Investigating Car Drivers' Information Demand after Safety and Security Critical Incidents

Lea Gröber
lea.groeber@cispa.saarland
CISPA Helmholtz Center for Information Security
Saarland University

Matthias Fassl
matthias.fassl@cispa.saarland
CISPA Helmholtz Center for Information Security
Saarland University

Abhilash Gupta
s8ahgupt@stud.uni-saarland.de
CISPA Helmholtz Center for Information Security
Saarland University

Katharina Krombholz
krombholz@cispa.saarland
CISPA Helmholtz Center for Information Security

ABSTRACT

Modern cars include a vast array of computer systems designed to remove the burden on drivers and enhance safety. As cars are evolving towards autonomy and taking over control, e.g. in the form of autopilots, it becomes harder for drivers to pinpoint the root causes of a car's malfunctioning. Drivers may need additional information to assess these ambiguous situations correctly. However, it is yet unclear which information is relevant and helpful to drivers in such situations. Hence, we conducted a mixed-methods online survey ($N = 60$) on Amazon MTurk where we exposed participants to two security- and safety-critical situations with one of three different explanations. We applied Thematic and Correspondence Analysis to understand which factors in these situations moderate drivers' information demand. We identified a fundamental information demand across scenarios that is expanded by error-specific information types. Moreover, we found that it is necessary to communicate error sources, since drivers might not be able to identify them correctly otherwise. Thereby, malicious intrusions are typically perceived as more critical than technical malfunctions.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

intelligibility, modern cars

ACM Reference Format:
Lea Gröber, Matthias Fassl, Abhilash Gupta, and Katharina Krombholz. 2021. Investigating Car Drivers' Information Demand after Safety and Security Critical Incidents. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3411764.3446862

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3446862

1 INTRODUCTION

In recent years, modern cars' automation levels increased from driver assistance to partial automation – thereby making car-integrated technology unprecedentedly complex. These cars increase driving safety while also reducing the burden on drivers. To date, modern automation features require constant supervision which drivers struggle to provide over a longer period of time [36]. However, even if they do pay attention, the reactions of the car may be hard to predict or explain, e.g. in case of an accident. In older cars, the blame was usually on the driver or some technical malfunction. Modern cars' behavior is becoming increasingly opaque due to a rising level of autonomy, while opening up new attack surfaces [2, 48, 55, 65–67], and exposing drivers to unknown threats. Hence, drivers increasingly rely on proper in-car risk communication. If drivers would receive relevant information they could: (1) explain the car's behavior, which also builds trust and confidence in the technology, (2) resolve liability issues, i.e., blame the correct party for the accident, and (3) take appropriate actions to avoid such accidents in the future.

However, to provide drivers with helpful explanations and warnings, we first need to understand the drivers' information demand in safety- and security-critical incidents. The impact and design of explanations and warnings have been extensively studied with respect to security warnings in browsers [1, 40, 41, 51–53]. However, the domain of partially-autonomous vehicles constitutes a special case, as it involves potentially life-threatening situations. Lim and Dey investigated the demand for intelligibility in context-aware applications [42]. However, they focused on desktop applications and explicitly did not cover any level of autonomy or high risk situations. Recent work of Smith et al. focused on high risk situations. The authors explored pilot reactions to attacks on avionic systems [59]. However, their emphasis was more on reactions and not on information demand in security critical situations.

To investigate drivers' information demand, we conducted a mixed-methods online survey on Amazon Mechanical Turk with $N = 60$ participants. At this point we want to distinguish the "drivers" in our study from real-world drivers. That is, in our study participants react to hypothetical scenarios relieving them from any driving-related tasks. We exposed participants to safety- and security-critical situations. We carefully selected ambiguous malfunctions for these situations which could be explained by either a

malicious intrusion or a technical defect: (1) a car with activated autopilot hits construction barrels on the highway, and (2) a car does not unlock upon the first click of the key. The survey provided one of the following explanations for these situations: (a) a malicious intrusion (security breach), (b) a technical malfunction, or (c) no explanation. Exposing participants to different explanations expands the exploratory space, as the context of the critical situations shifts according to the car's explanations. Adding a condition in which the car does not provide an explanation gives us insights about the participants' own interpretation of the error cause.

Afterward, we used open-ended questions to elicit the participants' information demand and quantitative questions to assess their trust, satisfaction, and operational intent. We used Thematic Analysis [4] to evaluate the qualitative data. Additionally, we applied Correspondence Analysis [16] to understand which factors in these safety- and security-critical situations moderate drivers' information demand. The quantitative data was analyzed with statistical tests to verify qualitative results.

We found a basic need for information across scenarios, which is expanded depending on perceived error causes. Technical malfunctions and malicious intrusions have little overlap resulting in more car or situation specific information demand. Malicious intrusions were consistently perceived as critical, even if other perceived error sources in the same scenario were not. There exists a gap between highly critical situations and less critical situations in terms of trust, satisfaction, and operational intent ratings. Additionally, we identified the need to communicate error sources, as participants are not aware of malicious intrusions. They also have trouble to assess and react to highly critical situations.

2 RELATED WORK

In the following, we discuss related work on intelligibility in human-computer interaction, trust and explainability in autonomous systems.

Intelligibility in Human-Computer Interaction

Our work is heavily influenced by Lim and Dey's paper "Assessing Demand for Intelligibility in Context Aware Applications" [40]. The authors conducted two experiments to elicit users' demand for information and to verify their findings. The first experiment was an online study carried out on Amazon Mechanical Turk [63]. Participants had to answer qualitative questions regarding the behavior of one of four context-aware applications. Additionally, Lim and Dey assessed participants' satisfaction ratings regarding their experience with the application. The second experiment assessed whether or not users' satisfaction levels rise if they are presented with the type of information they demand. The authors found, among other things, that users want any available information in critical situations, while at the same time they are hardly satisfied with the information they get. The authors, however, did not include autonomous vehicles or systems of any kind in their study. In the following year, Lim and Dey published a toolkit to support intelligibility in context-aware applications [41]. The toolkit was designed to assist developers with incorporating different intelligibility types into applications. However, since the context of driving a car is inherently different from using a desktop application, further work is necessary to investigate this specific use case and technology. Our study aims to close this gap in the literature. Bellotti et al. came up with four principles to support intelligibility and accountability in context-aware systems [3]. They identified a need to inform the user of a system's capabilities, provide feedback, ensure identity and action disclosure, and grant the user control over the system. While these principles are an excellent point of reference, their broad character does not allow for concrete design decisions. Our study provides actionable insights that help to improve car-driver communication in line with these principles. Research has also addressed the information needs of users in other areas. For example, McGuinness et al. conducted an interview study that identified themes influencing the willingness of users to use and trust an adaptive agent [15, 44]. In addition, Gregor et al. did a meta-review and identified what kind of explanations users of knowledge-based systems demand [25]. Jakobi et al. investigated long-term information demands in do-it-yourself smart home systems, identifying changing information demands over time [30]. Again, the results of these works cannot be directly transferred to the domain of modern cars. Therefore, our study will provide valuable contributions to complete the picture of the information needs of users in different contexts.

Explainable Artificial Intelligence in Autonomous Systems

Recent research focused on making the actions and internal processes of systems with varying levels of autonomy understandable, and communicating them to users [9, 27, 29, 32, 38, 56]. For instance, Hastie et al. [27] introduced a multimodal interface (MIRIAM) for remote autonomous systems. MIRIAM is intended to increase the transparency of the system and thus strengthen the operator's confidence in the system. The interface allows one to pose *why* and *what* questions to the system. Langley et al. [38] framed the concept of explainable agency for intelligent autonomous systems and claim that an agent needs to convey its internal reasoning to the user, and which actions it executed, among other things. These approaches form a good basis when it comes to conveying knowledge to users. However, depending on the situation, the drivers may not be receptive to different types of information. Therefore, it is important to investigate the information needs of drivers in order to provide them with adequate information adapted to the situation.

Trust in Automation

Among other things, our work studies how we can maintain a trustful communication between vehicles and drivers in the context of critical situations. Therefore, we discuss research about trust in automation [26, 28, 39, 43, 45, 54] in the following. Madhavan and Wiegmann found that the process of forming trust in a machine differs from trusting humans [43]. This is because humans initially treat other people with caution [54]. The trust relationship is built slowly, as long as the other person does not make any mistakes. In contrast to this, people usually assume that machines function flawlessly. Hence, they encounter them with a trust advance [39, 43]. With every mistake the machine makes, this trust is then corrected downwards [11]. However, this effect only occurs if the person has had no previous contact with the machine [43].

3 TECHNICAL BACKGROUND

Remote keyless system (RKS) technology was first introduced in cars in the 1980's [37]. Since then, the underlying technology of RKS has continuously evolved after each version was demonstrated to be exploitable. At the time of writing this, it uses encrypted rolling codes. However, this is also vulnerable to exploits as shown in various demonstrations [13, 20–22, 24, 33], the last one as recently as November 2020 [24]. This is most likely due to incorrect implementation of protocols or reliance on flawed protocols. The most common of these exploits are relay attacks (which repeat the signal from the driver's key to the car from a large distance using relays) and replay attacks which capture and block valid signals from the driver's key fob and use these signals later on. Vulnerabilities in cars are not limited only to car keys [67]. Researchers have already gained control of a moving car while sitting in the back seat [17] as well as from kilometers away [18]. They gained control of the steering wheel, brakes, windshield wiper, air conditioner, and the dashboard system. Recently, researchers found that they could fool Tesla's autopilot program into believing "phantom" signs. They were able to trick a Tesla to stop, by flashing a stop sign for a second on a billboard next to the road [23]. Apart from malicious intrusions, the computer systems of a car may suffer from technical malfunctions. The video used in our study shows an example of when the autopilot failed to recognize objects in its path and crashed through construction barrels [68].

As the number of computerized features in cars increases, so does the potential for exploits and malfunctions to be life-threatening [55, 68]. While car systems currently do not communicate warning messages about third party interference to the driver, scientists are working on solutions to detect malicious intrusions in vehicles to safeguard their internal functioning and ensure that such exploit attempts are thwarted [7, 10, 14, 46, 48, 66]. Such mechanisms can possibly be further developed to alert drivers about third-party intrusions.

For this study we chose scenarios inspired by technical malfunctions and exploits that either occurred in the real world or were demonstrated to be feasible by scientists. However, to the best of our knowledge, there is currently no mechanism to alert drivers of an ongoing attack, even if it were detected. For this study we assume the car is capable of such a detection and notification to the driver, to investigate which information people need in critical situations.

