Proceedings of the 2022 ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference
IDETC/CIE2021
August 14-17, 2022, St. Louis, MO

DETC2022-90958

DESIGNING PRIVACY RISK FRAMEWORKS FOR EVOLVING CYBER-PHYSICAL SOCIAL SYSTEMS: KNOWLEDGE GAPS ILLUMINATED BY THE CASE OF AUTONOMOUS VEHICLES AND BYSTANDER PRIVACY

Vivek Rao
Dept. of Mechanical Engineering
University of California, Berkeley
Berkeley, CA

Ankita Joshi
Dept. of Mechanical Engineering & Goldman School of Public Policy
University of California, Berkeley
Berkeley, CA

Soo Min Kang
Dept. of Mechanical Engineering
University of California, Berkeley
Berkeley, CA

Susan Lin
Dept. of Electrical Engineering & Computer Sciences
University of California, Berkeley
Berkeley, CA

(Erin) Junghyun Song
Dept. of Mechanical Engineering
University of California, Berkeley
Berkeley, CA

Drew Miller
Dept. of Mechanical Engineering
University of California, Berkeley
Berkeley, CA

Kosa Goucher-Lambert
Dept. of Mechanical Engineering
University of California, Berkeley
Berkeley, CA

Alice Agogino
Dept. of Mechanical Engineering
University of California, Berkeley
Berkeley, CA

ABSTRACT

Designers and engineers increasingly engage with and must design for sociotechnical systems, also described as cyber-physical-social systems (CPSS). Leading frameworks like System-Theoretic Process Analysis and Value-Sensitive Design intend to help designers consider the consequences and impacts of their work with CPSS. However, such frameworks may not sufficiently account for human-centered scenarios. This complicates designers' efforts to balance user needs with traditional forms of risk assessment. In this work, we explore foundations for the design of human-centered risk frameworks and examine a case study of autonomous vehicles and bystanders' privacy as an example CPSS to address this gap. We develop an exploratory scenario-based risk framework and conduct expert interviews with experienced professionals (N = 7) working in the fields of autonomous vehicle design, development, policy and security to understand their perspectives on risk assessment and gather feedback on our framework. Reconciling interview findings with existing knowledge of evolving CPSS, we identify three broad knowledge gaps that could motivate future research in this space. First, we argue that there is a knowledge gap in developing human-centered frameworks and best practices to consider all stakeholders during the design of evolving CPSS. Second, we argue that a knowledge gap exists in acknowledging, reconciling, and proactively managing disciplinary discontinuities in vocabularies and mental models in evolving CPSS. Lastly, we argue that a critical knowledge gap exists around how to adapt scenario-based frameworks to accommodate the shifting challenges of designing evolving CPSS. We conclude with a discussion of preliminary implications for designing human-centered frameworks for autonomous vehicles and CPSS more generally.

Keywords: cyber physical social systems; autonomous vehicles; human-centered design; data security and privacy

GLOSSARY

Cyber-Physical-Social Systems (CPSS): environments cohabited by humans and smart devices that are in virtual and physical interaction [1]
Human-centered: Regardless of human involvement, a way of thinking that focuses on human welfare aspects [2]
Scenario-based: An approach considering concrete descriptions of particular instances related to users or stakeholders, with the goal of envisioning particular outcomes [3]
Risks: Potential of situations involving exposure to danger in both cyber and physical spaces [4]

Bystander: an indirect stakeholder (any individual excluding the AV driver) [5] *(an operating definition that we explore further)*
Privacy: freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue gathering and use of data about that individual [6]
Interdisciplinarity: integration of information, data, techniques, tools, perspectives, concepts, and/or theories from two or more disciplines or bodies of specialized knowledge [7]

1. INTRODUCTION

Since Horst Rittel's well-known formulation of wicked problems, designers have been *explicitly* engaged in designing for complex systems [8]. This engagement has accelerated as designers have been required to address a continued convergence between technical factors, spanning cyber and physical domains, and social factors, encompassing social, political, and spatial dimensions, that interact dynamically to determine system performance and success [9]. Systems ranging from marine monitoring and observation infrastructure [10] to autonomous vehicles (AVs) [11] demonstrate this convergence, and have called *sociotechnical systems*, commonly used in systems engineering and organizational science research [9]. Separately, *cyber-physical-social systems* (CPSS), more commonly used in electrical, computer, and civil engineering research [12,13], have emerged as a specific instantiation of sociotechnical systems. CPSS, as defined by Yilma et al., are "[environments] *cohabited by humans and smart devices that are in a virtual and physical interaction*" [1]. We focus on CPSS, rather than sociotechnical systems, for its explicit invocation of interacting digital, physical, and social domains which must be reconciled in design.

A critical challenge in CPSS is balancing consideration of stakeholder, user, and social needs alongside complex technical factors [14]. Many frameworks and approaches to designing for CPSS, such as System-Theoretic-Process Analysis (STPA) [15], are highly effective at accounting for complex technical systems and the risks and challenges arising from their interoperability. Simultaneously, other approaches drawn from fields like Human-Computer Interaction (HCI), such as user-centered systems design [16], seek to help designers address and incorporate user and social needs to move forward in the context of CPSS. However, *risk frameworks* that are *human-centered* are less well-accounted for in many approaches to design for CPSS today. Combining these two lenses is especially essential as CPSS increasingly involves questions of privacy and information security [17], a source of risk that can be considered inherently human-centered [18,19].

In this concept paper, we seek to identify knowledge gaps that hinder integration of a human-centered perspective into risk assessment during the design of CPSS. We consider an example of AVs and bystander privacy, a representative CPSS in which a cyber-physical system, an AV, interacts with a social system, an urban environment. As described, this interaction may produce unexpected risks to bystander privacy and information security that warrant proactive design, development, and policy consideration for successful CPSS performance. We hypothesize that three themes warrant deeper exploration within CPSS, which we describe in Section 2: *human-centeredness in privacy risk assessment, human-centeredness in scenario-based risk assessment,* and *interdisciplinarity*.

To explore these themes in the context of our chosen example and develop our themes into research opportunities for the CPSS design community, we follow a conceptual approach outlined in Fig. 1. We first develop a prototype scenario-based framework describing risks presented to bystanders' privacy from a human-centered perspective. We conduct interviews (N = 7) with experts in AV design, development, and policy, focusing on security and privacy. We use our interview results to identify three preliminary knowledge gaps about human-centered risk assessment in evolving CPSS: a need for novel frameworks to apply human-centeredness to evolving CPSS design; a need to reconcile disciplinary differences in vocabulary and mental models in evolving CPSS design; a need to keep scenario-based frameworks agile as CPSS rapidly evolve, even during the course of the design process. The main contributions of this concept paper are (1) an examination of human-centered risk frameworks in bystander privacy related to AVs as an

