Multilayered Review of Safety Approaches for Machine Learning-based Systems in the Days of AI

Sangeeta Dey[a] and Seok-Won Lee[a,b,1]

[a]*Department of Artificial Intelligence,* [b]*Department of Software and Computer Engineering*

Ajou University, Suwon City, Republic of Korea 443-749

Abstract

Abstract: The unprecedented advancement of artificial intelligence (AI) in recent years has altered our perspectives on software engineering and systems engineering as a whole. Nowadays, software-intensive intelligent systems rely more on a learning model than thousands of lines of codes. Such alteration has led to new research challenges in the engineering process that can ensure the safe and beneficial behavior of AI systems. This paper presents a literature survey of the significant efforts made in the last fifteen years to foster safety in complex intelligent systems. This survey covers relevant aspects of AI safety research including safety requirements engineering, safety-driven design at both system and machine learning (ML) component level, validation and verification from the perspective of software and system engineers. We categorize these research efforts based on a three-layered conceptual framework for developing and maintaining AI systems. We also perform a gap analysis to emphasize the open research challenges in ensuring safe AI. Finally, we conclude the paper by providing future research directions and a road map for AI safety.

Keywords: Autonomous systems; Intelligent software systems; Machine learning; Safety analysis; Software engineering.

[1]Corresponding Author

1. Introduction

Recently, artificial intelligence (AI) has received increased attention from many sectors and fields. These diverse areas include autonomous driving, computer vision, medical diagnosis systems, gaming systems, etc. Various industries are overwhelmed by the positive potential of AI. This unprecedented advancement of AI has altered our perspectives on various business functions, including software-intensive intelligent systems development process. Machine learning (ML) is one of the greatest contributors to this revolution. The task of a software engineer has now transformed from writing thousands of lines of code to training, retraining, testing, and maintaining a learning model. However, it is essential to realize that every advancement of technology comes with surprises and concerns, and AI is no exception. AI revolution is not at its inception any more. However, the means to ensuring safety, transparency, and level of fidelity of AI systems are still unclear. Many researchers have already expressed apprehension related to the advent of AI especially in high-risk environments [1, 2]. Moreover, AI systems that equal or even exceed humans in cognitive tasks are both appealing and alarming [3, 4, 5]. Introducing a sense of ethics and morality has long been discussed as the top priority for the days of AI [6, 7]. Therefore, amid the excitement about improved efficiency due to AI, it is worth engaging in discussions on its potential risks, new challenges, and questionable impact on safety issues [8].

The process of reduction of human interventions in many sectors of industries is already underway. Automotive, aerospace etc. are heavily using ML algorithms to paving their way towards increasing autonomy [9]. A fully automated driver-less car is not a far-fetched dream in the days of AI [10]. However, a few recent accidents involving semi-autonomous cars [11] have negatively impacted our trust in full autonomy. It has been argued that the increasing autonomy of AI systems can have enormous impact on humanity [8, 9]. Use of systems that rely heavily on the decision making of an ML model should be a tremendous concern in high-risk environment. Although introduction of ML in controlling

complex engineering systems has been proved to be more efficient than unpredictable erroneous human controls in many cases, the robustness of such ML models should be assessed.

However, as stakeholders from various backgrounds and expertise participate in the process of ensuring safety of a complex systems, a consensus on the fundamental properties of autonomous systems; e.g. controllability, explainability, robustness to uncertain environment, etc. is necessary [12, 13]. Functional safety experts worry about the gap between the vision of the current automotive industry and the scope of the current safety standards landscape [9]. Traditional risk model and safety analysis [14] are also inadequate to handle the immense use of AI in safety-critical systems. Moreover, how the activities performed by experts of diverse expertise integrate to foster an emergent property like safety is not clear. For instance, how the artifacts flow across the various layers of methodical systems engineering at different levels of abstractions is still an open question. It is still unclear how the traceability can be maintained in a collaborative environment where the stakeholders not necessarily speak the same terms. Singla et al. have analyzed the differences between ML-based agile software projects and traditional agile software projects in terms of their execution processes, issues faced and the terms used to describe same concepts in these two types of workload [15].

Therefore, we believe that, we need to analyze the state-of-the-art safety approaches through the lens of a methodological engineering process. To the best of our knowledge, no systematic literature review of AI safety from a software engineering perspective has been done in recent times. The landscape of AI safety and beneficence research [16] discusses a vast range of research topics directed to AI safety. This article includes research areas such as validation, verification, control, security, etc. However, in order to perform a gap analysis on the state-of-the-art AI safety approaches, it is imperative to have a bigger picture of the recent research efforts from an engineering process perspective.

Research questions that we try to answer through our research are:

RQ1: How can we easily comprehend the complexity and challenges involved

in fostering safety of a complex intelligent systems?

Rationale: AI systems today are very complex at many layers. We argue that, not only the technical advances force us to give a deeper thought to safety related issues, but also the diversity of stakeholders participating in the systems engineering process amplifies the complexity. For example, a system level safety engineer may not be fully aware of the impact of the minute loopholes in the software module which vastly relies on ML algorithms. As different stakeholders with diverse expertise work at different levels of abstractions in the process of fostering safety, it is important to visualize the state-of-the art safety approaches from a layered perspective.

RQ2: How have safety concerns been addressed by the researchers along the phases of SE process?

Rationale: We acknowledge the paradigm shift that has taken place in the software development process. However, we believe that, the foundation of software engineering (SE) process entailing phases such as requirements engineering (RE), design, development, validation, verification and maintenance, still provides a strong methodological foundation to the whole process of intelligent software engineering even in this new paradigm. Understanding data requirements, designing the parameters and features of a learning model, training, tuning and testing of the ML model, and finally, maintaining or updating the model over time are new additions to the activities of phases such as RE, design, development, V & V, maintenance respectively. In our study we would like to map the research efforts in the field of AI safety along the phases of SE.

RQ3: What are the gaps in the current research efforts?

Rationale: After we find the answers to RQ1 and RQ2, we can have an accurate visualization of the areas that have not been explored yet. Finding the gap can eventually help us provide possible directions for future research.

RQ4: What are the future directions that may help reduce the gaps?

Rationale: We further want to analyze the existing gaps and provide our preliminary vision on the ways to reduce those gaps. Our paper finds the scope of improved collaborations among diverse stakeholders while analyzing current

state-of-the-art safety approaches from a multidisciplinary engineering process perspective.

In summary, the major contributions of this paper are:

-We provide a conceptual three-layered framework that helps us visualize the inherent complexity in developing and maintaining complex intelligent systems involving various stakeholders.

-We identify the challenges and risks that are of major concern along each layer of the framework.

-We review significant work conducted to address safety-related issues in intelligent systems in the last fifteen years.

-We perform a gap analysis to identify what aspects we are missing in literature and practice.

-Finally, we provide a research road map to expand the ongoing research on safe AI.

The remainder of the paper is organized as follows. In Section 2 we discuss the background of the research on safe AI systems. We summarize the related surveys in this area and explain the position of our survey in Section 3. A detailed research method of conducting a literature review is explained in Section 4. Section 5 introduces the proposed three-layered conceptual framework to better visualize the engineering process of complex intelligent systems. It also elaborates on the challenges and significant research efforts address the AI safety-related problems along each layer of the framework. We discuss our findings of literature review based on the research questions in Section 6. The limitation and threats to validity of this study are discussed in Section 7. Finally, we conclude the paper in Section 8.

2. Background

2.1. What is a "Safe AI system"?

Before we investigate the formal explanation of a safe AI system, we discuss the definition of 'safety'. The concept of safety has long been defined and

analyzed from multiple perspectives. Various domains have explained safety in different ways. Leveson explained that safety means absolutely no harm to people and no accidents with or without harming people [17]. According to IEC 61508, "Safety is freedom from unacceptable risk". This definition leads us to the concept of 'Risk' [18]. To analyze safety, the level of risk should be assessed. This definition also seems to be more practical than the previous one as it is almost impossible to engineer a fault-free system. Rather, this definition leaves an existing scope of risk up to a certain level of tolerance. Another definition of safety given by ISO 26262 [19] is "safety means the absence of unreasonable risk". This definition involves not only the probabilistic analysis of risk, but also the mechanisms to avoid harm and the possibilities of occurrences of such situations.

Recently, with the unprecedented emergence of AI based systems, the concept of 'safety' has started to entail a broader concept than the discussed definitions. AI techniques come with various inherent risks and behavior uncertainties due to a vast range of reasons: data-driven behavior (instead of code or rule-driven), self-learning or exploration, black-box nature, etc. As these systems are mostly driven by a few system-level objectives specified by the designers, it is important to ensure that the systems will not try to achieve their goals in an undesirable manner. In other words, the current safety concerns are not limited to failure, non-availability, and wrong outcomes; rather the concerns include reward hacking, negative side-effects, unsafe exploration, and insufficient robustness to distributional shift, etc. [8]. As argued by Varshney [20], it is not enough to minimize risk by defining a risk-minimal loss function. Instead, it is also important to address epistemic uncertainty in the underlying distribution of training and test instances. Moreover, as these AI systems are deployed in a socio-technical environment, the perception of safety or 'safe system' depends considerably on the confidence of society in such systems. From this perspective, a safe AI system should not only be engineered to behave safely but also be capable of explaining its behavior to a wide range of society.

2.2. When is a system "safe enough"?

While nowadays we have a common understanding that no system can be absolutely fail-free, we still do not have a consensus on the safety measurement criteria. We have various safety standards to certify a system as safe enough to deploy. However, the overall quantification (formalism) of how much safe is safe enough vary widely across various domains. Littlewood made a significant contribution in quantifying software safety with the help of evidence-based arguments and the confidence in those arguments [21]. With the help of multi-legged arguments, he showed how diversity in arguments can be utilized to prove dependability of a software system with a certain confidence. For example: if the overall argument is to support a claim of 10^{-4} pfd (probability of failure on demand), a statistical leg can support this claim with direct evidence whereas a logical leg can also fine-tune its confidence in the claim based on the confidence in the statistical leg.

Automotive industries that produce AI-based autonomous vehicles have also faced with the same challenge to acquire sufficient confidence in the safe behavior of a newly designed vehicle. As discussed earlier, with the advent of data-driven learning techniques, there is little scope of finding bugs in the code or models. Apart from gaining confidence in the usage of right set of training data, one of the promising ways to ensure safety is to test the system thoroughly in simulation-based or real-world situations. However, the challenge is to make sure that the designers have explored all possible scenarios and surprises that the system can encounter during testing. As Koopman mentioned in [13], miles on road is regarded as evidence of the safe behavior of the vehicle without any clear explanation of how many miles are enough to gain a certain level of confidence in the safety claim. For instance, if we assume there are 100 surprises in total, each arriving in every 100 million miles, then to prove that the systems have encountered all the surprises and has been corrected to handle each of those surprises, it has to be tested on at least one or two billion miles. This is nearly unattainable. Therefore, many researchers are now focusing on designing frameworks to plan to test wisely while limiting expensive on-road testing. We

discuss more on the testing and statistical evidences of AI systems safety in Section 3.3.

3. Related Surveys and our position

Since safety concerns of AI systems have gained attention in the last few years, many literature reviews, technical reports, and surveys have consolidated the relevant state-of-the-art approaches. We collected the related surveys while searching for the primary studies.

1. Based on the search strings (discussed in detail in the next section), we first collected the secondary studies (literature surveys, questionnaires, reports, summary, case studies, etc.). We found more than 40 such studies that matched with the relevant search keywords.

2. We selected only 14 studies based on their relevance to safety, perspective, and coverage. The selection criteria were as follow:

(i) The study is published between 2015-2020.

(ii) The study is peer-reviewed and written in English.

(iii) The study is focused on the safety aspects of AI, ML, intelligent software engineering, safety-critical systems (that use ML heavily).

The studies that review the application of various ML techniques to automate software engineering or other domain (without covering the safety aspect) have been excluded. We have deliberately included three recent studies on the integration of the software engineering process and ML life-cycle as part of our related work (despite violating the third criteria) [22, 23, 24, 25]. These studies do not solely focus on the safety aspects of intelligent software. However, we include them as these studies solidify our view of performing a literature survey on safety approaches from a software engineering perspective.

We can generally categorize the selected secondary studies as– domain-based (concerning a particular domain such as automobile, robotics, etc.), AI algorithm/ ML techniques-based (focusing on a particular type of algorithm or ML technique like deep learning, reinforcement learning), general AI systems-

based(surveying a vast range of safety-related research efforts applicable to all AI systems in general), and engineering process-based (surveys the safety approaches from a systematic engineering process point-of-view that considers collective contributions from diverse stakeholders at each phase).

There are a few domain-specific surveys [26, 27, 28, 29, 30] in the field of safety-critical systems such as driverless cars and robotics, that cover a vast range of engineering aspects such as design, control, architecture, etc. However, it is either difficult to understand the safety concerns of AI algorithms or ML techniques used in these systems [26, 27, 28] or it is difficult to generalize the safety concerns for all safety-critical domains [29, 30].Numerous reviews have been published on the robustness of ML techniques [31, 32, 33, 34] and assurance of ML-based systems [35, 36, 37, 38]. The target readers of those surveys are expected to have deep technical knowledge in ML/AI algorithms to comprehend such studies as they entail many minute technical details. There are also a few technical reports, research agendas published by Stanford AI research groups [39, 40]. These reports cover a broad range of topics related to AI safety, security, privacy, fairness, trust, etc. While these studies provide an overview of the scope of research contributions in the field of safe AI, analyzing the current research efforts from an engineering process perspective is not in the scope of those studies.