4 METHODOLOGY

Our study is designed to elicit drivers' information demand depending on different critical situations. Hence, our study lays the foundation to improve in-car risk communication to drivers and to provide helpful information at appropriate times. Accordingly, we identified the following research questions:

- **RQ1:** What information do drivers demand for safety- and security-critical incidents?
- **RQ2:** Which factors moderate information demand after critical incidents?
- **RQ3:** Which error sources for safety- and security critical incidents do drivers think of?

Since it would be unethical to put participants into critical situations we use an online survey with scenarios to investigate their attitudes, trust, satisfaction, and information demands. To cover a broad spectrum of situations, we selected a high-critical scenario (crashing against construction barriers) and a low-critical scenario (key malfunction). We specifically chose ambiguous scenarios in which the cause of vehicle malfunctions is not obvious. Since we confront participants with hypothetical scenarios, the participants ("drivers") are relieved from all driving-related tasks. This constraint is further strengthened as the car in the scenarios is not moving at the time we elicit participants' information demand. After each scenario, participants fill out a questionnaire with qualitative and quantitative questions. We apply *Correspondence Analysis (CA)* to investigate which factors moderate drivers' information demand. We describe each of the identified correlations in detail using qualitative data from the free text response questions.

4.1 Online Survey

All participants ($N = 60$) are exposed to two scenarios (C: crashing against construction barriers and K: key malfunction) in a randomly chosen sequence. Each scenario contains (1) an introductory text, (2) a description of the situation, and (3) the vehicle's explanation. The vehicle explains its behavior with one of the following explanations (randomly assigned per participant and used for both scenarios): **malicious intrusion (*MI*, $N = 17$)** by third parties, a **technical malfunction (*TM*, $N = 19$)**, or with **no explanation (*NO*, $N = 24$)**. Hence, scenarios (C and K) are studied within subjects and explanations (MI, TM, NO) are studied between subjects. After each scenario, participants fill out a questionnaire about their experience. The supplementary material provides the scenarios as presented to the participants.

Introductory text. The introductory text embeds each scenario in the setting of partially-autonomous vehicles by describing the vehicle's capabilities and limitations. This introduction directly addresses the participant to make the setting more tangible, thus making it easier for the participant to immerse into the situation. The text describes the car's functionality according to the claims on Tesla's website [61]. In particular, that it can automatically steer, accelerate, and brake within its lane. However, the text explicitly states that active driver supervision is required at all times. We did not want to study a specific brand of vehicle, but used the Tesla description for a realistic abstraction of such a vehicle. Hence, we did not specify the brand of the car in the survey. From the video illustrating scenario C, one cannot infer which car it is. Additionally, we omitted a description of the center console or visual representation of the error message to minimize the influence of factors beyond our main focus.

We chose scenarios in which the vehicle communicates a malfunction that could have been caused by a functional error or a malicious attacker. We hypothesize that in such cases the driver cannot identify the source of the malfunction without further context.

Scenario C: Crashing against construction barriers. This scenario asks the participant to imagine driving on the highway with an activated autopilot. The description explicitly emphasizes that this

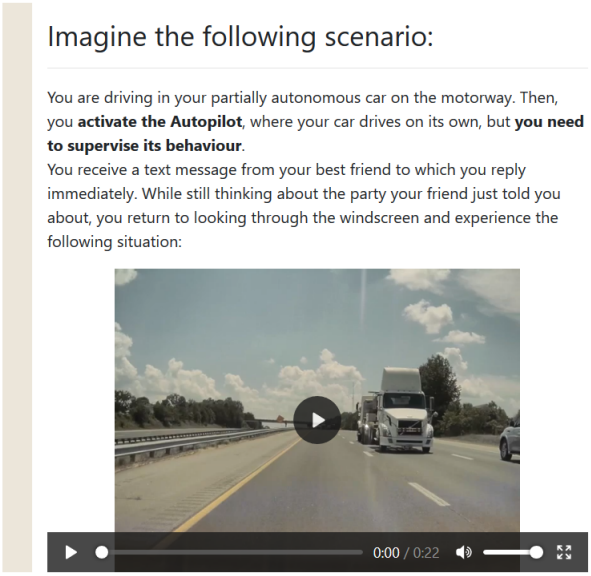

Figure 1: Scenario C: a vehicle crashing into construction barrels as presented in the survey. The supplementary material provides the complete version of the survey.

requires active driver supervision. Just like the introductory text of the setting, this description is designed to be as tangible and immersive as possible. Hence, it contains elements that should make it easy for the study participant to imagine herself in the situation. For example, instead of simply saying that the driver was briefly inattentive, the text provides a vivid description of why this is the case: *"You receive a text message from your best friend to which you reply immediately."* This not only ensures that the study participants can better identify with the situation but also establishes a common ground and thus leaves less room for interpretation and misunderstandings.

The actual situation is presented in a 22-second video [68]. It shows the collision of a vehicle with construction site barrels from the driver's perspective. This scenario is based on an actual event: A dashcam recorded this situation in a Tesla while the car's autopilot failed. In the video, the vehicle drives towards the end of a highway lane that is closed due to construction. For an unknown reason, it does not recognize the construction site barrier. The driver reacts too late and only intervenes after the vehicle has hit 10 barrels[1]. Figure 1 depicts the entire description of the scenario as presented to the participants. After this video, another tangible description clarifies that the driver, not the vehicle, activated the brake.

The vehicle in this scenario responds in one of three ways to the incident: explaining its behavior with a malicious intrusion (*MI*), attributing it to a technical malfunction (*TM*), or not explaining at all (*NO*):

MI *You look at the car's center console and learn that your car's behavior was caused by a hacker. They temporarily took control of the vehicle and steered it into the construction barrels.*

TM *You look at the car's center console and learn that your car's behavior was caused by a sensor malfunction. The front sensors did not recognize the construction barrels, causing the incident.*

NO [*no explanation is offered*]

After participants experienced the scenario and the vehicle's explanation, the survey continues with the open and closed questions shown in Table 1.

Scenario K: Key malfunction. In this scenario, the driver wants to unlock her vehicle with a remote key fob. However, it does not respond the first time and the driver needs to press the "unlock" button again to unlock the vehicle. We chose this scenario because the problem of cloning keys has been present for many years [13, 19, 20, 33, 34] and was recently prominent in the media again when a Tesla was stolen from a driveway [58]. Furthermore, this scenario is less critical than the other one, as it usually only causes material damage without threatening the lives of the vehicle's occupants. The attack mentioned by the malicious intrusion explanation refers to key fobs and vehicles that synchronize using rolling codes [33].

The vehicle in this scenario responds in one of three ways to the incident: explaining its behavior with a malicious intrusion (*MI*), attributing it to a technical malfunction (*TM*), or not explaining at all (*NO*):

MI *When you look at the car's center console you learn that someone may have cloned your key and can now use it to unlock your vehicle.*

TM *When you look at the car's center console you learn that the battery charge of your key is weak and that you need to replace it soon.*

NO [*no explanation is offered*]

After participants experienced the scenario and the vehicle's explanation, the survey continues with the open and closed-ended questions shown in Table 1.

Questionnaire. After each scenario, participants answered four qualitative open-ended questions regarding their (1) perception of the scenario, (2) next actions, (3) feelings about the scenario, and (4) demand for information. Likewise, participants answered four quantitative closed-ended questions regarding their (1) satisfaction with the vehicle's response, (2) trust in automation (using Jian et al.'s [31] scale), and (3) operational intent. All quantitative questions asked for a response on a 7-point Likert scale. Table 1 lists all qualitative and quantitative questions asked after each scenario.

4.2 Pilot Study

The goal of the pilot tests was to test and improve the comprehension of questions and scenario descriptions. We conducted a total of 6 pilot tests in which we asked participants to think-aloud while completing the survey. This not only allowed optimization of the texts and questions, but also revealed layout flaws. We iteratively conducted pilot tests and directly incorporated the results into the survey after each round of testing. We continued until we

[1] According to the video description the driver fell asleep behind the wheel of his Tesla. Although the driver acknowledges that the accident was mainly his fault, the vehicle is also held accountable: *"Automatic Emergency Braking totally failed me on the one time we needed it most. With all the phantom braking events we have experienced in the 2½ months we've owned it, it does seem like it would panic when it saw this coming."* [68] Note: The owner of the video has since taken it offline. Please contact the authors of this paper if you have further questions regarding it.

Table 1: Questionnaire after each scenario containing qualitative and quantitative questions.

Measure	Scenario Question	Answer Type
Perception/ Attention	What do you think happened in this scenario?	free text
Action	What will you do next as the driver?	free text
Driver Feeling	How do you feel about the vehicles response?	free text
Information Demand	What information should the car provide about the situation?	free text
Vehicle Satisfaction	I am satisfied with the vehicles behaviour in this specific situation.	7-point Likert
Trust in Automation Scale	According to Jian et al. [31] adjusted to partially-autonomous vehicles	7-point Likert
Operational Intent	After experiencing this incident, I would buy a vehicle of this kind again.	7-point Likert
	I would sue the manufacturer of the partially-autonomous vehicle.	7-point Likert
	I would continue to use the partially-autonomous vehicle.	7-point Likert
	I would warn my family and friends about the partially-autonomous vehicle.	7-point Likert

had covered every condition once and the participants completed the survey without any problems. Based on the outcome of the pilot tests we adjusted phrasing of the open-ended questions and conditions. For example, we slightly rephrased some questions to clarify the direct reference to the scenario. Additionally, we added gray bars to the left of each paragraph to provide visual guidance. The final analysis does not include the results of the pilot tests. We recruited pilot test participants from our university achieving an even distribution of women and men, computer-science students, and administrative employees, aged 23-45.

4.3 Recruitment and Participants

We recruited $N = 60$ study participants from Amazon Mechanical Turk (MTurk) [63]. Participants were randomly assigned to conditions (MI, TM, NO), resulting in an uneven distribution among conditions. We carefully balanced sample size considerations for our mixed methods study. We performed power calculations to estimate the number of participants for the quantitative analysis. For a statistical power of 0.8 and $\alpha = .05$ we estimated 60-80 participants for a medium effect size. With regard to the qualitative analysis, we are confident that the number of participants is sufficient as we reached saturation (see Section 4.4).