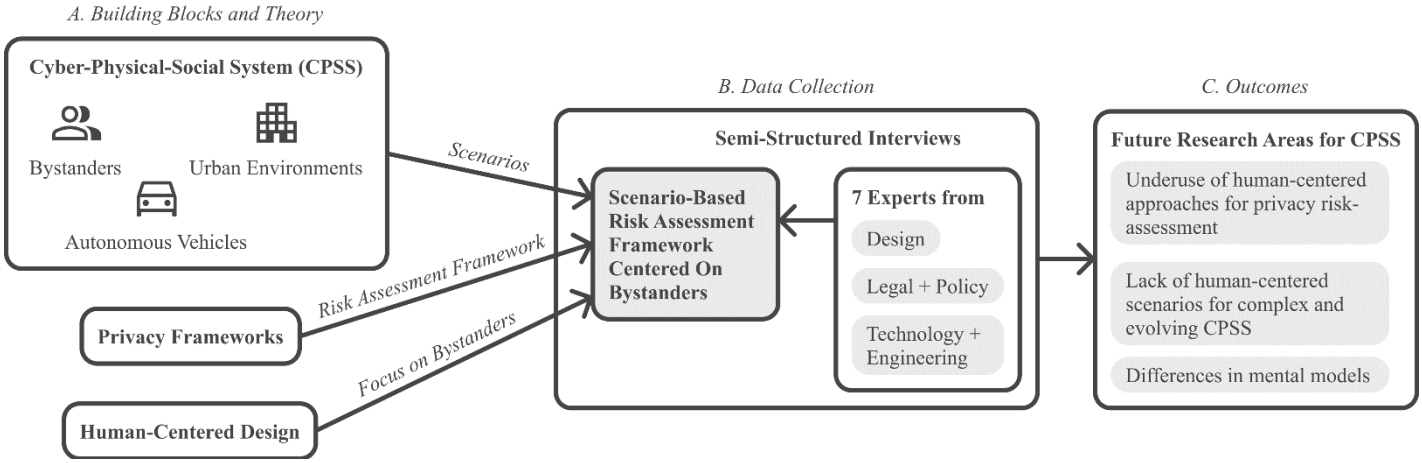

Figure I. A diagram of our research approach in this concept paper. To investigate bystander privacy in the context of autonomous vehicles, we synthesized existing research in related areas to create a framework and conducted expert interviews.

example of CPSS and (2) an overview of research opportunities and knowledge gaps to facilitate human-centered risk assessments in the design of CPSS.

We begin with a review of related work (Section 2), and describe our methodological approach (Section 3). Finally, we report and discuss our results (Section 4) and subsequent research questions exploring design research and practice regarding evolving CPSS (Section 5).

2. RELATED WORK & BACKGROUND

In this section, we consider related work on CPSS (2.1), risk assessment in design (2.2), and information security and privacy as related to autonomous vehicles (AVs) (2.3).

2.1 CPSS: Definitions, Design Frameworks and Interdisciplinarity

The concept of cyber-physical-social systems (CPSS) emerged partially to account for the fact that technical elements were "massively intertwined" [20] with human and social elements in cyber-physical systems [1,21]. In their recent review of CPSS, Yilma et al. identified five classifications of CPSS in literature [1]: *command and control*, as in Wang et al's description of smart cities [22]; *social sensing*, as in Ansari et al.'s description of human-centered production systems [23]; *self-organization*, as in Candra and Truong's description of reliability in data analysis [24]; *big data*, as in Zhu et al.'s description of mobile robotics positioning [25]; and *networking*, as in Sisyanto et al.'s description of a smart hydroponic farming system [26]. These classifications illustrate the range of applications of CPSS, and also their constituent characteristics. Yilma et al.'s definition of CPSS, which we adopt in this work, synthesizes these applications to reveal a common theme across *all* classifications, defining CPSS to be "an environment cohabited by humans and smart devices that are in a virtual and physical interaction." Here, we consider two elements of CPSS: *frameworks* to design for CPSS and the *interdisciplinarity* of CPSS design. We connect both to the *evolving nature* of CPSS themselves.

Frameworks for designing for CPSS are still emerging and draw on fields ranging from human-computer interaction to systems engineering and design. In their review of CPSS design methodologies, Zeng et al. recommend systems-level design methodologies to fully characterize, and design for, CPSS [12]; these include model- and contract-based approaches, which can account for the interaction between multiple technical components. However, the 'social' layer of CPSS is rendered in such formulations as 'user preferences,' which often insufficiently capture interactions between social environments or human actors and a given technical system. In contrast, Ansari et. al's formulation of human-centered production systems, an example of CPSS [23], distinguishes viewing humans as *users* of technology from viewing humans and machines as achieving cohesion through careful consideration and design [27]. Human-centered approaches must be a cornerstone of CPSS design frameworks.

Interdisciplinarity is a characteristic of CPSS design [28,29]. CPSS design inherently draws from disparate technical domains. However, CPSS design must also consider social systems, policy, and human behavior [30,31]. In Tsvetkova's analysis of research on human-machine networks, the authors identified dozens of disciplines involved in describing and characterizing how complex CPSS operated [32]. Crucial to realizing effective collaborations are the mental and conceptual models a team has of the work they do [33]. This is especially important in complex systems design, such as in safety science [34]**.** Esmander et al.'s study of mental models and vocabulary differences between software developers and accountants working with blockchain-enabled accounting systems, an example of CPSS, revealed significant gaps between disciplines. Some developers thought that the entire field of accounting was unnecessary due to blockchain, while accountants needed a clearer understanding of blockchain's resilience before considering any application. Meanwhile, accountants and developers had very different definitions and perceptions of 'trust' and 'transparency' in this application area [35]**.**

In this work, we expand on this previous research in three ways. First, we examine an emerging CPSS - AVs and their bystanders. Second, we build on Zeng's study on the 'social' layer of CPSS by focusing bystander privacy which captures interactions between multiple human actors (bystanders) and a technical system (AV). Third, we draw inspiration from Esmander's study of diverse stakeholders, by conducting expert interviews with practitioners who are designing CPSS to consider how frameworks are enacted in application.

2.2 Frameworks for Risk Assessment in Design

Risk assessment spans many research fields and application domains, and has given rise to frameworks specific to topics ranging from public health [36] to biosecurity [37] to child welfare [38]. Here we focus our review on *technical* risk and *interpersonal* or *social* risk, most relevant to the CPSS under consideration. A well-known standard for the development of AVs is the ISO/PAS 21448 Safety of the Intended Functionality (SOTIF) specification which builds upon ISO 26262; SOTIF addresses functional safety through technical, functional, and environmental requirements, and redirects focus toward "[maximizing] the portion of known safe scenarios" [39–41].

On the other hand, conventional cyber-risk frameworks, such as NIST, OCTAVE, and CORAS, are broadly oriented from the perspective of the technical system itself - to understand hazards that might emerge from attack or vulnerability of various components within the system [39,40]. Systems Theoretic Process Analysis (STPA), a framework originally from safety engineering, is now used in other related fields, including the AV space [42]. For example, in Mahajan et al.'s use of STPA to describe a lane-changing assist system [42], *high-level hazards* were defined as component or system failures that could cascade to catastrophic events. Large-scale risk frameworks blending technical with political considerations, such as those seeking to describe climate change, emphasize the importance of continuously updating scenarios to reflect changes in underlying systems and factors [43].

More recently, the usefulness of design methods from HCI in understanding privacy has been recognized; as Wong & Mulligan write, "design thus is not just a tool for solving privacy problems, but also a tool to broaden our understanding… about what privacy might entail" [44]. In the domain of AVs, value-sensitive design (VSD) has been increasingly adopted to understand and explore human risk. VSD, as described by Friedman et al., is the "... design of technology that accounts for human values … throughout the design process" [45]. This definition has, in application and research, sparked discussion on how to best incorporate *values*. Values in the AV industry have been traditionally considered in terms of economic worth or their relatedness to direct users [46–48]. VSD, however, highlights the need to incorporate all stakeholders when resolving value tensions and not just those of direct consumers of AVs [47]. Graubohm et al. identify distinct values associated with a range of stakeholders, both direct (such as passengers and drivers) and indirect (maintainers, politicians, traffic participants). Notably, the authors consider the effects on stakeholders' values from AV features and functionalities primarily internal to the vehicle, such as "video supervision of the vehicle interior" [49]. AV projects have already started utilizing VSD, such as the UNICARagil family vehicle program in Europe [49].

In this work, we seek to understand and build upon these existing frameworks in design and risk assessment in three ways. First, we extend on previous studies of technical risk by considering the *effects of technology*. Second, we extend upon VSD research by focusing on the topic of "bystander privacy" and by using scenario-based analysis to examine whether such approaches are used in disciplines contributing to AV development. Last, we build upon Graubohm et al.'s work to contribute a framework that incorporates not just the values of direct users of AVs, but also the values of bystanders.