Our paper differs from the other three types of surveys mentioned above in various ways. The objective of this paper is not to discuss the detailed technicality of state-of-the-art safety approaches. Rather our goal is to explore how research efforts fit from a layered systems engineering perspective. Recently, few researchers and practitioners have conducted literature reviews, questionnaires, surveys to understand the challenges of engineering ML-based software [22, 23, 24, 25]. Wan et al. and Ishikawa et al. have conducted questionnaire surveys including experienced ML-based software engineers to summarize the software engineering challenges and corresponding sources of difficulties faced during the development and validation of such software [22, 25]. Serban et al. have conducted a survey including ML practitioners to analyze how software en-

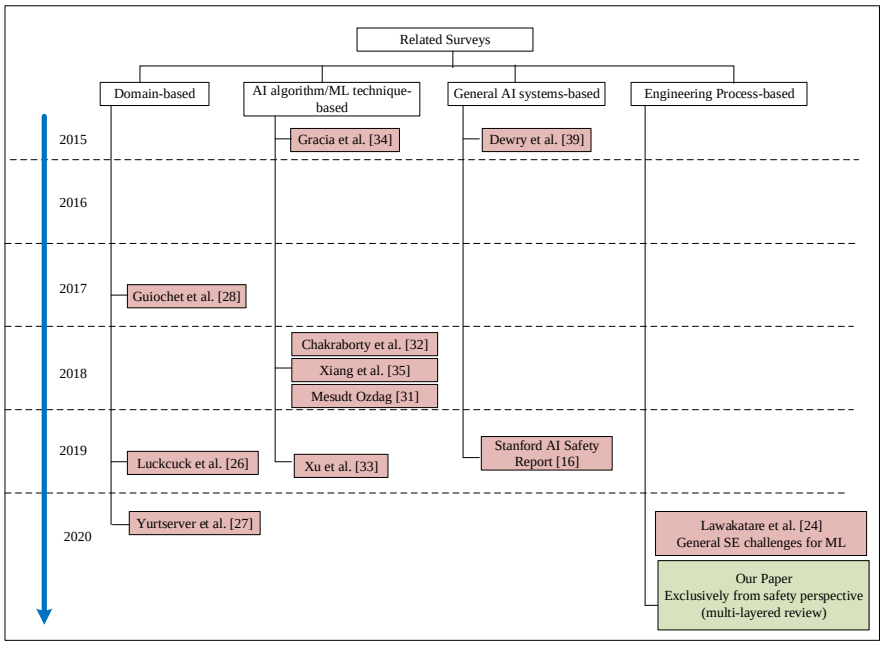

Figure 1: Related surveys and out position

gineering best practices are being used by the ML teams and how effective those practices are in the case of ML-based systems [23]. Silverio et al. have discussed challenges of trustworthy AI-based autonomous systems in industrial settings and also have provided future directions on reducing the gap between the development and operation of such systems [41]. Lwakatare et al. have summarized 23 software challenges and 8 solutions related to the large-scale ML systems after conducting a literature survey [24]. In quite a similar direction, Anh and Pekka have discussed the challenges and have provided a research agenda on continuous experimentation of AI software in large-scale systems [42]. Few of the challenges discussed in our survey overlap with their findings. However, their studies do not focus on safety. Instead that study focus on the quality attributes of software in general.

To the best of our knowledge, no survey has been done yet to analyze the relevant research areas through the lens for diverse stakeholders and their con-

tribution to the engineering process from a safety perspective. Our paper aims to find the scope of collaboration to fill the gaps in the continuity of the recent research efforts when analyzed from a multidisciplinary engineering process perspective. Fig. 1 summarizes the relevant literature surveys and our position.

4. Research Method

4.1. Research questions

We have already explained the research questions in Section 1. RQ1 is slightly different than the rest of the questions as we try to answer RQ1 based on the overall view of how a complex AI system is conceived, designed, developed, verified, and maintained. We envision a three-layered conceptual framework that facilitates further analysis of the recent research efforts along the layers. We describe our vision in detail in Section 5 and explore the state-of-the-art safety approaches based on our conceptualization of the problem space and solution space regarding safe AI.

4.2. Search strings used

We conducted the search on 29-Oct-2020 with the search strings to retrieve the recent studies as mentioned in Table 1. We initially attempted to search based on the title and abstract. However, we were overwhelmed by more than 10,000 spurious search results for most of the queries. Therefore, we decided to limit our initial search on the titles and follow snowballing method afterward to retrieve other relevant studies that were missed out by the search operation. The search results were filtered by the range of publication years from 2005 to 2020. In case of Springer, the search results were further filtered by discipline and sub-discipline.

4.3. Search Strategies and data sources

We conducted the search in two phases. In Phase-1, we directly searched databases like IEEE xplore, ScienceDirect, Springer-link, ACM Library, Scopus

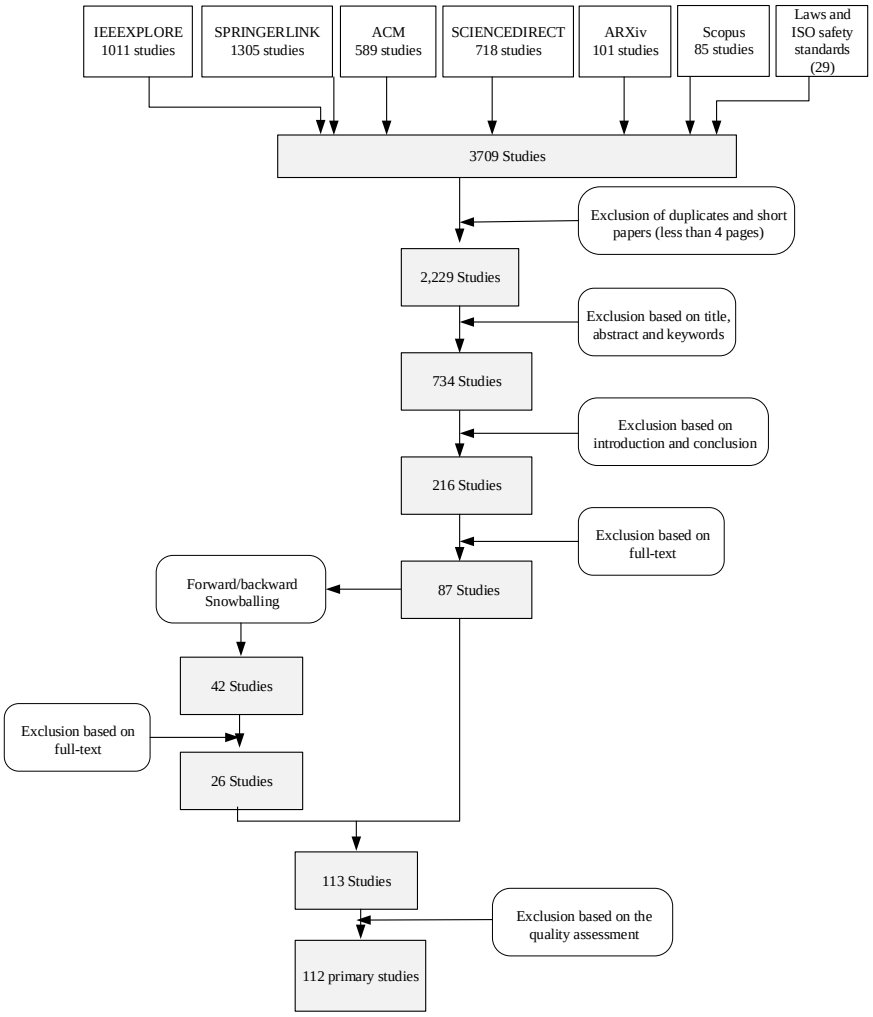

Figure 2: Study selection process

and arXiv. We collected research papers published within the 15-year time period between 2005 and 2020. After getting a moderate number of search results from these data sources, we followed the forward and backward snowballing approach [43] to find new relevant papers (from the references and the citation lists) in Phase-2.

4.4. Study Selection Process

In Phase-1, we initially found more than 3000 papers directly by performing database search. However, not all of those studies were relevant to our literature review. Our main aim was to collect studies focusing on the intersection of safety engineering, artificial intelligence, and software engineering. Therefore, for example, studies focusing only on safety engineering without considering autonomy, AI techniques, or SE process were excluded from the collection. The detailed inclusion and exclusion criteria are described in Table 2. In Phase-1, we removed duplicates and excluded irrelevant papers after reading the title, abstract, and in some cases introduction. In Phase-2, we read the full-text to thoroughly understand the motivation and contribution of each work. Finally, we selected only 112 papers that we agreed were relevant and significant for our study (Fig. 2).

4.5. Study quality assessment

We assessed the quality of the selected studies based on a set of six questions. A complete list of the questions is provided in Table 3. Most of the questions can have three answers: Yes (Y)=1, No (N)=0, Partial (p)=0.5 except for Q3, Q4 and Q6. Q3 can only have two answers Y=1 for general and N=0 for a domain-specific solution. Similarly, Q4 has two answers Y=1 for contribution to research and N=0 for contribution to practice. In general, the papers that scored above 4 out of 7, were selected. Each of the selected papers was thoroughly assessed by each of the authors individually and any disagreement was discussed till a consensus was reached.

Table 1: Search strings used to retrieve relevant primary studies

Objective	**Search String**
To retrieve studies on Artificial Intelligence and safety or trust or reliability or assurance-related concerns and corresponding solutions	"artificial intelligence" AND (safe OR trust OR reliab OR assurance)
To retrieve studies on safety, reliability, risks or robustness or assurance-related concerns of machine learning or deep learning and corresponding solutions	("machine learning" OR "deep learning") AND (safe OR robust OR risk OR reliab OR assurance)
To retrieve studies on automotive industries or any autonomous/unmanned safety-critical systems and safety-related issues.	(auto OR unmanned OR safety-critical) AND (safe OR verification)
To retrieve studies on machine learning (especially neural networks)-based systems verification or testing	("machine learning" OR "neural networks" OR "deep learning") AND (verif OR testing)
To retrieve studies that focus on the correlation between software engineering, requirements engineering, and machine learning.	("software engineering" OR "requirements")AND "machine learning"

Table 2: Overview of the inclusion and exclusion criteria

Inclusion Criteria	**Exclusion Criteria**
1. Primary studies or safety standards. 2. Studies published in the English language. 3. Peer-reviewed studies except for the studies published on Arxiv. 4. If the study is published on Arxiv then it should have at least one citation by a peer-reviewed paper. 5. Studies that focus on AI, ML intelligent Software Engineering and corresponding safety-related issues. 6. Studies published between 2005 and 2020.	1. Secondary studies. 2. Duplicate studies. (only longer and more complete versions were accepted.) 3. Studies that only focus on safety-related research (safety lifecycle, safety artifacts, etc,) without consideration of the recent advancement of AI. 4. Short studies (less than 4 pages).

Table 3: Quality assessment criteria

QA Scenario Component	**Security Requirements Components**
Are the motivation and goal of the study well explained in the paper?	Y=1, N=0, p=0.5
Is the proposed approach adequately explained with necessary details?	Y=1, N=0, p=0.5
Is the study applicable to all domains or to a specific domain?	Y=1, N=0
Does the study provide value for research or practice?	Y=1, N=0
Is there any discussion about the results or threats to validity?	Y=1, N=0, p=0.5
Does the study has a section on related work?	Y=1, N=0
Does the study provide future direction or open scope for further research or investigation?	Y=1, N=0, p=0.5

Except for one paper that was published in IEEE software magazine, all other papers qualified to be part of our study. The reason we excluded that 4 page long paper on "Software engineering for machine learning applications" was it lacked detailed explanation of the solution and discussion on the limitation as it was only a theme issue. We made another exception regarding the quality assessment in case of safety standards. Most of the articles discussing standards are from web-based search or part of technical reports, etc. These articles did not go through the rigorous quality assessment process as per the criteria mentioned in Table 3. Instead, they have been selected based on their timeliness and relevance to our study.

5. Three-layered conceptual framework for safety-driven AI system engineering

As appropriately argued by Koopman, many different areas require coordination to ensure safety [44]. Acknowledging the fact that there is a cognition gap among the various disciplines involved in the process of risk analysis, we need to provide a set of guidelines to the diverse stakeholders. To formalize the participation and responsibility of each stakeholder, we propose a three-layered framework to conceptualize complex intelligent systems (Fig. 3). The framework shows how a safe output space is achieved for such systems starting from an initial incomplete problem space. We can visualize how diverse the stakeholders and the primary artifacts are, in each layer at a system level and ML-based component level. In the days of AI, at the ML-based component level, the stakeholders come from AI or ML specific background. This was not very common in the case of traditional systems without any machine intelligence. These paradigm shifts bring in a lot of challenges in exploring the problem space and solution space. The layers of the framework are listed below:

- **Problem definition layer:**

  In this layer, at a system level, domain experts and requirements engineers work closely with users to gather requirements. The aim of these participants is to understand the expectations of the users and the society, goals of the system, possible situations/scenarios, etc. With the introduction of ML-based components, conceiving a rich problem space has become more complex than in traditional systems. ML experts, data scientists, HCI experts need to work closely with system-level stakeholders to understand the ML model requirements, data requirements, domain definitions, quantitative targets, etc.

- **Safety-driven modeling and development layer:**

  In this layer system engineers and safety experts work in collaboration to perform system-level risk analysis, risk handling of emergent behavior of

the system. In other words, in this layer risk-minimizing safety goals, requirements, etc. are derived from system-level risks. Safety standards are followed throughout the process of designing and developing the system. At the component level, inherent risks of ML models, effects of adversarial attacks, corner cases are identified. Unlike traditional software-intensive systems, ML-based components are designed and trained based on objective functions following AI/ML specific safety standards. Safe learning decisions on the safety-aware rewards, penalty, etc. are made by the ML experts at this layer.

- **Verified safety compliance layer:**

  A system is assumed to be acceptable safe only when the involved stakeholders gain enough confidence in the emergent safe behavior. Traditionally, a system is usually verified by formal models and various types of testing. QA experts and users play a key role to come to a consensus regarding the level of safety of the system. However, safety assurance and verification have become extremely challenging with the inherent uncertainty and data dependency of ML models. Therefore, at this layer, ML experts, HCI experts, data scientists play a crucial role not only to validate training and testing data but also to evaluate overall robustness, scenario coverage, performance, etc. of the ML-based component.