We chose MTurk because it enables us to effectively investigate the information demand of a broad set of people, as opposed to e.g. lab studies. Additionally, we wanted a culturally homogeneous sample that is known to be suitable for security research. Prior work by Redmiles et al. suggests that MTurk responses regarding security and privacy experiences, advice sources, and knowledge are more representative of the U.S. population than are responses from a census-representative panel [50]. To participate in our study, MTurk workers needed to own a car and be located in the US. We selected car ownership as a criterion to ensure that participants have experience with regular cars. None of the participants owned a partially-autonomous car. 13 participants reported having previous experience in driving or riding cars with autonomous driving features. Driving experience varied between 7 and 52 years (median 21, mean 23.94). Additionally, we required a HIT Approval Rate[2] for all Requesters' HITs greater than 95%, and that they have more than 100 approved HITs. In the pilot test, participants completed the survey in about 20 minutes, so we compensated participants with $3 for the completion of the survey. However, participants invested more time than anticipated (26 minutes on average) which resulted in a wage below the US federal minimum ($7.25). To remedy this situation, we gave a $0.50 bonus to all participants. A total of 23 woman and 27 men took part in our study with ages ranging between 24 and 73 (median 27, mean 40.67). Table 3 in the appendix shows a detailed overview of our participants' demographics.

4.4 Coding Procedure

We used open coding according to Strauss and Corbin [60] to evaluate the qualitative data. In total, we created 6 codebooks, one for each scenario and condition.

Two researchers independently coded answers to open-ended questions for each scenario and condition in two iterations. Initially, one of them skimmed the first half of each dataset and constructed an initial version of the codebook. The draft version of the codebook captured the dataset's concepts and topics. Afterward, both researchers used this codebook to code the second half of the data. They tagged pieces of the answers with labels, at once summarizing, categorizing, and describing the data [6]. After this first iteration of coding, the two researchers discussed their codes and adapted the codebook accordingly. During the second iteration, the two researchers coded the first half of the dataset. In cases where the discussion of the second iteration also led to a change in the codebook, the researchers coded the second half of the dataset again. This resulted in an *inter-rater reliability* Krippendorff's α [35] between 0.77 and 0.91 for each codebook. We achieved saturation after the first coding iteration for 5 codebooks. In the Crash, *NO* condition one participant reported to repair the sensor which added a new concept to this codebook in the second coding iteration.

4.5 Analysis

We conducted *Thematic Analysis* [4] to identify topics, correlations and themes in the coded data. Further, we applied *Correspondence*

[2]"A Human Intelligence Task, or HIT, is a question that needs an answer. A HIT represents a single, self-contained, virtual task that a Worker can work on, submit an answer, and collect a reward for completing. HITs are created by Requester customers in order to be completed by Worker customers." [64]

Analysis [16] to explore the relationship between different situational factors and the occurrence of information demand codes. The information demand codes are a result of the open coding procedure from the previous section. The different situational factors that might moderate information demand are a result of the Thematic Analysis.

4.6 Ethical Considerations

Our university's ethical review board (ERB) evaluated and approved this research project. To enable informed consent, we explained the study objective to the participants, stated that participation is voluntary and that they may abort the survey at any time. Further, we did not collect any personally identifiable information (PII). At the end of the survey, we provided links to our webpage and contact information in case participants had further questions.

5 RESULTS

We first used Thematic Analysis to identify concepts, topics and connections in the coded data. Those insights then form the basis for a subsequent Correspondence Analysis of situation-related information needs. Table 2 shows an overview of all information types elicited in the study with explanations and quotations. Table 4 in the Appendix shows a comparison of all codebooks grouped by themes. All quotes in this section are unaltered including spelling mistakes.

5.1 Results of Thematic Analysis

The results of the Thematic Analysis are grouped by high level codes about perceived error causes. For each, we report on similarities and differences, as well as specifics of both scenarios. In addition, we talk about differences in the perception of both scenarios and about first trends in the need for information.

5.1.1 Malicious Intrusion as Perceived Error Source. Across both scenarios nobody thought of security breaches as possible error sources, unless they were primed for it in the *MI* condition. This suggests that security breaches are a concept that is not deeply rooted in people's minds when it comes to driving. However, if the participants were then made aware of a malicious intrusion, this was perceived differently depending on the situation.

In the key scenario people were unsure about how the attack was carried out: *"I don't know how someone would go about cloning a key."* (P34). They tried to make sense of the situation, each coming up with different explanations to what might have happened, being more or less close to the actual attack we had in mind: *"Someone accessed the computer in the vehicle and made a clone of the entry system."* (P37), *"[...] there was someone standing nearby with some sort of rf reader and intercepted the authentication code used to unlock the vehicle. the first click to unlock the vehicle did nothing because it went to the interceptor, the second time unlocked because it was gong to the car, not the rf reader"* (P20). 2 participants thought that the malfunction was actually a security functionality, impeding attacks: *"it's actually good that it doesn't unlock right away because it will take longer for the hacker to access it"* (P37). The participants reacted to the key scenario with mixed feelings. 5 participants perceived the scenario as *scary* (P30). One participant expressed that *"Hacking is a real concern."* (P21). However, at the same time 9 participants perceived the warning of the car in a positive way, e.g. stating that they were *satisfied* (P21,63), and *happy* (P65). This is likely the case because the car warned its driver prior to a potential theft: *"Since the car wasn't stolen/missing after a stranger cloned my key, it seems the security features are working for the time being"* (P29). Nevertheless trust issues may remain as one participant stated *"I would be paranoid about the issue really being resolved once it had been corrected."* (P34).

In the crash scenario participants understood that the accident was caused by a malicious intrusion, but were uncertain about what exactly happened: *"somehow the hacker was able to disable the safety features of the vehicle [...]"* (P20). Additionally, participants had different ideas about hacker capabilities. For example, 1 participant stated that *"The car should have stopped much quicker. Even if a hacker impacted the steering, the brakes should have been activated because of collision warnings."* (P27), and a second one stated: *"[...] I would figure the systems would only allow things like that if they were being manually overridden from withing the car itself"* (P39). To add to this, 7 participants stated that they would continue to drive manually, while only 2 reported to call the police or get the car towed. 12 participants had predominantly negative feelings with regard to the car's behavior, stating they were *irritated* (P29), and *angry* (P52). In contrast to the key scenario, participants did not appreciate the car's explanation of the situation. This is likely because the accident already happened and the car failed to notify the driver early. 2 participants explicitly classified the situation as potentially lethal: *"[...] It is scary to think that someone can hack the system and potentially kill you. [...]"* (P30). With regard to responsibility, 15 participants held *hackers* (P4) accountable for the accident. Out of those, 5 participants acknowledged that the driver is guilty of not paying attention to the road and 1 person blames *"[...] the people who designed the vehicle [...] "* (P34).

5.1.2 Technical Malfunction as Perceived Error Source. Technical malfunctions were the most named error sources in the *NO* and *TM* conditions across both scenarios. Thereby, participants demonstrated a good understanding of and intuition for technical error sources. In general, the concepts and themes mentioned in the *NO* and *TM* conditions broadly overlapped in both scenarios.

13 participants identified a *"bad battery"* (P24) as a potential error in the key scenario, *NO* condition. In the *TM* condition everybody who correctly understood the scenario identified the key's battery as the error source. 3 participants misinterpreted the scenario to be about an electric vehicle. We excluded them from the analysis of this scenario. In *TM* condition, the majority had neutral to slightly positive feelings about the car, describing its behavior as *helpful* (P19), and *acceptable* (P9). 5 participants had negative feelings, expressing they would *"prefer that it [the car] warns me before the battery gets so low that i may stop working correctly"* (P33). In the *NO* condition the majority had neutral to slightly negative feelings, stating that batteries being low are a *common occurrence* (P22) and that they *"didn't like how it [the car] was unresponsive"* (P24).

In the crash scenario 15 participants thought the accident was caused by a technical malfunction in the *NO* condition. In the *TM* condition, 22 participants correctly attributed the error to a *sensor malfunction* (P32). In both conditions the majority was extremely unsatisfied with the car's reaction, stating they were *"upset*

Table 2: Consolidated codebook of participants' information demand across all scenarios and conditions

Code	Description	Example Quotes
Question Types		
What	What happened in the situation?	"It should provide a report of what happened […]", "It should say that there is a breach in the system or something of that regard […]"
Why	Why did the malfunction occur?	"It should also have some kind of an explanation as to why it didn't brake"
Who	Who is the attacker?	"Who is responsible."
When	When did the attack happen?	"when it was hacked"
How	How did the attack happen?	"Any information about how it was exploited by the hacker"
Car		
Status	Status information of malfunctioning parts	"Status of the remote; low battery indicator; weak signal strength maybe"
Diagnostic Report	Car's diagnostic report, e.g. error codes, damage	"The car should provide a report about the damage - when the car collided with a hazard, how fast it was traveling, any potential damage to look out for", "if the autopilot is still working"
Decision Process	Car's internal decision process leading to accident	"How it interpreted the situation and any negative reactions to the incident."
Parameters	Car's parameters during accident, e.g. velocity etc.	"show a graph of some sort of how long/distance it continued driving from the first hit of a cone to when the vehicle eventually stopped along with the speed, if it slowed down at all etc"
General Usage	General information about how to use the car	"How many clicks is necessary to unlock the car"
Situation		
Preventative Measures	How can such accidents be avoided in the future?	'[…] what steps I can take next to keep this from happening again."
Message	Message, Warning, or Alert about Incident	"It can send a message that it only got a partial signal the first time.", "It would be great if the car could give a warning […]"
Troubleshooting	Information to resolve the issue manually and clues to find the attacker	"It should tell you when it was copied and that way you could try to figure out who it was"
Recommendations	Recommendation how to react to the situation	"Do the sensors need to be checked?"
Quality of Warning		
Visual	Demand visual message	"The car should save the visual evidence if it has a built in dash cam"
Audio	Demand audible message	"The car should have an automatic warning system […] like a voice warning"
Before/During	Demand message prior to or during the incident	"The car should have sounded a warning of the cones approaching."
None		
None	No information demand	"Nothing at all, unless there's a reason why the fob truly needed more presses […]", "Nothing really, it seems self-explanatory to me"

and frightened" (P19), *"surprised and a little panicked"* (P32), or *scared* (P23). The message in the *TM* condition had no positive effect on the overall impression of the situation. Similar to the *MI* condition, participants demanded to *"be forewarned if a sensor is failing or has failed"* (P69). In terms of liability, 7 participants in the *TM* and 9 participants in the *NO* condition held the driver accountable for the accident: *"The driver (me) was not paying adequate attention to the situation [...]"* (P28). 8 participants in the *TM* and 3 participants in the *NO* condition blamed poor design: *"Apparently the sensors weren't programmed to recognize the particular obstacles [...]"* (P15), *"Shouldn't the vehicle be able to recognize the signs warning of the lane ending in the first place."* (P33). 1 participant wanted the car to *"acknowledge that it made a mistake"* (P39).

