Learning from the Skies - An Analogy Based Approach to Understanding how to Improve Autonomous Vehicle Software Regulations by Looking at the Aviation Industry

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia - Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Garrett Burroughs

Fall 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

“Discovering the unexpected is more important than confirming the known.” – George E. P. Box

Introduction

When we use software that has the potential to have an effect on our safety, there is an expectation that the software has been rigorously tested, and that there is some level of guarantee that the software will not malfunction and cause harm to those using it. In regards to an industry like aviation, the Federal Aviation Administration bears the responsibility of certifying aircraft (Kennedy & Towhidnejad, 2017). While the aviation industry does not have a flawless track record, it has been able to maintain a very low fatal crash rate with only 1.049 accidents per 100,000 flight hours yielding a fatal crash reported in 2020 (NTSB, 2021). The aviation industry also has a very mature ecosystem of automated tools to assist with operation with the first form of an autopilot system being introduced in 1917. While the aviation industry can’t be taken blindly as the pinnacle of safety regulation, it has a long and successful history with much to learn from.

In contrast, in regard to the automated vehicle (AV) industry, there is a stark lack of comprehensive regulations for certifying software to be used in the control of AVs. Analogous to the FAA, the National Highway Transportation and Safety Administration (NHTSA) is the regulatory entity that is currently in charge of imposing regulations on the autonomous vehicle industry. In their own words “Many companies today test vehicles with higher levels of automation to ensure that they operate as intended, but many experts indicate that more work remains to be done by developers to ensure their safe operation before they are available for consumers to purchase.” (NHTSA, n.d) Moving forward the NHTSA is also expecting, and supporting, a continued shift towards more automated control systems, with the hope of having

fully autonomous vehicles . A breakdown of how this shift has already been happening can be seen in figure 1, taken from a 2023 report from the world economic forum.