2.3 Consideration of Information Security and Privacy in Autonomous Vehicles

AVs present unique multidisciplinary challenges for the design process, especially so with consideration to the security and privacy of bystanders. Earlier studies regarding security of AVs have focused on adversarial sensor attacks on cameras and lidar units [50–52], challenges with vehicle-to-x connectivity features [53,54], and developing cybersecurity-risk assessment frameworks [55,56]. With regards to AV privacy issues, prior studies have surveyed users and found that they are concerned with issues of data privacy and hacking [57], performance reliability, and AVs' interaction with pedestrians and other drivers [58–60]. In addition to perceived usefulness and performance, studies show that being able to trust AV technology is a key determinant for AV adoption [61,62].

In addition to surveying users regarding AV concerns and adoption, studies have used human-centered methods to design human-machine interaction experiences [63] and vehicle interiors [64]. In the realm of AV bystanders, one study examining pedestrians' and bicyclists' opinions with AVs concluded that more interactions with AVs would lead to a more positive attitude for the technology [65]. Other studies take a more human-centered approach to design interactions and modes of communication between AVs and pedestrians, such as Loecken's work on virtual interaction models and She's work on information communication styles between vehicles and pedestrians [66–68]. Bloom et al.'s research on perceptions of autonomous vehicles' data collection suggested that a majority of surveyed individuals were willing to spend at least five minutes to opt out of data collection, and had high levels of discomfort associated with secondary uses of data gathered by autonomous vehicles [69].

In this work, we extend on prior research addressing various elements of AVs, pedestrian trust, and data privacy in two ways. Extending from She's, Loecken's, and Bloom et al.'s research, we seek to understand not how bystanders perceive AVs, but how designers and other stakeholders in AVs' development *consider bystanders.* Furthermore, we specifically consider implications for pedestrians that are related to data privacy and security, with a scenario-based lens.

Table 1: Semi-structured Interview Questions

Section Topic	**Sample Questions**
Introduction	Could you briefly tell us about your role, responsibility, and affiliation? What aspect of your role is related to autonomous or automated vehicles (AV)?
Experiences with Current Cybersecurity Practices	How do you define security and privacy in your work? What do you think are gaps and/or roadblocks around assessing AV Privacy in your domain (cybersecurity, policy and law, or engineering), if any?
Bystanders	Who do you perceive as "bystanders" in AV settings? Why? Talk us through how you consider AV systems and their interaction with bystanders. Are there specific frameworks or tools you leverage to consider the security and privacy of AV users and bystanders?
Our Framework	How could you envision using a framework like this in your work related to security or autonomous vehicles? Why? What overall outcomes do you expect from implementing this framework? What scenarios may not be well-described by it?

3. METHODS

In this section, we describe our interview and study protocols (3.1), preliminary framework development (3.2), and data collection and analysis procedures (3.3).

3.1 Interview Study Protocols and Details

This study was approved by UC-Berkeley's Institutional Review Board. Pairs of researchers conducted 45-minute, semi-

structured interviews for all 7 participants. Each participant was offered an Amazon Gift Card for their participation in the interview. Interviews were held and recorded on Zoom with the consent of the participants. Recordings were immediately transcribed and de-identified.

Our interview approach sought to foreground questions in terms of experts' direct experience with AVs. Thus, terms like 'cyber-physical-social system' were explicitly not invoked by interviewers in questioning. Each interview broadly followed the structure outlined in Table 1, with introductions, cybersecurity and privacy-specific questions, a discussion about bystanders, and then finally, a presentation of our prototype framework.

3.2 Preliminary Framework Development

To develop a preliminary human-centered scenario-based framework to assess privacy risks of AVs to secondary stakeholders - bystanders - we began by first cataloging the types and scope of sensors currently or projected to be deployed in AVs. Multiple types and scales of sensors are standard in current designs of AVs, including global positioning systems (GPS), lidar, radar, and multiple cameras [69,70]. The type and scope of sensors indicate what types of data might be readily collected by AVs and allowed us to extrapolate follow-on impacts. Here, we draw on two primary research topics. First, we follow Insua et al.'s work on developing an adversarial risk analysis framework, which informs how our framework relates cyber- and physical threats, and their connection to cost to victims [71]. Second, we follow Cavoukian's work on operationalizing privacy-by-design, to help identify unique scenarios for consideration [72]. We extend our framework from the thesis that human-centered design applied to stakeholders beyond the vehicle can help, in Cavoukian's terms, "prevent privacy-invasive events before they happen" [72]. To further learn about the specific scenarios and impacts of situations of the bystander in AV suites, we identified the definition of "bystander" as *an indirect stakeholder (any individual excluding the driver)*. This definition is inspired by Yao et al.'s and Sleeper et al's work on privacy considerations for [5,73]. We also accounted for vehicles with all levels of automation, from level 3 (conditional automation), level 4 (high automation), to level 5 (full automation) [74]. This framework may allow AV industries to consider a variety of cases in which automation may be harmful.