5.1.3 Human Error as Perceived Error Sources. Apart from technical malfunctions and malicious intrusions, participants also identified other potential error sources. Especially if no explanation for the car's behavior was offered, participants blamed the malfunction on themselves across both scenarios. In the key scenario, 6 participants in the *NO* condition made statements like *"Sometimes [...] you don't press it [the key] correctly so you need to do it again"* (P22), or *"I didn't press the button hard enough"* (P49). Nobody mentioned human failure as the error source in the *TM* or *MI* condition in the key scenario. In the crash scenario, on the other hand, the concept came up more frequently. This is likely the case, as the description pointed out that the driver was inattentive. Here, 9 participants of the *NO* condition stated that they *"stopped paying attention in a situation where I should have been supervising"* (P25). 6 participants (*TM*) and 5 participants (*MI*) made similar statements.

5.1.4 Design of the Car as Perceived Error Source. Some participants thought the malfunctions were not actual malfunctions, but intended by design, e.g. in the key scenario, or limits of the cars functionality in the crash scenario. When no explanation was given in the key scenario, 5 participants explained the car's malfunction with statements like: *"The car was programmed to unlock at two clicks [...]"* (P48). Note, that out of those 3 participants understood the malfunction as a security feature: *"I feel safer with this and know that my car would not open for just any one just for the remote that I have"* (P59). Nobody in the *MI* or *TM* conditions thought the malfunction was intended by design. In the crash scenario 3 participants in the *NO* and 6 participants in the *TM* condition thought that the malfunction was due to limited functionality of the autopilot: *"The car was apparently only programmed for any*

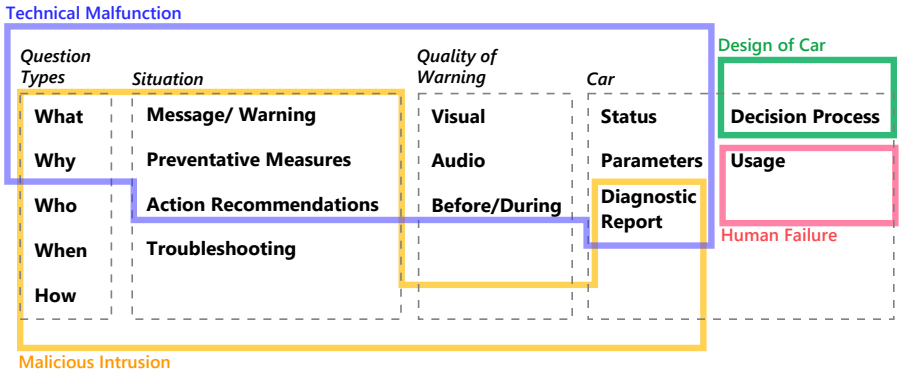

Figure 2: Overview of how information demand (in the background) corresponds to the perceived cause of error (colored boxes) across both scenarios.

side abstruction" (P74), or *"I think the vehicle got confused. It knew there was a road there but wasn't aware of the construction."* (P56). Nobody in the *MI* condition thought the malfunction was due to gaps in functionality.

5.1.5 Perceived Criticality of Scenario. The qualitative findings suggest that participants perceive the key scenario less critical than the crash scenario. This is indicated by different impressions participants have about both scenarios as well as their reported actions to the scenarios. However, the *MI* condition of the key scenario constitutes a special case, as 14 participants reported on calling the police or contacting the manufacturer. Thus, this condition was also perceived as more critical. The overall gap between key and crash scenario was also evident in the quantitative data. The scores of trust, operational intent, and satisfaction in the key scenario were significantly higher than in the crash scenario. For each dependent variable we ran MANOVA. The test provides information about Wald-type statistic (WTS), the ANOVA-type statistic (ATS) and re-sampling versions of these test statistics [57]. Using WTS and ATS, there was a significant effect of the scenarios on the trust scale rating, satisfaction rating, and operational intent rating, df=1, $p<0.001$.

5.1.6 First Trends in the Need for Information. A fundamental need for information of the study participants became apparent across scenarios and conditions. It includes the questions why the malfunction occurred and what happened in the situation. In addition, the need to receive a warning or message from the car was widely expressed. Depending on the perceived severity of the situation and on the error source, participants asked for additional information. Figure 2 illustrates the information types, grouped by perceived error source across all scenarios. For technical malfunctions participants generally cared more about information on the car and were more specific about the kind of warning they wanted. If participants thought a malicious intrusion was the error source, they were more interested in information about the situation including different question types about the attack. The perceived error source human failure resulted in interest about how to properly use the car or the key. Last but not least, if participants thought the malfunction was due to limited functionality they wanted to know more about the car's internal decision process.
In the following section, we present the results from our Correspondence Analysis to identify more fine-grained trends in information demand.

5.2 Correspondence Analysis

Based on the Thematic Analysis, we identified different situational factors that might moderate information demand (*moderating factors*):

- **Highly Critical Situations (HiCrit)** Participant perceived the situation as highly critical.
- **Less Critical Situations (LessCrit)** Participant perceived the situation as less critical.
- **Technical Malfunction (TM)** Participant identified a technical malfunction as the error cause.
- **Malicious Intrusion (MI)** Participant identified a malicious intrusion as the error cause.
- **Human Failure (Human)** Participant identified a human failure as the error cause.
- **Design of Car (Design)** Participant perceived the malfunction as an intended design choice.
- **Life Threatening (Threat)** Participant perceived the situation as life-threatening.
- **Positive Impression (Pos)** Participant had a positive impression of the car's response to the situation.
- **Negative Impression (Neg)** Participant had a negative impression of the car's response to the situation.
- **Neutral Impression (Neut)** Participant had a neutral impression of the car's response to the situation.

We applied Correspondence Analysis between *moderating factors* and *information demand codes* (shown in Table 2) to explore their relationship. We explored this relationship using biplots (shown in Figure 5) and checked each conclusion against the raw data. These biplots visualize the relationship between the moderating factors (blue dots) and information demand (red triangles). Put simply, the further away labels are from the origin, the more discriminating they are, and smaller angles between a moderating factor and an

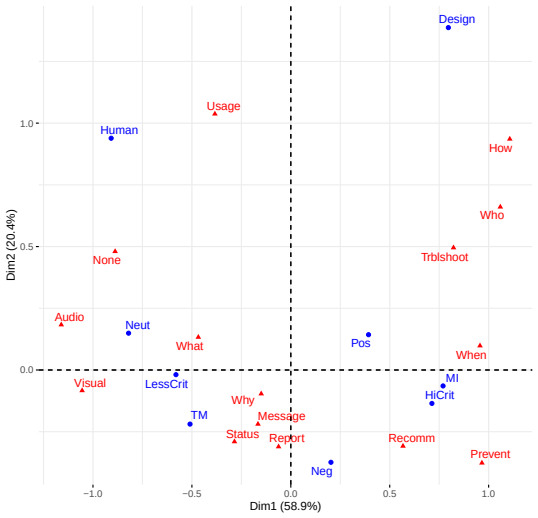

Figure 3: *Key* scenario

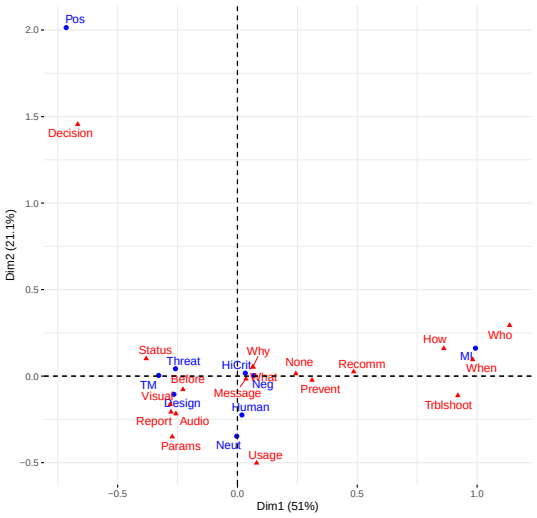

Figure 4: *Crash* scenario

Figure 5: Asymmetric biplots of *moderating factors* (blue dots) and *information demand codes* (red triangles). The dimensions correspond to the eigenvalues that cover the largest percentage of variance.

information demand label (connected through the origin) indicate an association of the two.

Relative inertias indicate for each cell of the contingency table (refer to Tables 10 and 7 in the Appendix) the relative contribution to the total value of the chi-square statistic. The higher the value of a cell, the higher the association of the respective row and column categories. We report relationships with relative inertia larger than 0.01 only if they are grounded in the qualitative data.

Appendix C provides tables with exact results of the Correspondence Analysis. The following paragraphs report on information demand trends depending on moderating factors.

5.2.1 Perceived Error Cause. Participants identifying a **malicious intrusion (MI)** as the error cause in a scenario, was globally a strongly discriminating factor for information demand. Participants were more interested in information about the situation than in information about the car. In the crash scenario *MI* was the only factor that had an impact on information demand. It led to increased demand for the information types *Who, When, How, Preventative Measures, Troubleshooting,* and *Action Recommendations*. In the key scenario *MI* is a strongly discriminating factor. Similar to the crash scenario there is increased demand for *Who, When, Preventative, Recommendations*. One participant asked *"how and when it [the key] was cloned"* (P37). This person thought that the car's computer was hacked to clone the key and that the second click on the key was a security mechanism. Because of this *How* is also closely associated with the moderating factor *Design*.

Globally, the perceived error cause **technical malfunction (*TM*)** resulted in participants being more interested in information about the car and being more specific about the quality of warning they want. In the crash scenario *TM* led to increased demand for the type *Before*: *"The car should have indicated there was something in it's path."* (P8). A positive impression of the car's response to the situation is an outlier in the *crash* scenario. It is positively associated with *Decision*. This is the case because only two participants demanded information about the internal reasoning of the car in the situation and one of them misunderstood the situation at least partially: *"It's ability to recognize a collision and pull to the side of the road is good." (P58)*. In the key scenario *TM* let to increased demand for *Status* information and less demand for *When* and *Troubleshooting*.

Globally, the perceived error cause **human failure (Human)** is not a strongly discriminating factor. It is more closely associated with technical malfunctions. In the *crash* scenario and *NO* condition one participant wanted information about *"[...] changing lanes"* (P42) which led to increased demand for the type *Usage*. *Human failure* is a discriminating factor in the *key* scenario with increased demand of the types *Usage* and *None*. Participants typically wanted to know *"how many clicks [are] necessary to unlock the car"* (P48).