All the above-mentioned layers are based on a layer of basic factors, like assumptions, level of autonomy, regulatory constraints, financial constraints, ethical constraints, data constraints, etc. This framework provides better visualization of how a safe output space of AI systems is designed across the layers starting from the initial naive problem space.

5.1. Layer-1: Challenges and research efforts

In the last few years, researchers started discussing the challenges faced by software engineers while working on ML techniques for complex AI systems [22, 45, 46, 47]. As most of the current intelligent systems are software-intensive,

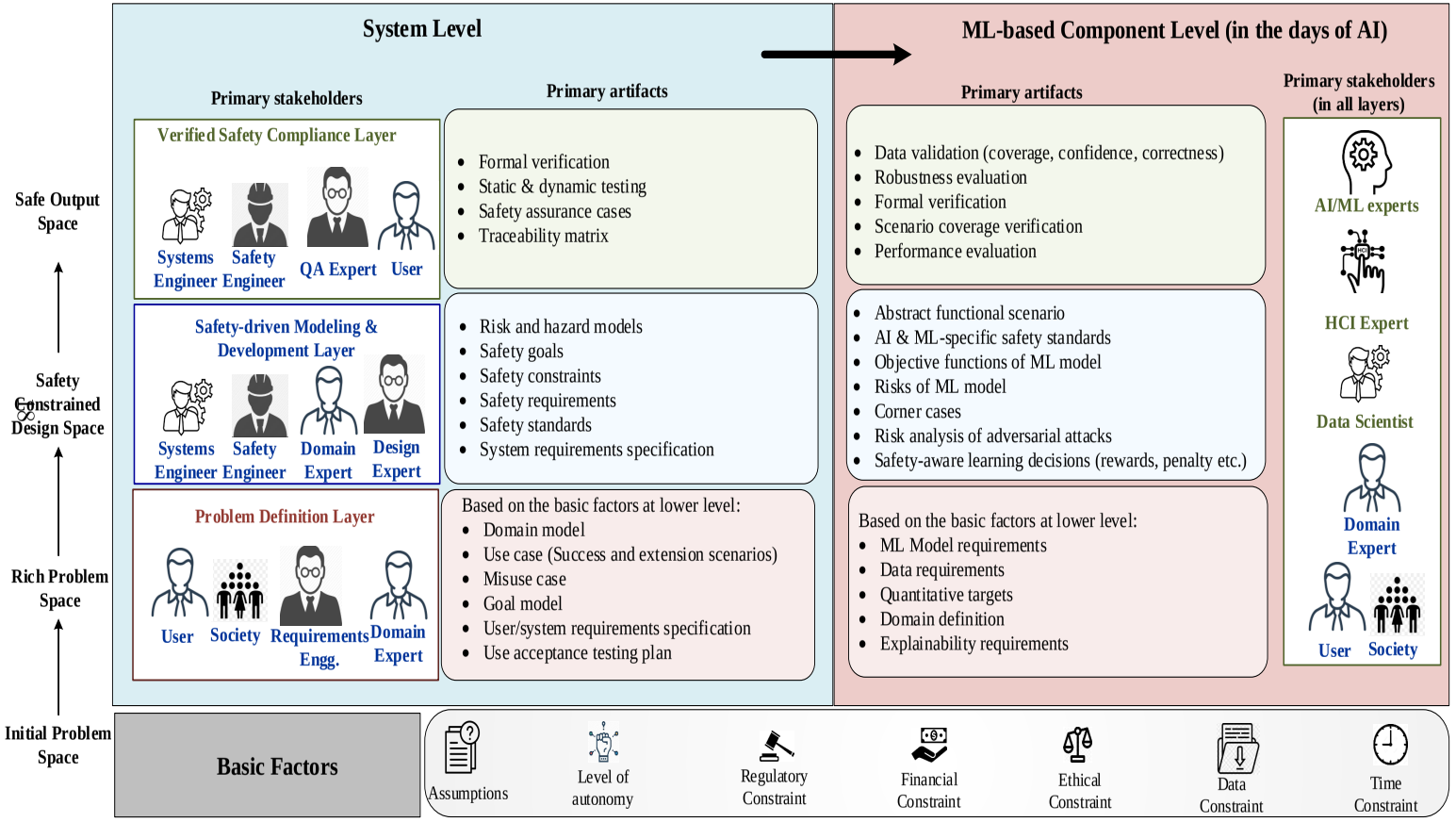

Figure 3: An integrated three-layered conceptual framework for AI systems engineering

we choose to analyze the challenges from a software engineering perspective in detail. Software research community has always asserted the importance of initiating the engineering process by having comprehensive understanding of the problem space and expectations of customers (users).We reflect the same understanding in our layered framework (Fig. 3). In order to successfully explore the safe solution space in Layer-3, the first step should be to start with exploration of the rich and relevant problem space. Therefore, in this subsection, we explain the challenges faced by requirements engineers, domain experts, and data scientists in the early phase of engineering.

(1) Shortcomings of traditional requirements engineering-driven approach:

With the advent of deep learning, the traditional end-to-end RE process became futile. It is hard to make users' expectations explicit when the operating environment itself is extremely uncertain. Stating all possible 'shall' statements in the early phase of engineering is impractical with the inherent uncertainty and lack of clarity on the relevant context. Bosch et al. discuss that requirements-driven approaches may need to be complemented by other approaches [48]. The authors identify three distinct approaches that may coexist during the development of intelligent software:

(i) RE-driven: Development according to well-understood specifications. This approach may be used only when the new feature is well understood.

(ii) Output/data-driven: Development according to a given quantitative target. The goal here is to improve the metric by experimenting with different solutions.

(iii) AI-driven: Development of components using ML/DL based on an already available large dataset.

The authors envisioned a holistic integrated development approach (DevOp) incorporating all the above-mentioned approaches in which the system consists of traditional software and AI components and also there is scope for continuous deployment. However, this integrated framework requires further validation and comprehensive guidelines for its usage. We need to further understand the

real challenges at Layer-1 by thoroughly investigating the core issues from RE perspective.

(2) Understanding the problem domain:

Problem domain understanding is equally important in the case of traditional and intelligent system engineering practices. It is always one of the most complex activities during the early phase of engineering. The complexity is even higher in systems with ML components where the system learns about the domain-specific concepts through training data [22, 49]. Rahimi et al. [50] explain this challenge using an example from an automated pedestrian collision avoidance system. The concept of 'pedestrian' is not clear in terms of what it means in a particular context. A person walking a bike (instead of riding it) or a person in a wheelchair should also be included in the semantics of pedestrians to ensure safety. The author suggested that a thorough understanding of the domain is possible by:

(i) Benchmarking the domain

(ii) Interpreting the domain dataset

(iii) Interpreting the domain learned by ML model for further validation

The authors proposed to create a domain ontology based on the web search result of the domain concept ('pedestrian' in the example). This ontology can be further used to assess whether the training data represents the problem domain as depicted in the ontology by extracting features from the dataset. Incorrect or missing correlation between ontology element and the dataset can be helpful in identification of the gap or incompleteness of the dataset.

(3) Setting quantitative targets (functional requirements):

The main objective of RE activities for any system is to state the users' expectations explicitly. However, setting explicit quantitative targets (which are often referred to as functional requirements of ML component) is a great challenge, not only because it is hard to declare desired output, but also it is difficult for users to understand ML related performance metrics such as recall, precision, etc. [51]. Data scientists need to take part in RE actively to help the client to set a metric that is not too technical, yet scientific enough to

measure the performance. For example: 'Lift' (improvements of performance) can be explained by introducing a comparison of ML predictions to random predictions. More about these topics are discussed in the upcoming sections on setting targets for validations and testing.

(4) Setting qualitative targets (non-functional requirements):

While establishing quantitative targets is already gaining the attention of the research community, a few researchers are also discussing qualities or non-functional requirements associated with the functional requirements [52, 53]. It is argued by Horkoff, in today's time we are unknowingly relying more on quality than quantity to gain trust [53]. For example: rather than relying on 99.99% of the accuracy of the target to ensure safety, more efforts need to be invested in justifying transparency, testability, explainability, reliability, fairness, etc. She also mentioned that further research needs to be conducted regarding a thorough understanding of the new definition, catalog, target, and trade-offs for NFRs for different kinds of ML algorithms used in intelligent systems. Nakamichi et al. [54] made a recent contribution by proposing a quality model, quality characteristics, and a measurement method for ML-based software systems. One of the most important qualities from the safety perspective is the robustness of the ML model, especially for perception tasks where a slight change in the input can cause misclassification. Hu et al. [55] proposed how to formally specify robustness requirements for such ML-based component by identifying the invariant and equivariant. Each robustness requirements mainly consists of three components: a formal definition of transformation over the inputs, a range of values for transformation parameters, and a corresponding indication of invariant and equivariant. However, deriving an exhaustive list of invariant and equivariant is an open area of research for ML-based components deployed in an uncertain environment.

(5) Lack of requirements analysis and modeling techniques to address uncertainty:

To analyze the intrinsic uncertainty and unpredictability of ML models, concrete analysis and modeling technique is required to be performed during RE

phase. However, not enough attention has been paid to end-to-end modeling and analysis methods. Recently, F. Ishikawa proposed a goal-based evidence-driven RE modeling to analyze the goals and unresolved uncertainty of ML models [56]. The authors explained how the model can depict the evidences captured by experiments and operation to validate or invalidate the feasibility or performance level. More efforts need to be invested in developing automated tools to link between decision making by the ML models and the collected evidences during testing and operation.

(6) Explaining 'black-box' to users:

'Safety' and 'trust' are correlated. Lack of transparency/explainability leads to weak assurance of safety and as a result users or the society as a whole lack trust in such systems. Therefore, some of the literature emphasizes the importance of the explainability of AI systems. Kohl et al. [52] report that a lack of understanding of some phenomenon motivates certain groups of stakeholders to seek explanation in a certain context. Therefore, we can consider including explainability requirements as a new addition to the non-functional requirements family. While eliciting explainability requirements, other requirements, such as security and cost, may conflict with them. This will eventually lead to exploring the rich problem space even further by performing trade-off analysis. Vogelsang and Borg mentioned that in case of ML, explainability is twofold: explain what has been learned and how each prediction has been made by the model (in the context of the predictive model) [51]. Although explainable AI systems have been garnering attention recently, the ML research community is yet to formalize situations that should demand an explanation. Moreover, further research is necessary on the appropriate level of abstraction to attain the required explainability of a system.

(7) Declaring hidden consumers:

For any system, it is of the highest priority to know the target users and consumers of the output. Complex AI systems with one or more ML components are often developed without a proper understanding of who is accessing the output (e.g., the prediction output directly or log files indirectly later) [45].

Inadequate access control strategy can have a significant impact on the overall emergent safe behavior of the systems as undeclared consumers may use the output in an unintended way [47]. Belani et al. express their concern over undeclared consumers as this hidden risk factor has not been sufficiently scrutinized [49]. We believe that identifying and documenting the right set of consumers are essential activities at Layer-1 to safeguard the system from unintended usage in the future.

Discussion:

We believe that research on RE for AI systems is at its beginning. Only a limited part of the literature has discussed the challenges faced at an early stage of AI systems engineering. Instead, research has focused on the technical excellence of AI algorithms and their applications. However, as we discuss the challenges at Layer-1 in this subsection, we summarize the current understanding of RE and SE research community for AI systems in Table 4. This table shows the latest guidelines for each of the phases of RE and specifies recent advances on new types of requirements that should be part of the requirements specification in the days of AI.

5.2. Layer-2: Challenges and research efforts

In this section, we focus on the analysis and design issues that are closely related to safety concerns. As shown in the framework, in Layer-2, safety engineers, designers, developers, ML experts are required to collaborate to explore the safety constrained design space. Therefore, we will discuss risk analysis, safety requirements, safety standards of autonomous systems.

(1) Safety-driven design of complex systems:

The preferred way to build a safe system is to consider safety from the very beginning of requirement engineering. Firesmith described a taxonomy for four kinds of safety requirements named as- pure safety requirements, safety-significant requirements, safety constraints, and requirements for safety systems [57]. However, elicitation of safety requirements was out of the scope of this work. To the best of our knowledge, the necessity of a change in the tradi-

Table 4: Summary of state-of-the-art RE approaches for safe and trustworthy AI

RE Activity	**Guidelines**
Requirements Elicitation [22, 50, 49, 54]	-Include data scientists and legal experts -Benchmark the domain -Elicit new data sources -Identify sensitive/protected features of the data -Situations that demand an explanation to help users
Requirements Analysis [53, 56]	-Discuss performance measures that are easily understandable for users -Conditions for data pre-processing, cleaning, etc. -Required level of automation needed in the process to meet the constraint -Evidence-driven goal-based requirements modeling and analysis (Insufficient attention is paid to requirements analysis activities)
Requirements Specification [50, 52, 53, 51, 54, 55]	-Data requirements -ML model requirements -ML process requirements -Quantitative targets -Measurable qualitative targets -Explainability requirements -Ethical and legal requirements -Robustness requirements
Requirements V & V [50, 55]	-Confidence in data -Data dependencies -ML process requirements -Quantitative targets -Robustness targets (Not enough work is done on requirements validation)
Requirements Evolution [22, 46]	-Documenting dataset and model versions -Data dependencies -Requirement-data-feature-output traceability (Insufficient attention is paid to requirements evolution)

tional accident model due to the emergence of software was first identified by Leveson [58]. The authors explained how the traditional accident model could be enhanced by accommodating social, cultural, and organizational aspects. A complete hazard analysis methodology named STAMP (System Theoretic Accident Model and Process) was proposed by researchers in [59] and [60], in which accidents were viewed as control flaws (failure in the interactions among the components) instead of a component failure. This methodology not only helped to analyze the source of hazards and deriving safety constraints but also helped to make appropriate design decisions to enforce the derived constraints. This safety-driven design approach STPA (System Theoretic Process Analysis) is explained in [61] with the help of a case study on spacecraft. Although this work encompassed the socio-technical factors influencing the design of a safe system, it precludes the hazards caused by human error. Moreover, this work does not exclusively address the inherent uncertainty and opacity of ML-based software-intensive systems. Therefore, we will not probe this research further.