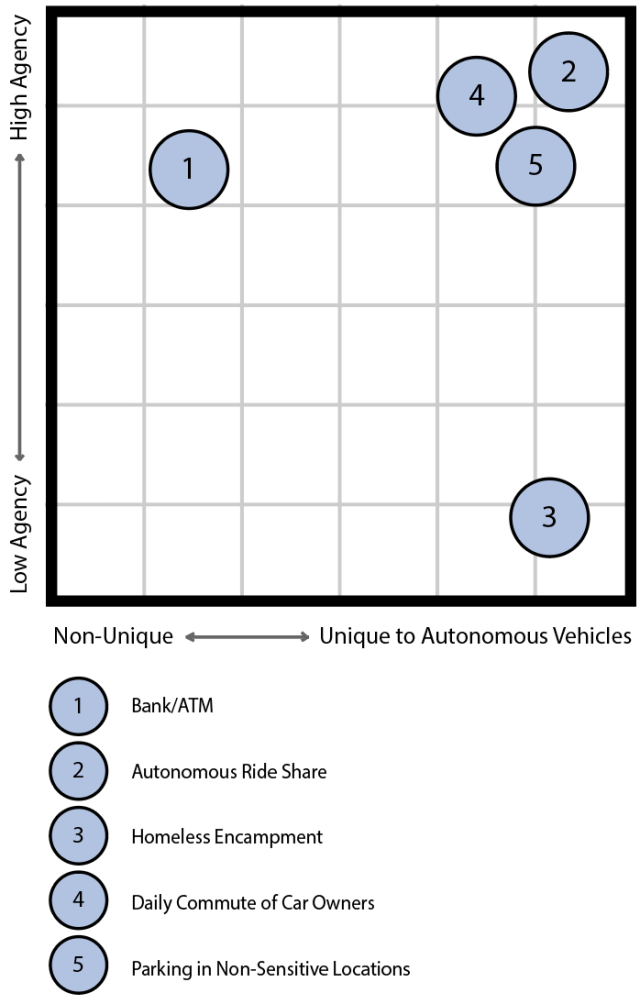

Figure 1. Framework for Scenarios

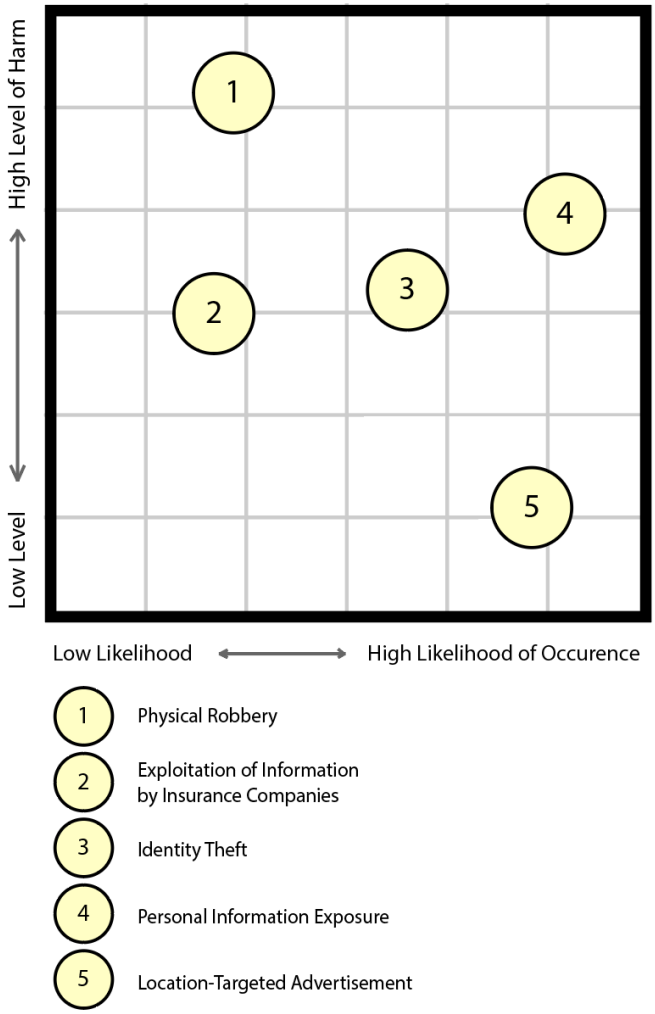

Figure 2. Framework for Impacts

Our framework, as specifically instantiated here, is concerned with developing and integrating best practices to consider bystander privacy during the decision-making process surrounding the development and regulation of AVs. We seek for it to be *generalizable* to allow stakeholders involved in CPSS development to quickly identify and evaluate risk scenarios in a human-centered fashion.

First we identify dimensions of (1) level of bystander consent, what we term agency, and (2) uniqueness of privacy risk presented by AVs, as opposed to other devices and systems (Fig. 1). These dimensions describe various *scenarios* in which AVs may create privacy risk. Shown in the figure are five example scenarios presented to interviewees to illustrate how a tool like this could help stakeholders in AV development conceptualize risk scenarios for consideration, analysis, and management.

Second, we identify dimensions of (1) likelihood of occurrence and (2) level of harm (Fig. 2). These dimensions help establish the *impacts* that might result from autonomous vehicles' collection of bystander data.

Table 2: Interview Participant Information, by Subject

Participant Number	Domain of Expertise	Years of Experience in the Automotive / Information Security / AV sectors
P1	Technology, Security	20+
P2	Security, Design	5-10
P3	Technology, Policy	20+
P4	Policy	5-10
P5	Policy	10-20
P6	Technology, Security	10-20
P7	Technology	10-20

Table 3: Interview Participant Information, Overview

Demographic Aspect		Percentage
Domain of Expertise	Technology	57%
	Security	43%
	Policy	43%
	Design	14%
Years of Experience	1-5	0%
	5-10	28%
	10-20	43%
	20+	28%

3.3 Data Collection & Analysis

From the AV and security industries, we contacted participants with backgrounds, roles, and expertise in the areas of technology, policy, security, and design. Demographic background details about the 7 participants interviewed are listed in Table 2 and Table 3. Participants had an average of 14 years of experience specifically in the automotive, security and/or AV sectors. We note that several participants represented more than one discipline, accounting for a >100% total in Table 3. After transcribing the interviews, we utilized thematic analysis on our data. We identified key quotes and formulated key takeaways for each interview, and clustered key findings across interviews to surface thematic patterns in the data.

4. FINDINGS & EMERGING HYPOTHESES

In this section, we review preliminary findings, organized by theme, and discuss how they inform emerging hypotheses. We first address how our interviewees consider risk from human-centered perspectives (Section 4.1). Next, we consider emerging disciplinary gaps that occur during consideration of AVs and privacy (Section 4.2). Lastly, we describe challenges and opportunities for scenario-based frameworks in assessing risks associated with AVs and bystanders (Section 4.3).

4.1. Theme 1: Human-centeredness in Privacy Risk Assessment in Evolving CPSS

4.1.1. Hypothesis 1.1: Frameworks leveraged by technologists and policy experts appear to focus on technical risk, rather than human-centered risk considering bystanders and other stakeholders.

Interviews with experts in cybersecurity, technology and policy suggest the importance of technical- and cyber-risk-focused approaches, rather than human-centered risk as related to bystanders. This is revealed in the majority of interview findings, with 6 out of 7 participants (excluding P2) implying that they do not consider bystanders in their work related to AVs. As P7 said,

> "But I don't think, and I have not seen… a general concern about protecting the security of the people around the vehicle… all the places that I've worked in… [is] usually the most concerned [with] what the user is experiencing, rather than other people that may be around." **(P7)**

There are many different frameworks and methodologies for assessing risk that interviewees have found useful in their work with AVs, including threat-based methodologies and safety prevention protocols. Interestingly, P1 discussed *moral* risks that may occur, which approached a discussion of values and stakeholders, but stayed at a level of frameworks rather than implications. In discussing a hypothetical example of an accident involving members of disadvantaged communities, and the possibility that this would raise issues of discrimination in autonomous systems, P1 identified:

> "... a contrast [between the] moral decision-making element [and] security and hazard analysis." **(P1)**

Meanwhile, P7 focused their response on safety analysis, a practice to identify failure modes and points in a system. In their discussion of their work with AVs specifically, software controls the vehicle, increasing the size of the attack surface. P7 framed their consideration of risk in these terms:

> "Functional safety [is] trying to identify the hazards derived from unintended activation of certain functions." **(P7)**

P7 went on to identify common methodologies such as threat analysis and "damage scenarios" that can account for all types of harm that can possibly happen. Both P1 and P7 referenced approaches such as SFOP (Safety, Financial, Operational, and Privacy) [75] or TARA (Threat Agent Risk Assessment) [76].

These findings suggest that despite the interest in stakeholders and end-users in AVs and CPSS more broadly, those tasked with developing and designing such systems rarely consider human-centered risk associated with non-end-user stakeholders in their work. Notably, it is revealed that the only participant who had a divergent viewpoint, P2, has a partial design role; this suggests that among key stakeholders in AVs' development, designers offer a distinct perspectival role regarding human-centered risk of non-end-user participants.

4.1.2. Hypothesis 1.2: Human-centered frameworks for risk are nascent in their application to AVs.

Policies regarding AVs are evolving and findings suggest that human-centered considerations are not a primary concern for practitioners. The AV industry is emerging, as P6 suggests, and it is not necessarily oriented towards human-centered challenges, and bystanders are not familiar with the idea of privacy and security regarding AV systems:

> "Reading the privacy policy of [a] Google or Apple [product] is far easier than reading [the privacy policy of] your favorite [car] manufacturer."
>
> "[AVs] are perpetually five years away." **(P6)**

Considering the lack of knowledge for most consumers at this time, this implies that human-centered considerations may be accounted for after further use and development. In contrast, P2, a systems engineer with responsibilities related to design, described the use of test cases in their work:

> "... [we] define through test cases, which shows whether we are discriminatory or not [when creating a framework for AVs]." **(P2)**

P2 later surfaced the concept of value sensitive design (VSD), and highlighted the importance of engaging both stakeholders and end users. VSD is intended to account for situations stemming from a broader base of stakeholders than may be immediately evident. P2 further underlined the importance of moral psychology, using deontological arguments for high risk scenarios while consequential arguments for low risk scenarios.

These findings suggest that the AV developers and designers may not yet be acclimated to human-centered considerations within the field. In particular, it is revealed that the shortage of consumers and available case studies with the use of AVs makes it difficult to create and assess frameworks. We see a research opportunity for frameworks and processes that can better account for human-centered considerations.

