determine what commands are needed to reach the desired state. The desired state is determined by the Mode Logic units. The resulting information is then outputted

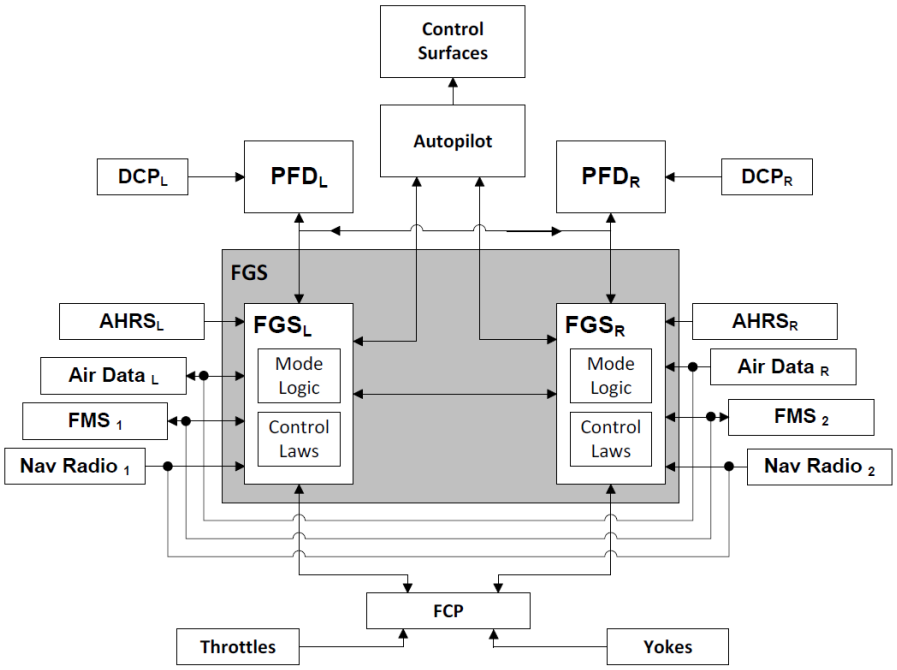


Figure 2: Flight control guidance system

to the autopilot system, the primary flight display (PFD), and the flight control panel (FCP). For more information on the input/output data of the FGS, and related components listed in the figure, see [10] for details.

Design requirements

Figure 3 shows the design process specifications provided by DO-178C for software of the highest criticality. Through the development process, high level requirements of an avionics software system are refined to low level requirements, which are then used to develop the final source code for the system. At each step, several forms of verification are required. For instance, certification requires that low level requirements are proven to meet high-level requirements, and source code is proven to meet low level requirements. In Figure 3, the dotted lines for test activity specify what are usual empirical verification steps (i.e. black box testing, for instance).

These are steps that can potentially be modified with formal analysis rather than black box testing.

The case study report considers additional ways in which formal methods can be applied at other verification steps. In the case of the flight guidance system, the following formal method uses are discussed in the report:

- Theorem proving techniques to ensure high level synchronization requirements between channels;
- Model checking techniques to verify correctness of mode logic for a single channel;
- Abstract interpretation to verify correctness of control law source code.