Kuper et al. introduced the concept of verification-friendly design of neural networks [62]. Varshney explained how four common safety strategies (inherenetly safe design, safety reserves, safe fail, and procedural safeguards) can be mapped to an ML context [20]. The authors emphasized that ML models are very different in terms of the inherent uncertainty in train and test data, and their probability distribution. Rejecting a less confident decision made by the mode can be an option to fail safely. However, it is important to define the decision boundary carefully as the distance from the boundary is not always inversely proportional to confidence. A part of the input space with low density can contain much epistemic uncertainty as the boundary may be based on inductive bias. In the same direction, Gu and Easwaran proposed Feature Space Partitioning Tree (FSPT) to partition feature space and to reject input instances from the low-density feature space [63]. In the case of reinforcement learning, safe outcome has been confirmed by introducing risk-aware policies and rewards [64], safety-aware planner [65], safety supervisor [66], etc. Although these contributions were very significant in terms of ensuring safety at the ML component

level, they lack insight into how the safety standard can be defined and mapped against system or sub-system level safety goals.

(2) Lack of method to model uncertain environment including human behavior:

For safety-critical AI systems, combinations of numerous variables lead to an unlimited number of situations to model, which results in an impractical verification process. The complexity amplifies when human is in the loop. Human's behavior is mostly variable and uncertain. Therefore, for semi-autonomous systems, the problem of environment modeling is two-fold. Research on verification of AI systems can get momentum only if there is a well-understood technique to model the uncertain environment. As complete formal modeling of the uncertain environment seems to be challenging by many researchers, attention is paid towards introspective modeling of the environment. For example: identifying and analyzing the assumptions that a system makes about its environment can be helpful to verify whether the system is capable of monitoring the right variables or not. Seshia et al. have addressed such issues with the help of control theory. Extraction of monitorable assumptions is proved to be feasible for simple controllers [67, 68, 69]. To address the issues of modeling unpredictable human behavior, one way could be gathering data about real and simulated environments to learn about the environment model. Some researchers have shown it to be effective for verification and control of an autonomous vehicle to generate human behavior models from driving simulators and human subject experiments [70, 71, 72].

(3) Scenario-based safe design and development of autonomous systems:

For safety-critical systems like driverless cars, deployed in an uncertain environment, collecting sufficient safety requirements is an exhaustive task. The risks and potential hazards are mainly hidden in the operational world and its numerous variations. Therefore, very recently, researchers started focusing on purposefully varying the operation scenarios of systems to elicit safety requirements in the early phase of the system life-cycle. Bach et al. [73] presented a

methodology for a model-based design of scenarios from real-world test data. Abstraction of temporal and spatial information act as the key enables of not only coherent modeling of scenario but also support specification of requirements and derivation of test cases. In a similar direction, Till et al. [74], proposed three levels of abstraction for scenarios along the V-model of development process following ISO-26262 (this standard will be discussed later). These researchers elaborated the concept of 'Scenario' and defined three layers of abstractions of scenarios:

(i) Abstract functional scenario in concept phase: Involves identifying semi-formal hazardous scenarios including operational scenarios and malfunctioning behavior.

(ii) Detailed logical (technical) safety scenarios in development phase: Involves describing scenarios including parameter ranges of the state values that are used to represent functional scenarios.

(iii) Concrete scenarios for validation and verification: These scenarios represent the operational scenarios with concrete values of each parameter. Proposed process steps of the usage of such safety concerned scenarios can be very helpful to generate the artifacts at each step and to maintain traceability among them.

(4) Safety standard to guide for analysis and design process:

Standards are believed to be one of the best ways to guide and assess (in later phases) the development of a particular system through specification. Especially for AI systems, standards can provide explicit specification/requirements for explainability, robustness, fail-safe design [75]. ISO and IEEE are the two leading bodies that have been developing various standards regarding safety requirements of autonomous machinery. Table 5 summarizes some of the relevant standards in this area. However, none of them exclusively considers AI. The use of ML commences an overall paradigm shift in the design and development process. Unfortunately, these standards fail to ML-specific concerns. Nevertheless, some of the safety considerations to ensure safety are rightly identified by Google [76].

1. Is the objective function appropriate?

2. Has the exploration space been sufficiently constrained?

3. Does the model's training reflect the current real world?

4. Can the risk of data poisoning be mitigated?

5. Has the AI system been adversarially tested?

Best practices to address these concerns should be collected in formal standards. The formulation of safety standards entails risk analysis, risk control, and risk monitoring [77]. These standards are mostly under development. Formalizing AI safety standards is an ongoing endeavor. Many researchers are working on the same from different perspectives. For example, Ozlati and Yampolsky mention the diversity of AI systems in [77] and considered that different categories of AI systems may have diverse risks and mitigation strategies. Therefore the authors suggested using a modified Delphi methodology study as a starting point of a standing body that can develop and evaluate AI safety standards under AI SDO. Keeping the diversity of AI systems in mind, the authors recommended that the modified Delphi study should cover separate risk assessments for different system categories. Luo et al. focused on environment-centric safety requirements of automated unmanned systems [78]. Environment safety requirements are elicited from the entities of the environment- other systems, human, constraints. The authors classify such requirements along MAPE-K process. After conducting a literature survey, the authors conclude that few gray areas need further research, such as methodology to solve safety concerns (collision avoidance), optimizing safety constrained learning technique (MDP), etc. Most discussed domain-specific standards in the days of AI: Recently, the automotive industry has made significant progress in developing and testing driverless cars. However, as of today, neither the industry nor the government can fully assess the safety of self-driving cars. Therefore, there is a sudden rush to set standards for such AI-based autonomous vehicles among the public organization like IEEE and also public sectors like Safety First for Automated Driving (SaFAD) led by Audi, BMW, etc. In this subsection, we will explain some of the standards related to an autonomous vehicle in detail.

ISO 26262. ISO 26262 is the derivative of IEC 61508 [79, 19]. It mainly covers automotive development, production, and maintenance of safety-critical systems. The key component of ISO 26262 is the automotive safety lifecycle (ASL) which describes the fundamental concepts of safety plan, safety manager, safety review and audit. ASL consists of six phases: management, development. production, operation, service and decomission. This standard also defines the automotive safety integrity level (ASIL). Based on safety analysis of the critical functions of the system, a risk analysis is performed. The risk analysis combines the probability of exposure, controllability of a driver, the severity of outcome resulting in ASIL from A to D. As per this standard, development and verification practices should correspond to the corresponding ASIL. However, as argued by Borg et al. [36], with the advent of ML algorithms (especially less transparent DNN), traditional standards fall short. Salay et al. analyzed ISO 26262 from ML perspective to identify the key factors of conflict [80]. The researchers found gaps in the software development requirements of ISO 26262, and proposed requirements to fill those gaps. One of the major contributions of their work is the elaboration on connecting data to safety concerns while working with ML algorithms. Prior knowledge of the function to be performed by ML component plays a significant role in fostering safety. The ways input can change without affecting the output are termed as invariants. Invariance to lighting level, positions, etc. is directly associated with the safe outcome of the learning model. Similarly, equivariants describe types of change in input that should result in a particular type of change in the output. Along with these two specifications, different kinds of constraints like probabilistic, pattern-based, and context-based constraints on the input and output and control the safe behavior of ML component. Moreover, analyzing data distribution, its coverage of edge-cases also enable developers and safety engineers to assess the expected safe behavior of the AI-based system. The researchers also mention that model selection, feature selection, training, and testing specification are the key artifacts in arguing the safety case of an ML algorithm.

UL-4600. Koopman et al. working with UL (Underwriters' Laboratories) proposed an initial draft of UL-4600 standard for fully autonomous vehicles [81]. To the best of our knowledge, UL-4600 is the latest and the most advanced standard that aims to address the challenges of the full autonomy of HAV. The traditional standards lack flexibility as they are usually census-based and updated every 5 to 10 years. However, in the days of AI, developers are exploring new technologies rapidly to provide a better solution to the concerned problem. Therefore, flexible standards like UL-4600 gained attention in recent times. UL-4600 does not prescribe direct guidance to the proper development process. Rather, it guides on building the safety case (which will be discussed later in the next section) for HAV [82]. A safety case is a very important artifact for safe systems design. Identified topics that are planned to be addressed in this standard are:

(i) Definition of operational design domain (e.g., weather, scenarios, etc.)

(ii) ML faults (e.g., training data gaps, etc.)

(iii) External operation faults (e.g., fault of other vehicles, etc.)

(iv) Faulty behavior of the non-driver humans (e.g., pedestrians, etc.)

(v) Non-deterministic system behavior (e.g., test planning, etc.)

(vi) High residual unknowns (e.g., requirements gaps, etc.)

(vii) Lack of human oversight (e.g., passenger handling, etc.)

(viii) System-level safety metrics.

This standard emphasizes that it is more effective to continually evaluate and improve the residual risk present in the system than to conform to a standard during deployment. Therefore, developers need to be actively involved and take responsibility for safety risk identification and self-assessment over the iterations of the development life-cycle.

Discussion: In 2020, several new standards from various sources for AI-based systems are likely to be rolled out [90, 91, 92, 93, 94, 95, 96]. We could not discuss these standards in detail as most of the standards are still under development and not many open-access documents are available regarding these standards. However, as Riccardo Mariani [97] mentioned that, with the arrival of the new

Table 5: Overview of the safety standards and the relevant autonomous systems

Safety Standards	**Autonomous Systems**
ISO/DIS 3691-4 [83]	Driverless trucks
ISO 13482 [84]	Personal Care Robots
ISO 19014 [85]	Earth moving machinery
ISO17757 [86]	Earth moving machinery and mining
ISO 18497 [87]	Agricultural machines
IEC 62267 [88]	Automated urban guided transport
ISO 26262 [19]	Road Vehicles
ISO/PAS 21448 [89]	Road Vehicles

safety standards from various sources, it is expected that those standards will be written from diverse perspectives of AI-based systems. Therefore, the main goal should be to analyze those standards and minimize the overlap.

5.3. Layer-3: Challenges and research efforts

As rightly argued by J. Morton et al., Trust is the prime concern that needs to be established before a complete release [98]. Many researchers focused on validation and verification of the system life cycle to prove that the system is acceptably safe enough to be deployed. In this subsection, we will explain the challenges to perform end-to-end validation and verification of AI systems. Seshia et al. explained the shortcomings of the current practices and proposed to move towards the paradigm of Verified Artificial Intelligence [99]. Further, we discuss the directions that researchers have been following recently to address those challenges.

(1) Lack of formal specification to verify the system:

Traditional formal verification is mostly founded upon strong mathematical statements of the way system should behave. However, for ML-based sys-

tems, it is extremely difficult to describe the expected behavior precisely in a mathematical way. For instance: there is no concrete method for a module of an autonomous car that uses computer vision to perform object recognition, human-object classification. As it seems to be nearly impossible to formally specify the exact behavior of any ML component, few researchers have tried to solve the problem from a different perspective. Instead of formalizing the component level behavior, end-to-end system-level behavior specification can be used for verification purposes. Seshia et al. suggested that specification mining techniques can be used in such cases [100]. Jan Leike et al presented a suite of reinforcement learning environment to assess the conformity with the intended safe behavior [101]. The authors also classified various safety problems in the case of RL. For example, specification problems, safe interruptability, reward gaming, safe exploration, etc. However, the cost of verification and validation of such components is not trivial. Especially for domains like automotive systems, aircraft systems, verification approach is not scalable for the real world unless they are designed that way. However, more research is required to ensure that the intention of the designer is rightly articulated into the ML component through well-designed cost and reward functions.

(2) Lack of system modeling approaches for data-driven ML components:

Formally modeling complex deep neural networks with millions of data, several layers, stochastic behavior, and hundreds of features to learn poses a challenge. To model such ML-based components, an explanation based on generalization and abstraction is needed and both input and probabilistic (uncertain) output need to be formally modeled and explained. Furthermore, such uncertain output and its corresponding effect on the system-level specification needs to be formally modeled. More significant research on formalism of Markov Decision Process [102], probabilistic logics [103, 71], and counterfactual reasoning can lead to the mitigation of the problem of systematic modeling of data-driven ML component.

(3) Insufficient method for quantitative verification:

Apart from formal specification and modeling of ML components, training and testing data play a very important role in verification of the ML algorithm or component. The behavior of a frozen learning model (with no continuous learning strategy) may vary with a small perturbation of the test data, These adversarial perturbations pose a new challenge to verifying ML-based component and using them as a part of safety-critical systems such as autonomous cars [104, 105, 106, 107]. Moreover, the traditional boolean outcome of the verification and validation process is inadequate for ML. Quantitative requirements (data requirements, equivariant, and invariant specification, etc.) can contribute to design a quantitative verification process. Semi-autonomous systems with both machine and human controllers can be considered as hybrid systems [108, 109, 110] and therefore can follow a probabilistic process of verification. As suggested by Seshia et al. in [99], randomized formal methods to systematically generating training and testing data can be one of the options to move towards formal verification of ML algorithms. Randomized formal methods need to be improved to address the constraints on the legal input and output space. Randomness requirements can define the output distribution. More rigorous research on constrained random sampling is expected to aid the process [111]. Additionally, SMT solving can also be extended by combining with optimization problems to handle similar issues [112, 113]. An in-depth survey verification of neural networks can be found in [35].