4.2. Theme 2: Interdisciplinarity in the design of evolving CPSS.

4.2.1. Hypothesis 2.1: Mental Models of CPSS differ across multidisciplinary participants.

Participants had varying perceptions of the current considerations for security and privacy in the AV industry and the future effects on privacy as AVs become more common. As policy expert P5 said, their mental model of what 'safety' represents invoked questions rather than a definitive explanation:

> "The big question that… still remains somewhat unsolved… is how do you define a safe autonomous vehicle… it might be easy to say 'safer than a human driver,' [but] then the question is… how much safer and how are you measuring that." **(P5)**

Within our interviews, we inquired about the relationship between security and privacy. There was a mixed response on how interrelated privacy and security are, and not all participants explicitly defined the terms. While 4 out of 7 participants mentioned that security is a given or necessary component, 2 out of 7 participants mentioned that the AV industry lacks a specific definition on what is considered safe or secure enough. P6, whose roles crossed security and technology, articulated two radically different mental models of privacy associated with AVs, one positive, and one negative:

> "[One school of thought is] there's going to be so many more sensors and … collection of data and that's going to create problems… The second school of thought… [is] you will enjoy greater privacy with autonomous vehicles, because… [we] will see more obfuscation of data just because it's a shared experience." **(P6)**

Participant P7, a technologist, shared another mental model of privacy related to AVs - that it was no source of risk:

> "I have never thought about having privacy as an issue, other than in the way that we are consuming data for the development of the vehicles … I honestly don't know if there's any … [concerns for] the way that those images are being used." **(P7)**

Participant P3, a technologist working with policy, added further nuance to P7's perspective, arguing that AV privacy risks simply duplicated risks associated with other aspects of daily life:

> "Your sense of anonymity… doesn't exist in public spaces … why is it different for AVs?" **(P3)**

This point was mentioned by 4 out of 7 participants, illustrating the range of diverse perspectives on privacy risks associated with AVs among our interviewees.

Also revealing of mental models were analogies participants drew to explain critical topics. Related to P3's point above, Participant P4 described AVs' data collection risks this way:

> "... these are **just smartphones on wheels**. And it really is a good analogy there because there are just as many different entities interested in obtaining information gained from a smartphone." **(P4)**

P6 described users' and bystanders' abilities to manage their data and privacy preferences this way:

> "... once you get into the autonomous vehicle [consumers' ability to understand privacy risks] gets even worse, I mean … this stuff is as close to black magic as anything that we see in the world." **(P6)**

These findings suggest that diverse mental models exist among experts in considering concepts that range from the essential, such as what AVs are, to the inherently broad, such as what constitutes "security" and "privacy." While our sample size is not sufficient to draw definitive conclusions about the relationship between mental models and discipline, these results present an opportunity for further research into the nature of these disciplinary differences. Considering the importance of shared mental models in design and development [33], future models and frameworks for addressing bystander privacy risks in AVs should take into account stakeholders' diverse perceptions of foundational concepts. These findings echo and further develop Esmander et al.'s research on significant differences in mental models between accountants and software developers, highlighting the need for reconciliation across disciplines in the design and development of AVs [35].

4.2.2. Hypothesis 2.2: Vocabulary of CPSS differs across multidisciplinary participants.

Zooming in from differing mental models, several vocabulary terms presented conflicting disciplinary perspectives. In discussing how AVs' data collection interfaces with bystanders, we introduced the concept of agency, critical to consent in data sharing. P6, a technologist, used the term as follows:

> "... I don't know how anything has high agency - [users and bystanders] have no idea this is happening, right?" **(P6)**

While evincing a clear opinion about the nature of agency in data collection, P6 illustrates clear fluency with the term agency as used in the context of data collection. In contrast, P4, a policy expert, had a different response to agency:

> "[You will need to] distinguish how you're using the term from the more traditional legal uses of the term agency." **(P4)**

This comment from P4 highlights differences in vocabulary and contextual associations of key terms between disciplines critical to AV development.

This finding suggests that the interdisciplinary nature of AV development will invite significant vocabulary challenges as disciplines engage with one another. The example of agency focuses on the nuances of our guiding design framework. As technologists, we bring a technical lens to both our work and vocabulary; in contrast to our experience, P4, as a policy expert, challenged the notion of 'agency' as a viable dimension for our framework, given its disciplinary implications. This finding suggests that calibrating frameworks to account for disciplinary context will be essential to AVs and CPSS generally.

4.3. Theme 3: Human-centeredness in scenario-based risk assessment.

4.3.1. Hypothesis 3.1: Scenario-based frameworks need to account for ongoing contextual change surrounding CPSS.

CPSS of AVs present numerous stakeholders and constantly evolving policy, technology, and social conditions which are not captured through scenario based-frameworks. P4 suggested that identifying various stakeholders is a crucial precursor for scenario-based analysis:

> "Before you try to establish a framework for how entities can use data … figure out who all the potential stakeholders are and I don't think that is easy. I think that [stakeholders] will continue to increase." **(P4)**

Stakeholders will likely increase and change over time. This complicates efforts to understand these stakeholders, as noted above, but may also make prior scenario-based analyses obsolete. This applies not only to the role of stakeholders but also the policy context in which AVs are implemented. P5 argued that policies related to technology implementation must be considered into scenario-based risk assessment:

> "...the way that [autonomous vehicles] are rolled out are pretty radically different…if you just lump autonomous as a robot taxi then you're missing a lot of what is actually happening." **(P5)**

Interestingly, AV implementation policies continue to evolve, as discussed in section 4.2.1, further complicating this assessment. P2 articulated the need for scenario-based frameworks to account for ongoing technology change:

> "[uniqueness to autonomous vehicles] will definitely go down naturally as technology progresses and as sensors that we're using are no longer unique to autonomous vehicles" **(P2)**

P2's argument that as AVs become more prevalent, specific AV technologies, e.g. lidar, may no longer remain unique to the application of AVs. This finding also supports P5's recommendation on integrating implementation policies by

suggesting that applications of specific technologies may evolve overtime, thereby modifying the perceived risk of those technologies in the context of Avs.

These findings suggest that as AVs continue to evolve, scenarios to describe their impact, and ultimately inform thoughtful design decision-making must shift as well. Notable among these findings is the fact that technological change is only part of the changing landscape. Social factors and implementation factors may also undergo quick change, requiring scenarios to shift to account for them. These results follow work in climate risk assessment, which also emphasized continuously updating scenarios [38].

4.3.2. Hypothesis 3.2: Scenario-based frameworks need a mechanism to be translated into design processes.

While scenario-based frameworks provide a structure to consider the consequences of AVs on bystanders, these frameworks need mechanisms to allow them to be translated into the traditional process of engineering, design, and policymaking. P2, a systems engineer with responsibility for design, argued:

> "…how you get into the actual engineering or [other] decisions that are being made…that translation layer is going to be very important." **(P2)**

P2's argument that scenario-based frameworks should include a "translation layer" suggests that the work of converting insights into engineering or design requirements requires specific effort. P2 went on to share an example of a scenario where a pedestrian wants to cross a street in front of an AV that could be driving very quickly or very slowly, translating into "requirements on smoothness in terms of acceleration and deceleration." The need for integrating scenario-based frameworks in policy making related to AVs was described by P5, who suggested that scenario-based frameworks would "definitely help policymakers' number one [priority]":

> "...some language and clarity… for the level of exposure that you should expect and there are some litigations and these are some areas where you look to create mitigations and safeguard." **(P5)**

The integration of scenario-based frameworks in engineering, design, and policy processes currently appears to be lacking. This finding is consistent with the low prevalence of human-centered risk frameworks in the development of AVs and associated policies as discussed in section 4.1.

5. KNOWLEDGE GAPS, RESEARCH OPPORTUNITIES AND TAKEAWAYS FOR DESIGN OF EVOLVING CPSS

While our findings are specifically grounded in autonomous vehicles, they have implications for research into *evolving* CPSS and invite research questions extending from our themes. These, along with corresponding implications, are described in Table 4.