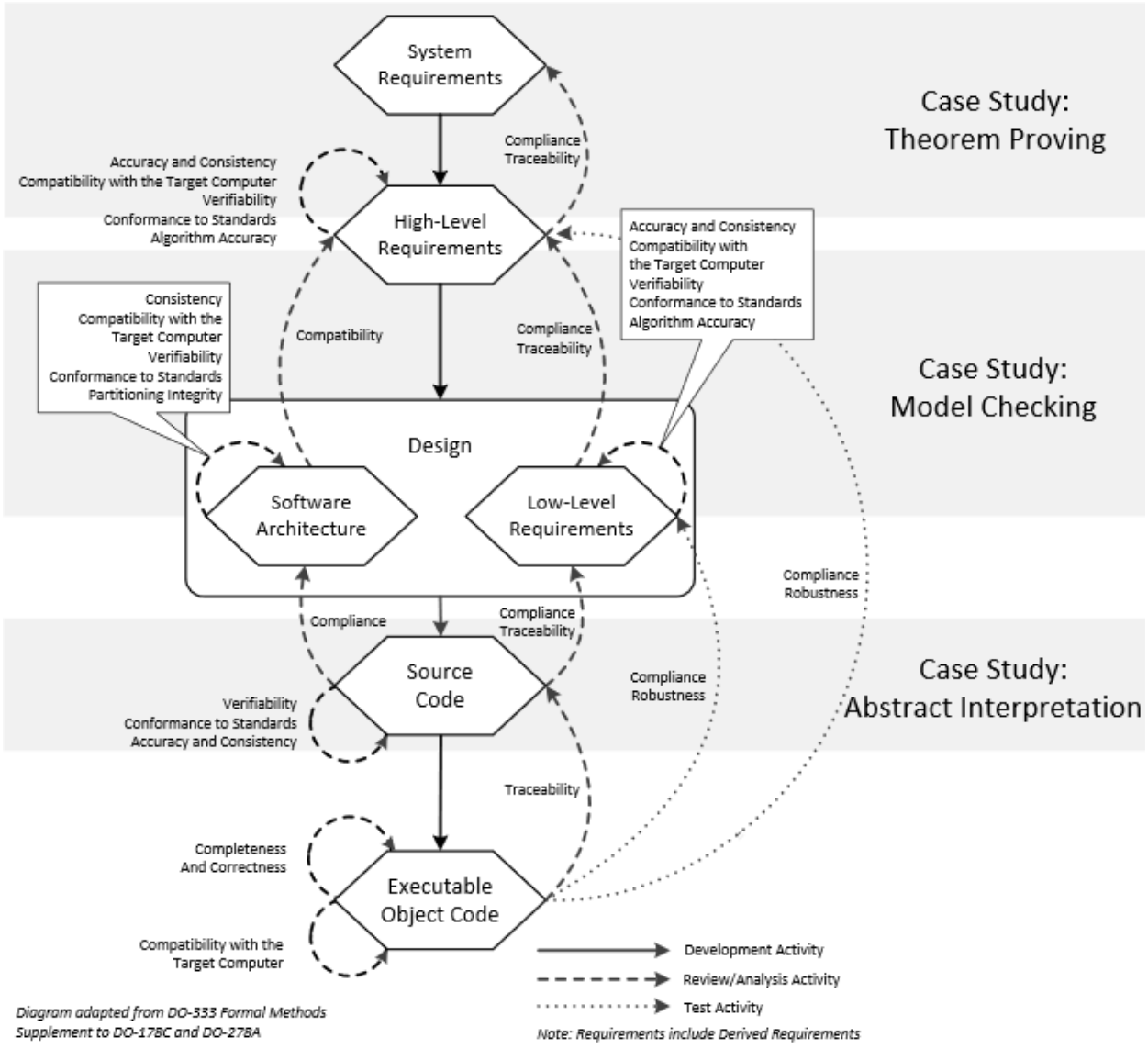


Figure 3: Design process for highest criticality software in DO-178C

TQL (tool qualification level)

Not all formal verifications require a full "by-hand" process of analysis. In fact, some if not all of the proof process may be automated by verification software. While this simplifies the direct requirements for certification, it adds more indirect requirements, in that the verification tools used must also have reliability assurances. According to DO-178C, a tool requires qualification if it eliminates, reduces, or automates certification processes, and its output is used

without verification. The qualification used must ensure that the results of using the tool are as reliable as the original processes that are eliminated, reduced, or automated.

Tool qualification is determined according to DO-333 (*Software Tool Qualification Considerations*) specifications. DO-333 gives five different Tool Qualification Levels (TQLs). Each level defines the activities needed to qualify the tool for the level. In addition, DO-333 provides three criteria for categorizing tool uses to determine what TQL a tool needs:

- **Criteria 1:** The tool's output will become a part of the avionics software.
- **Criteria 2:** The tool is used to justify *another* tool's elimination or reduction of a verification process, and the tool automates part of its verification for the other tool, and thus could miss an error.
- **Criteria 3:** A tool that directly automates a verification process of the avionics systems.

These three criteria and the criticality level of the avionics software are used to determine the TQL of the automating tool.