Recent surge in research on safe deep neural network (DNN)

Safety assurance of neural networks in particular has received much attention in the last few years. Various strategies of testing have been adopted by researchers to gain the confidence that the neural network can be safely used in safety-critical systems; for instance, white box testing [114, 115], gray box testing [116], feature-guided black box testing [117], mutation testing [118, 119], concolic testing [120], etc. Researchers have also paid attention to the testing criteria suitable to ensure safe output of a DNN-based system [121, 122]. Byun and Rayadurgam proposed a manifold-based ML testing framework [123]. The

authors argue that compared to neuron coverage manifold-based coverage is a more effective measure of assurance. In the same direction, another recent study by Harel-Canada et al. argued the unsuitability of neuron coverage as a V & V metric for neural networks [124]. The assessment showed that the increase of neuron coverage may rather hinder the way of generating an effective test suite for neural networks. Falsification approach (testing against corner cases) has also gained interest among researchers as this approach can successfully analyze the situation where a system may fail [125, 126]. In case of formal verification, numerous approaches have been adopted by the researchers. For example, input-output range specification-based verification [127, 128, 129, 130], solver-based verification [131], reachability-based verification [132, 133, 134, 135], etc.

(4) Difficult to perform rigorous run-time testing to address the uncertainty:

Morton et al. proposed a method for deriving close-loop testing strategies for safety-critical systems [98]. Koopman et al. made remarkable contributions in the field of safety validation of automated vehicles [10, 13]. The authors proposed a phase-wise testing approach that not only mitigates the risks but also identifies the assumption violations and the unexpected situation at runtime [10]. Researchers have also focused recently on safety verification of autonomus systems with neural networks-based controller at the system-level in the presence of hardware faults like lidar faults etc. [136, 137]. Although this approaches can be helpful to reduce the testing load, more thoughts need to be given towards the traceability of the testing artifacts from the system-level to the component-level.

(5) Difficult to evaluate robustness against adversarial attacks on ML-based systems (safety meets security):

In the last few years, many researchers have expressed their concerns about the potential threats to the stability of ML-based systems posed by adversarial attacks. It is difficult to predict such attacks, and it is also complicated to model the response of a component or system as a whole to such attacks. Therefore, to develop a reliable system it is imperative to not only analyze the inherent

risks of ML-techniques, but also to protect them from intentional adversarial attacks. To ensure functional integrity of modern ML-based systems safety and security related knowledge should be used in combination. Szegedy et al., Biggio et al. first paid attention to adversarial examples that can easily deceive neural networks [138, 139]. If the attacker adds a small perturbation to an image with the proper calculation, a well-trained neural network (NN) can misclassify the image with surprisingly high confidence. Such unstable behavior can lead to catastrophic consequences in case of safety-critical systems that depend heavily on computer vision to take decisions. Numerous recent works have analyzed different ways to fool deep neural networks (DNN) [105, 140, 141, 142]. Bastani et al. proposed metrics to measure robustness against such adversarial examples [143]. Very recently, Naseer et al. proposed formal methods to analyze noise tolerance, training bias, and input sensitivity of neural networks [144]. Similarly, RL agents can also be heavily manipulated by malicious attacks. Huang et al. [145] have recently shown that RL-algorithms such as DWN, TRPO, A3C can be vulnerable to malicious inputs. Even a small perturbation can lure an RL agent to move to an undesirable state and take unsafe action. White and black-box attacks have been well investigated in this work. In case of white-box attacks, the attacker is assumed to have access to the policy network. Whereas, black-box attacker have only partial or no such information. The researchers show that white-box attackers are more effective than black-box attackers. It is possible to confuse an RL agent with trained policy even in real-world black-box scenario. For instance, lane following policy of an autonomous car can be deliberately altered by placing a small mark on the road surface or road signs.

Defenses against adversarial attacks:

Various defense mechanisms have been proposed to ensure robustness of ML models. We briefly consider the two most discussed defense mechanisms.

(i) Adversarial training:

This is a brute force process of generating as many adversarial examples as possible and using them to train the model in advance. Since Szegedy et al. [138] showed the existence of adversarial examples to fool DNNs, many

researchers focused on ensuring robustness of learning models from such adversarial attacks [140, 146, 147]. As discussed by Hazan et al., dealing with adversarial perturbation can eventually help to optimise a ML model in a more robust way [148]. One of the major challenges faced in training DNNs with adversarial examples is synthesizing a sizable number of adversarial examples. Various ways have been proposed to synthesize such examples in whitebox settings [106, 107, 138, 140, 149, 150]. Another challenge is to generate physical-world adversarial examples (2D photos, adversarial patches, 3D prints, etc.). These physical or real-world adversarial examples have been demonstrated for various domains such as face recognition, image classification, speech-to-text, etc. [151, 152, 153].

(ii) Defensive distillation:

In this defense mechanism, a model is trained to provide outputs in terms of probability instead of hard labels. The distillation process reduces the gradients used to create the adversarial example. As a result, this defensive mechanism of a DNN can reduce the effectiveness of adversarial sample from 95% to less than 0.5%. Detailed analysis of the state-of-the-art defensive measures can be found in recent surveys on robust deep learning [31, 32, 33].

(7) Inadequate practice of demonstrating assurance cases for ML-based system:

Despite ML showing promising improvements in performance due to its introduction in many complex systems, it will always lack confidence of the users and society unless a proper assurance case is provided. However, unfortunately, there is currently no formal practice of producing end-to-end safety assurance cases. Palin et al. [154] proposed patterns for designing safety cases covering all aspects of ISO 26262 for the automotive domain. However, these proposed reusable safety arguments did not consider the complexities that ML techniques bring. A fault-free system can still behave in an unintended way due to the intrinsic uncertainty of ML techniques. Therefore Gauerhof et al. proposed a safety assurance case for a pedestrian detection function using Graphical Structuring Notation (GSN) [155]. In this approach, the risks of under-specification

(unclear tasks and environments), deductive gap (incorrect learning of features from insufficient data), and semantic gap (unclear domain concepts) have been reduced by defining corresponding arguments and evidences. This type of well-structured validation targets helps gain confidence. Matsuno et al. [156] explained how the inherent uncertainty of ML models affects the strategy and activities for safety assurance. According to these researchers, continuous argument engineering is useful in such cases to determine the weakness of a model, which can never be pre-calculated. They also developed tool support to assess and track the latest state of assurance. A similar idea was previously proposed by Denney et al. [157] and it was applied to the aviation system domain. The authors showed how safety management system needs to manage the safety cases not only during the development and deployment period but also at run-time based on real-time operational data. However, this approach did not explicitly handle the risks and uncertainty of ML models. Recently, patterns for arguments safety assurance of ML in the medical diagnosis system have been proposed as well [158, 159]. In these approaches, the researchers provided a detailed structure of assurance cases using GSN while considering medical settings and ML activities. These patterns can be widely used in other safety-critical domains, given sufficient settings or context-specific information about the domain.

Discussion. Despite putting rigorous efforts on V & V of ML-based systems, as argued by Brundage et al., not having a formal consensus on metric to measure general property like safety of these systems, there will be always a tension between the verifiability claims and the generality of such claims [160].

6. Discussion of research questions

In this section, we revisit our research questions to finally map the primary studies to answer the research questions from an engineering process perspective. Although in the previous section, we discussed the challenges and research efforts along each layer, we are going to summarize our findings from the literature review in this section. For the ease of understanding and to have a better

traceability, we first make a list of the primary studies and assign a unique ID to each of them as shown in Table 6. In this table, we also summarize the perspective, domain, objective and specific ML techniques that each of the studies focuses on. In case of a paper written for (or tested on) a specific domain, we specify the name of the domain. Otherwise, we mention it as "General". Similarly, we mention NS (non-specific), if the study is not exclusively designed for any particular ML technique. DNN, RL, NN stand for Deep Neural Networks, Reinforcement Learning, and Neural Networks respectively.

6.1. RQ1: How can we easily comprehend the complexity and challenges involved in fostering safety of complex intelligent systems?

To visualize the complexity and challenges faced by multiple stakeholders involved in the process of engineering safe AI systems, we analyzed the primary studies based on the proposed three-layered framework depicted in Fig. 3. In Table 7, we map the primary studies to each layer of the three-layered framework. Compared to the other two layers, the Problem Definition Layer has received less attention. As this layer involves activities like analyzing the problem to be solved, understanding the domain, setting the right targets, it is imperative to focus more on this layer to avoid late realization of setting incorrect targets and objectives. As the table shows, many researchers are focusing on the validation and verification-related challenges in the third layer. While we acknowledge the absolute necessity of formal verification of ML-based systems to gain trust, we also believe having a clear idea about "what to verify", "against which metrics to verify", "what are the qualitative and quantitative targets" is equally important to verify and validate a system in the right way. In layer-2, more work needs to be done on modeling uncertain environment from a software engineering perspective. Most of the standards included in the review need to be updated to accommodate the new challenges that are brought in by the advent of ML algorithms.

In a nutshell, with the help of the three-layered framework, we can easily observe that a lot of areas are still open for research to strengthen a strong

Table 6: List of the primary studies

ID	References	Perspective	Domain	ML-technique	Objective
P001	Ishikawa Nobukaju [22]	Software engineer	General	NS	Understanding engineering process-related challenges
P002	Arpteg et al. [45]	Software engineer	General	Deep learning	Understanding engineering process-related challenges
P003	Amershi et al. [46]	Software engineer	General	NS	Understanding engineering process-related challenges
P004	Rahimi et al. [50]	Software Engineer, Domain expert, Requirements engineer	General	NS	Specifying concepts in safety-critical domain to reduce conceptual uncertainty in ML-based components
P005	Kohl et al. [52]	Software Engineer, Domain expert, Requirements engineer	General	NS	Unifying the notion of explainability in case of ML-basesd systems
P006	Sculley et al. [47]	Software engineer, system engineer	General	NS	Exploring ML-specifc risk factors for maintainable ML-based systems from engineering perspective
P007	Bosch et al. [48]	Software engineer, AI expert,Requirements engineer, Data scientist, system eng	General	NS	Discussing holistic approach of software development in the days of AI
P008	Horkoff [53]	Software Engineer, Requirements Engineer	General	NS	Setting qualitative targets for ML-based systems
P009	Vogelsang et al. [51]	Data scientist, Requirements Engineer	General	NS	Understanding RE challenges for ML
P010	Belani et al. [49]	AI expert, requirements engineer, system engineer	General	NS	Defining RE taxonomy for AI
P011	Ishikawa et al. [56]	AI expert, requirements engineer, system engineer	General	NS	Discussing goal-based requirments engineering methods to address intrinsic uncertainty of ML
P012	Nakamichi et al. [54]	AI expert, requirements engineer, system engineer	General	NS	Defining quality model, quality characterics and measurements for ML-based systems
P013	Hu et al. [55]	Software Engineer, Domain expert, Requirements engineer	General	NS	Specifying and testing robustness requirements of ML-based componenets
P014	Cihon Peter [75]	Governance	General	NS	To reframe itnernational standards as tools of AI policy.
P015	Google [76]	Governance	General	NS	Discussing concrete issues on AI governance

ID	References	Perspective	Domain	ML-technique	Objective
P016	Ozlati Shabnam and Roman Yampolskiy. [77]	System engineer, AI expert	General	NS	Adopting formal risk assessment practices for safe AI development
P017	Luo et al. [78]	System engineer, safety engineer	Unmanned automated systems	NS	Setting up a taxonomy of environment-centric safety requirements for automated unmanned system
P018	ISO 3691-4:2020[83]	NA	Driverless industrial truck	NS	Specifying safety requirements and verification for driverless industrial trucks
P019	ISO 13482:2014 [84]	NA	Robots and robotic devices	NS	Specifying safety requirements for personal care robots
P020	ISO 19014-1:2018 [85]	NA	Earth-moving machinery	NS	Methodology to determine safety-related parts of the control system and performance requirements
P021	ISO 17757:2017 [86]	NA	Earth-moving machinery and mining	NS	Autonomous and semi-autonomous machine system safety
P022	ISO 18497:2018 [87]	NA	Highly automated agricultural machines	NS	Defining principles for design for safety of highly automated agricultural machines
P023	IEC 62267:2009 [88]	NA	Railway applications	NS	Defining safety requirements for automated urban guided transport (AUGT)
P024	ISO/PAS 21448:2019 [89]	NA	Road vehicles	NS	Guiding on confirming safety of the intended functionality
P025	Koopman et al. [81]	System engineer, safety engineer	Fully autonomous vehicle	NS	Setting a scope requirement for safety assurance case
P026	ISO/IEC PAS 21448:2019 [90]	AI experts	General	NS	Artificial intelligence — Concepts and terminology
P027	ISO/IEC CD 23053 [91]	AI experts	General	NS	Framework for AI systems using ML
P028	ISO/IEC AWI 23894 [92]	AI experts	General	NS	Guidelines on risk management of AI
P029	ISO/IEC AWI TR 24027 [93]	AI experts	General	NS	Guidelines to reduce bias in AI systems and AI aided decision making
P030	ISO/IEC AWI TR 24027 [94]	AI experts	General	NS	Providing an overview of trustworthiness in artificial intelligence

ID	References	Perspective	Domain	ML-technique	Objective
P031	ISO/IEC CD TR 24029-1[95]	AI experts	General	Neural Network	Poviding guidelines on the assessment of the robustness of neural networks
P032	ISO/IEC CD TR 24029-1[96]	AI experts	General	NS	Governance implications of the use of artificial intelligence by organizations
P033	ISO AWI 38507[19]	System engineer, safety engineer	Road vehicles	NS	Provides vocabulary on road vehicle safety
P034	Salay et al. [80]	ML expert, safety engineer, system engineer	General	NS	Discussing the impact of ML on the guidelines of ISO 26262.
P035	UL 4600 [82]	System engineer, safety engineer, ML expert	Autonomous car	NS	Describing a safety case approach to ensuring autonomous product safety
P036	Owens et al. [61]	System engineer	Outer planet exploratory system	NS	Describing integrated safety-driven design methodology
P037	Bach et al. [73]	System engineer, safety engineer	Autonomous car	NS	Specifying model-based scnearios to develop and test autonomous cars.
P038	Menzel et al. [74]	System engineer, safety engineer	Automated vehicles	NS	
P039	Gu, Xiaozhe, and Arvind Easwaran [63]	ML experts	General	NS	Identifying training space and avoiding exploiting beyond that to ensure safety
P040	Chow et al. [64]	ML experts	General	RL	Presenting efficient reinforcement learning algorithms for risk-constrained Markov decision processes
P041	Chen et al. [66]	ML experts	Autonomous car	RL	Incorporating human decision-making model in RL to control AVs for safe operations.
P042	Rong, Jikun, and Nan Luan [65]	ML experts	Autonomous car	RL	Planning with safe policies for RL-based autonomous driving.
P043	K. R. Varshney [20]	ML experts	General	NS	Defining the concept of safety, risk factors and safety strategies in case of ML.
P044	Kuper et al. [62]	ML expert	General	DNN	Verification of DNN.
P045	Lee et al. [114]	ML expert	General	DNN	Verification of DNN.