Theme 1. Human-centered approaches for CPPS privacy risk assessment appear not to be widely used, highlighting the need for CPSS to emphasize the 'social' alongside the cyber and the physical. In many ways, these findings reinforce Zeng et al.'s analysis of systems-level modeling of CPSS: CPSS are predominantly analyzed and modeled via technical analyses [12]. Our preliminary findings suggest that CPSS-like autonomous vehicles have significant effects on stakeholders that may not be readily considered by traditional frameworks. Our research question for the field of evolving CPSS is thus *how can human-centered approaches for describing risks integrate with existing technical frameworks for analyzing CPSS?* This issue becomes especially crucial considering our hypotheses for Theme 3, about the changing conditions of AVs and particularly the proliferation of stakeholders.

Theme 2. Differing disciplinary participants evince different vocabularies and mental models of critical components of autonomous vehicles, which has several implications for future CPSS research. First, as much of CPSS design and analysis activity is interdisciplinary [28,29], gaps in vocabularies and mental models between disciplines will likely complicate many CPSS design and analysis efforts. For example, differences in mental models for "privacy" risks may imply differences in "human values" in the contexts of Value-Sensitive Design for CPSS [45]. Furthermore, these gaps may expand as various disciplines follow different trajectories to navigate evolving CPSS and the conditions surrounding them. Second, as evolving CPSS introduces *entirely new* vocabularies and concepts to absorb, further divergences can only be expected. Esmander et al.'s study of diverging mental models concerning the adoption of blockchain highlighted this: software developers had vastly different mental models of blockchain than accountants did, despite both groups working on the same accounting system [35]. Our corresponding research question for the field of evolving CPSS is thus *what design ontologies and frameworks can facilitate interdisciplinary shared mental models even as CPSS and their contexts shift rapidly?*

Theme 3. Scenario-based frameworks designed to aid in the design of autonomous vehicles may rapidly become obsolete due to changing contexts directly relates to the theme of evolving CPSS. Scenario-based frameworks, like SOTIF [41], offer design practitioners the ability to envision and account for specific contexts in ways that more abstract frameworks cannot. However, in CPSS, these scenarios may quickly go out of date; our findings suggest that for the case of autonomous vehicles and bystander privacy, this obsolescence has already occurred. Best practices from other domains, e.g. climate change, are to continuously update scenarios and their associated risks [43]. Our corresponding research question for the field of evolving CPSS is twofold: first, *how can we ensure that scenarios related to design frameworks for CPSS remain relevant amid changing conditions?* Second, *how can we enable CPSS designers to envision and account for concrete and relevant scenarios?* Methods to explore these questions may lie at the intersection of traditional design, speculative design [77], and strategic foresight [78]. These latter approaches invite an exploration of future *possibilities*, potentially accounting for evolving CPSS.

Table 4: Summary of Knowledge Gaps, Research Questions, and Potential Implications.

CPSS Themes & Gaps	Research Questions for Evolving CPSS	Implications on CPSS Design Research
Human-centeredness in privacy risk assessment	What is the difference between technical privacy risks and human-centered risks considering bystanders and other stakeholders?	Understanding the ways in which human-centered and technical frameworks diverge and converge and using this understanding to build holistic design tools for CPSS.
	What are barriers to adopting human-centered risk assessment in technical, design, and policy disciplines?	Making human-centered frameworks more prevalent in the design of CPSS across the technical and policy domains.
Human-centeredness in scenario-based risk assessment	How can we account for the complexity of stakeholders in CPSS scenarios?	Seamless integration of the "social" during CPSS design.
	How can scenario-based frameworks better account for changing policy, technology, or social dimensions characterizing CPSS?	Ensuring that human-centered scenario frameworks remain relevant and reliable as CPSS evolve.
	How can we enable CPSS designers to envision and account for concrete and relevant scenarios?	Improving the quality and reliability of human-centered scenario frameworks for CPSS design.
Interdisciplinarity in the design of evolving CPSS	How does the vocabulary to describe CPSS topics differ across various disciplines, and how can we bridge and reconcile these differences?	Reconciling different mental models across disciplines involved in designing CPSS and affording more seamless collaboration through a shared vocabulary.
	What ontologies and frameworks facilitate interdisciplinary dialogue as CPSS contexts shift?	Enabling interdisciplinary collaboration during CPSS design CPSS as its related mental models evolve.

This work has several limitations. First, a relatively small sample size limits the generalizability of our findings. To address this, ongoing research involves interviewing more practitioners. Second, the inherently complex nature of autonomous vehicles as related to bystander privacy means that all disciplinary and functional roles related to this CPSS were not engaged. We hope to interview participants from disciplines not already represented in the future. Third, CPSS is multifaceted, and consideration of all elements of autonomous vehicles and privacy, for example infrastructure and services, could not be explored here. We thus view our initial focus on autonomous vehicles and bystander privacy as a point of departure for further research. Last, given the sparseness of our data, we cannot establish a strong conclusion about what a human-centered scenario-based framework would look like; we intend to conduct a survey study similar to Bloom's [69], to validate findings.

6. CONCLUSIONS

In this work, we explore the challenges and opportunities for developing human-centered risk frameworks for cyber-physical-social systems. We examine the example of autonomous vehicles and their data privacy risks and seek to explore how practitioners working in this field consider human-centered risk in their work. Through interviews with experts, we identify three themes that invite further development of human-centered risk frameworks to support and impact design of CPSS. First, few frameworks adopted by practitioners appeared to be human-centered. Second, differing disciplinary contributors to autonomous vehicles had differing vocabularies and mental models of critical aspects of designing for CPSS. Lastly, scenario-based frameworks, even when human-centered, risked quick obsolescence without updates due to the changing components and context of CPSS. These gaps and opportunities for design researchers exploring evolving CPSS.

7. ACKNOWLEDGEMENTS

The authors would like to thank Yuhan Xie for their contributions, and Dr. Euiyoung Kim for inspiring this research area. The authors acknowledge support from the Center for Long-Term Cybersecurity to make this research possible.

REFERENCES

[1] Yilma, B. A., Panetto, H., and Naudet, Y., 2021, "Systemic Formalisation of Cyber-Physical-Social System (CPSS): A Systematic Literature Review," Comput. Ind., **129**, p. 103458.

[2] "What Is Human-Centered Design?," Interact. Des. Found. [Online]. Available: https://www.interaction-design.org/literature/topics/human-centered-design. [Accessed: 12-May-2022].

[3] Carroll, J. M., 1997, "Chapter 17 - Scenario-Based Design," *Handbook of Human-Computer Interaction (Second Edition)*, M.G. Helander, T.K. Landauer, and P.V. Prabhu, eds., North-Holland, Amsterdam, pp. 383–406.

[4] "Cybersecurity Risk - Glossary | CSRC" [Online]. Available:

https://csrc.nist.gov/glossary/term/cybersecurity_risk. [Accessed: 12-May-2022].

[5] Sleeper, M., Schnorf, S., Kemler, B., and Consolvo, S., 2015, "Attitudes toward Vehicle-Based Sensing and Recording," *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, Association for Computing Machinery, New York, NY, USA, pp. 1017–1028.

[6] Garfinkel, S. L., 2015, "NISTIR 8053. de-Identification of Personal Information," Natl. Inst. Stand. Technol. US Dep. Commer. Gaithersburg Md. USA.

[7] National Academy of Sciences, National Academy of Engineering, and Institute of Medicine, *Facilitating Interdisciplinary Research*, Washington, DC: The National Academies Press.

[8] Rittel, H. W., and Webber, M. M., 1973, "Dilemmas in a General Theory of Planning," Policy Sci., **4**(2), pp. 155–169.

[9] Heydari, B., Szajnfarber, Z., Panchal, J., Cardin, M.-A., Holtta-Otto, K., and Kremer, G. E., 2020, "Analysis and Design of Sociotechnical Systems," J. Mech. Des., **142**(12).

