A tale of automation safety: Lessons learned from automotive to aviation and beyond

Gotcheva, N[1]

1 VTT Technical Research Centree of Finland

KEYWORDS: automation, organizational factors, institutional factors, aviation, storytelling

ABSTRACT

Industrial automation is increasing due to the potential to reduce costs, and expectations to increase productivity, efficiency, agility, safety. The latest developments are fuelled by technological leaps, such as AI advancements for robotic automation, metaverse, machine vision and "humanlike" machine perception, to name a few. However, the generic narrative has often been that the workers should adapt to the automation.

From an organizational factors perspective, it is critical to design and implement automation solutions in a way that allows the people in organizations – from shop floor workers to top managers - to make sense of the underlying conditions and make decisions that control the potentially unsafe and dynamic conditions to prevent risks from actualizing. Organizational factors, such as decision-making, communication, incentives systems, competence development and training, leadership, management and culture for safety, as well as political, social, economic and regulatory context all play an important role for creating conditions for safe automation. Previous research in the context of offshore drilling automation indicated that organizational factors are influenced by automation systems, and they influence the way in which these systems are applied in a specific organizational setting [1].

This paper offers a tale of automation safety, bringing in insights, lessons learned and historical accounts from aviation to automotive industry and beyond. It advances the understanding on the role of non-technical, organizational factors and business and operational environment that have contributed to the Boeing 737 MAX crashes and linking them to historical accounts for developing regulatory foundations for automotive safety. Latent deficiencies in these factors have been present decades ago in the Boeing's case but their cumulative effect on safety have not been timely and effectively addressed. Research method is scoping review of public sources and publications. The value of cross-industry learning is emphasized: although different safety-critical industrial domains have specific standards, requirements and regulatory context, there are similarities, which allow for transferability of lessons learned to support safety oversight and overall safe operations in complex sociotechnical industrial settings.

The paper concludes by emphasizing the value of cross-industry organizational learning and the importance of knowing the past to shape the future of safe automation.

1 INTRODUCTION

Almost 60 years ago, Ralph Nader, an American lawyer, published his influential book *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*. Although formally trained as a legal professional, Nader has actually been one of the pioneering safety advocates, whose vigilance, ability to speak up and to confront the powerful institutional establishments of the American automotive corporations have led to remarkable safety outcomes. Nader's seminal work resulted in the first regulations in the transport domain and the establishment of the *US National Traffic and Motor Vehicle Safety Act in 1966*, requiring the adoption of new or upgraded vehicle safety standards. This legislation also got political support and led to the establishment of the US traffic administration agency 4 years later - *the National Highway Traffic Safety Administration (NHTSA)* was established in 1970. Essentially, this means that the automotive industry could not be self-regulating itself.

During these years, it has been customary to blame the driver for the road injuries and fatalities, or what became known as the "*nut behind the wheel*" approach. The phase refers to generally driving a vehicle but it has a negative connotation as it is usually used to describe someone who drives recklessly or dangerously. Nader had challenged the widespread notion that bad drivers were responsible for crashes – while it was rather the failure of automakers to address safety in vehicle design.

Nader is not the only historical safety advocate, there were others like him. For example, also Crystal Eastman (1881-1928) was an American lawyer, who actively advocated for legislative means to prevent accidents and ensure workplace safety and health. Their activities have had a major impact on automotive, consumer and workplace safety fields while also affecting thought leadership about safety in high-hazard domains globally.

2 FIVE ERAS OF TRANSPORTATION SAFETY

The NHTSA has conducted a historical analysis, where five eras of transport safety were identified that summarizes the different features, advances, alerts and driver-assistance technologies, which have been developing since the 1950s. The invention of the seat belts is another story that links aviation to automotive or traffic safety. The current standard – a three-point seatbelt – was developed by Nils Bohlin, a Swedish engineer at Volvo, in 1959. Interestingly, before joining Volvo, Bohlin had experience working on aircraft ejection seats, where safety and quick-release mechanisms were critical, fuelling the invention of the three-point belt [2]. Also, the first prototype of Maneuvering Characteristics Augmentation System (MCAS) was developed in the 1960s - a basic pitch control system known as the *stick shaker* was installed in the Boeing 707 to avoid stalling [3]. Overall, many important inventions and events that have shaped the developments in automation safety, have had happened in the 1960s, more than six decades ago.