ID	References	Perspective	Domain	ML-technique	Objective
P046	Naseer et al. [144]	ML expert	General	DNN	Verficiation of DNN.
P047	Sun et al. [131]	ML expert	General	DNN	Verficiation of DNN.
P048	Harel et al. [124]	ML expert	General	DNN	Discussing the right mteric for verification of DNN
P049	Byun, T., and Rayadurgam, S. [123]	ML expert	General	DNN	Proposing manifold-based test generation as a better metric for ML aussurance than neuron coverage.
P050	Fazlyab et al. [132]	ML expert	General	DNN	Verficiation and reachability analysis of DNN.
P051	Ivanov et al. [136]	ML expert, system engineer	Autonomous car	DNN	Verifying safety of DNN-based autonomous cars
P052	Hoang et al. [137]	ML expert	General	DNN	Analyzing resilience of DNN
P053	Koopman et al. [10]	System engineer	Autonomous car	NS	Designing a framework for safety validation of autonomous cars
P054	Seshia et al. [99]	ML expert	General	NS	Designing AI-based systems against verifiable requirements for better assurance.
P055	Ghosh et al. [108]	Control system engineer	Autonomous driving, aircraft controller	NS	Diagnostic and repairing specification for hybrid systems
P056	Li et al. [69]	Control system engineer	General	NS	Formalizing human-in-the-loop control systems
P057	Nilim et al. [102]	Control system engineer	General	NS	Handling robust control problem of Markov decision process.
P058	Fawzi et al. [104]	ML expert	General	NN	Analyzing robustness of classifier against adversarial perturbation
P059	Seshia et al. [100]	ML expert	General	DNN	Formally specifying DNN
P060	Sadigh, D., Kapoor, A [103]	Control system engineer	Quadrotos, autnomous vehicles	NS	Achieving safe control with probabilistic signal temporal logic.
P061	Dutta et al. [127]	ML expert	General	DNN	Analyzing output range for DNN
P062	Ehlers, R. [128]	ML expert	General	NN	Verification of NN
P063	Huang et al. [129]	ML expert	General	NN	Safety verification of NN
P064	Katz et al. [130]	ML expert	General	NN	Verification of NN
P065	Nguyen et. al [105]	ML expert	General	DNN	Analyzing adversarial attacks on DNN.

ID	References	Perspective	Domain	ML-technique	Objective
P066	Dezfooli et al. [106]	ML expert	General	DNN	Analyzing adversarial attacks on DNN.
P067	Goodfellow et al. [107]	ML expert	General	DNN	Analyzing adversarial attacks on DNN.
P068	Chakraborty et al. [111]	Control system engineer	General	NS	Formal verification of control system
P069	Yasser et al. [112]	Control system engineer	General	NS	Formal verification of control system
P070	Tuncali et al. [113]	Control system engineer	General	DNN	Reasoning about safety of a NN-based system by a simulation-based approach
P071	Pei et al. [115]	ML expert	General	NN	Testing of NN-based system
P072	Tian et al. [116]	ML expert	Autonomous car	NN	Testing of NN-based system
P073	Wicker et al. [117]	ML expert	General	NN	Testing of NN-based system
P074	Lei et al. [121]	ML expert	General	NN	Testing of NN-based system
P075	Sun et al. [122]	ML expert	General	NN	Testing of NN-based system
P076	Wang et al. [118]	ML expert	General	NN	Testing of NN-based system
P077	Ma at al. [119]	ML expert	General	NN	Testing of NN-based system
P078	Sun et al. [120]	ML expert	General	NN	Testing of NN-based system
P079	Dreossi et al. [125]	ML expert, system engineer	General	NS	Verification of system with ML-based components
P080	Tuncali et al. [126]	Control system engineer	Autonomous vehicle	NN	Testing of NN-based system
P081	Xiang, W., Johnson, T. T. [133]	Control system engineer	Control systems	NN	Tesitng and analyzinf reachability of NN controllers
P082	Ivanov et al. [134]	Control system engineer, ML expert	Control systems	NS	Safety verificaion of NN controller-based systems
P083	Akintunde et al. [135]	ML expert, system engineer	Hybrid systems	NS	Analyzing reachability of neural agent-environment systems
P084	Dennis et al. [109]	ML expert	Agent-based systems	NS	Practical verification of decision-making
P085	Rajeev Alur [110]	System engineer, ML expert	Robotics systems	NS	Formal verification of hybrid system
P086	Szegedy et al. [138]	ML expert	General	NN	Discussing properties of NN
P087	Biggio et al. [139]	ML expert	General	NS	Simulating evasion attack scenarios against ML algorithms at test time
P088	Papernot et al. [140]	ML expert	General	NN	Analyzing attacks on DNN

ID	References	Perspective	Domain	ML-technique	Objective
P089	Bastani et al. [143]	ML expert	General	NN	Measuring robustness of NN
P090	Grosse et al. [141]	ML expert	Malware classification system	NN	Analyzing attacks on DNN
P091	Gu, S., Rigazio, L. [146]	ML expert	General	NN	Designing NN architecture robust to attacks
P092	Hazan et al. [148]	ML expert	General	NN	Analyzing attacks on DNN
P093	Papernot et al. [142]	ML expert	General	NN	Analyzing attacks on DNN
P094	Huang et al. [145]	ML expert	General	NN	Analyzing attacks on DNN
P095	Shaham et al. [147]	ML expert	General	NN	Adverserial training to increase local stability of NN
P096	Carlini et al. [149]	ML expert	General	NN	Evaluating robustness of NN
P097	Chen et al. [150]	ML expert	General	NN	Analyzing attacks on DNN
P098	kurakin et al. [151]	ML expert	General	NN	Analyzing attacks on DNN
P099	Carlini et al. [152]	ML expert	General	NN	Analyzing attacks on DNN
P100	Eykholt et al. [153]	ML expert	General	NN	Analyzing attacks on DNN
P101	Palin et al. [154]	Safety engineer	Automotive	NS	Safety assurance based on ISO 26262
P102	Gauerhof et al. [155]	ML expert, systems engineer	Autonomous car	NS	Setting validation targets for ML-based automated driving
P103	Matsuno et al. [156]	ML expert	General	NS	Safety assurance of ML
P104	Denney et al. [157]	ML expert	General	NS	Safety assurance of ML-based system
P105	Picardi et al. [158]	ML expert	Medical diagnosis system	DNN	Safety assurance of ML-based mponent
P106	Picardi et al. [159]	ML expert	Medical diagnosis system	DNN	Safety assurance of ML-based component
P107	Morton et al. [98]	Systems engineer	General	NA	Testing safety-critical systems
P108	Leike et al. [101]	ML expert	General	RL	Designing test suite for safety properties verification of RL-based agents
P109	Lwakatare et al. [161]	Software engineers	General	NS	Discussing engineering challenges for ML-based systems.
P110	Varshney, K. R. [162]	ML expert, system engineer	General	NS	Discussing the necessity of the consensus on concepts like safety, trust, etc for ML-based safety-critical systems
P111	Sadigh et al. [71]	Control system engineer	autonomous control systems	NS	Modeling and verification of uncertain environment including human driver.
P112	Sadigh et al. [72]	Control system engineer	autonomous control systems	NS	Modeling and verification of uncertain environment including human driver.

Table 7: Primary studies mapped to the challenges of each layer in the three-layered framework

Layer	**Challenges**	**Primary studies addressing the challenges**
Layer-1:Problem Definition Layer	1. Understanding the problem domain.	P001, P004, P010
	2. Setting quantitative targets	P009
	3. Setting qualitative targets	P005, P008, P012, P013
	4. Requirements modeling techniques to address uncertainty	P011
	5. Explaining black box to users	P035, P039
	6. Declaring hidden customers	P002, P006, P010
Layer-2: Safety-driven modeling and analysis layer	1. Safety-driven system-level design	P036, P039, P040, P041, P042, P043
	2. Modeling uncertain environment	P056, P111, P112
	3. Scenario-based safe design and development	P037, P038
	4. Appropriate safety standards	P014, P015, P016, P017, P018, P019, P020, P021, P022, P023, P024, P025, P026, P027, P028, P029, P030, P031, P032, P033, P034, P035
Layer-3: Verified safety compliance layer	1. Formal method to verify the system	P059, P135
	2. Safety-modeling approaches for ML-based components	P059, P135
	3. Quantitative verification	P054, P055, P058, P065, P066, P067, P068, P069, P070, P071, P072, P073, P074, P075, P076, P077, P078, P079, P080, P081, P082, P083, P045, P047, P049, P050
	4. Rigorous run-time testing	P053, P107, P051, P052
	5. Robustness against adversarial attacks	P086, P087, P088, P089, P090, P091, P092, P092, P093, P094, P095, P096, P096, P097, P098, P099, P100, P046, P065, P066, P067
	6. Demonstrating assurance cases	P101, P102, P103, P104, P105, P106

foundation (layer-1 and 2) of the overall system engineering of complex ML-based systems.

6.2. RQ2: How have safety concerns been addressed by the researchers along the phases of SE process?

Summary of the state-of-the-art safety approaches at the system-level and ML-based component level along the phases of software engineering life-cycle is shown in Table 8 and Fig. 4. We did not map [22, 45, 46, 80, 161, 162] as these papers do not exclusively focus on any of the particular SE activities. Instead, these studies focus on an overall engineering process of developing ML-based systems. The reason why no primary study could be directly mapped to the development phase for ML-based components is that in case of ML, the line between the design and development is very thin. The key concept here is to take safe design decisions while training the ML model. For example, safe exploration, safe policies, safety-aware rewards, etc. All these approaches are mapped to the design phase of ML-based component, rather than its development phase. All the safety-related standards are mapped to system-level development as the standards usually provide guidelines to the overall development process of the safety-critical systems. As shown in Fig. 5, there has been a recent surge in the research on verification and validation of safety-critical systems with ML-based components since 2016. However, more effort needs to be paid to conceptualize and analyze the rich problem space of AI systems in the early phases such as requirements engineering and design. It is very important to have a systematic start of the engineering process as it often plays a key role in successful product development. Moreover, not enough attention is paid to the seamless maintenance and evolution of complex AI systems as it can be seen in both Fig. 4 and 5.

6.3. RQ3: Research Gap Analysis

The most significant concern is that two different communities or engineering disciplines are responsible for ensuring safety of intelligent systems. Safety as

Table 8: State-of-the art safety approaches for complex intelligent systems with respect to software engineering process

Level	**SE Phases**				
	Requirements Engineering	**Design**	**Development**	**V & V**	**Maintenance**
System level	P007, P010, P011, P017, P037, P038	P036, P054, P055, P111, P112	P006, P007, P014, P015, P016, P018, P019, P020, P021, P022, P023, P024 P025, P026, P027, P028, P029, P030, P031, P032, P033, P035, P037, P038	P035, P051, P053, P060, P071, P072, P079, P080, P081, P082, P083, P084, P085, P101, P107, P108	P104
ML component level	P004, P005, P008, P009, P012, P013	P039, P040, P041, P042, P043, P044, P056, P067, P091	-	P044, P045, P046, P047, P048, P049, P050, P052, P057, P058, P059, P061, P062, P063, P064, P065, P066, P067, P069, P070, P073, P074, P075, P076, P077, P078, P086, P087, P088, P089, P090, P091, P092, P093, P095, P097, P098, P099, P100, P101, P102, P103, P105, P106	-

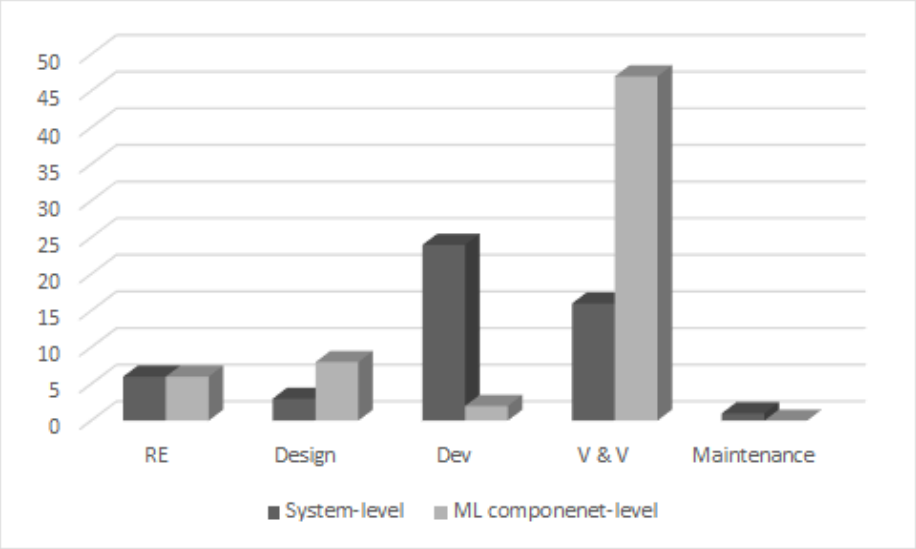

Figure 4: Number of primary studies along the phases of SE activities at system-level and ML component level