[10] Singh, M. P., 2014, "Norms as a Basis for Governing Sociotechnical Systems," ACM Trans. Intell. Syst. Technol. TIST, **5**(1), pp. 1–23.

[11] Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., and Zhao, K., 2015, "Cyber-Physical-Social System in Intelligent Transportation," IEEECAA J. Autom. Sin., **2**(3), pp. 320–333.

[12] Zeng, J., Yang, L. T., Lin, M., Ning, H., and Ma, J., 2020, "A Survey: Cyber-Physical-Social Systems and Their System-Level Design Methodology," Future Gener. Comput. Syst., **105**, pp. 1028–1042.

[13] Dressler, F., 2018, "Cyber Physical Social Systems: Towards Deeply Integrated Hybridized Systems," *2018 International Conference on Computing, Networking and Communications (ICNC)*, IEEE, pp. 420–424.

[14] Baxter, G., and Sommerville, I., 2011, "Socio-Technical Systems: From Design Methods to Systems Engineering," Interact. Comput., **23**(1), pp. 4–17.

[15] Ishimatsu, T., Leveson, N. G., Thomas, J. P., Fleming, C. H., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H., and Hoshino, N., 2014, "Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis," J. Spacecr. Rockets, **51**(2), pp. 509–522.

[16] Norman, D. A., and Draper, S. W., eds., 1986, *User Centered System Design: New Perspectives on Human-Computer Interaction*, CRC Press, Hillsdale, N.J.

[17] Malatji, M., Von Solms, S., and Marnewick, A., 2019, "Socio-Technical Systems Cybersecurity Framework," Inf. Comput. Secur., **27**(2), pp. 233–272.

[18] LeFebvre, R., 2012, "The Human Element in Cyber Security: A Study on Student Motivation to Act," *Proceedings of the 2012 Information Security Curriculum Development Conference*, ACM, New York, NY, USA, pp. 1–8.

[19] Mancuso, V. F., Strang, A. J., Funke, G. J., and Finomore, V. S., 2014, "Human Factors of Cyber Attacks: A Framework for Human-Centered Research," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, SAGE Publications Sage CA: Los Angeles, CA, pp. 437–441.

[20] Horvath, I., 2012, "Beyond Advanced Mechatronics: New Design Challenges of Social-Cyber-Physical Systems," *Proceedings of the 1st Workshop on Mechatronic Design, Linz (Austria), 27-29 June, 2012*, Citeseer.

[21] Kant, V., 2016, "Cyber-Physical Systems as Sociotechnical Systems: A View towards Human–Technology Interaction," Cyber-Phys. Syst., **2**(1–4), pp. 75–109.

[22] Wang, P., Yang, L. T., and Li, J., 2018, "An Edge Cloud-Assisted CPSS Framework for Smart City," IEEE Cloud Comput., **5**(5), pp. 37–46.

[23] Ansari, F., Khobreh, M., Seidenberg, U., and Sihn, W., 2018, "A Problem-Solving Ontology for Human-Centered Cyber Physical Production Systems," CIRP J. Manuf. Sci. Technol., **22**, pp. 91–106.

[24] Candra, M. Z., and Truong, H.-L., 2016, "Reliable Coordination Patterns in Cyber-Physical-Social Systems," *2016 International Conference on Data and Software Engineering (ICoDSE)*, IEEE, pp. 1–6.

[25] Zhu, Z., Wen, Y., Zhang, Z., Yan, Z., Huang, S., and Xu, X., 2020, "Accurate Position Estimation of Mobile Robot Based on Cyber-Physical-Social Systems (CPSS)," IEEE Access, **8**, pp. 56359–56370.

[26] Sisyanto, R. E. N., and Kurniawan, N. B., 2017, "Hydroponic Smart Farming Using Cyber Physical Social System with Telegram Messenger," *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, IEEE, pp. 239–245.

[27] Hadorn, B., Courant, M., and Hirsbrunner, B., 2016, *Towards Human-Centered Cyber-Physical Systems: A Modeling Approach*, Université de Fribourg.

[28] Vogel-Heuser, B., Böhm, M., Brodeck, F., Kugler, K., Maasen, S., Pantförder, D., Zou, M., Buchholz, J., Bauer, H., and Brandl, F., 2020, "Interdisciplinary Engineering of Cyber-Physical Production Systems: Highlighting the Benefits of a Combined Interdisciplinary Modelling Approach on the Basis of an Industrial Case," Des. Sci., **6**.

[29] Darwish, A., and Hassanien, A. E., 2018, "Cyber Physical Systems Design, Methodology, and Integration: The Current Status and Future Outlook," J. Ambient Intell. Humaniz. Comput., **9**(5), pp. 1541–1556.

[30] Smirnov, A., Levashova, T., Shilov, N., and Sandkuhl, K., 2014, "Ontology for Cyber-Physical-Social Systems Self-Organisation," *Proceedings of 16th Conference of Open Innovations Association FRUCT*, IEEE, pp. 101–107.

[31] Sowe, S. K., Simmon, E., Zettsu, K., De Vaulx, F., and Bojanova, I., 2016, "Cyber-Physical-Human Systems: Putting People in the Loop," IT Prof., **18**(1), pp. 10–13.

[32] Tsvetkova, M., Yasseri, T., Meyer, E. T., Pickering, J. B., Engen, V., Walland, P., Lüders, M., Følstad, A., and

Bravos, G., 2017, "Understanding Human-Machine Networks: A Cross-Disciplinary Survey," ACM Comput. Surv. CSUR, **50**(1), pp. 1–35.

[33] Wood, M., Chen, P., Fu, K., Cagan, J., and Kotovsky, K., 2014, "The Role of Design Team Interaction Structure on Individual and Shared Mental Models," *Design Computing and Cognition'12*, Springer, pp. 209–226.

[34] Blokland, P., and Reniers, G., 2020, "Safety Science, a Systems Thinking Perspective: From Events to Mental Models and Sustainable Safety," Sustainability, **12**(12), p. 5164.

[35] Esmander, R., Lafourcade, P., Lombard-Platet, M., and Negri-Ribalta, C., 2020, "A Silver Bullet? A Comparison of Accountants and Developers Mental Models in the Raise of Blockchain," *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–10.

[36] Mindell, J. S., Boltong, A., and Forde, I., 2008, "A Review of Health Impact Assessment Frameworks," Public Health, **122**(11), pp. 1177–1187.

[37] Dahlstrom, A., Hewitt, C. L., and Campbell, M. L., 2011, "A Review of International, Regional and National Biosecurity Risk Assessment Frameworks," Mar. Policy, **35**(2), pp. 208–217.

[38] Pecora, P. J., Chahine, Z., and Graham, J. C., 2013, "Safety and Risk Assessment Frameworks: Overview and Implications for Child Maltreatment Fatalities," Child Welfare, **92**(2), pp. 143–160.

[39] Kirovskii, O. M., and Gorelov, V. A., 2019, "Driver Assistance Systems: Analysis, Tests and the Safety Case. ISO 26262 and ISO PAS 21448," *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, p. 012019.

[40] Rao, D., Pathrose, P., Huening, F., and Sid, J., 2019, "An Approach for Validating Safety of Perception Software in Autonomous Driving Systems," *International Symposium on Model-Based Safety and Assessment*, Springer, pp. 303–316.

[41] Walker, A., 2019, "SOTIF the Human Factor," *European Conference on Software Process Improvement*, Springer, pp. 575–584.

[42] Mahajan, H. S., Bradley, T., and Pasricha, S., 2017, "Application of Systems Theoretic Process Analysis to a Lane Keeping Assist System," Reliab. Eng. Syst. Saf., **167**, pp. 177–183.