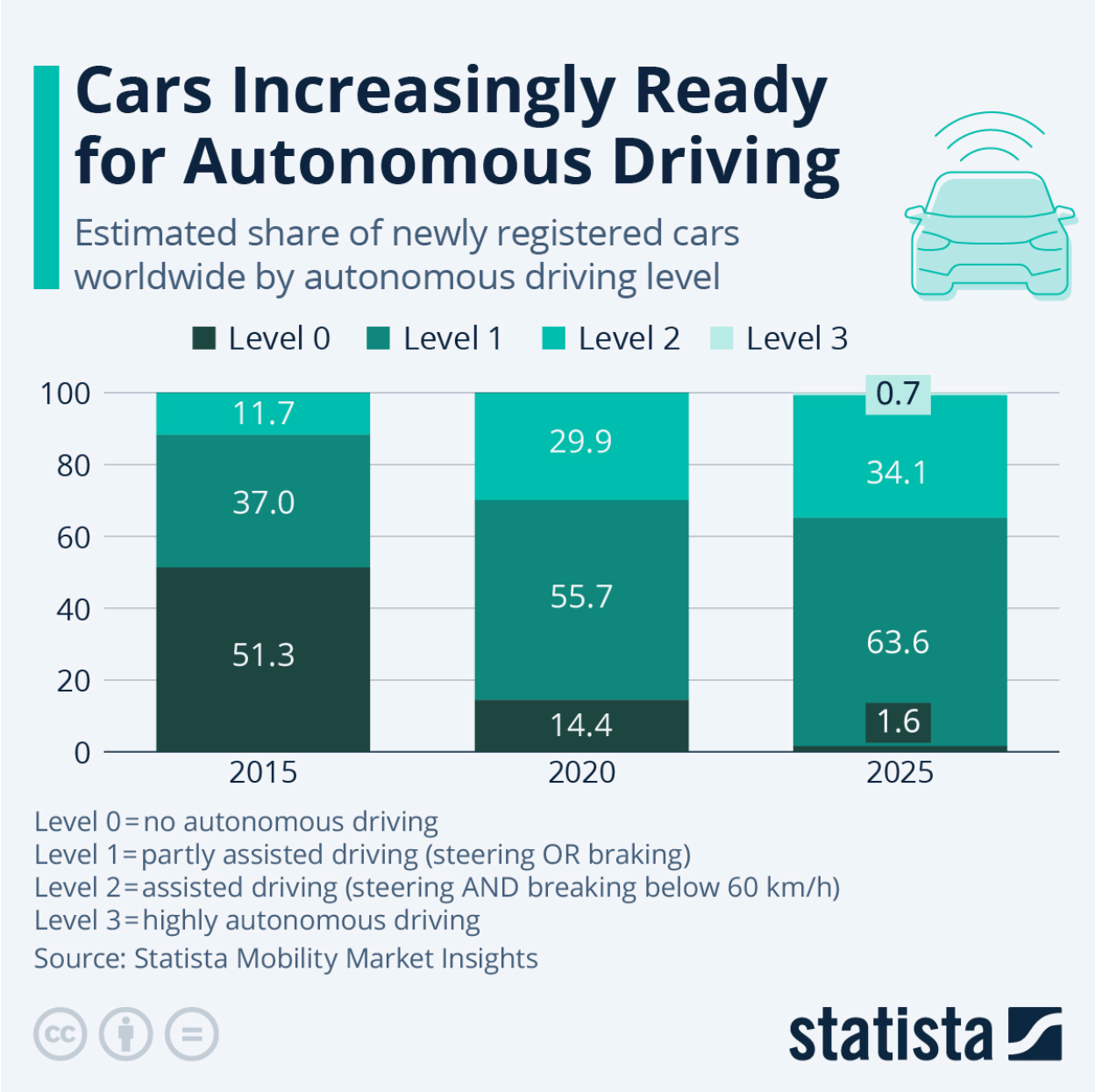

Figure 1. Trend of the breakdown of automated driving systems from 2015 to 2025 (projected). The level of autonomous features has grown significantly from 2015 and doesn't show signs of stopping, with very few cars having no autonomous features currently. (Buchholz, 2023)

With this trend, it is essential that regulations continue to be developed within the AV industry to help support safer

Within this paper, I analyze how the Aviation industry relates to the autonomous vehicle industry through Schwarz-Plaschg's approach of leveraging analogies for imagining and governing emerging technologies. By taking a look at how the aviation industry has handled similar challenges to those that the AV industry faces, I discover key insights into why the disparity exists, how we can go about changing it, and what the future for AV regulations could look like. Throughout the analysis of both aviation and autonomous vehicle sociotechnical systems, I have concluded that the main disparity between the industries comes from the differences in how the systems are viewed, as well as a narrower approach to verification within AV software as compared to aviation software.

Problem Definition - Autonomous Vehicle Regulations are Lagging Far Behind

The aviation industry has long recognized the necessity of formal software verification and testing, particularly through the implementation of the DO-178C standard. This regulatory framework mandates comprehensive testing, validation, and certification for all safety-critical software used in aircraft (RTCA, 2011). Despite some controversy about the document's requirements, its release has brought about a measurable improvement within the airworthiness of aviation software (Youn et al., 2015, p. 4). However, as evidenced by the Boeing 737 Max disaster, even such rigorous frameworks can fail when regulatory oversight is compromised or incomplete (Majority Staff, 2020). This failure highlights the importance of continuous regulation and oversight throughout the entire software lifecycle, a lesson that is crucial for

industries like autonomous vehicles, where software plays an equally critical role in safety. Even with the very strong guidelines that were implemented by the FAA, there were still gaps that existed that allowed for catastrophic failure on two different occasions. There is always more work that can be done to make regulations more comprehensive and improve the reliability of safety critical systems.

In contrast, the AV industry is still in its early stages of regulatory development. In a 2020 literature review, Wishart (2020) compiled 33 different standards from across the AV space, taking a look at private and public standards. Within this review, Wishart noted that the field of verification and validation (V&V) is very mature, and there have been many improvements with software V&V within the AV sphere. Wishart also noted how vast and varied the different verification modes are, often only covering a small portion of safety considerations. Despite there being solid research into verification of software systems in autonomous vehicles, the NHTSA has only issued weak guidelines that are unenforceable and are very broad in scope, telling companies where they should focus rather than enforcing compliance. (Claybrook, 2018, p. 36)

Lack of regulation within the AV industry is also not due to lack of issue. With there being 4 different deaths attributed to autonomous vehicles in 2018, there was still a lack of any movement from congress (Canis, 2019). Cains (2019) discusses many of the reasons legislation was facing pushback was due to issues regarding the creation of a new entity, public testing policies, cybersecurity legislation, and data concerns. While these concerns are valid, and should be taken into consideration, they do not completely block any form of legislation being passed. This failure to progress on AV regulatory legislation indicates that there is a lack of urgency that is not seen in other safety critical areas such as the aviation industry.

