Holistic Understanding of Challenges with Autonomous Vehicles

Tamir BECHOR
Center for Information Systems & Technology (CISAT), Claremont Graduate University
Claremont, CA 91711, U.S.A

Hengwei ZHANG
Center for Information Systems & Technology (CISAT), Claremont Graduate University
Claremont, CA 91711, U.S.A.

Leonard CRUZ
Captain, US Army, 7th Signal Command (Theater)
Fort Gordon, GA 30905, U.S.A.

ABSTRACT

The increased presence of computers and interconnectedness in automobiles presents challenges and risks in effectively managing the advancement of a technology that society can benefit from. This set of problems is diverse and is not explicitly technical with some concerning social acceptance, liability, and cybersecurity. The amount of data that describes the current conditions and forces shaping autonomous vehicles is overwhelming to process. The intent of this paper is to provide a foundational understanding of associated challenges by reducing and ordering this data into consumable sets for drawing practical conclusions and relationships. The strategic goal of this research is to lay the groundwork for a Governance, Risk Management, and Compliance (GRC) framework that enables organizations to effectively manage risks associated with autonomous vehicles.

Keywords: Autonomous Car, Cybersecurity, Challenges, Concerns, GRC.

1. Introduction

Society is entering an automotive epoch that is defined by the emergence of self-driving vehicles. This paradigm shift to an increasingly connected car brings both incredible capability and risk as the worlds of the internet and automobiles collide. In 2016, President Obama stated that self-driving cars could had prevented tens of thousands of deaths a year if implemented. In 2015, 35% of new cars sold will be connected; by 2020, that rises to 98% and to 100% by 2025 [1]. Autonomous vehicle technology has the potential to create economic opportunities, innovation, improvements to the quality of life, and safety. The pace that autonomous vehicle technology has advanced has introduced a wide array of risks that society is not prepared for. Both the interconnected intelligent system and expansion of capabilities enabled by a system of people, infrastructure, software, etc. of autonomous vehicles is unprecedented [2,3,4] and introduces a host of complex cyber security challenges. In 2015, two researchers revealed critical security flaws by remotely hijacking a Jeep Cherokee that left a passenger helpless and at their mercy. This spurred numerous similar efforts exploring the security of this technology and highlighted risks to freedom, privacy, safety, security, and lack of control of this technology to the forefront [5]. Regulators in an effort to address these issues have begun developing legal and regulatory controls [6], and putting out new regulations.

Underestimating the complexity and dynamic nature of this technology can result in compliance and practices with affects that can be more harmful than good. Numerous organizations both private and public have produced research, studies, and reports providing a substantial eclectic collection of information relating to autonomous vehicle technology. However, there have been relatively fewer efforts to integrate and synthesize this staggering amount of big data into consumable information. Providing order to this data is further complicated by a lack of standardization of terminology. The intent of this research is to reduce the amount of information to a manageable list and then take this list and apply it to a model for managing risk. These insights will help to identify area for further investigation and research, and outline implications for further practices.

The current state of research for autonomous vehicles is generally centered on three focus areas: 1) technological capabilities/limitations [7,8], 2) communication security/reliability [9,10], and 3) legal responsibilities and authorities [6,11,12]. Based on our knowledge, there is a lack of research that informs how this technology is adapted by society.

Developing a base taxonomical model incorporating the social, technological, regulatory, and organizational entities and their linkages to serve as the basis for understanding the forces at work. These insights will serve as a road map towards proposing a framework to manage both known and unknown risks holistically.

This paper is organized as follow. Section 2 provides the overview of the Research Method. Section 3 provides the results of the research and organization of data into consumable information. Section 4 provides discussion and implications of research results. Section 5 maps the long-term objectives of this research effort. Section 6 provides the conclusive current state of autonomous vehicles supported by this research.

2. Research Method

The research method applied in this study to conduct systematical review follows the traditional three-stage process of systematic studies: Planning, Conducting and Reporting [13, 14, 15, 16].

Specifically, the content analysis suggestions by Weber [17], and the methodology for taxonomy development by Nickerson et al., [18] are absorbed in the conducting stage.

Planning

Data Collection. Cataloging data sources that describe the current stage of autonomous vehicle technology. The following stages describe the approach for producing the final Candidate Document List (CDL).