2 participants perceived the malfunction as an intended **Design** feature of the car in the *crash* scenario. They were interested in *"how it [the car] interpreted the situation and any negative reactions to the incident."* (P58). Additionally, they had the impression that the car pondered on what would be the best reaction to the situation *"[...] the autopilot made the best decision of the situation. Staying on the lane was safer than swerving to either lane. [...]"* (P35), and humanizing it *"I would hope that it knows it made a mistake [...]"* (P38). In the *key* scenario the design factor is more closely associated with the perceived error cause *malicious intrusion*. This is because participants perceived the double clicking of the key as an addition security feature: *"In the manual there should be an explanation of why I would have to push the button twice and if there is a trouble*

shooter for this" (P59). People demanded more information about *Who, How, Usage, Troubleshooting*.

5.2.2 Criticality of the situation. Across both scenarios participants associated **highly critical situations (HiCrit)** more closely with technical malfunctions and malicious intrusions than with human failure or design issues. Highly critical situations did not spark increased information demand with any particular information type in the crash scenario. Participants were broadly interested in all information types they were aware of. In the *Key* scenario, participants associated highly critical situations more strongly with malicious intrusions than with other perceived error causes. This resulted in an increased information demand of *When, Preventative Measures* and *Action Recommendations*. There was decreased demand for *Status* and *None*.

Globally, situations which participants perceived as **less critical or not critical (LessCrit)** are a strongly discriminating factor for information demand. In those situations participants had increased demand for the information types *Status, Usage* and *None* and decreased demand for *Before*. There is no evidence in the codebook that the *crash* scenario was perceived less critical. This is why LessCrit is not present as a moderating factor in Figure 4. In the *Key* scenario less critical situations are more strongly associated with technical malfunctions. There is increased information demand for the types *Status and None*. The demand for the information types *When, Preventative Measures, Troubleshooting,* and *Action Recommendations* decreased.

6 DISCUSSION AND IMPLICATIONS

First, we discuss the combined results of perceived error causes and situational characteristics to highlight the lessons learned. Based on those we derive actionable implications for design that may form the baseline for a meaningful communication of technical error sources and malicious intrusions.

Our analysis of information demand indicates differences between (1) scenarios perceived as less or highly critical, and (2) between the error causes technical malfunction (*TM*) and malicious intrusion (*MI*). While the fundamental need for information remained similar across the conditions and scenarios, participants demanded additional information depending how they perceived the error source. Furthermore, we observe a more differentiated splitting of information codes between *TM* and *MI* in the key scenario, which is perceived as less critical, than in the crash scenario, which is perceived as highly critical. A key finding is that while the participants could imagine many different causes of vehicle failures from technical malfunctions, human error, to deliberate design decisions, no one mentioned malicious intrusions. However, we argue that complete threat models cannot be expected from drivers, and that the gaps we have identified must be taken into account to support drivers when they need it most. For this reason, the following discussion pays special attention to the specifics of *MI* error causes and differentiates them from the needs in terms of *TM* error causes.

6.1 Lessons Learned about Perceived Error Causes

The experimental setup not only allowed an investigation of given error causes, but also revealed which error sources and threats the participants were aware of. We found that, if possible, participants tried to find simple explanations for the presented scenarios. This resulted in an increased attribution to human failure in the NO condition across both scenarios. Additionally, participants commonly named technical malfunctions as potential error sources in all conditions. This may be due to the fact that cars used to cope with mostly technical malfunctions in the past, and cars suffering from malicious intrusions are at the moment still the rare exception. Interestingly, participants tried to explain malfunctions as intended design choices, e.g., to enhance the security of the vehicle. This was mentioned in the context of clicking twice to unlock the car in the key scenario and could potentially be borrowed from experiences in the online world, such as Two-Factor Authentication. However, this at least indicates fuzzy concepts with regard to enhancing security which is not an uncommon concept. E.g. Distler et al. found that software displaying security mechanisms to its users is better received than equal software that does not [8]. Apart from this, participants demonstrated no sensitivity to security. Unless primed for it, nobody thought of security breaches in the context of car accidents. This indicates the need for guidance in security critical situations and is reflected by the increased demand for the information type *Action Recommendation*. Moreover our results indicate that simply stating the error cause is not enough in highly critical situations. While this is sufficient to place the scenario in the correct context, it is not sufficient to help participants assess and react to the situation correctly. This is true for both *TM* and *MI*.

6.2 Lessons Learned about Situational Factors

We found that the more critically the situation is perceived, the greater the need for information but the worse the situation is perceived in terms of trust, satisfaction and intentions to act, regardless of whether the car offers an explanation or not. This coincides with the results of Lim and Dey [40], who also found that people in critical situations have a broad need for information and are difficult to satisfy even if their information demand is met. We believe that in the context of vehicles, however, it is precisely these extreme situations that require special attention, since people need the best possible information, especially in critical, potentially life-threatening scenarios. For less critical situations, on the other hand, it was already possible in this study to satisfy the participants' need for information. The majority of participants was satisfied with the explanation that the battery was empty and needed to be replaced in the key scenario. This was reflected in a neutral to positive impression and a reduced need for information. This scenario also illustrates the key issue our study tackles: how critically a situation is perceived depends on its context. Since the participants do not consider *MI* as a source of error, they are dependent on a classification of the situation. However, the context and thus the need for information changes through the classification. If *MI* is then identified as the error source in the key scenario, the participants classify the scenario as critical, also reflected by dropping satisfaction and

operational intent scores. At the same time, they are grateful for the indication of a possible security breach.

6.3 Implications for Design

All implications for design are based on the the findings of the Thematic and Correspondence Analysis and have to be validated in future work. We identified a fundamental information demand across all conditions and scenarios. Communicating the error cause (*Why*), explaining *What* happened in the situation and alerting the driver (*Warning/Message*) help to describe the situation and make the driver aware of malfunctions or threats. Depending on the situation and malfunction drivers wanted additional information. In case of *MI*, participants were typically interested in situational and attack specific information. The following design recommendations can help drivers to understand security critical situations and to act accordingly:

(1) **Provide Precise Action Recommendations.** Across both scenarios, the study participants wanted concrete recommendations for action. These could relate, for example, to what should be done next in a concrete situation, such as calling the police. However, it can also be higher level recommendations on how to remedy the security breach. Information types: *Action Recommendation*
(2) **Explicitly Communicate Threats.** In the *crash* scenario many of the study participants misjudged the current threat situation. This led to most of the participants simply driving on, which could be potentially life-threatening in this scenario. Therefore it is important to communicate threats realistically and understandably. Information types: *What, Why, Message/Warning*
(3) **Communicate Preventative Measures.** Participants across both scenarios demanded information on how to prevent security breaches of this kind in the future. This information not only contributes to a better understanding of the situation, but at the same time educates the driver and makes her sensitive to the subject. Information types: *Preventative Measures*
(4) **Provide Information About the Attack Vector.** The majority of participants wanted to know what happened and how this was possible. It is important to communicate the information at a level that the drivers can understand. Here it may be necessary to adapt the information to the level of expertise of the driver or to have her select the degree of detail she wants to know about. Information types: *Who, When, How*
(5) **Provide Investigative Cues.** Many participants wished for hints that could help them identify the attacker, e.g., the time and place of the attack or whether someone has already gained access to the vehicle. Information types: *Diagnostic Report, Troubleshooting, Who, When, How*

People in the *TM* and *NO* conditions, however, were interested in different types of information. They typically demanded more information about the car and were more specific about the quality of warnings they expected. The following design recommendations could serve as a baseline to design suitable communication structures for technical malfunctions:

(1) **Provide Visual and Auditory Alerts.** The study participants demanded visual and auditory signals, which ideally draw their attention to the defective part before malfunctions occur. This can be, for example, a *beep* sound to attract the driver's attention, or a flash of the key before the battery charge becomes too low. Information types: *Message/ Warning, Visual, Audio, Before/During*
(2) **Provide Status Information of Malfunctioning Parts.** Study participants most often inquired about the status of the faulty parts. In the *key malfunction* scenario, they wanted information about the battery status and how long the charge would last. In the *crash* scenario they demanded information about the state of the front sensor. Information types: *Status*
(3) **Provide Diagnostic Report.** Some of the study participants requested a diagnostic report from the vehicle. The report should contain information about the malfunction and the damage report. Additionally the car's parameters during the accident such as velocity can be supplemented. Information types: *Diagnostic Report, Parameters*
(4) **Communicate Next Actions.** Similar to the *MI* condition, the study participants wanted actionable recommendations. However, they focus more on what the driver needs to do in order to repair the defect and relate less to the specific circumstances of the situation. Information types: *Action Recommendation*
(5) **Explain Car's Internal Decision Process.** Some participants thought the malfunction was due to the autopilot's lacking functionality. They were interested in how the car perceived the situation and what caused it to misbehave. Information types: *Decision Process, Why*

Our results are consistent with the four principles supporting intelligibility and accountability in context-aware systems [3]. Here, the identified information types of our study complement the principles with details for the domain of semi-autonomous vehicles, with malicious intrusions identified as special cases. As the work of Jacobi et al. suggests [30], information needs can change over time. This certainly needs to be considered for the domain of cars in general. However, we argue that (highly) critical situations are a special case because they are rarely experienced. In order to establish a practical relevance, we would like distinguish ourselves from the NIST Cybersecurity Framework [47]. It focuses primarily on building and maintaining critical infrastructure and thus provides a set of activities to achieve specific cybersecurity outcomes. However, it is not tailored to achieve good computer-human communication.

7 LIMITATIONS

Our study has several limitations, some of which originate from the study design, while others are intrinsic to the measures we use to gather our data. First, we drew our sample from MTurk. Hence, it is not representative of the population of American car owners, since MTurk users are usually between 18 and 48 years old and have some level of college education [50]. However, as we were particularly interested in the specifics of malicious intrusions, MTurk serves a suitable population for our purpose [50]. Second, we confront participant with hypothetical scenarios. This means that the participants have to imagine experiencing the described

situation. Although we tried to make the scenarios as tangible as possible, they cannot offer the same quality as a personal experience. Due to the hypothetical character of the study, participants are relieved from any driving-related tasks. Additionally, at the point in time of the scenarios, when we asked for the driver's information demand, the car is not moving (anymore). Hence, the "drivers" - in that sense - are no longer drivers as they are not constrained by typical driving tasks when we elicited information demands. Although participants reported demand for visual and auditory alerts in response to a detected malfunction while driving, we acknowledge this general limitation to our scope of work. Since only 13 participants reported having previous experiences in driving or riding cars with autonomous driving features, this lack of experience among participants likely biased our results as well. Nevertheless, there is evidence that hypothetical surveys are able to identify tendencies [5], which can be verified in future work. Yet, we do not claim our results to be exhaustive, especially with regard to the information types we elicited.