Extensions of DO-178C requirements list for formal methods

DO-178C has a list of objectives that must be met at each criticality level. In Table 6, provided in the report, the first seven objectives listed are standard 178C objectives. The report includes explanations of how theorem provers were used to meet several of these objectives. The last four objectives are DO-333 objectives required to justify the formal methods used. Among other reasons, these latter objectives are used to ensure that

Objective	Description	A	B	C	D	Notes
A-3.1	High-level requirements comply with system requirements.	■	■	■	■	Established by proof the system requirements are implemented by the high-level requirements and the system architecture.
A-3.2	High-level requirements are accurate and consistent.	■	■	■	■	Accuracy is established by formalization of the high-level requirements. Consistency is established by proving the absence of logical conflicts.
A-3.3	High-level requirements are compatible with target computer.					Not addressed
A-3.4	High-level requirements are verifiable.	■	■	■		Established by formalizing the requirements and completion of the proof.
A-3.5	High-level requirements conform to standards.	□	□	□		Partially established by specifying the high-level requirements as formal properties.
A-3.6	High-level requirements are traceable to system requirements.	■	■	■	■	Established by verification of the system requirements, and by demonstrating the necessity of each high-level requirement for satisfying some system requirement.
A-3.7	Algorithms are accurate.	■	■	■		Correctness of the pilot flying selection logic is established by proof.
FM.A-3.8	Formal analysis cases and procedures are correct.	■	■	■		Established by review.
FM.A-3.9	Formal analysis results are correct and discrepancies explained.	■	■	■		Established by review.
FM.A-3.10	Requirements formalization is correct.	■	■	■		Established by review.
FM.A-3.11	Formal method is correctly defined, justified, and appropriate.	■	■	■	■	Established by review.

■ *Full credit claimed* □ *Partial credit claimed* *Satisfaction of objective is at applicant's discretion*

Table 6. Summary of objectives satisfied by theorem proving

- The formal models into which avionic system components are translated conservatively model the components, and any additional properties added to the avionics system in the formal model do not violate this conservatism.
- The formal statements into which informal requirements are translated is also conservative.
- No lemmas or theories used in the formal process are left unproven.
- All notation is precise and unambiguous.

Some DO-333 objectives are met by meeting related requirements in DO-178C. Other objectives are related to the soundness of the software tools and are often met by citing research papers that analyze the soundness of the tools in question.

Summary

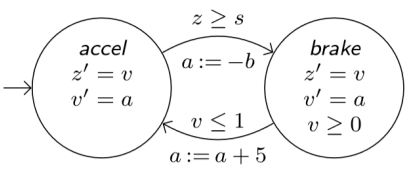
A broad range of formal methods may apply to certification of safety critical systems, as shown in the avionics case studies. There are no hard restrictions on the degree of automation. However, all forms of formal verification and automation must be justified by meeting additional objectives to the certification process. DO-178C and DO-333 do not give any guidance overall as to what types of formal methods or software to use. System designers can benefit from this lack of guidance though, since they have ample freedom in how to approach the certification process.

VI. Hybrid Systems and Future Verification Techniques

Currently, outside the realm of avionics, there is limited discussion of formal methods for certification. Certification for non-avionics industries is generally less restricted. However, researchers are extending and automating formal methods for algorithms used in many safety critical systems. This research is motivated by the likelihood that certification techniques for many safety-critical systems will transition towards formal methods as systems become increasingly complex.

To give an idea of what challenges are considered in this realm of research, we will discuss the research of David Platzer [11]. Platzer has performed a considerable amount of work examining *differential dynamic logic* (dL) and its application to *hybrid systems*. Such systems exhibit behavior that must be described in both discrete and continuous domains. Many safety-

critical cyberphysical systems are hybrid. dL provides semantics for describing combinations of discrete and continuous behaviors formally and ways to formally state safety requirements for these systems. In addition, Platzer has developed a software tool, KeYMaera, for verifying safety requirements as defined with dL. Below, we discuss how dL models hybrid systems and some of the advantages of dL models over alternative models, as described in [11].



(a)

$$
\begin{aligned}
& q := accel; \qquad /* \ initial \ mode \ is \ node \ accel \ */ \\
& \big(\quad (?q = accel; \quad z' = v, v' = a) \\
& \cup \ (?q = accel \wedge z \geq s; \quad a := -b; \quad q := brake; \quad ?v \geq 0) \\
& \cup \ (?q = brake; \quad z' = v, v' = a \,\&\, v \geq 0) \\
& \cup \ (?q = brake \wedge v \leq 1; \quad a := a + 5; \quad q := accel)\big)^*
\end{aligned}
$$

(b)

Figure 4: Different models for an extremely simplified train control system in [11].