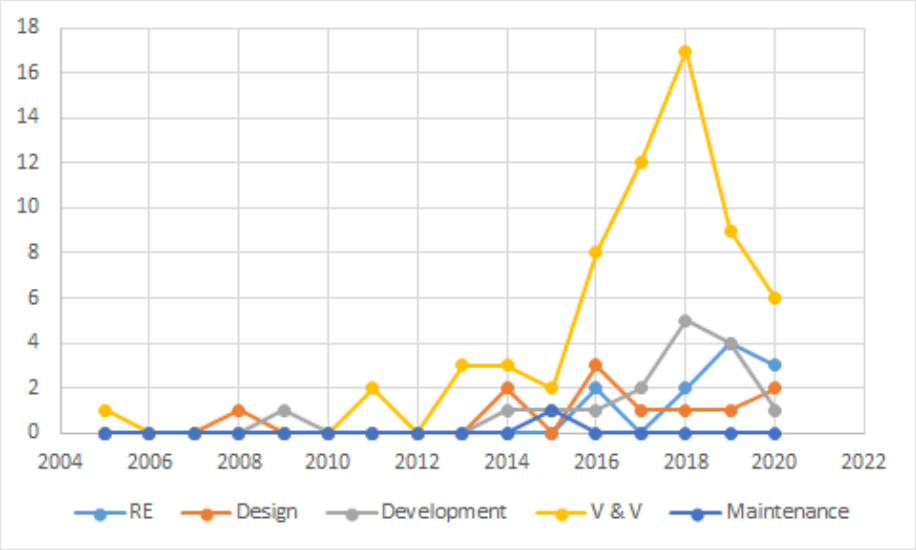

Figure 5: Trend of research on safety approaches from an engineering perspective in the last 15 years

argued by many researchers is an emergent property of a system. The source of hazard at a system level could be control flaws, inadequate control action, and inadequate control execution, etc. Artifacts and metrics for the safety analysis at the system level, such as safety goal model, safety argument, and safety integrity level, etc. have already been identified. However, when intelligence is introduced in the system through an ML component mainly designed by AI experts, the identified source of hazards are different in terms of complexity and level of abstraction. An ML component can perform incorrectly because of the wrong choice of training data (supervised learning) or wrong choice of policy, unsafe exploration, delayed rewards, etc. (unsupervised learning). There is no common baseline of the metrics and artifacts to ensure or explain the safety constraint from an ML point of view. In the same direction, Varshney discussed a much-needed future technical agenda on defining how trust, reliability, robustness, etc. are traced to safety [162]. There is a significant gap between the two levels of safety analysis at the system level and the component level whenever any intelligence is introduced by using ML component (Fig. 6). The open research questions are:

(1) How to bridge the safety analysis gap from a safety viewpoint?

(2) How to enhance traceability of these artifacts from the system level down to the component level?

(3) What is the formal taxonomy for safety analysis in the case of ML components?

(4) Is there any standard specially designed to assess the level of safety and the acceptable range of uncertainty of ML-based components in complex AI systems?

The gap between research and practice: Koopman explained that there is a significant contrast between the safety principles in research and practice in automotive industry [163]. He argued that although ISO 26262 looks promising as a standard for the level of safety of automotive systems, uncertainty in the operating environment still poses some threat to complete deployment. Salay made a notable contribution to update ISO 26262 to accommodate technologies such

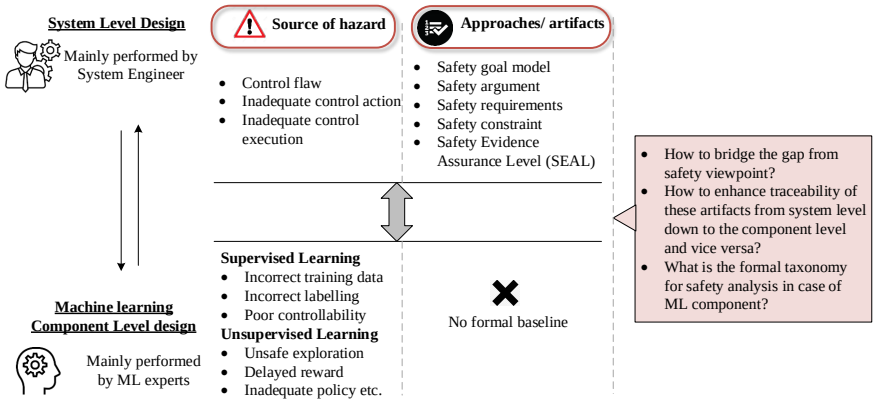

Figure 6: Gap analysis of the state-of-the art safety approaches of complex intelligent systems

as ML [80]. Lawakate et al. conducted an empirical investigation to deduce a taxonomy of SE challenges for several domains that use ML-based components heavily [161]. The authors emphasized that the challenges of a seamless engineering process that includes the development and evolution of ML-based components are very significant.

6.4. RQ4: Future Scope:

6.4.1. Addressing multi-disciplinary challenge: Collective Intelligence

The recent accidents on the autonomous systems were mostly linked to insufficient training (inadequate dataset) or choosing the wrong level of automation. The root cause was insufficient coordination between ML experts and safety engineers at an early phase of systems engineering. Requirement specification should describe data requirements, values consensus (from multiple participants), the reaction of a system to a fault, etc. This is a multidisciplinary challenge where collective intelligence can be a great asset. To ensure safety, many different domain areas need to be coordinated as shown in the framework. Data scientists, HCI experts, safety engineers, software engineers, etc. all need to collaborate to ensure safety. Instead of relying on the knowledge of individuals, we should use the collection as an emergent intelligence to solve engineering

problems. We can rely on all to work together, collaborate, and share individual knowledge to achieve a goal. In a nutshell, we can have a paradigm shift from traditional safety engineering to a broader concept of collective knowledge engineering.

6.4.2. Enhanced traceability of the artifacts across the layers of the integrated framework

Due to the lack of an integrated framework, it is unclear how we can trace safety-driven design of AI systems. Most of the research work focusing on safety-driven ML do not specify clearly how their design/ learning decisions relate to the system level safety-related concepts. Traditional understanding of forward and backward traceability has less impact in the days of AI. Therefore, we define horizontal and vertical traceability of safety-driven design of AI systems.

Horizontal Traceability: traces of safety engineering process and design decisions along the same layer at system-level and ML-based component-level involving multiple participants.

Vertical Traceability: traces of safety analysis across the layers.

Instead of relying on the tacit knowledge of the experts, we recommend keeping a record of all design decisions and the rationales behind them. Therefore, we need to specify ML related categories of risks, the way those risks are adding on to the system-level risks. Thereafter, the experts can mitigate each risk with safety constraints and record them in the artifacts.

7. Threats to validity

In this section we discuss the known threats to the validity of our literature survey. We also explain how we mitigated the threats. Moreover, we summarize the limitation of our study. As discussed in [164], identified threats to four types of validity (internal, external, construct and conclusion) can be mapped to the following phases of the literature survey.

1. Planning phase:

In this phase, we set the valid research questions which were evaluated later by the graduate researchers working on AI systems engineering. We documented the rationale behind each of the research questions. We followed a stepwise process for the search method with explicit actions and outcomes. The complete list of venues or databases and search strings are mentioned in Section 4.3 and 4.2, so that the SLR can be replicated in future. The finalized list of primary studies after applying the inclusion and exclusion criteria are rechecked at least twice before moving to the next phase.

2. Conducting phase:

In order to mitigate the threat of incomplete research information or inaccessible full version of papers, we have contacted the relevant authors whenever needed. We mitigated the publication bias by excluding the grey literature from the study. During this phase, each of the paper has been cross-checked for their completeness. Along with the title and abstract, the introduction of each paper was carefully read to confirm that the perspective the work is not misunderstood. The quality of the papers is evaluated quantitatively to mitigate the threat of subjective quality assessment. Threat of duplication was mitigated by carefully choosing the full paper version (if available) over a smaller and earlier version of the same work.

3. Reporting phase:

In this phase, we report our analysis based on the research questions after analyzing 112 primary studies. These many studies are good enough to mitigate the threat of low generalizability of primary studies. We have covered safety-related papers written from various perspectives (software engineer, ML experts, safety engineer, etc) and applied to a diverse domain, to increase the generalizability of our final report.

Limitations:

Our study is primarily based on the proposed three-layered conceptual framework to engineer AI systems. This framework is designed based on our knowledge on the relevant area of research. It helps us to analyze the state-of-the-art safety approaches from the perspective of multiple stakeholders along each phase

of the system engineering.However, an end-to-end evaluation of the effectiveness of the proposed framework is out of the scope of this paper. The survey covers primary studies mainly from the software engineering process perspective. However, there are other relevant studies on AI safety can be found from the discipline of statistics, human-computer interaction, etc. Those studies are not discussed in this literature review.

8. Conclusion

The use of ML techniques to impart intelligence creates many challenges to ensuring safety. In this paper, we summarized the current state-of-the-art research contributions in this area. We explained a three-layered conceptual framework that can help visualize the stakeholders and their contributions to engineering a complex intelligent system from a safety perspective. We analyzed the gap in the current research that should be addressed. We also described how this three-layered framework can help enhance the traceability of safety-driven design across all the layers in the future. We believe that it is worth exploring how the artifacts move across the layers in different forms to facilitate the safety analysis. Instead of relying on tacit design knowledge (or tacit machine learning knowledge of AI experts), it is helpful to document all the rationales behind each decision to eventually gain the trust of the stakeholders. For future work, we plan to design a proper stepwise methodology to guide multiple disciplines to work together for safety analysis and verification of AI systems.

Acknowledgement. This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (NRF-2020R1F1A1075605).

References

[1] C. Agrell, S. Eldevik, A. Hafver, F. B. Pedersen, E. Stensrud, A. Huseby, Pitfalls of machine learning for tail events in high risk environments (2018). doi:10.1201/9781351174664-381.

[2] S. Russell, D. Dewey, M. Tegmark, Research priorities for robust and beneficial artificial intelligence, Ai Magazine 36 (4) (2015) 105–114.

[3] T. Everitt, G. Lea, M. Hutter, AGI safety literature review, arXiv preprint arXiv:1805.01109.

[4] M. Brundage, Taking superintelligence seriously: Superintelligence: Paths, dangers, strategies by nick bostrom (oxford university press, 2014), Futures 72 (2015) 32–35.

[5] N. Soares, B. Fallenstein, Aligning superintelligence with human interests: A technical research agenda, Machine Intelligence Research Institute (MIRI) technical report 8.

[6] E. Davis, Ethical guidelines for a superintelligence, Artificial Intelligence 220 (2015) 121–124.

[7] A. F. Winfield, C. Blum, W. Liu, Towards an ethical robot: internal models, consequences and ethical action selection, in: Conference towards autonomous robotic systems, Springer, 2014, pp. 85–96.

[8] D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman, D. Mané, Concrete problems in ai safety, arXiv preprint arXiv:1606.06565.

[9] H. Monkhouse, I. Habli, J. McDermid, S. Khastgir, G. Dhadyalla, Why functional safety experts worry about automotive systems having increasing autonomy, in: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 2017, pp. 1–6.

[10] P. Koopman, M. Wagner, Toward a framework for highly automated vehicle safety validation, Tech. rep., SAE Technical Paper (2018).

[11] N. A. Greenblatt, Self-driving cars and the law, IEEE spectrum 53 (2) (2016) 46–51.

[12] T. Mikolov, A. Joulin, M. Baroni, A roadmap towards machine intelligence, in: International Conference on Intelligent Text Processing and Computational Linguistics, Springer, 2016, pp. 29–61.

[13] P. Koopman, The heavy tail safety ceiling, in: Automated and Connected Vehicle Systems Testing Symposium, 2018.

[14] M. V. Stringfellow, N. G. Leveson, B. D. Owens, Safety-driven design for software-intensive aerospace and automotive systems, Proceedings of the IEEE 98 (4) (2010) 515–525.

[15] K. Singla, J. Bose, C. Naik, Analysis of software engineering for agile machine learning projects, in: 2018 15th IEEE India Council International Conference (INDICON), IEEE, 2018, pp. 1–5.

[16] https://futureoife.org/landscape/researchlandscapeextended.pdf.

[17] N. G. Leveson, Engineering a safer world: Systems thinking applied to safety, The MIT Press, 2016.

[18] IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, April 2010.

[19] ISO 26262:2018-Road Vehicles- Vehicle Safety, ISO, 2018.

[20] K. R. Varshney, Engineering safety in machine learning, in: 2016 Information Theory and Applications Workshop (ITA), IEEE, 2016, pp. 1–5.

[21] B. Littlewood, D. Wright, The use of multilegged arguments to increase confidence in safety claims for software-based systems: A study based on a BBN analysis of an idealized example, IEEE Transactions on Software Engineering 33 (5) (2007) 347–365.

[22] F. Ishikawa, N. Yoshioka, How do engineers perceive difficulties in engineering of machine-learning systems?-questionnaire survey, in: 2019 IEEE/ACM Joint 7th International Workshop on Conducting Empirical Studies in Industry (CESI) and 6th International Workshop on Software Engineering Research and Industrial Practice (SER&IP), IEEE, 2019, pp. 2–9.

[23] A. Serban, K. van der Blom, H. Hoos, J. Visser, Adoption and effects of software engineering best practices in machine learning, in: Proceedings of the 14th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2020, pp. 1–12.

