Different Degrees of Regulation for Robotics

Adam Hall[1] and Emmett Wise[1]

Abstract— **There is debate regarding the regulatory level of safety-critical robotic systems. At the moment, some safety-critical robotic industries self-regulate, which allows for unfettered innovation. Self-regulation is abnormal for safety-critical systems because people's lives are at risk. Most safety-critical systems are heavily regulated. These regulatory rules provide the public with an assurance that the product is safe. However, regulatory compliance, under heavy regulation, is expensive and time consuming, which increases the cost of innovation. In order to save money, some companies take shortcuts that can compromise older, certified systems. As a result, heavy regulation of the robotics industry will slow innovation and not ensure consumer safety. In order to protect robotic innovation, safety-critical robotics companies should be allowed to self-regulate.**

I. Introduction

Modern autonomy is slowly being folded into safety critical systems, which raises questions regarding the regulatory levels of future autonmous systems. Product regulation falls on a spectrum from self-regulation to strict regulation. Due to the proliferation of autonmous systems, there isn't a regulatory precedent for government regulators to follow. As a result, governments are allowing some autonomous safety-critical systems to self-regulate. This form of regulation enables unfettered innovation and experimentation. However, this lack of regulation can lead to dangerous products that are potentially fatal, so most safety-critical systems are heavily regulated. Regulatory compliance is time consuming and expensive, which debilitates innovation. This paper explores whether or not we can trust the current scheme of self-regulation for autonomous safety-critical systems.

II. Self-Regulation

Self-regulation facilitates rapid innovation and development. The essence of this relationship can be seen in internet based software products. In order to keep up with the ever changing social media market, platforms like Facebook, Twitter, and Snapchat are modified daily by developers. Updates to internet based software products go through an internally defined quality assurance system – a form of self-regulation. The quality assurance system does not have to meet a regulatory minimum, which allows the company to rapidly deploy new features. The ability to independently deploy features allows these companies to innovate at incredible speeds. The rapid development of such companies is a testament to how self-regulation can allow innovation to flourish.

However, unregulated rapid development is more likely to have errors in the final product than heavily regulated development. For example, some unregulated autonomous features use nerual networks. Neural network algorithms lack explainability – the developer cannot determine exactly how or why the algorithm acts the way it does. When a system lacks explainability, the likelihood for an error to lurk in a product is even greater. If the system is safety critical, then these mistakes have the potential to be fatal for the user. Knowing the potential consequences, some companies release products with autonomous features in control of safety critical systems.

One example of a consumer product that uses automated safety critical systems is the Tesla autonomous driving mode. Current regulation allows Tesla to dictate its own quality assurance program. After autonomous driving mode updates are approved internally, Tesla is capable of remotely updating its car without having to apply for a new type approval. Type approval is a certification from a country's governing body that the car meets regulation. Companies send in a small subset of cars to test, which are representative of the model they are trying to approve. The approval assumes that the car will not be modified, which the over the air updates violate [1]. Some countries deviate from this form of regulation for autonomous vehicles. For example, the US Department of Transportation's stance is to follow self-regulation and intervene as necessary [2]. At this point, there is not enough data to statistically say if autonomous vehicles are safe or not. [3] suggests that it would take decades, if not hundreds of years, of driving to be statistically certain about autonomous vehicle algorithms using the current autonomous car fleet. As a result, the current laissez-faire approach is accelerating the company's ability to collect data, allowing for aggressive innovation. Sadly, this agressive innovation, has come at the cost of some lives.

III. Heavy Regulation

Safety critical engineering and robotic industries often face intense regulation. Regulation is important to provide the public an assurance that products of such industries are safe to use. For the companies of regulated industries, complying to regulation is often expensive and extends the time to market of new technologies. This leads to safety-critical systems that are already certified by regulating bodies to be reused across many new product iterations. Over time, this can result in safety-critical systems becoming outdated, limiting the performance of the overall system. This can lead to hacks and workarounds to squeeze as much performance as possible out of these safety-critical systems. A problem

[1] Both authors are with the Space & Terrestrial Autonomous Robotic Systems (STARS) laboratory at the University of Toronto Institute for Aerospace Studies (UTIAS), Canada. emmett.wise@robotics.utias.utoronto.ca

can arise when these hacks and workarounds become so complex that the entire system becomes compromised. In extreme cases, the assurances that a safety-critical system is safe can be violated.