Modeling hybrid systems

To give an example of what behavior must be modeled in a hybrid system, consider Figure 4(a). This is a *hybrid automata* for a train control system, presented in [11]. Hybrid automata are similar to finite state automata. However, finite state automata are only used to modeling discrete changes in systems. Figure 4(a) is a simplified model of the behavior for a train control system in regards to breaking and accelerating. This system is described by a discrete parameter, a, representing the acceleration of the train, controlled by system software. While the software discretely changes this state parameter ($a := -B$ on breaking, etc.), how we determine when to make these discrete changes may be dependent on the position, z, of the train, and the velocity, v. These are continuous properties whose continuous transitioning must be described in between discrete state changes. Here, the continuous transitions are described in nodes ($z' = v$ and $v' = a$). Each edge represents discrete changes. Below each edge, the discrete

changes are described, and above each edge, the conditions under which those discrete changes occur is given (the top edge, for instance, indicates the system brakes ($a := -b$) when the position z passes a certain point s ($z \geq s$).

Safety for hybrid automata (or any other hybrid model) requires a different approach to property verification than finite-state automata. While finite-state system properties can be verified by exhaustively searching for all potential states (a technique used in model-checking), hybrid automata have an infinite number of potential states due to continuous domains. Model checking for hybrid automata requires approximate discretizations of continuous parameters. Since any resulting state search for discrete values is, then, not exhaustive for the continuous state, discretization is more useful for verifying what properties do NOT hold for a machine, rather than what properties do hold.

dL provides new ways to handle verification using *hybrid programs*. The hybrid program for the train control system is shown in Figure 4(b). Rather than specifying modes using nodes, the mode is specified by q. The program is represented by the union of four possible transitions (two for the continuous transitions shown in nodes in the original graph, and two for the transitions on edges). Expressions beginning with ? represent conditions required for a certain transition to hold. For example, on the last line $?q = brake \wedge v \leq 1$ indicates that the system must be in break mode and have at most a velocity of 1 for the acceleration to be increased by 5 and the system to switches to *accel mode* ($a := a + 5; q := accel$).

To verify complex properties for complex systems without exhaustive state testing, we generally need some way to simplify the problem, and verify "incrementally." Here, we can do so if we have a means to decompose our safety requirements or the components of our system, such that we verify properties for each component in isolation. In hybrid automata, the

components are interdependent (nodes are connected by edged), thus making property verification for components in isolation difficult. dL does not have this problem, and thus can use *Compositional Verification* (verifying individual parts to verify the whole.)

Summary of formal methods

The formal semantics and proof techniques of dL are the foundation of analysis in Platzer's verification tool KeYMaera. KeYMaera has been used to verify safety properties for several complex safety critical systems, such as train control systems, traffic control systems, and adaptive cruise control algorithms [12][13][14][15]. Here, we have given a brief overview of the basics of dL and how it assists in the verification process. More information regarding KeYMaera, dL, and its applications can be found at *http://symbolaris.com/info/KeYmaera.html*.

VII. Conclusions

Existing standards in the automotive industry are not sufficient for addressing problems arising from vehicles becoming more autonomous. Significant new legislation or adaptation must be introduced before these new technologies are safe for mass production and consumer use. However, regulatory bodies are aware of these concerns and have taken steps to initiate conversations to solve such shortcomings of the current state of the art.

Standards in the avionics industry do not exactly translate perfectly to the automotive realm. Despite this, they still provide important lessons to take in to consideration when developing standards for vehicles. This influence has already been felt with the introduction of laws mandating electronic stability control in cars, which bear resemblance to laws mandating and regulating "X-by-wire" systems.

Formal methods in testing can also be integrated into the certification process. As autonomous technology adds complexity to existing systems, testing for compliance increases in difficulty. With formal methods, new testing procedures could be introduced to ensure consumer safety and manufacturer compliance.