To explore both why this discrepancy exists, as well as gain insight as to how it might be remedied, this research examines existing guidelines from both aviation and automotive regulatory bodies. It also compares these guidelines to identify commonalities and differences in the safety challenges each industry faces. While the aviation industry provides a potential model for the AV industry, the differences between airborne and ground-based systems must also be considered to understand how issues translate. By analyzing these differences and investigating how regulatory frameworks can be tailored to meet the specific needs of AVs, this research aims to provide a better understanding of the disparities that exist, and use that understanding to provide insights into what aspects should be considered as the regulatory landscape moves forward.

Research Approach - Using analogies to bridge the gap

With software use for automation in the aviation industry being more mature than that in the AV industry, the aviation industry serves as a good candidate to draw insight from. This paper leverages the approach of Claudia Schwarz-Plaschg, in her paper "The Power of Analogies for Imagining and Governing Emerging Technologies". The analogies are used to both identify key areas that should be looked at more closely within the AV industry as well as to understand how those areas might be improved.

Analogical Imagination

Schwarz-Plaschg provides a well argued approach as to why analogies are quite powerful when it comes to their ability to "explore and anticipate the development and societal implications of emerging technologies" (Schwarz-Plaschg, 2018, p.140). The article mainly focuses on the field of nano-technology, and how, by drawing on analogies created from many other sociotechnical systems, "actors can draw lessons from the past for the future, which is

simply not possible by only looking at the future" (2018, p. 143). The article provides specific examples of creating analogies from existing technological artifacts to demonstrate how they can provide better insights into the field of nano-technology. For example, the field of medicine is used to create an analogy of how nanofood might be regulated, in which the regulation of nanofood should be as strictly regulated as medicine (2018, p. 142). These examples illustrate how innovative perspectives can arise from the analysis of existing systems. An example of how these analogies can provide insight can be seen in figure 2 taken from Schwarz-Plaschg's paper on analogies.

Table 1 Analogies in a public engagement setting on nanofood

Analogy with	Issue	Line of discussion and argumentation
Nuclear energy	Mistrust in expert opinions	Reference to the debate about nuclear energy in the 1970s and how experts made inconsistent predictions concerning the decomposition of radioactive material
GM food	Consumer sovereignty	Critique of how genetically modified (GM) foods were sold ("it is good for you"); argument that such promises would also not be acceptable with nanotechnology
Asbestos	Risk anticipation and regulation	Long-term consequences were unknown with asbestos and it could be similar with nanotechnology; demands for regulation
Medicine	Regulation	Nanotechnology should be as strictly regulated as medicine
GM food	Industry benefits	Comparison with GM food to argue that only producers will benefit from nanotechnology
Functional food	Societal acceptance	Not only discussion of potential consumer benefits of nanofood but also questioning of the promised benefits as "just marketing"; the analogy also suggested that nanofood might sell as well as existing functional food products
GM food	Societal acceptance and labelling	If nanofood were labelled like GM food, it would not be accepted by consumers
Mobile phones	Risk anticipation and societal acceptance	With certain new technologies (mobile phones), long-term risks are not properly studied; distinction between nanotechnological domains: in some (e.g. electronics), nanotechnology is more acceptable than in others (e.g. food)
X-rays	Hypes and risk anticipation	X-rays as an example for a new technology that was hyped and entailed collateral damage
GM food	Labelling and regulation	GM food labelling shows that regulation has flaws; if it were analogous with nanotechnology, regulation would be meaningless
GM food	Societal rejection	The GM food case illustrates the possibility of a similar societal rejection of nanofood

Figure 2. Analogies in public engagement setting on nanofood. Despite the industries having significant differences, key insights from past issues can provide value to emerging industries. (Schwarz-Plaschg, 2018, p. 142)

Analogies as Argumentation

Schwarz-Plaschg also recognizes the idea that analogies are imperfect, and may be misleading if taken at face value. Analogies can hold strong value in argumentation, and persuasion, which can be beneficial when it comes to acceptance or progression of important concerns within a system, however, they can also "create specific understandings of reality by establishing similarities and simultaneously shielding them against potential counter-arguments" (2018, p 144). Because of this ability to shield from potential counter-arguments, it is important to approach analogies as "strategic devices" (2018, p. 144). While they may not always uncover the truth of the situation, they provide valuable insights as to what is worth looking at in the system.