Stage 1: Search Preparation. Aggregated data by associating similar or interchangeable terms to a common concept. For example, autonomous car defined by SAE J3016 [19] is synonymous with “connected car”, “self-driving car”, “automated car”, “autonomous vehicle”, and “smart car”. This mapping resulted in a search dictionary.

Stage 2: Search. Conducted searches using the search dictionary and compiled the initial list.

Stage 3: Selection of studies. Criteria for document selection: a). Propose, leverage, or analyze the following, but not limited to: conflicts of social values, competing interests between social groups, and societal mechanisms directly influencing autonomous vehicle technology; b) Primarily focused in the U.S. The resulting list represents the raw CDL.

Stage 4: Evaluation by experts. The raw CDL was reviewed by a panel of experts of various specialties within the autonomous vehicle technology

Stage 5: Content analysis and document selection. Two key outputs for this stage is 1) Initial build of reoccurring and key terms, ideas, and principles and 2) List reduction of raw CDL. Criteria for document selection during this stage: a) Acceptance and recognition in their respective industries; b) Primary sources of information. The resulting list represents the final CDL.

Conducting

Document Analysis. The final CDL is represented in Table 1 and is comprised of 4 non-government and 11 government sponsored documents. The government documents are produced by government departments and central government organizations, including parliamentary publications, legislation, policy documents, discussion documents, and reports. Non-government documents are from the private sector and research agencies.

Table 1：Final Candidate Document List (CDL)

Document No.	Title	Authorship	Type
DC1	Automakers Commit to Privacy Principles to Protect Vehicle Personal Data: Industry Recognizes Need to Take Proactive Steps in Age of Connectivity	Auto Alliance, Global Automakers	2014
DC2	Automotive Security Best Practices: Recommendations for security and privacy in the era of the next-generation car	Intel, McAfee	2016
DC3	A Framework for Automotive Cybersecurity Best Practices	Auto- ISAC	2016
DC4	A Summary of Cybersecurity Best Practices	NHTSA	2014
DC5	National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles	NHTSA	2014
DC6	Internet of Things: Privacy & security in a connected world	FTC	2015
DC7	Proactive Safety Principles	DOT, NHTSA	2016
DC8	Vehicle Cybersecurity: DOT and Industry have efforts under way, but DOT Needs to Define Its Role in Responding to a Real-world Attack (*)	GAO	2016
DC9	Federal Motor Vehicle Safety Standards; V2V Communications	NTHSA	2017
DC10	Driver Privacy Act of 2015	Congress	2015
DC11	Security and Privacy in Your Car Act 2015	Bill	2015
DC12	Security and Privacy in Your Car Study Act	Bill	2017
DC13	Federal Automated Vehicles Policy	NHTSA	2016
DC14	Preliminary Statement of Policy Concerning Automated Vehicle	NHTSA	2016
DC15	Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk	Senator ED MARKEY	2015

This CDL was reviewed and evaluated by a panel of researchers and practitioners, and stated that this “is a comprehensive list of documents” [20].

Content Analysis. The content of the CDL is iteratively mapped using data analytical tools to produce and refine grouping categories using a coding schema. Analogous or similar ideas and themes are tagged to analyze frequency and overlap. The coding schema is applied to systematically process data from the CDL.

Coding schema. (Adopted from Weber [16]): a) Define the uniting interests; b) Specify the coding rule; c) Test the coding on a sample of text; d) If the target ideas/words are not affected, revise the coding rule and repeat

3. Research Results

Reporting

Qualitative Results. The results identified 23 variables that comprise the raw Autonomous Vehicle Variables (AVV) from the CDL. Understanding the context of the raw AVV and application of axial coding further aggregated these categories into eight categories comprising the Autonomous Vehicle (AV) Focus Areas. The AV Focus Areas are then organized into three layers of the cyber multiverse model proposed by Dr. Van den

Berg et al. [21]. This research proposes the following model that describes how the AV Focus Areas are organized into respective domains that are described as Autonomous Vehicle Layers.

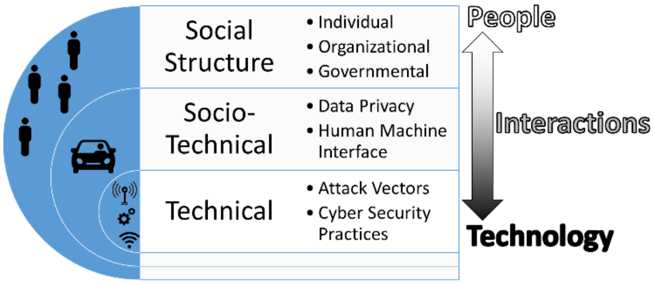


Figure 1: Autonomous Vehicle Layers

Technical: Technology that enables the autonomous vehicle activities in cyberspace.