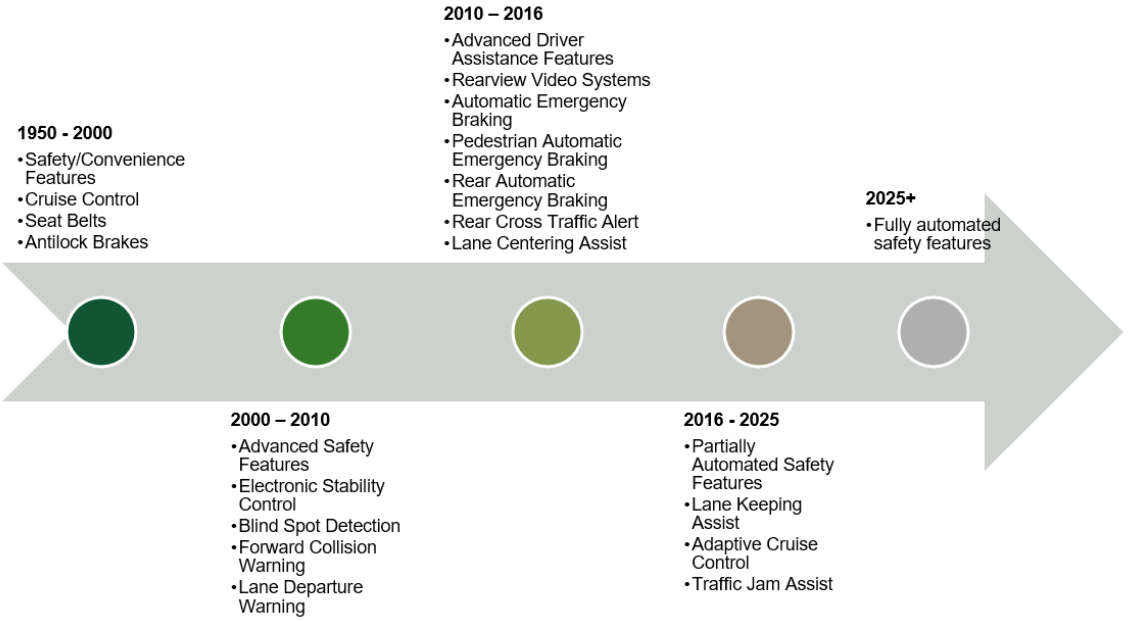

Figure 1. *Five eras of transport safety [4].*

3 A TALE OF AUTOMATION SAFETY IN AVIATION

On 29 October 2018, Lion Air flight 610 took off from Jakarta for a domestic flight to Pangkal Pinang, on the Indonesian island of Banka: 30 minutes after takeoff, the plane crashed into the Java Sea, killing all 189 passengers and crew. On 10 March 2019 Ethiopian Airlines flight 302 bound for Nairobi, Kenya crashed only 6 minutes after takeoff, from Addis Ababa, Ethiopia, killing all 157 people on board.

Historically, a long and wavy road have led to these accidents. Following the Boeing 737 MAX accidents, the role of Boeing's Maneuvering Characteristics Augmentation System (MCAS) has gathered growing attention in various reports and studies. MCAS is an automation system that has a significant impact on pilot operations and has a direct impact on aircraft control. This software system was designed in relation to hardware change in the Boeing's aircraft – the changed size and position of the engine to increase fuel efficiency changed the aerodynamics of the aircraft, which required additional means for adjustment without pilot's intervention through the MCAS software. In the design phase, this system was considered to have a low safety impact, of which users would not need to undergo additional simulator training. However, MCAS, as any automation system, had been designed and implemented based on certain cultural assumptions, decisions have been made and approved under

established leadership and within defined resources, and affected by the broader organizational set up and the institutional and regulatory environments.

The role of the regulator for approving this system, and the gradual emergence of blurred lines of responsibilities are important historical developments here. The Federal Aviation Administration (FAA) is responsible for the regulation and oversight of civil aviation within the U.S., as well as operation and development of the National Airspace Systems, and its mission is to ensure safety of civil aviation. The Boeing 737 MAX was approved under the FAA's "Organizational Designation Authorization" (ODA) program, which was launched in 2005 to standardize the oversight of aircraft manufacturers, approved to perform certain functions on the FAA's behalf, for example determining compliance with aircraft certification regulations.