Third, as our study follows a mixed-methods approach, we have to deal with a sample size trade-off. This means that it might be necessary to recruit more participants in order to detect small effects; however, this conflicts with qualitative data analysis. We did power calculations to estimate our sample size for an estimated medium effect between scenarios, resulting in $N = 60$. Although we usually reached saturation within the first round of coding, $N = 60$ was still manageable in terms of qualitative evaluation.

8 CONCLUSION

We identified 18 information types ranging from situational aspects to question types over car and warning specifics. Some of these information types form a basic need for information across scenarios. Depending on the perceived error cause, people may demand more situational or car specific information. The findings could be used to display relevant, sought-after information in appropriate contexts and inform design decisions for human-car interaction.

Moreover, we found that malicious intrusions were consistently perceived as critical, even if other perceived error sources in the same scenario were not. Critical situations sparked increased information demand, while at the same time making it hard to satisfy people. However we believe that particularly these situations require our attention, since people need the best possible information, especially in critical, potentially life-threatening scenarios.

Last but not least, we found the need to properly communicate error sources. Participants did not identify malicious intrusions in any scenario, unless being primed for it. If primed, they were not able to assess the situation correctly and act accordingly. In case of technical malfunction a similar effect surfaced in the crash scenario were people were unsure of the Autopilots capabilities and reasoning. We also found that simply prompting the error source is not sufficient in highly critical situations as this solely places the malfunction in the correct context leaving many open questions. We argue that complete threat models cannot be expected from drivers, and that the gaps we have identified must be taken into account to support drivers when they need it most.

Our study is an important first step to improve in-car risk communication to drivers and to provide helpful information at appropriate times. Depending on the situation this may build drivers' confidence and trust in the safety and security of the car, while it also may improve their decision-making capabilities in critical situations. Future work could test and validate our results, e.g. in providing drivers with relevant information and measuring how they assess and react to different situations. If feasible, it would be beneficial to test our results in a more realistic setting, though it is not ethical to have participants experience highly critical situations first hand. More realistic study set-ups could also investigate drivers' information demand while being constrained with driving-related tasks, which we did not cover. Last, but not least our insights could be used to develop or enhance interface solutions for cars to meaningfully communicate error sources in the future.

ACKNOWLEDGMENTS

At this point, we would like to express our sincere thanks to Dr. Michael Schilling and Prof. Dr. Sascha Fahl. The discussions and feedback helped to improve this work. We thank our reviewers for their detailed and constructive feedback. Finally, we would like to acknowledge the work of our study participants that ultimately made this project possible.

REFERENCES

[1] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Berkeley, 257–272.

[2] Paul Andre, Sanjay Chetwani, Kailasnath Dornadula, and Ashok Teckchandani. 2003. Automotive security and monitoring system. US Patent App. 10/073,725.

[3] Victoria Bellotti and Keith Edwards. 2001. Intelligibility and accountability: human considerations in context-aware systems. *Human–Computer Interaction* 16, 2-4 (2001), 193–212.

[4] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[5] Jae Bong Chang, Jayson L Lusk, and F Bailey Norwood. 2009. How closely do hypothetical surveys and laboratory experiments predict field behavior? *American Journal of Agricultural Economics* 91, 2 (2009), 518–534.

[6] Kathy Charmaz. 2014. *Constructing grounded theory*. Sage, London.

[7] Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng. 2018. Detecting attacks against robotic vehicles: A control invariant approach. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, New York, 801–816.

[8] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B Roenne, Peter YA Ryan, and Vincent Koenig. 2019. Security-Visible, Yet Unseen?. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, New York, 1–13.

[9] Finale Doshi-Velez, Mason Kortz, Ryan Budish, Chris Bavitz, Sam Gershman, David O'Brien, Stuart Schieber, James Waldo, David Weinberger, and Alexandra Wood. 2017. Accountability of AI under the law: The role of explanation. *arXiv* (2017). arXiv:arXiv:1711.01134

[10] Raj Gautam Dutta, Feng Yu, Teng Zhang, Yaodan Hu, and Yier Jin. 2018. Security for safety: a path toward building trusted autonomous vehicles. In *Proceedings of the International Conference on Computer-Aided Design*. ACM, New York, 1–6.

[11] Mary T Dzindolet, Scott A Peterson, Regina A Pomranky, Linda G Pierce, and Hall P Beck. 2003. The role of trust in automation reliance. *International journal of human-computer studies* 58, 6 (2003), 697–718.

[12] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[13] Flavio D Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès. 2016. Lock it and still lose it—on the (in) security of automotive remote keyless entry systems. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Berkeley.

[14] Jairo Giraldo, Sahand Hadizadeh Kafash, Justin Ruths, and Alvaro A Cardenas. 2020. DARIA: Designing Actuators to Resist Arbitrary Attacks Against Cyber-Physical Systems. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, New York, 339–353.

[15] Alyssa Glass, Deborah L McGuinness, and Michael Wolverton. 2008. Toward establishing trust in adaptive agents. In *Proceedings of the 13th international conference on Intelligent user interfaces*. ACM, New York, 227–236.

[16] Michael Greenacre. 2017. *Correspondence analysis in practice*. CRC press, Boca Raton.

[17] Andy Greenberg. 2013. Forbes, "Hackers Reveal Nasty New Car Attacks–With Me Behind The Wheel (Video)". https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/. Accessed: 2021-01-11.

[18] Andy Greenberg. 2015. Wired, "Hackers Remotely Kill a Jeep on the Highway—With Me in It". https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed: 2021-01-11.

[19] Andy Greenberg. 2016. Wired, A New Wireless Hack Can Unlock 100 Million Volkswagens. https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/. Accessed: 2019-15-11.

[20] Andy Greenberg. 2017. Wired, "Just a Pair of These $11 Radio Gadgets Can Steal a Car". https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/. Accessed: 2021-01-11.

[21] Andy Greenberg. 2018. Wired, "Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob". https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/. Accessed: 2021-01-11.

[22] Andy Greenberg. 2019. Wired, "Hackers Could Steal a Tesla Model S by Cloning Its Key Fob—Again". https://www.wired.com/story/hackers-steal-tesla-model-s-key-fob-encryption/. Accessed: 2021-01-11.

[23] Andy Greenberg. 2020. Wired, "Split-Second 'Phantom' Images Can Fool Tesla's Autopilot". https://www.wired.com/story/tesla-model-x-autopilot-phantom-images/. Accessed: 2021-01-11.

[24] Andy Greenberg. 2020. Wired, "This Bluetooth Attack Can Steal a Tesla Model X in Minutes". https://www.wired.com/story/tesla-model-x-hack-bluetooth/. Accessed: 2021-01-11.

[25] Shirley Gregor and Izak Benbasat. 1999. Explanations from intelligent systems: Theoretical foundations and implications for practice. *MIS quarterly* (1999), 497–530.

[26] Peter A Hancock, Deborah R Billings, Kristin E Schaefer, Jessie YC Chen, Ewart J De Visser, and Raja Parasuraman. 2011. A meta-analysis of factors affecting trust in human-robot interaction. *Human factors* 53, 5 (2011), 517–527.

[27] Helen Hastie, Francisco J Chiyah Garcia, David A Robb, Atanas Laskov, and Pedro Patron. 2018. MIRIAM: A multimodal interface for explaining the reasoning behind actions of remote autonomous systems. In *Proceedings of the 2018 on International Conference on Multimodal Interaction*. ACM, New York, 557–558.

[28] Kevin Anthony Hoff and Masooda Bashir. 2015. Trust in automation: Integrating empirical evidence on factors that influence trust. *Human factors* 57, 3 (2015), 407–434.

[29] Andreas Holzinger. 2018. From machine learning to explainable AI. In *2018 World Symposium on Digital Intelligence for Systems and Machines (DISA)*. IEEE, New York, 55–66.

[30] Timo Jakobi, Gunnar Stevens, Nico Castelli, Corinna Ogonowski, Florian Schaub, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. 2018. Evolving needs in iot control and accountability: A longitudinal study on smart home intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–28.

[31] Jiun-Yin Jian, Ann M Bisantz, and Colin G Drury. 2000. Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics* 4, 1 (2000), 53–71.

[32] W Lewis Johnson. 1994. Agents that Learn to Explain Themselves. In *AAAI-94 Proceedings*. AAAI, Palo Alto, 1257–1263.

[33] Samy Kamkar. 2015. Drive it like you hacked it: New attacks and tools to wirelessly steal cars. *Presentation at DEFCON* 23 (2015).

[34] Swati Khandelwal. 2016. Hackernews, "Car Thieves Can Unlock 100 Million Volkswagens With A Simple Wireless Hack". https://thehackernews.com/2016/08/hack-unlock-car-door.html. Accessed: 2021-01-11.

[35] Klaus Krippendorff. 2004. *Content analysis: An introduction to its methodology*. Sage, London. chap. 11 pages.

[36] Thomas Kundinger, Philipp Wintersberger, and Andreas Riener. 2019. (Over) Trust in Automated Driving: The Sleeping Pill of Tomorrow?. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, New York, 1–6.

[37] Matt Lake. 2001. The New York Times, "HOW IT WORKS; Remote Keyless Entry: Staying a Step Ahead of Car Thieves". https://www.nytimes.com/2001/06/07/technology/how-it-works-remote-keyless-entry-staying-a-step-ahead-of-car-thieves.html. Accessed: 2021-01-11.

[38] Pat Langley, Ben Meadows, Mohan Sridharan, and Dongkyu Choi. 2017. Explainable agency for intelligent autonomous systems. In *Twenty-Ninth AAAI Conference*. AAAI, Palo Alto.

[39] John D Lee and Katrina A See. 2004. Trust in automation: Designing for appropriate reliance. *Human factors* 46, 1 (2004), 50–80.

[40] Brian Y Lim and Anind K Dey. 2009. Assessing demand for intelligibility in context-aware applications. In *Proceedings of the 11th international conference on Ubiquitous computing*. ACM, New York, 195–204.

[41] Brian Y Lim and Anind K Dey. 2010. Toolkit to support intelligibility in context-aware applications. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. ACM, New York, 13–22.

[42] Brian Y Lim, Anind K Dey, and Daniel Avrahami. 2009. Why and why not explanations improve the intelligibility of context-aware intelligent systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, 2119–2128.

[43] Poornima Madhavan and Douglas A Wiegmann. 2007. Similarities and differences between human–human and human–automation trust: an integrative review. *Theoretical Issues in Ergonomics Science* 8, 4 (2007), 277–301.