[43] O'Neill, B. C., Carter, T. R., Ebi, K., Harrison, P. A., Kemp-Benedict, E., Kok, K., Kriegler, E., Preston, B. L., Riahi, K., and Sillmann, J., 2020, "Achievements and Needs for the Climate Change Scenario Framework," Nat. Clim. Change, **10**(12), pp. 1074–1084.

[44] Wong, R. Y., and Mulligan, D. K., 2019, "Bringing Design to the Privacy Table: Broadening “Design” in “Privacy by Design” Through the Lens of HCI," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, NY, USA, pp. 1–17.

[45] Friedman, B., Kahn, P. H., Borning, A., and Huldtgren, A., 2013, "Value Sensitive Design and Information Systems," *Early Engagement and New Technologies: Opening up the Laboratory*, Springer, pp. 55–95.

[46] Watkins, K. E., 2021, "Using Value Sensitive Design to Understand Transportation Choices and Envision a Future Transportation System," Ethics Inf. Technol., **23**(1), pp. 79–82.

[47] Christian Gerdes, J., Thornton, S. M., and Millar, J., 2019, "Designing Automated Vehicles Around Human Values," *Road Vehicle Automation 6*, G. Meyer, and S. Beiker, eds., Springer International Publishing, Cham, pp. 39–48.

[48] Umbrello, S., and Yampolskiy, R. V., 2022, "Designing AI for Explainability and Verifiability: A Value Sensitive Design Approach to Avoid Artificial Stupidity in Autonomous Vehicles," Int. J. Soc. Robot., **14**(2), pp. 313–322.

[49] Graubohm, R., Schräder, T., and Maurer, M., 2020, "Value Sensitive Design in the Development of Driverless Vehicles: A Case Study on an Autonomous Family Vehicle," Proc. Des. Soc. Des. Conf., **1**, pp. 907–916.

[50] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Tramer, F., Prakash, A., Kohno, T., and Song, D., 2018, "Physical Adversarial Examples for Object Detectors."

[51] Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., Chen, Q. A., Fu, K., and Mao, Z. M., 2019, "Adversarial Sensor Attack on LiDAR-Based Perception in Autonomous Driving," *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, New York, NY, USA, pp. 2267–2281.

[52] Petit, J., Stottelaar, B., and Kargl, F., "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," p. 13.

[53] Zhang, T., Antunes, H., and Aggarwal, S., 2014, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," IEEE Internet Things J., **1**(1), pp. 10–21.

[54] Lu, N., Cheng, N., Zhang, N., Shen, X., and Mark, J. W., 2014, "Connected Vehicles: Solutions and Challenges," IEEE Internet Things J., **1**(4), pp. 289–299.

[55] Kong, H.-K., Hong, M. K., and Kim, T.-S., 2018, "Security Risk Assessment Framework for Smart Car Using the Attack Tree Analysis," J. Ambient Intell. Humaniz. Comput., **9**(3), pp. 531–551.

[56] Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., and Wang, J., 2021, "A Systematic Risk Assessment Framework of Automotive Cybersecurity," Automot. Innov., **4**(3), pp. 253–261.

[57] Woldeamanuel, M., and Nguyen, D., 2018, "Perceived Benefits and Concerns of Autonomous Vehicles: An Exploratory Study of Millennials' Sentiments of an Emerging Market," Res. Transp. Econ., **71**, pp. 44–53.

[58] Schoettle, B., and Sivak, M., 2014, "A Survey of Public Opinion about Connected Vehicles in the U.S., the U.K., and Australia," *2014 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 687–692.
[59] Kaur, K., and Rampersad, G., 2018, "Trust in Driverless Cars: Investigating Key Factors Influencing the Adoption of Driverless Cars," J. Eng. Technol. Manag., **48**, pp. 87–96.
[60] Kyriakidis, M., Happee, R., and de Winter, J. C. F., 2015, "Public Opinion on Automated Driving: Results of an International Questionnaire among 5000 Respondents," Transp. Res. Part F Traffic Psychol. Behav., **32**, pp. 127–140.
[61] Dirsehan, T., and Can, C., 2020, "Examination of Trust and Sustainability Concerns in Autonomous Vehicle Adoption," Technol. Soc., **63**, p. 101361.
[62] Panagiotopoulos, I., and Dimitrakopoulos, G., 2018, "An Empirical Investigation on Consumers' Intentions towards Autonomous Driving," Transp. Res. Part C Emerg. Technol., **95**, pp. 773–784.
[63] Gowda, N., Sirkin, D., Ju, W., and Baltzer, M., 2016, "Tutorial on Prototyping the HMI for Autonomous Vehicles: A Human Centered Design Approach," *Adjunct Proceedings of the 8th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, Association for Computing Machinery, New York, NY, USA, pp. 229–231.
[64] Brooks, J. O., Mims, L., Jenkins, C., Lucaciu, D., and Denman, P., 2018, *A User-Centered Design Exploration of Fully Autonomous Vehicles' Passenger Compartments for at-Risk Populations*, SAE Technical Paper.
[65] Penmetsa, P., Adanu, E. K., Wood, D., Wang, T., and Jones, S. L., 2019, "Perceptions and Expectations of Autonomous Vehicles – A Snapshot of Vulnerable Road User Opinion," Technol. Forecast. Soc. Change, **143**, pp. 9–13.
[66] Löcken, A., Golling, C., and Riener, A., 2019, "How Should Automated Vehicles Interact with Pedestrians? A Comparative Analysis of Interaction Concepts in Virtual Reality," *Proceedings of the 11th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, Association for Computing Machinery, New York, NY, USA, pp. 262–274.
[67] She, J., 2020, "Advisory and Adaptive Communication Improves Trust in Autonomous Vehicle and Pedestrian Interaction," *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, p. V008T08A037.
[68] She, J., Neuhoff, J., and Yuan, Q., 2021, "Shaping Pedestrians' Trust in Autonomous Vehicles: An Effect of Communication Style, Speed Information, and Adaptive Strategy," J. Mech. Des., **143**(9).
[69] Bloom, C., Tan, J., Ramjohn, J., and Bauer, L., 2017, "Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles," *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pp. 357–375.
[70] Kocić, J., Jovičić, N., and Drndarević, V., 2018, "Sensors and Sensor Fusion in Autonomous Vehicles," *2018 26th Telecommunications Forum (TELFOR)*, pp. 420–425.
[71] Insua, D. R., Couce-Vieira, A., Rubio, J. A., Pieters, W., Katsiaryna, L., and Rasines, D. G., 2021, "An Adversarial Risk Analysis Framework for Cybersecurity," Risk Anal., **41**(1), pp. 16–36.
[72] Cavoukian, A., 2009, "Privacy by Design: The 7 Foundational Principles," Inf. Priv. Comm. Ont. Can., **5**, p. 12.
[73] Yao, Y., Basdeo, J. R., Mcdonough, O. R., and Wang, Y., 2019, "Privacy Perceptions and Designs of Bystanders in Smart Homes," Proc. ACM Hum.-Comput. Interact., **Vol. 3**(Article 59).
[74] Barabas, I., Todoruţ, A., Cordoş, N., and Molea, A., 2017, "Current Challenges in Autonomous Driving," *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, p. 012096.
[75] Schmittner, C., Dobaj, J., Macher, G., and Brenner, E., 2020, "A Preliminary View on Automotive Cyber Security Management Systems," *2020 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 1634–1639.
[76] Cui, J., and Sabaliauskaite, G., 2017, "On the Alignment of Safety and Security for Autonomous Vehicles," *Proc. IARIA CYBER*, pp. 1–6.
[77] Kotecha, M. C., Chen, T.-J., McAdams, D. A., and Krishnamurthy, V., 2021, "Design Ideation Through Speculative Fiction: Foundational Principles and Exploratory Study," J. Mech. Des., **143**(8).
[78] Bezold, C., 2010, "Lessons from Using Scenarios for Strategic Foresight," Technol. Forecast. Soc. Change, **77**(9), pp. 1513–1518.