In essence, the ODA program effectively allowed the aircraft manufacturers to certify parts of their own designs with limited, if any, federal regulatory oversight. According to Boeing data, as of March 2017, FAA delegated all 91 certification plans to Boeing's ODA. It all started in the 1950s, with the rapid expansion of the aircraft industry, which necessitated the development of various forms of organizational delegation by FAA to meet specific needs. Figure 2. illustrates the development and evolution of organizational delegation since mid-1950s.[5], [6], [7].

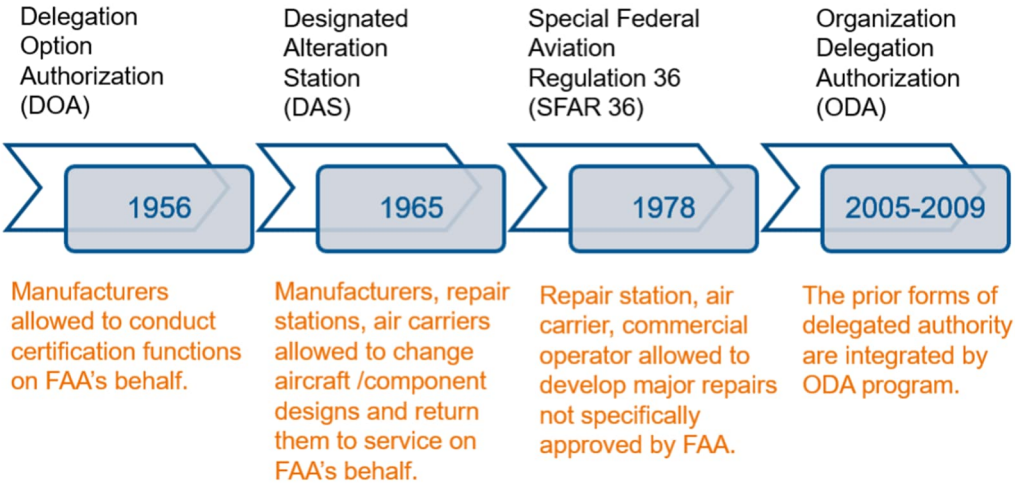

Figure 1. *History of delegated authority in the Federal Aviation Administration (FAA) [8].*

New aircraft designs are considered "high-risk areas" and require independent oversight but although Boeing initially aimed at developing a brand-new aircraft, pressed by the competition with Airbus over winning back established clients, such as American Airlines, Boeing opted for a modified design of existing aircraft to ensure fuel efficiency, comparable to the one by Airbus.

In the mid-1990s, a major event happened when Boeing purchased McDonnell Douglas and the two companies merged. The focus on efficiency started actually at the board room, where McDonnell Douglas executives have increasingly focused attention towards increasing efficiency, cutting costs and maximizing profits for the shareholders, while taking the engineering excellence and safety for granted. Other critical events followed, such as the move of HQs from Seattle to Chicago, with management moving away from the engineering.