Schwarz-Plaschg uses several examples of analogies being used within debates on the use of nanotechnologies. One particular example goes into the "asbestos-nano" analogy, where the similarities of carbon nanotubes and asbestos fibers are brought up as a health concern that might exist within nanotechnology. If taken at face value, this analogy indicates that nanoparticles could turn "equally harmful in the future" (2018, p. 145). While there ended up not being much scientific evidence for this harm, this analogy did encourage further examination of the health and environmental effects of nanoparticles. (2018, p. 145). This example illustrates how even with the analogy not being a complete one to one mapping, it still helped uncover an area of nanotechnology that had not been focused on sufficiently previously.

Application of Analogies to Autonomous Vehicle Regulations

As seen, analogies can be very useful for both gaining insight into how a new sociotechnical system might proceed, as well as for highlighting important features of the system that might need further investigation or development. For these reasons, this approach seems especially promising for analyzing the development of regulations within the context of

Autonomous Vehicles. The primary area to draw analogies from is that of the Aviation industry. The aviation industry can provide many valuable analogies such as how to provide thorough regulation while still allowing for innovation to exist. The aviation industry can also provide analogies giving insight into things like understanding the role of public opinion and trust exist in a widely used and safety critical system. The very robust guidelines that exist within the DO-178C can provide an example as to what factors need to be considered when constructing a comprehensive set of guidelines for control systems in safety critical situations. The 737 MAX disaster can provide insight into what happens when those regulations fail, and how to navigate interactions between regulatory authorities, companies, and the public. Drawing analogies from these well documented artifacts allows for a better understanding of considerations that need to exist within the development of regulations within the AV industry.

In order to perform this research, I list out a number of issues that currently exist within the regulatory framework of the AV industry. Once these issues have been identified, I then select an analogous reference for these issues, and provide relevant insights gained from those analogies. To form each analogy, I look at the relevant contexts of the issue from the source industry, and then identify the key insights that can be used to draw the analogy. After the analogy is drawn, a comparison to the target industry can be made, where industry specific context can be taken into account to gain new insights. An overview of this approach can be seen in figure 3.

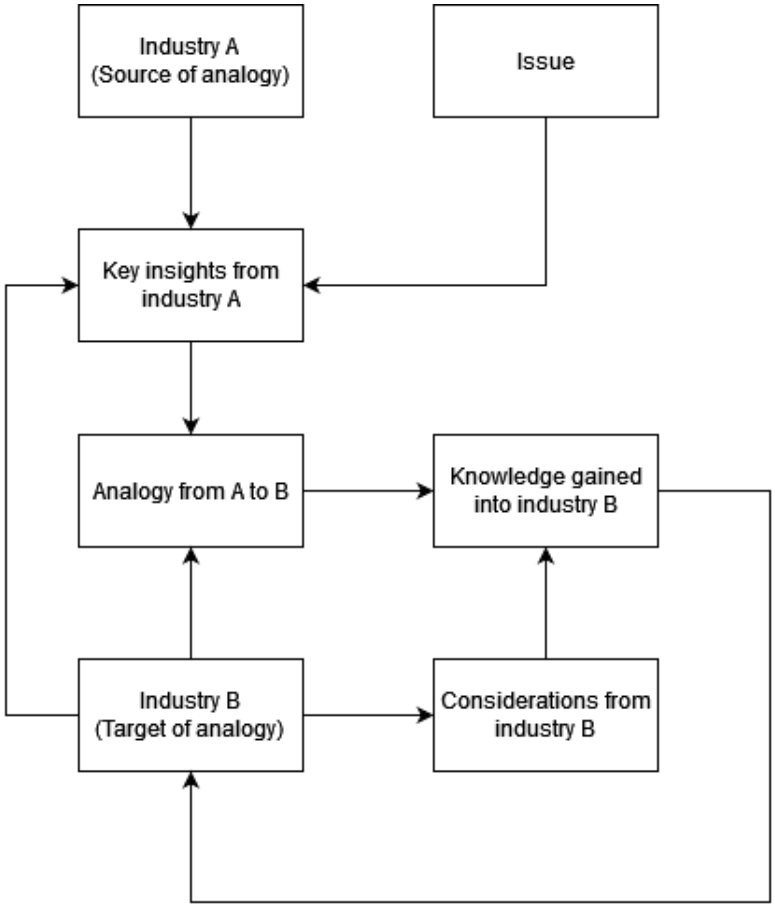

Figure 3. An overview of the process to draw imaginative analogies from one industry to another. By drawing on analogies created from the source industry while also considering context of the target industry, new insights can emerge (Created by Author)

Schwarz-Plaschg's approach provides a framework for gaining knowledge in emerging systems by analyzing previous events. Within the context of this problem, this approach has the potential to uncover areas of interest and innovative concepts within the area of AV regulations by drawing from the aviation industry and other regulatory successes and failures.