[44] Deborah L McGuinness, Alyssa Glass, Michael Wolverton, and Paulo Pinheiro Da Silva. 2007. A Categorization of Explanation Questions for Task Processing Systems. In *ExaCt*. AAAI, Palo Alto, 42–48.

[45] Stephanie M Merritt and Daniel R Ilgen. 2008. Not all trust is created equal: Dispositional and history-based trust in human-automation interactions. *Human Factors* 50, 2 (2008), 194–210.

[46] Hyeran Mun, Kyusuk Han, and Dong Hoon Lee. 2020. Ensuring Safety and Security in CAN-based Automotive Embedded Systems: A Combination of Design Optimization and Secure Communication. *IEEE Transactions on Vehicular Technology* (2020).

[47] NIST. 2021. Cybersecurity Framework. https://www.nist.gov/cyberframework. Accessed: 2021-01-11.

[48] Stefan Nürnberger and Christian Rossow. 2016. –vatiCAN–Vetted, Authenticated CAN Bus. In *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, Cham, 106–124.

[49] OPM.GOV. 2021. EDUCATION LEVEL. https://dw.opm.gov/datastandards/referenceData/1435/current?index=E. Accessed: 2021-01-11.

[50] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 2019 IEEE Symposium on Security and Privacy (SP), Vol. 00*. IEEE, New York, 227–244.

[51] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages.. In *SOUPS*. USENIX Association, Berkley.

[52] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, New York, 272–288.

[53] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. ACM, New York, 1–13.

[54] John K Rempel, John G Holmes, and Mark P Zanna. 1985. Trust in close relationships. *Journal of personality and social psychology* 49, 1 (1985), 95.

[55] Ishtiaq Rouf, Robert D Miller, Hossen A Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. 2010. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study.. In *USENIX Security Symposium*, Vol. 10. USENIX Association, Berkley.

[56] Wojciech Samek. 2019. *Explainable AI: Interpreting, explaining and visualizing deep learning*. Springer Nature, Cham.

[57] Markus Pauly Sarah Friedrich, Frank Konietschke. 2020. MANOVA.RM Documentation. https://cran.r-project.org/web/packages/MANOVA.RM/MANOVA.RM.pdf. Accessed: 2021-01-11.

[58] Fabian A. Scherschel. 2018. Heise, "Schlüssel-Hack: Autos von Tesla lassen sich in Sekunden öffnen". https://www.heise.de/security/meldung/Schluessel-Hack-Autos-von-Tesla-lassen-sich-in-Sekunden-oeffnen-4161136.html. Accessed: 2021-01-11.

[59] Matthew Smith, Martin Strohmeier, Jonathan Harman, Vincent Lenders, and Ivan Martinovic. 2020. A view from the cockpit: exploring pilot reactions to attacks on avionic systems. *NDSS* (2020).

[60] Anselm Strauss and Juliet M Corbin. 1997. *Grounded theory in practice*. Sage, London.

[61] Tesla. 2020. Tesla's Autopilot. https://www.tesla.com/autopilot. Accessed: 2019-07-10.

[62] Daniel Wessel Thomas Franke, Christiane Attig. 2021. ATI Scale. https://ati-scale.org/. Accessed: 2021-01-11.

[63] Amazon Mechanical Turk. 2021. Amazon Mechanical Turk. https://www.mturk.com/. Accessed: 2021-01-11.

[64] Amazon Mechanical Turk. 2021. FAQs - About Amazon Mechanical Turk. https://www.mturk.com/worker/help. Accessed: 2021-01-11.

[65] Marko Wolf, André Weimerskirch, and Christof Paar. 2004. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*. isits AG, Bochum.

[66] Eray Yağdereli, Cemal Gemci, and A Ziya Aktaş. 2015. A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation* 12, 4 (2015), 369–381.
[67] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON* 24 (2016).
[68] YouTube. 2020. "AReallyBadDay: Tesla Crash into Construction Barrels". https://www.youtube.com/watch?v=i9r4nS5EjjQ. Accessed: 2020-09-17.

A PARTICIPANT DEMOGRAPHICS

Table 3 contains an overview of the participants demographic split by conditions.

	TM	MI	NO	Total
Gender				
Women	7	9	7	23
Men	17	8	12	37
Age				
Min	25	24	24	24
Max	73	59	69	73
Median	37	36	38	37
Mean	40.73	38.94	42.36	40.67
Education				
Min	4	4	4	4
Max	21	13	17	21
Median	13	10	10	10
Mean	11.00	10.17	9.89	10.35
Driving Experience				
Min	9	7	8	7
Max	48	44	52	52
Median	20	22	22	21
Mean	23.43	23.70	24.78	23.94
ATI Scale				
Min	1.55	2	3.55	1.55
Max	6	6	5.88	6
Median	4.66	4.55	5	4.66
Mean	4.53	4.34	4.80	4.56

Table 3: Participant demographics. Education reported according to OPM educational level [49]. Driving experience in years. Affinity for technology interaction(ATI) scale [12] results on a scale from 1-6. Higher values indicate a tendency to actively participate in intensive technology interaction [62].

B CODEBOOKS

Table 4 shows an comparative overview of the six codebooks. Each codebook contains high level codes about participants' perceptions of what happened in the scenario, feelings about the car's response to the scenario, reported next actions after the scenario, and information demand in the scenario.

C RESULTS OF CORRESPONDENCE ANALYSIS

We provide the contingency tables of the key (Table 5) and crash (Table 8) scenario. Also we provide the results of the Correspondence Analysis for both scenarios including chi-square distances and relative inertias.

Table 4: Comparative overview of the six codebooks. Mean inter-rater reliability of each codebook reported with Krippendorff's α [35].

Key - NO K's α: 0.842	Key - TM K's α: 0.795	Key - MI K's α: 0.815	Crash - NO K's α: 0.906	Crash - TM K's α: 0.771	Crash - MI K's α: 0.819
Perceptions of what happened					
Technical Malfunction	Technical Malfunction	Technical Malfunction	Technical Malfunction	Technical malfunction	Technical Malfunction
Human Failure	Human Failure	Hack/ Intrusion	Human Failure	Human Failure	Hack/ Intrusion
Security/ Safety Mechanism	Correct Description	Security/ Safety Mechanism	Technical Limits	Technical Limits	Human Failure
Design of Car	Incorrect Description	Correct Description	Correct Description	Correct Description	Minor Damage
Correct Description		Incorrect Description	Incorrect Description	Incorrect Description	Accident Avoided
		Uncertainty			
Feelings about car's response to situation					
Not Vehicle's Fault	Not Vehicle's Fault	Vehicle behaved appropriately	Negative Feeling	Negative Feeling	Negative Feeling
Positive Feeling	Positive Feeling	Positive Feeling	Surprised Feeling	Safety Hazard	Potentially lethal
Neutral Feeling	Neutral Feeling	Neutral Feeling	Neutral Feeling	Positive Feeling	Neutral Feeling
Negative Feeling	Negative Feeling	Negative Feeling	Positive Feeling	Surprised Feeling	Lost Trust
Safety Feeling	Safety Feeling	Safety Feeling	Safety Hazard	Worked properly	General wariness of AI
Improvement is needed	Car should react earlier	Insecurity Feeling	Driver should be attentive	Need for Fallback Mechanism	Need for Improvement
			Improvement is needed	Driver should be attentive	
Next Actions					
Key/ Battery Repair	Key/ Battery Repair	Key/ Lock Repair	Continue with Autopilot	Deactivate Autopilot	Call Manufacturer
Supervise Car/ Key	Use Key Analogously	Contact Manufacturer/ Dealer	Take over Manual Control	Take over Manual Control	Pull Over Car
Testing of Key	Use 2nd Key of Car	Contact Police	Inspect Car	Assess Car Damage	Turn off Autopilot
Adaption of One's Behaviour	Continue with Actions		Repair	Get Professional Help	Continue Driving Manually
Continue with Actions			Take care not to repeat HF	Report to Police	Never Use Autopilot Again
Check Manual			Don't use Autopilot	Report to Insurance	Monitor Autopilot
No Action				Report to Manufacturer	Fix Accident Scene
				Reflect on One's Responsibility	Call Police
				Get Rid of Car	Check Car for Damage
				Understand Car Mechanics/Tech	Get Car Towed
					Never Drive this Car Again
Information Demand					
Message/ Warning	Message/ Warning	Message/ Warning	Status of Malfunctioning Parts	Status of Malfunctioning Parts	What happened
Why	Status of Key	What happened?	Car's Diagnostic Report	Car's Diagnostic Report	Why it happened
Status of Key	Action Recommendations	Why did it happen?	Why it happened	Why it happened	Who is attacker
No Information Demand	Audio Reponse	How was it possible?	What happened	What happened	Preventative Meassures
Logs + Analytics	Visual Response	When did attack happen?	Car's Decision Process	Preventative Measures	Data for Fix
Usage Instructions	No Information Demand	Investigative Clues	Car's Parameters During Accident	Car's Parameters During Accident	Message/ Warning
Action Recommendations		Error Codes	Warning/ Message	Message/ Warning	When it happened
Troubleshooting		Status of Key	Audio Warning	Visual Warning	Action Recommendations
		Action Recommendations	Visual Warning	Audio Warning	Damage Report
		Preventative Measures	No Information Demand	Warn Before/ During Accident	No Information Demand
			Usage Instructions		
			Preventative Measures		
			Action Recommendations		
			Warn Before/During Accident		

Table 5: Contingency table table of moderating factors and information demand codes of all conditions in the Key scenario.

	What	Why	Who	When	How	Status	Report	Decision	Param	Usage	Prevent	Message	Trblshoot	Recomm	Visual	Audio	Before	None
HiCrit	0	5	1	6	1	3	1	0	0	0	3	4	3	5	0	0	0	0
LessCrit	4	7	0	0	0	16	1	0	0	2	0	12	1	2	1	1	0	11
TM	2	5	0	0	0	12	1	0	0	1	0	7	0	2	1	0	0	5
MI	0	5	2	7	1	3	1	0	0	0	3	4	3	5	0	0	0	0
Human	0	3	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	4
Design	1	0	1	2	1	0	0	0	0	1	0	0	3	0	0	0	0	1
Threat	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Pos	1	2	2	6	1	7	0	0	0	1	1	6	4	5	0	0	0	3
Neg	2	8	0	4	0	10	1	0	0	0	2	6	3	5	0	0	0	0
Neut	2	5	0	0	0	4	1	0	0	0	0	4	0	0	1	1	0	8

Table 6: Chi-Square Distances of moderating factors and information demand codes of all conditions in the Key scenario.