1. Attack Vectors: The security posture of autonomous vehicles technology organized into four categories: Hardware, Software, Networking, and Cloud.
2. Cyber Security Practices: Defense in depth & threat detection and protection

Socio-Technical: Cyber activities executed and behaviors of individuals using technology.

1. Data Privacy. Accepted practices of sharing or restricting individual or proprietary data to third parties. Topics related to data privacy are the following seven: Transparency, Choice, Data Sharing, Data Minimization, Data Security, Integrity & Access, & Accountability.
2. Human Machine Interface. How interactions between the vehicle and user occur. Examples include the nature of how the vehicle informs the user of operating conditions or how control of the vehicle is transitioned to the user.

Social-Structure: Management and governance efforts to structure the automotive cyberspace.

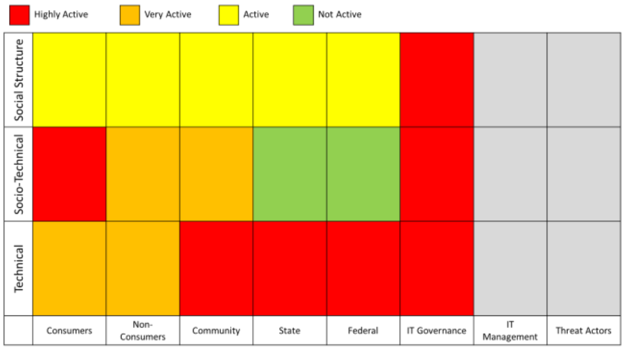
1. Individual: Respective requirements either prior to or while operating autonomous vehicles (i.e., education, certifications, etc.).
2. Organizational: Self-organization of activities forming internally and externally.
3. Governmental: Formal controls established by authoritative entities.

Stakeholders: Eight groups of people that interact with the AV Focus Areas.

- Consumers. Owners and operators.
- Non-consumers. Directly affected by the use of this technology but is not a consumer. Can include bystander or passive user such as a passenger.
- Community. Academia and industry.
- State. Provincial or state government.
- IT Governance. An entity that provides accountability and strategy to organizational management. More specifically, IT Governance is interested in the allocation of resources, management actions and goals, and results of meeting strategic objectives.
- Federal. National level government.
- IT Management. Organizational leadership that executes in order to support goals and strategic objectives.
- Threat Actors. Individuals or groups concerned with exploiting autonomous vehicles for a specific goal illegally or immorally.

Quantitative Results. Activity within a given AV layer by each stakeholder is measured relative to actions related to an AV Focus Area. The actions are proactive in nature with the intent to shape a given AV Focus Area. Not all stakeholders are in a position to shape AV Focus Areas and rather are shaped by AV Focus Areas. IT Management is in a support position to achieve desired objectives for IT Governance. The interest of AV Focus Areas by IT Management is a means towards achieving a goal.

Conversely, Threat Actors are not shaped nor are they generally interested in directly shaping AV Focus Areas. Broadly, Threat Actors seek to exploit AV Focus Areas to meet objectives.



🟥 Highly Active 🟧 Very Active 🟨 Active 🟩 Not Active

	Consumers	Non-Consumers	Community	State	Federal	IT Governance	IT Management	Threat Actors
Social Structure	🟨	🟨	🟨	🟨	🟨	🟥		
Socio-Technical	🟥	🟧	🟧	🟩	🟩	🟥		
Technical	🟧	🟧	🟥	🟥	🟥	🟥		

Figure 2: Stakeholders Levels of Activity within each AVL

The graphical representation of activity by stakeholders within each AVL provides a grouping for these stakeholders. The eight stakeholders tend to naturally fall into groups by common levels of activity and inactivity within a given layer.

Drivers of Technology and Behaviors. Consumers, Non-Consumers, and the Community are very active in the technical layer and uniquely very active in the socio-technical layer.

Drivers of Policy and Controls. Formally structured entities such as state and federal are highly active in the technical layer and uniquely inactive in the socio-technical layer.