Results - Understanding how the aviation industry has handled key issues that parallel AVs

Looking into how the aviation industry has previously handled some of the main issues that the AV industry is currently facing can provide insight into how the AV industry might

proceed in the future. The main issues identified are disjoint regulations, public trust and accountability. A high level outline of the analogies drawn can be seen in table 1.

Issue	**Analogous Industry**	**Analogy**
Public Trust	Aviation	The aviation industry has a much lower tolerance for catastrophic failures within the system
Disjoint Regulations	Aviation	The aviation industry relies on DO-178C as its primary source of truth
Accountability	Aviation	The aviation industry provides strong third party review of companies to ensure they are following guidelines

Table 1. Analogies drawn from three key issues within the AV industry by analyzing the aviation industry (created by author)

I. Public Trust - Autonomous vehicles are viewed as harm reduction

The response to failures within the AV space seem to prompt much less legislative action when compared to the aviation industry. This is likely, in part, due to autonomous vehicle technology being viewed as a form of harm reduction, rather than as a safety critical system. Despite having multiple recorded deaths due to autonomous vehicles, including a death from an autonomous uber and the death of 3 tesla drivers in 2018, legislation that encouraged the development and testing of autonomous vehicles faced controversy in congress (Canis, 2019). While the death toll remains small at this time, it is also important to consider that the number of autonomous vehicles on the road currently is rather small, with only about a projected 26,000 units being created in 2024, compared to the 288 million vehicles on the road. Contrasted with

the Boeing 737 Max disaster, where two planes failed resulting in the death of 346 people, which launched a large-scale investigation conducted by the house committee on transportation and infrastructure (Majority Staff, 2020).

In terms of discourse about AVs, one of the primary reasons for introducing autonomous vehicles is to reduce the large number of fatalities incurred by human error, with there being an estimated 37,133 automotive fatalities in 2017 (Canis, 2019). The main page regarding AV's and safety on the NHTSA's website discusses autonomous features as safety mechanisms in themselves, rather than talking about the safety of the software. Figure 4 shows a graphic that is on the NHTSAs website as of november 2024 talking about the "Five Eras of Safety", which fails to comment on how the software is being made safer.