	What	Why	Who	When	How	Status	Report	Usage	Prevent	Message	Trblshoot	Recomm	Visual	Audio	None	Total
HiCrit	1,352	0,054	0,155	3,597	0,669	1,649	0,155	0,676	3,889	0,147	0,614	1,949	0,338	0,225	3,606	19,077
LessCrit	0,979	0,167	1,225	5,106	0,817	2,024	0,041	0,49	1,838	1,179	1,76	1,718	0,245	0,857	3,05	21,496
TM	0,151	0,001	0,761	3,169	0,507	3,626	0,075	0,075	1,141	0,44	2,155	0,357	1,01	0,254	0,22	13,942
MI	1,437	0,009	2,287	5,365	0,567	1,951	0,11	0,718	3,43	0,256	0,457	1,574	0,359	0,239	3,831	22,592
Human	0,338	3,114	0,169	0,704	0,113	1,549	0,169	4,086	0,254	1,211	0,479	0,676	0,085	0,056	10,651	23,654
Design	0,789	1,408	2,945	1,424	5,241	1,937	0,211	2,945	0,317	1,514	9,634	0,845	0,106	0,07	0,014	29,4
Pos	0,255	2,221	1,679	1,919	0,37	0,04	0,824	0,038	0,045	0,002	1,188	0,881	0,412	0,275	0,442	10,591
Neg	0,041	0,858	0,866	0,042	0,577	0,534	0,021	0,866	0,378	0,007	0,121	0,68	0,433	0,289	4,62	10,334
Neut	0,74	0,489	0,549	2,289	0,366	0,213	0,37	0,549	0,824	0,001	1,556	2,197	1,916	3,645	8,776	24,479
Total	6,082	8,322	10,636	23,615	9,227	13,524	1,977	10,443	12,116	4,758	17,965	10,878	4,903	5,91	35,21	175,565

Table 7: Relative inertias of moderating factors and information demand codes of all conditions in the Key scenario.

	What	Why	Who	When	How	Status	Report	Usage	Prevent	Message	Trblshoot	Recomm	Visual	Audio	None	Total
HiCrit	0,008	0	0,001	0,02	0,004	0,009	0,001	0,004	0,022	0,001	0,003	0,011	0,002	0,001	0,021	0,109
LessCrit	0,006	0,001	0,007	0,029	0,005	0,012	0	0,003	0,01	0,007	0,01	0,01	0,001	0,005	0,017	0,122
TM	0,001	0	0,004	0,018	0,003	0,021	0	0	0,006	0,003	0,012	0,002	0,006	0,001	0,001	0,079
MI	0,008	0	0,013	0,031	0,003	0,011	0,001	0,004	0,02	0,001	0,003	0,009	0,002	0,001	0,022	0,129
Human	0,002	0,018	0,001	0,004	0,001	0,009	0,001	0,023	0,001	0,007	0,003	0,004	0	0	0,061	0,135
Design	0,004	0,008	0,017	0,008	0,03	0,011	0,001	0,017	0,002	0,009	0,055	0,005	0,001	0	0	0,167
Pos	0,001	0,013	0,01	0,011	0,002	0	0,005	0	0	0	0,007	0,005	0,002	0,002	0,003	0,06
Neg	0	0,005	0,005	0	0,003	0,003	0	0,005	0,002	0	0,001	0,004	0,002	0,002	0,026	0,059
Neut	0,004	0,003	0,003	0,013	0,002	0,001	0,002	0,003	0,005	0	0,009	0,013	0,011	0,021	0,05	0,139
Total	0,035	0,047	0,061	0,135	0,053	0,077	0,011	0,059	0,069	0,027	0,102	0,062	0,028	0,034	0,201	1

Table 8: Contingency table of moderating factors and information demand codes of all conditions in the Crash scenario.

	What	Why	Who	When	How	Status	Report	Decision	Param	Usage	Prevent	Message	Trblshoot	Recomm	Visual	Audio	Before	None
HiCrit	21	21	1	2	3	10	8	2	3	1	5	22	3	3	3	4	18	2
LessCrit	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TM	14	14	0	0	0	10	7	2	3	0	2	15	0	1	3	4	16	1
MI	7	7	1	2	3	0	0	0	0	0	3	6	3	2	0	0	1	1
Human	8	8	0	1	1	5	5	0	3	1	3	5	2	1	2	2	5	1
Design	4	4	0	0	0	4	2	0	1	0	1	2	0	1	1	1	2	0
Threat	4	4	0	0	1	4	3	1	1	0	2	7	0	0	1	1	8	1
Pos	1	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
Neg	19	19	1	2	3	8	6	1	2	0	5	21	2	3	3	4	17	2
Neut	2	2	0	0	0	0	1	0	1	0	0	2	1	0	0	1	2	0

Table 9: Chi-Square Distances of moderating factors and information demand codes of all conditions in the Crash scenario.

	What	Why	Who	When	How	Status	Report	Decision	Param	Usage	Prevent	Message	Trblshoot	Recomm	Visual	Audio	Before	None	Total
HiCrit	0,002	0,002	0,062	0,018	0,007	0,076	0,012	0,018	0,112	0,444	0,038	0,071	0,007	0,007	0,042	0,039	0	0,003	0,962
TM	0,016	0,016	0,543	1,268	1,992	0,753	0,25	0,423	0,085	0,362	0,855	0,018	1,992	0,494	0,177	0,276	0,983	0,139	10,644
MI	0,312	0,312	2,916	4,56	6,325	2,976	2,268	0,496	0,992	0,142	1,536	0,019	6,325	1,911	0,921	1,205	3,094	0,331	36,642
Human	0,014	0,014	0,313	0,1	0,019	0,087	0,827	0,73	1,622	3,001	0,299	1,342	0,633	0,019	0,306	0,029	0,672	0,033	10,059
Design	0,039	0,039	0,136	0,317	0,498	2,316	0,21	0,317	0,211	0,091	0,003	0,726	0,498	0,506	0,288	0,069	0,404	0,362	7,03
Threat	0,658	0,658	0,224	0,524	0,038	0,234	0,154	0,433	0,002	0,15	0,117	0,172	0,823	0,823	0,001	0,058	1,561	0,269	6,9
Pos	0,217	0,217	0,024	0,055	0,087	1,355	0,252	16,2	0,11	0,016	0,165	0,63	0,087	0,087	0,102	0,134	0,543	0,063	20,342
Neg	0,009	0,009	0,132	0,086	0,077	0,316	0,276	0,241	0,482	0,465	0,003	0,314	0,121	0,077	0	0,001	0,059	0,011	2,68
Neut	0,006	0,006	0,071	0,165	0,26	0,992	0,079	0,165	1,355	0,047	0,496	0,006	2,108	0,26	0,307	0,892	0,084	0,189	7,49
Total	1,276	1,276	4,422	7,092	9,303	9,106	4,327	19,02	4,972	4,717	3,512	3,299	12,59	4,184	2,144	2,702	7,401	1,4	**102,748**

Table 10: Relative Inertias of moderating factors and information demand codes of all conditions in the Crash scenario.

	What	Why	Who	When	How	Status	Report	Decision	Param	Usage	Prevent	Message	Trblshoot	Recomm	Visual	Audio	Before	None	Total
HiCrit	0	0	0,001	0	0	0,001	0	0	0,001	0,004	0	0,001	0	0	0	0	0	0	0,009
TM	0	0	0,005	0,012	0,019	0,007	0,002	0,004	0,001	0,004	0,008	0	0,019	0,005	0,002	0,003	0,01	0,001	0,104
MI	0,003	0,003	0,028	0,044	0,062	0,029	0,022	0,005	0,01	0,001	0,015	0	0,062	0,019	0,009	0,012	0,03	0,003	0,357
Human	0	0	0,003	0,001	0	0,001	0,008	0,007	0,016	0,029	0,003	0,013	0,006	0	0,003	0	0,007	0	0,098
Design	0	0	0,001	0,003	0,005	0,023	0,002	0,003	0,002	0,001	0	0,007	0,005	0,005	0,003	0,001	0,004	0,004	0,068
Threat	0,006	0,006	0,002	0,005	0	0,002	0,001	0,004	0	0,001	0,001	0,002	0,008	0,008	0	0,001	0,015	0,003	0,067
Pos	0,002	0,002	0	0,001	0,001	0,013	0,002	0,158	0,001	0	0,002	0,006	0,001	0,001	0,001	0,001	0,005	0,001	0,198
Neg	0	0	0,001	0,001	0,001	0,003	0,003	0,002	0,005	0,005	0	0,003	0,001	0,001	0	0	0,001	0	0,026
Neut	0	0	0,001	0,002	0,003	0,01	0,001	0,002	0,013	0	0,005	0	0,021	0,003	0,003	0,009	0,001	0,002	0,073
Total	0,012	0,012	0,043	0,069	0,091	0,089	0,042	0,185	0,048	0,046	0,034	0,032	0,123	0,041	0,021	0,026	0,072	0,014	1

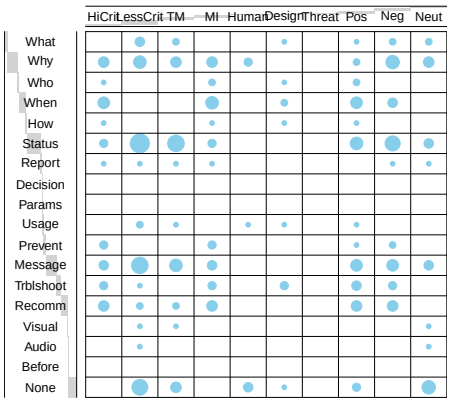

Figure 6: *Key* scenario

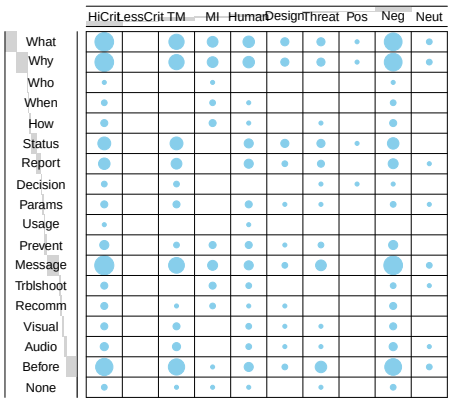

Figure 7: *Crash* scenario

Figure 8: Balloon plot representation of the contingency table table of *moderating factors* and *information demand* codes. Bigger dots indicate larger chi-square distances. Refer to tables 6 and 9 in the Appendix for exact results.