Common to both abovementioned groups is a moderate level of activity in the Social Structure layer.

Drivers of Innovation. IT Governance is highly active in all layers.

The following groups are not proactive in shaping AV Focus Areas.

Implementers. IT Management equipped with the structure and resources to innovate. This group is generally shaped by AV Focus Areas.

Exploiters. Threat actors that choose to operate outside societal constructs and norms. This group generally exploits AV Focus Areas.

Interactions. The interactions between stakeholders are all centered on AV Focus Area and the nature of these interactions can be classified as the following:

Controlling. There exists formal controls and processes that one stakeholder exerts on another.

Supports. Formal or informal relationship where a stakeholder supports another with respects to a focus area.

Influences. Informal relationship where a stakeholder indirectly shapes or advises another.

4. Discussion

A majority of the available research tended to focus on the Technical layer. The Social Structure layer was the second most researched area. Less than 7% of research was focused on the Socio-Technical layer. In terms of types of groups that accounted for the sources for current research, approximately 63% of research was non-government sponsored.

At this time, the volume of research indicates that the private sectors are significantly more active and tend to have a technical focus. Nonprofit standards organizations such as ISO and AUTO ISAC tend to be focused on social structures and controls.

The intersection of people and technology at the socio-technical layer is the most debatable and difficult to reconcile. There are several examples describing how the practice of sharing or restricting individual or proprietary data conflicts with public safety, individual privacy, freedom, and market competitiveness. Specific approaches to information exchange and interactions between the user and autonomous vehicles is largely philosophical. For example, what is an appropriate level of engagement from the user when a fully autonomous vehicle during operation? The answer to questions such as this has many implications that will either accelerate or decelerate this technology [22, 23].

Generally, both drivers of technology and policy are interested in laws and regulations associated with the social structure layer, however, level of activity within this layer is moderate at best. This trepidation in the social structure layer stems from the lack of holistic understanding of implications associated with autonomous vehicles. The lack of activity in the social structure layer favors innovation and inhibits increased adoption.

Formal policies and controls have the highest potential to quickly and effectively influence autonomous vehicle technology. For example, governmental policies placing liability on the vendor will increase consumer willingness for adoption, but conversely influence manufacturers to take deliberate and calculated advances in technology.

Convergence of technology within the automobile complicates the matter of securing the autonomous vehicles. A balanced approach to automotive engineering and cyber security requires manufacturers expand the scope of automotive designs and lifecycles. Cyber security for autonomous vehicles is relatively new and are being developed and informed by other industries. Controlling the flow of data is also complicated by convergent systems connected to the cloud.

5. Future Work

The ordering of data describing the current state of autonomous vehicles in society provides a critical foundation to inform a framework that manages risk. An information technology best practice of Governance, Risk Management, and Compliance (GRC) provides a framework that coordinates how an organization balances strategic objectives with responsibilities mandated by compliance. Research from Nicolas Racz et al. [24] assert that

"*GRC is an integrated, holistic approach to organisation-wide governance, risk, and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies, and external regulations through the alignment of strategy, processes, technology, and people, thereby improving efficiency and effectiveness.*"

Their GRC relational model emphasizes a mutually governing and supporting relationship [25].

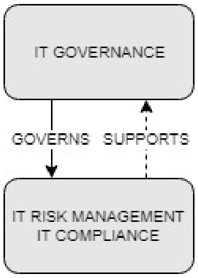


Figure 3: The relationship of IT governance to IT risk management and IT compliance

Future work will leverage this model as a basic unit for organizing the autonomous vehicle ecosystem with stratification based on levels of automation defined by SAE and NHTSA (Levels 0-5) [19,24]. Using GRC as a basis of approach will provide a framework that is familiar to facilitate implementation. A complete understanding of the autonomous vehicle ecosystem will inform a balanced and harmonious approach to the adoption of autonomous vehicle technology.

> *"GRC, simply put, is to provide collaboration between the silos of governance, risk, and compliance. It is to get different business roles to share information and work in harmony. Harmony is a good metaphor, we do not want to discord where the different parts of the organization are going down different roads and not working together. We also do not want everyone singing the melody as different roles (such as risk, audit, and compliance) have their different and unique purposes."*
>
> *-Michael Rasmussen [OCEG]*

6. Conclusion

The current state of autonomous vehicles is highly energized and unordered. The innovation of technology by the technical research community continues to outpace the social understanding and adoption by the community at large. The trajectory for advancement of autonomous vehicles will reach a standstill until policies can formalize controls regarding autonomous vehicles for common use. Formation of these policies will push this technology past its tipping point to ubiquity. This underscores the importance of governance partnered and informed by the community and research.