The epitome of heavily regulated industries is commercial aircraft manufacturing. To produce a certified aircraft, the manufacturer must certify their aircraft design, production repeatability, and final product's airworthiness [4]. Each certification has its own tedious approval process. Completing these processes can cost companies hundreds of millions of dollars and years of work [5]. This cost can make or break the profitability of a new aircraft program. Once an aircraft is certified, modifications to the certified design are easier than certifying a new design. In most cases, the modifications are safe, but as new technologies are layered on top of outdated safety-critical systems, the safety of the entire system can become compromised. An example of a modification compromising a safety-critical system is the upgrade of the Boeing 737 to the 737 Max.

Boeing was forced to upgrade the 737 to the 737 Max [6] due to market pressure from Airbus, their main competitor. In 2010, Airbus announced an engine upgrade that improved fuel efficiency by a significant margin and maintained current flight characteristics. As a result, this upgrade improved fuel efficiency without invalidating previous pilot training or requiring major plane recertification. Due to the 737's wing clearance, Boeing couldn't achieve the same performance without modifying the position of the 737's engines or designing a completely new aircraft. Boeing elected to modify the position of the 737's engines, calling this modified plane the 737 Max. This choice was made in part due to the high cost of certification of a new aircraft. Although moving the engines seemed like a straightforward adjustment, the changes had a fairly significant impact on the overall aerodynamics of the airplane.

The change in overall aerodynamics of the plane meant the 737 Max handled differently than the 737, specifically when the 737 Max was climbing at a steep angle. In order to compensate for this difference in performance, Boeing introduced a stack of additional safety features, which allowed for 737 pilots to fly 737 Max aircraft with minimal retraining. Although these features fixed some problems, they introduced unforeseen failure modes. Since 2018, the Boeing 737 Max has crashed two times resulting in the deaths of over 300 people. Both incidents appear directly tied to the house-of-cards constructed to accommodate the new engine.

IV. Conclusion

We argue against heavy regulation of safety-critical autonomous systems because regulation doesn't necessarily ensure safety and can cripple innovation. Heavy regulation attempts to ensure public safety, but competition in heavily regulated industries forces companies to find workarounds to squeeze performance out of antiquated, certified systems. As seen with the 737 Max, these workarounds can compromise the overall safety of the system and nullify the purpose of the regulations. Additionally, the cost of compliance makes innovation extremely difficult and slow. In the case of Tesla, the increased cost would be further exacerbated by the amount of data required to get statistically relevant measurements. As a result, we believe that current regulatory schemes do not provide an optimal balance of innovation and safety.

References

[1] B. Schmitt, "Swedish concerns about tesla's ota updates could become global nightmare," 2019. [Online]. Available: https://www.thedrive.com/tech/26219/swedish-concerns-about-teslas-ota-updates-could-become-global-nightmare.

[2] U. D. of Transportation, "Preparing for the future of transportation: Automated vehicle 3.0," 2018. [Online]. Available: https://www.transportation.gov/av/3.

[3] N. Kalra and S. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?," 2016. [Online]. Available: https://www.rand.org/pubs/research_reports/RR1478.html.

[4] "Aircraft certification," *FAA seal*, 2016. [Online]. Available: https://www.faa.gov/aircraft/air_cert/.

[5] P. Shankara, "Certifiably cheaper," *Aerospace Testing International*, 2018. [Online]. Available: https://www.aerospacetestinginternational.com/online-magazines/in-this-issue-showcase-2019.html.

[6] M. Yglesias, "The emerging 737 max scandal, explained," *Vox*, 2019. [Online]. Available: https://www.vox.com/business-and-finance/2019/3/29/18281270/737-max-faa-scandal-explained.