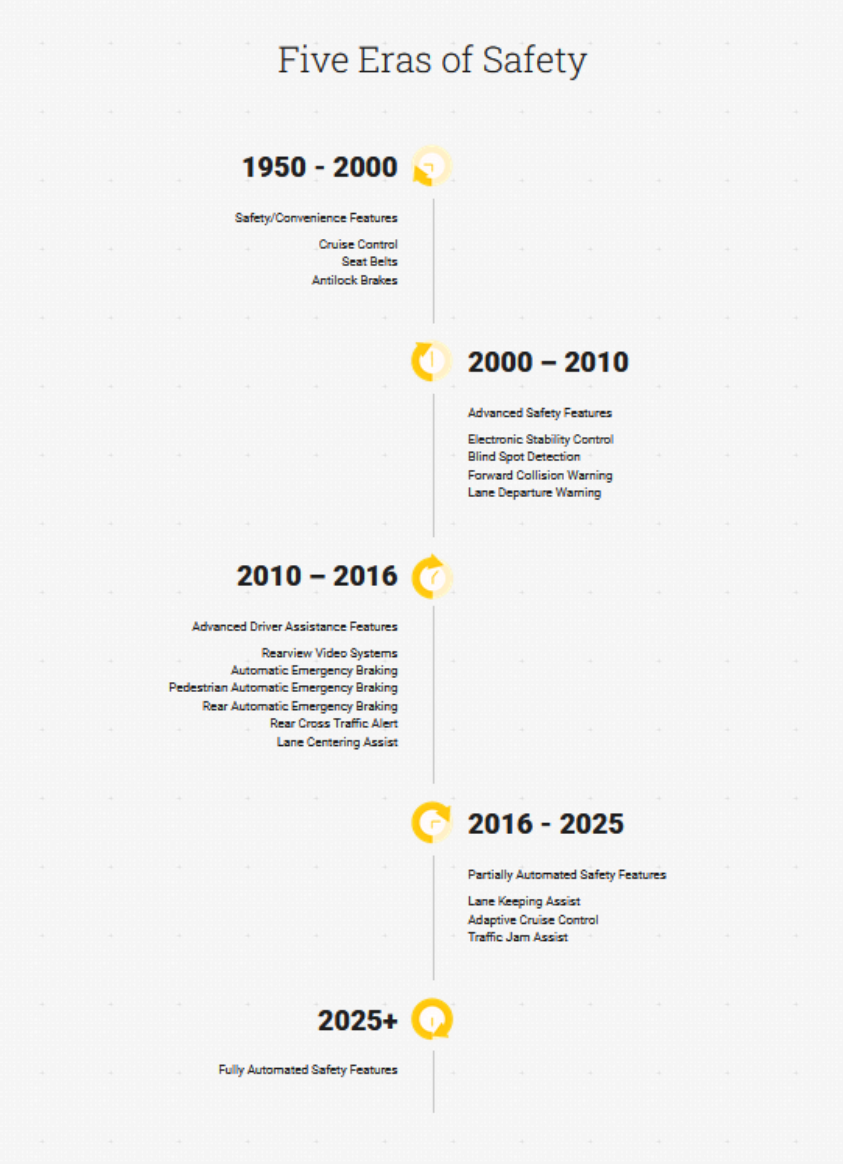

Figure 4. The "Five Eras of Safety" as outlined by the NHTSA on their website. This graphic posted on the NHTSA website illustrates that the discourse is focused on how autonomous systems can provide safety as opposed to how autonomous systems can be made safer. (NHTSA, N.D)

Treating autonomous vehicle features as a form of harm reduction, rather than a safety critical system in itself may be one cause for the lack of regulations in the industry, as well as the slower regulatory response. It is possible that even with an imperfect, and potentially dangerous

system, the AV industry will still gain favorable public and organizational opinion if it crosses the bar of being better than what currently exists.

Despite the possibility of having a weakly regulated industry gaining favorable public opinion, the AV industry should still be held to the high standard that the aviation industry is held to. As mentioned earlier, the aviation industry has very little tolerance for errors and catastrophic failures, taking action and enacting legislation in response to any failure. Despite AVs mainly being seen as a mode for harm reduction, if the industry was approached the same as the aviation industry, then there may have been safety legislation enacted in response to the fatalities that occurred in 2018. This shift in thinking about Autonomous Vehicles as a safety critical system, and therefore having a low tolerance for errors is essential in paving a path towards more robust regulations within the industry.

II. Disjoint Regulations - The need to define the AV software development life cycle

In the field of aviation, there exists DO-178, a document that lays out a comprehensive set of guidelines for writing safety critical software within the aviation industry. The first issue of this document was created in 1982, and has since been updated with 3 major versions to keep up with new developments within the industry. The latest version, DO-178C was released in 2011 (ConsuNova, Inc., n.d). While not perfect, this document aims to provide guidelines across the development process. This is not just limited to the software itself, but other "tools" that may be included in the development process, such as verification tools, developer environments, and compilers for the software (Pothon, 2012).

Dakić and Živković (2021) discuss the importance of creating a well defined Software development life cycle (SDLC), which outlines all of the different parts that go into developing

software for autonomous vehicles. The authors define the SDLC of autonomous vehicles to include the Internet of things, Continuous integration and Continuous development, security challenges, software testing, input data, and simulation. While many of these topics are outside the scope of this paper, it is able to define a starting point for what a document similar to the DO-178C might look like if developed for the AV industry. Similarly, microsoft has outlined another possible look at the development lifecycle as seen in figure 5. This view puts more of an emphasis on the data driven side of the development process.