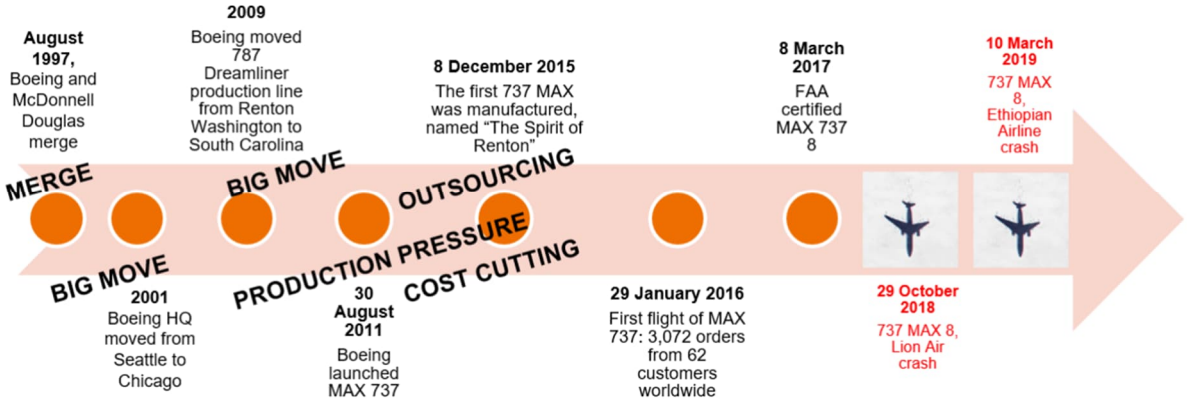

Figure 1. *Boeing: A simplified timeline of some of the critical events [9].*

3 A TALE OF AUTOMATION SAFETY IN AUTOMOTIVE

Tesla's Autopilot is intended to enable cars to steer, accelerate and brake automatically within their lane, while enhanced Autopilot can assist in changing lanes on highways but does not make vehicles autonomous. One component of Autopilot is Autosteer, which is using advanced cameras, sensors and computing to navigate tighter, more complex roads [10].

On 26 April 2024, the US The National Highway Traffic Safety Administration (NHTSA) informed "that their investigation into Tesla's Autopilot had identified at least 13 fatal crashes in which the Tesla Autopilot had been involved. In August 2021, NHTSA launched a three-year Autopilot safety investigation, when it identified at least 13 Tesla crashes involving one or more death, and many more involving serious injuries, in which "foreseeable driver misuse of the system played an apparent role". The NHTSA raised concerns that Tesla's Autopilot name "may lead drivers to believe that the automation has greater capabilities than it does and invite drivers to overly trust the automation". Essentially, the federal regulator NHTSA stated that drivers may be expecting their Tesla to do too much and this they do not pay attention when the feature is on [11], [12].

Tesla's Autopilot is an example that nowadays there are many inventions and investments in safety in vehicle design. However, the strive to offload the driver towards increased automation may be indicative for the "*nut behind the wheel*" attitudes towards the driver as the human element in the system. The risks arising from the shared assumptions of automotive designers and software developers and the organizational and other non-technical factors for ensuring automation safety need greater attention. There are many lessons from the past that we need to revisit and learn from to make the future safer.

5 CONCLUSION

The contribution of this short paper is that it sheds new light on the historical context, and how different non-technical factors have been affecting the development and thinking in the field of automation safety. Broader applicability of the regulatory and organizational lessons learned related to automation design and implementation is relevant also for other industrial domains.

REFERENCES

1. Gressgård, L. J., Hansen, K, & Iversen, F. (2013). Automation systems and work process safety: assessing the significance of human and organizational factors in offshore drilling automation'. Journal of Information Technology Management, 24(2), 47.
2. Who invented seat belts and when? From concept to essential safety feature, https://carbuzz.com/features/when-who-invented-seat-belts/
3. https://en.wikipedia.org/wiki/Maneuvering_Characteristics_Augmentation_System

4. NHTSA, https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety
5. 737MAX-timeline-W-1020x2759.jpg (1020×2759) (seattletimes.com)
6. Airbus wins big with American Airlines | Business | Economy and finance news from a German perspective | DW | 21.07.2011
7. First 737MAX, 'Spirit of Renton,' makes first flight | Renton Reporter
8. Office of Inspector General analysis of FAA documents, Report Number: AV-2016-001, 2015
9. Gotcheva, N., & Ylönen, M. (2021). Regulatory lessons from accidents due to institutional failures: Boeing 737 MAX and Deepwater Horizon. VTT Technical Research Centre of Finland. VTT Research Report No. VTT-R-00804-21
10. https://www.tesla.com/autopilot
11. USA Today, retrieved on 27.4.2024 https://www.msn.com/en-us/money/other/critical-safety-gap-between-tesla-drivers-systems-cited-as-nhtsa-launches-recall-probe/ar-AA1nK8Vy
12. The Guardian (2024) Tesla Autopilot feature was involved in 13 fatal crashes, US regulator says, retrieved on 27.4.2024, https://www.theguardian.com/technology/2024/apr/26/tesla-autopilot-fatal-crash
13.