The NHTSA in the United States has taken a front seat to ensuring the safe introduction of these technologies and states should heed the recommendations set forth in their preliminary statement. With the automotive industry poised for a technical revolution, states should heed the NHTSA's recommendations to maintain consumer safety as a top priority.

References

[1] Checkoway, S., et. al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces". *National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration.* 2011. Web.

[2] Markey, E. "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk". 2015. Web.

[3] Pagliery, J. "Automakers don't protect you enough from car hackers, senator says". *CNNMoney.* 9 Feb., 2015.

[4] Greenberg, A. "Senate Report Slams Automakers for Leaving Cars Vulnerable to Hackers". *Wired Magazine.* 2 Feb., 2015.

[5] "Preliminary Statement of Policy Concerning Automated Vehicles". *National Highway Traffic Safety Administration*. N.d. Web.

[6] FAA, "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap", 2013

[7] L. Humphrey, "Certification and Design Challenges for Autonomous Systems", 2014

[8] M.S. Reddy, "The Impact of RTCA DO-178C on Software Development", Cognizant 20-20 insights, 2012

[9] SAE, "ARP4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," 1996.

[10] Cofer, D., Miller, S. "Formal Methods Case Studies for DO-333". 2014. Web. <http://shemesh.larc.nasa.gov/people/bld/ftp/NASA-CR-2014-218244.pdf>

[11] Platzer, A. "Differential Dynamic Logic for Hybrid Systems". *Journal for Automated Reasoning*. 2008. pp 143-189

[12] Platzer, A., Quesel, J. "European Train Control System: A case study in formal verification". *11th International Conference on Formal Engineering Methods, ICFEM, Rio de Janeiro, Brasil, Proceedings*, volume 5885 of *LNCS*, pages 246-265. Springer, 2009.

[13] Loos, S., Platzer, A., Nistor, L. “Adaptive cruise control: Hybrid, distributed, and now formally verified”. *17th International Symposium on Formal Methods, FM, Limerick, Ireland, Proceedings*, volume 6664 of *LNCS*, pages 42-56. Springer, 2011.

[14] Loos, S., Platzer, A. “Safe intersections: At the crossing of hybrid systems and verification”. *14th International IEEE Conference on Intelligent Transportation Systems, ITSC'11, Washington, DC, USA, Proceedings*, pages 1181-1186. 2011.

[15] Kouskoulas, Y., Renshaw, D., Platzer, A., Kazanzides, P. “Certifying the safe design of a virtual fixture control algorithm for a surgical robot”. *Hybrid Systems: Computation and Control (part of CPS Week 2013), HSCC'13, Philadelphia, PA, USA, Apr. 8-13, 2013*, pages 263-272. ACM, 2013.

[16] “Quick Reference Guide to Federal Motor Vehicle Safety Standards and Regulations”. *U.S. Department of Transportation.* Feb. 2011. Web.

[17] “An Introduction to Functional Safety and IEC 61508”, Application Note, MTL Instruments Group, 2002.

[18] “IEC 61508 Overview Report”, *Exida*, Jan. 2006. Web.

[19] IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, 2000.

[20] F. Redmill, “IEC 61508: Principles and Use in the Management of Safety”, *Computing and Control Engineering Journal*, vol. 9, issue. 5, pp. 205 – 213, 1998.

[21] ISO 26262-1:2011 Road Vehicles – Functional Safety, International Standardization Organization, 2011.

[22] D. Wanner, A. Stensson Trigell, L. Drugge, and J. Jerrelind, “Survey on fault-tolerant vehicle design”, *26th Electric Vehicle Symposium, Los Angeles, CA*, *Proceedings*, May 2012.

[23] UNECE, “DRAFT ESC GTR Version 5”, 2008.

[24] UNECE, “Regulation No. 79 – Amend. 78 – Rev. 2”, 2006.

[25] P. Jakobsen, “Proposal for amendment of ECE R13: Improved HGV brake compatibility”, *72nd GRRF*, Feb. 2012.

[26] "AUTOSAR: Home." Home : AUTOSAR. Web. 4 May 2015. <http://www.autosar.org/>.

[27] RTCA, "DO-178C - Software Considerations in Airborne Systems and Equipment Certification," 2011

[28] SAE, “ARP4754 – Guidelines For Development of Civil Aircraft and Systems,” 2010.