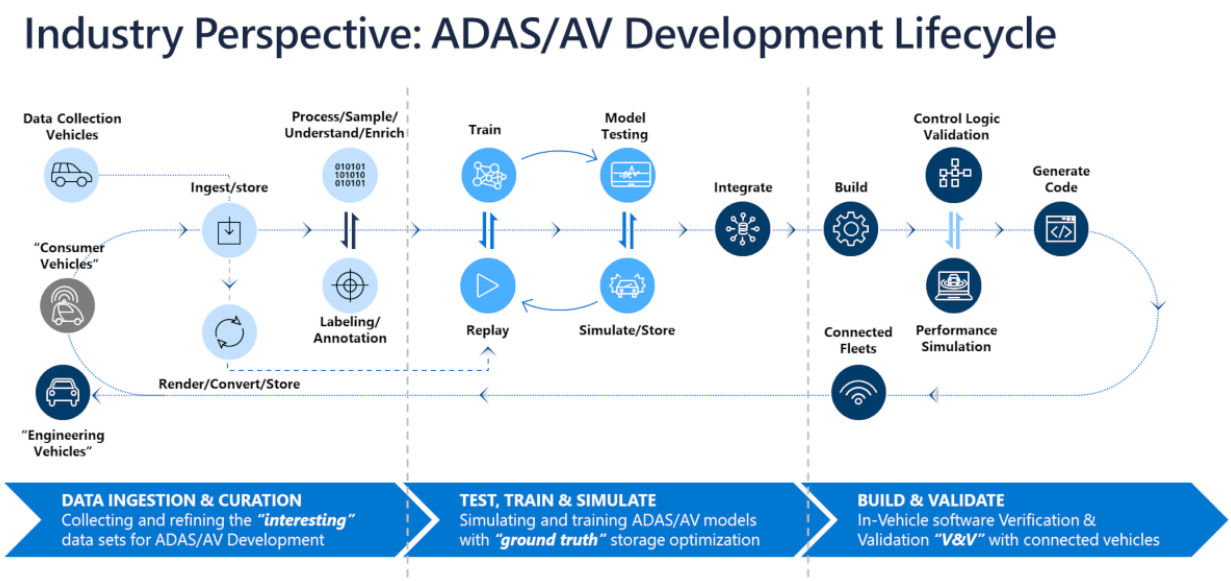

Figure 5. An autonomous vehicle software development lifecycle as defined by microsoft. This is just one definition of the software development lifecycle demonstrating that regulating AV software extends far past just regulating the code itself. (Microsoft, 2024)

While both of these views may be an incomplete picture of the SDLC as a whole, they put an emphasis on the number of complex different systems that interact in order to develop software within the AV space. Ensuring that AV systems are safe and reliable goes far beyond just verifying the code that the software is running, but also including things like ensuring sensor reliability, transmission connectivity, and all the other systems that go into play to make AVs work. Similar to what has been done in the aviation industry, it is important that the AV industry creates a well defined SDLC, as well as puts in place guidelines across the entire development lifecycle to ensure a high quality of safety throughout the system.

The importance of creating a well defined scope for regulation can also be seen with the failure of the Boeing 737 MAX. The implementation and training of the new software can be seen as one of the final portions of the software development lifecycle within aviation. The committee report (Majority Staff, 2020, p. 25) outlined that in the case of the MCAS system, a new control software was developed that altered the way that pilots controlled the plane, however, regulatory oversight allowed this system to be implemented without proper simulator training for pilots who had flown a similar type of aircraft. While in this case, there did exist some regulations that required training, and in this instance that requirement was waived due to pressures from Boeing, this example emphasizes the importance of covering all aspects of the software development process in regards to regulation. Drawing an analogy to the autonomous vehicle industry, it is possible that added training, and potentially licensure, may help drivers be better equipped to operate their vehicles and prevent catastrophic failures.

Moving forward, taking a broader look at how the software systems interact with their users, hardware, and real world will provide a better understanding of all the areas for failure and provide insight into what areas need regulatory improvement.

III. Accountability - The AV industry needs third party review

The aviation industry has a well-established framework for accountability through certifications, inspections, and regulatory oversight. The Federal Aviation Administration (FAA) and equivalent bodies worldwide ensure that any failure is traced to its source—whether in software, hardware, or procedural execution—by enforcing strict certification processes and accountability measures across all players in the industry. DO-178C, as part of this regulatory framework, defines distinct roles and responsibilities throughout the development lifecycle, from manufacturers to software developers, with each party held accountable for maintaining and verifying the safety and reliability of their contributions (ConsuNova, Inc., n.d.). If an issue arises, the specific areas of accountability are already outlined, making it clear where improvements or consequences are needed.

For autonomous vehicles (AVs), accountability remains a growing challenge. The AV industry has yet to implement a universally accepted accountability framework similar to that in aviation, leading to ambiguity in determining responsibility during accidents or failures. Unlike aviation, where responsibility chains are established through processes like the DO-178C and the FAA's mandates, the AV sector currently operates within a patchwork of standards, often varying by region or company, which makes assigning responsibility more complex. When an AV incident occurs, it is often unclear whether fault lies with the manufacturer, software developers, or even data suppliers. This lack of clarity undermines public trust and has prompted calls for an accountability structure akin to aviation's, where standardized, transparent roles and responsibilities are outlined for the entire AV lifecycle. Developing such a framework would help the AV industry address safety concerns and earn the public’s confidence, ensuring that

incidents are followed by clear investigations, corrections, and, when necessary, regulatory or legal repercussions.