The results of this research suggest that beneath the volumes of data for autonomous vehicles therein lies an ecosystem. The nature of this ecosystem is complex, expansive, and dynamic. This ecosystem is a system of entities with specific relationships existing in defined spheres working towards respective goals.

7. References

[1] Gissler, adreas. "connected vehicle: succeeding with a disruptive technology." 2015.

[2] Müller, Lars, Malte Risto, and Colleen Emmenegger. "The social behavior of autonomous vehicles." Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. ACM, 2016.

[3] Young, Angelo. “Car Hacking: Security Experts Caution Automakers on Greater Need for Cybersecurity and Anti-Hacking Measures.” International Business Times 28.07(2015)

[4] Schellekens, Maurice. "Car hacking: navigating the regulatory landscape." Computer Law & Security Review 32.2 (2016): 307-315.

[5] Mulligan, Deirdre K., and Kenneth A. Bamberger. "Public Values, Private Infrastructure and the Internet of Things: The Case of Automobiles." (2016).

[6] Pipes, Sarah. “Spy Car: Hacked Vehicles and Potential Internet of Things Regulation.” ISACA News (2015)

[7] Charette, Robert N. "This car runs on code." IEEE spectrum 46.3 (2009): 3.

[8] Han, Kyusuk, André Weimerskirch, and Kang G. Shin. "Automotive cybersecurity for in-vehicle communication." IQT QUARTERLY. Vol. 6. No. 1. 2014.

[9] Klinedinst, Dan, and Christopher King. "On board diagnostics: Risks and vulnerabilities of the connected vehicle." CERT Coordination Center, Tech. Rep (2016).

[10] Kim, Dong Hee, Seung Jo Baek, and Jongin Lim. "Measures for Automaker's Legal Risks from Security Threats in Connected Car Development Lifecycle." KSII Transactions on Internet & Information Systems 11.2 (2017).

[11] Kennedy, Caleb. "New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles." Mich. Telecomm. & Tech. L. Rev. 23 (2016): 343.

[12] McGehee, D. V., Brewer, M., Schwarz, C., & Smith, B. W. (2016). Review of Automated Vehicle Technology: Policy and Implementation Implications.

[13] Keele, Staffs. "Guidelines for performing systematic literature reviews in software engineering." Technical report, Ver. 2.3 EBSE Technical Report. EBSE. sn, 2007.

[14] Wohlin, Claes, et al. Experimentation in software engineering. Springer Science & Business Media

[15] Sapienza, Gaetana, Ivica Crnkovic, and Pasqualina Potena. "Architectural decisions for HW/SW partitioning based on multiple extra-functional properties." Software Architecture (WICSA), 2014 IEEE/IFIP Conference on. IEEE, 2014.

[16] Muccini, Henry, Mohammad Sharaf, and Danny Weyns. "Self-adaptation for cyber-physical systems: a systematic literature review." Proceedings of the 11th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. ACM, 2016.

[17] Weber, Robert Philip. Basic content analysis. No. 49. Sage, 1990.

[18] Nickerson, Robert C., Upkar Varshney, and Jan Muntermann. "A method for taxonomy development and its application in information systems." European Journal of Information Systems 22.3 (2013): 336-359.

[19] SAE On-Road Automated Vehicle Standards Committee. "Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems." SAE Standard J3016 (2014): 01-16.

[20] A private conversation

[21] Van den Berg, Jan, et al. "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education." Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium. 2014.

[22] Czempiel, Ernst-Otto. "Governance and democratization." Governance without government: Order and change in world politics (1992): 250-71.

[23] Debernard, S., et al. "Designing Human-Machine Interface for Autonomous Vehicles." IFAC-PapersOnLine 49.19 (2016): 609-614

[24] McCarthy, C., and K. Harnett. "National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicle." Report No. DOT HS 812 (2014): 073.

[25] Racz, Nicolas, Edgar Weippl, and Andreas Seufert. "A process model for integrated IT governance, risk, and compliance management." Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010). 2010.