Conclusion

While autonomous vehicle technology might increase driver safety, in order for the system to be a success it is still important that the systems are reliable. It is clear that as it stands, there needs to be a shift in thinking that the role of safety in autonomous vehicles has in order to create a more robust regulatory framework. This research serves to be a stepping off point, to define the areas which need to be developed more, and to guide how they might proceed.

As identified, before looking at how to develop strong regulations, the discourse first has to be changed to encourage regulations to be enacted in the first place. Aviation has seen strong regulation in the past, and yet is still a successful industry filled with innovation. If followed in its footsteps, it is possible that the AV industry can end up in the same place. After establishing a shift in discourse to encourage the need for regulation within this industry, they can then be developed by having a strong understanding of the software development lifecycle, and the different systems that need to interact to make AV software successful. With this approach, it is possible to prevent potential catastrophic, and life threatening failures, and improve the safety of AVs.

The aviation industry is very mature and equally complex. There is no doubt further lessons that can be learned from studying it in regards to developing software regulations. While it has many similarities to the AV industry, they are not the same. In applying these lessons, it is crucial to consider the differences that make the AV industry unique. While there is no one to one mapping, the aviation industry is able to point in the right direction.

References

Buchholz, Katharina. (2023). Charted: Autonomous driving is racing ahead. *World economic forum.* https://www.weforum.org/stories/2023/02/charted-autonomous-driving-accelerating-mobility/

Canis, Bill. (2019). *Issues in autonomous vehicle testing and deployment.* Congressional Research Service. [Government Report]

ConsuNova, Inc. (2024, March 31). DO-178C Explained. https://consunova.com/do-178c-explained. [company website]

Hemphill, T. A. (2020). Autonomous vehicles: U.S. regulatory policy challenges. T*echnology in Society* (61).

Kennedy, J. D., & Towhidnejad, M. (2017). Innovation and certification in aviation software. [Paper Presentation]. 2017 Integrated Communications, Navigation and Surveillance Conference (ICNS), 3D3-1-3D3-15. Herndon, VA, USA.

Leveson, N. G. (2016). *Engineering a safer world: systems thinking applied to safety*. Cambridge, MA: MIT Press.

Lin, P. (2015). *Autonomes fahren: Technische, rechtliche und gesellschaftliche aspekte*. Berlin, Heidelberg: Springer.

Majority Staff of the Committee on Transportation and Infrastructure. (2020) Executive Summary (p.p. i-33). In *The design, development & certification of the Boeing 737 MAX.* Washington, DC: Government Printing Office.

Microsoft. (2024). Reference architecture for autonomous vehicle operations - Microsoft mobility reference architecture. Microsoft Learn. [Company website]

NTSB. (2021). *U.S. Civil Aviation Fatalities and Flight Activity Decreased in 2020*. National Transportation Safety Board. https://www.ntsb.gov/news/press-releases/Pages/NR20211117.aspx. [Government Website].

NHTSA. (n.d.). *Automated Vehicles for Safety*. National Highway Traffic Safety Administration. nhtsa.gov https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety. [Government website].

Pothon, Frederic (2012). *DO-178C/ED-12C vs DO-178B/ED-12B: Changes and improvements*. Ada Core. [Company Report].

Rapita Systems. (n.d.). *Introduction to do-178*. DO178.org https://www.do178.org/do178_introduction.html. [Company website].

Schwarz-Plaschg, C. (2018). The power of analogies for imagining and governing emerging technologies *Nanoethics, 12*(2), 139-153.

Torens, C., & Adolf, F. (2015). *Using formal requirements and model-checking for verification and validation of an unmanned rotorcraft*. [Paper Presentation]. 2nd Software Challenges in Aerospace Symposium. Kissimmee, FL, USA.

Youn, W. K., Hong, S. B., Oh, K. R., & Ahn, O. S. (2015). Software certification of safety-critical avionic systems: DO-178C and its impacts. *IEEE Aerospace and Electronic Systems Magazine*, 30(4), 4–13.

Wishart et al. (2020) Literature Review of Verification and Validation Activities of Automated Driving Systems. SAE International 3(4), 267-324.