[24] L. E. Lwakatare, A. Raj, I. Crnkovic, J. Bosch, H. H. Olsson, Large-scale machine learning systems in real-world industrial settings: A review of challenges and solutions, Information and Software Technology 127 (2020) 106368.

[25] Z. Wan, X. Xia, D. Lo, G. C. Murphy, How does machine learning change software development practices?, IEEE Transactions on Software Engineering.

[26] M. Luckcuck, M. Farrell, L. A. Dennis, C. Dixon, M. Fisher, Formal specification and verification of autonomous robotic systems: A survey, ACM Computing Surveys (CSUR) 52 (5) (2019) 1–41.

[27] E. Yurtsever, J. Lambert, A. Carballo, K. Takeda, A survey of autonomous driving: Common practices and emerging technologies, IEEE Access 8 (2020) 58443–58469.

[28] J. Guiochet, M. Machin, H. Waeselynck, Safety-critical advanced robots: A survey, Robotics and Autonomous Systems 94 (2017) 43–52.

[29] J. Guo, U. Kurup, M. Shah, Is it safe to drive? an overview of factors, metrics, and datasets for driveability assessment in autonomous driving, IEEE Transactions on Intelligent Transportation Systems.

[30] A. M. Nascimento, L. F. Vismari, C. B. S. T. Molina, P. S. Cugnasca, J. B. Camargo, J. R. de Almeida, R. Inam, E. Fersman, M. V. Marquezini, A. Y. Hata, A systematic literature review about the impact of artificial intelligence on autonomous vehicle safety, IEEE Transactions on Intelligent Transportation Systems.

[31] M. Ozdag, Adversarial attacks and defenses against deep neural networks: a survey, Procedia Computer Science 140 (2018) 152–161.

[32] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, D. Mukhopadhyay, Adversarial attacks and defences: A survey, arXiv preprint arXiv:1810.00069.

[33] H. X. Y. M. Hao-Chen, L. D. Deb, H. L. J.-L. T. Anil, K. Jain, Adversarial attacks and defenses in images, graphs and text: A review, International Journal of Automation and Computing 17 (2) (2020) 151–178.

[34] J. Garcıa, F. Fernández, A comprehensive survey on safe reinforcement learning, Journal of Machine Learning Research 16 (1) (2015) 1437–1480.

[35] W. Xiang, P. Musau, A. A. Wild, D. M. Lopez, N. Hamilton, X. Yang, J. Rosenfeld, T. T. Johnson, Verification for machine learning, autonomy, and neural networks survey, arXiv preprint arXiv:1810.01989.

[36] M. Borg, C. Englund, K. Wnuk, B. Duran, C. Levandowski, S. Gao, Y. Tan, H. Kaijser, H. Lönn, J. Törnqvist, Safely entering the deep: A review of verification and validation for machine learning and a challenge elicitation in the automotive industry, arXiv preprint arXiv:1812.05389.

[37] J. Schumann, P. Gupta, Y. Liu, Application of neural networks in high assurance systems: A survey, in: Applications of Neural Networks in High Assurance Systems, Springer, 2010, pp. 1–19.

[38] J. M. Zhang, M. Harman, L. Ma, Y. Liu, Machine learning testing: Survey, landscapes and horizons, IEEE Transactions on Software Engineering.

[39] D. Dewey, S. Russell, M. Tegmark, et al., A survey of research questions for robust and beneficial ai. future of life institute (2015).

[40] R. Mallah, The landscape of ai safety and beneficence research. input for brainstorming at beneficial AI 2017, Beneficial AI 2017.

[41] S. Martínez-Fernández, X. Franch, A. Jedlitschka, M. Oriol, A. Trendowicz, Research directions for developing and operating artificial intelligence models in trustworthy autonomous systems, arXiv preprint arXiv:2003.05434.

[42] A. Nguyen-Duc, P. Abrahamsson, Continuous experimentation on artificial intelligence software: a research agenda, in: Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2020, pp. 1513–1516.

[43] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th international conference on evaluation and assessment in software engineering, 2014, pp. 1–10.

[44] P. Koopman, M. Wagner, Autonomous vehicle safety: An interdisciplinary challenge, IEEE Intelligent Transportation Systems Magazine 9 (1) (2017) 90–96.

[45] A. Arpteg, B. Brinne, L. Crnkovic-Friis, J. Bosch, Software engineering challenges of deep learning, in: 2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), IEEE, 2018, pp. 50–59.

[46] S. Amershi, A. Begel, C. Bird, R. DeLine, H. Gall, E. Kamar, N. Nagappan, B. Nushi, T. Zimmermann, Software engineering for machine learning: A case study, in: 2019 IEEE/ACM 41st International Conference

on Software Engineering: Software Engineering in Practice (ICSE-SEIP), IEEE, 2019, pp. 291–300.

[47] D. Sculley, G. Holt, D. Golovin, E. Davydov, T. Phillips, D. Ebner, V. Chaudhary, M. Young, J.-F. Crespo, D. Dennison, Hidden technical debt in machine learning systems, in: Advances in neural information processing systems, 2015, pp. 2503–2511.

[48] J. Bosch, H. H. Olsson, I. Crnkovic, It takes three to tango: Requirement, outcome/data, and ai driven development., in: SiBW, 2018, pp. 177–192.

[49] H. Belani, M. Vukovic, Ž. Car, Requirements engineering challenges in building ai-based complex systems, in: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), IEEE, 2019, pp. 252–255.

[50] M. Rahimi, J. L. Guo, S. Kokaly, M. Chechik, Toward requirements specification for machine-learned components, in: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), IEEE, 2019, pp. 241–244.

[51] A. Vogelsang, M. Borg, Requirements engineering for machine learning: Perspectives from data scientists, in: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), IEEE, 2019, pp. 245–251.

[52] M. A. Köhl, K. Baum, M. Langer, D. Oster, T. Speith, D. Bohlender, Explainability as a non-functional requirement, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), IEEE, 2019, pp. 363–368.

[53] J. Horkoff, Non-functional requirements for machine learning: Challenges and new directions, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), IEEE, 2019, pp. 386–391.

[54] K. Nakamichi, K. Ohashi, I. Namba, R. Yamamoto, M. Aoyama, L. Joeckel, J. Siebert, J. Heidrich, Requirements-driven method to determine quality characteristics and measurements for machine learning software and its evaluation, in: 2020 IEEE 28th International Requirements Engineering Conference (RE), IEEE, 2020, pp. 260–270.

[55] B. C. Hu, R. Salay, K. Czarnecki, M. Rahimi, G. Selim, M. Chechik, Towards requirements specification for machine-learned perception based on human performance, in: 2020 IEEE Seventh International Workshop on Artificial Intelligence for Requirements Engineering (AIRE), IEEE, 2020, pp. 48–51.

[56] F. Ishikawa, Y. Matsuno, Evidence-driven requirements engineering for uncertainty of machine learning-based systems, in: 2020 IEEE 28th International Requirements Engineering Conference (RE), IEEE, 2020, pp. 346–351.

[57] D. Firesmith, Engineering safety requirements, safety constraints, and safety-critical requirements, Journal of Object technology 3 (3) (2004) 27–42.

[58] N. Leveson, A new accident model for engineering safer systems, Safety science 42 (4) (2004) 237–270.

[59] M. V. Stringfellow, N. G. Leveson, B. D. Owens, Safety-driven design for software-intensive aerospace and automotive systems, Proceedings of the IEEE 98 (4) (2010) 515–525.

[60] N. G. Leveson, A systems-theoretic approach to safety in software-intensive systems, IEEE Transactions on Dependable and Secure computing 1 (1) (2004) 66–86.

[61] B. D. Owens, M. S. Herring, N. Dulac, N. G. Leveson, M. D. Ingham, K. A. Weiss, Application of a safety-driven design methodology to an

outer planet exploration mission, in: 2008 IEEE aerospace conference, IEEE, 2008, pp. 1–24.

[62] L. Kuper, G. Katz, J. Gottschlich, K. Julian, C. Barrett, M. Kochenderfer, Toward scalable verification for safety-critical deep networks, arXiv preprint arXiv:1801.05950.

[63] X. Gu, A. Easwaran, Towards safe machine learning for cps: infer uncertainty from training data, in: Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, 2019, pp. 249–258.

[64] Y. Chow, M. Ghavamzadeh, L. Janson, M. Pavone, Risk-constrained reinforcement learning with percentile risk criteria, The Journal of Machine Learning Research 18 (1) (2017) 6070–6120.

[65] J. Rong, N. Luan, Safe reinforcement learning with policy-guided planning for autonomous driving, in: 2020 IEEE International Conference on Mechatronics and Automation (ICMA), IEEE, 2020, pp. 320–326.

[66] D. Chen, L. Jiang, Y. Wang, Z. Li, Autonomous driving using safe reinforcement learning by incorporating a regret-based human lane-changing decision model, in: 2020 American Control Conference (ACC), IEEE, 2020, pp. 4355–4361.

[67] W. Li, L. Dworkin, S. A. Seshia, Mining assumptions for synthesis, in: Ninth ACM/IEEE International Conference on Formal Methods and Models for Codesign (MEMPCODE2011), IEEE, 2011, pp. 43–50.

[68] S. Ghosh, D. Sadigh, P. Nuzzo, V. Raman, A. Donzé, A. L. Sangiovanni-Vincentelli, S. S. Sastry, S. A. Seshia, Diagnosis and repair for synthesis from signal temporal logic specifications, in: Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, 2016, pp. 31–40.

[69] W. Li, D. Sadigh, S. S. Sastry, S. A. Seshia, Synthesis for human-in-the-loop control systems, in: International Conference on Tools and Algo-

rithms for the Construction and Analysis of Systems, Springer, 2014, pp. 470–484.

[70] D. Sadigh, S. Sastry, S. A. Seshia, A. D. Dragan, Planning for autonomous cars that leverage effects on human actions., in: Robotics: Science and Systems, Vol. 2, Ann Arbor, MI, USA, 2016.

[71] D. Sadigh, K. Driggs-Campbell, A. Puggelli, W. Li, V. Shia, R. Bajcsy, A. L. Sangiovanni-Vincentelli, S. S. Sastry, S. A. Seshia, Data-driven probabilistic modeling and verification of human driver behavior, in: AAAI Spring Symposium-Technical Report, 2014, pp. 56–61.

[72] D. Sadigh, S. S. Sastry, S. A. Seshia, A. Dragan, Information gathering actions over human internal state, in: 2016 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), IEEE, 2016, pp. 66–73.

[73] J. Bach, S. Otten, E. Sax, Model based scenario specification for development and test of automated driving functions, in: 2016 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2016, pp. 1149–1155.

[74] T. Menzel, G. Bagschik, M. Maurer, Scenarios for development, test and validation of automated vehicles, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 1821–1827.

[75] P. Cihon, Standards for ai governance: international standards to enable global coordination in ai research & development, Future of Humanity Institute. University of Oxford.

[76] Google White Paper, Perspectives on issues in AI governance.

[77] S. Ozlati, R. Yampolskiy, The formalization of ai risk management and safety standards, in: Workshops at the Thirty-First AAAI Conference on Artificial Intelligence, 2017.

[78] Y. Luo, Y. Yu, Z. Jin, H. Zhao, Environment-centric safety requirements for autonomous unmanned systems, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), IEEE, 2019, pp. 410–415.

[79] ISO/IEC, IEC 61508-functional safety of electrical/electronic/programmable electronic safety-related systems.

[80] R. Salay, R. Queiroz, K. Czarnecki, An analysis of iso 26262: Using machine learning safely in automotive software, arXiv preprint arXiv:1709.02435.

[81] P. Koopman, U. Ferrell, F. Fratrik, M. Wagner, A safety standard approach for fully autonomous vehicles, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2019, pp. 326–332.

[82] J. Yoshida, UL 4600 draft puts safety onus on av hopefuls, https://www.eetimes.com/ul-4600-draft-puts-safety-onus-on-av-hopefuls/.

[83] ISO, ISO 3691-4:2020-industrial trucks — safety requirements and verification — part 4: Driverless industrial trucks and their systems (2020).

[84] ISO, ISO 13482:2014- robots and robotic devices — safety requirements for personal care robots (2014).

[85] ISO, ISO 19014-1:2018- earth-moving machinery — functional safety — part 1: Methodology to determine safety-related parts of the control system and performance requirements (2018).

[86] ISO, ISO 17757:2017- earth-moving machinery and mining — autonomous and semi-autonomous machine system safety (2017).

[87] ISO, ISO 18497:2018- agricultural machinery and tractors — safety of highly automated agricultural machines — principles for design (2018).

[88] IEC, IEC 62267:2009- railway applications - automated urban guided transport (AUGT) - safety requirements (2009).

[89] ISO, ISO/PAS 21448:2019- road vehicles – safety of the intended functionality (2019).

[90] ISO/IEC, ISO/IEC CD 22989.2-artificial intelligence — concepts and terminology.

[91] ISO, ISO/IEC CD 23053.2- framework for artificial intelligence (AI) systems using machine learning (ML).

[92] ISO/IEC, ISO/IEC CD 23894- information technology — artificial intelligence — risk management.

[93] ISO/IEC, ISO/IEC AWI TR 24027- information technology — artificial intelligence (AI) — bias in ai systems and ai aided decision making.

[94] ISO, ISO/IEC TR 24028:2020 -information technology — artificial intelligence — overview of trustworthiness in artificial intelligence.

[95] ISO/IEC, ISO/IEC DTR 24029-1 artificial intelligence (AI) — assessment of the robustness of neural networks.

[96] ISO/IEC, ISO/IEC CD 38507-information technology — governance of it — governance implications of the use of artificial intelligence by organizations.

[97] J. Yoshuda, Multiple standards to emerge in 2020 for ai-driven vehicles (Accessed on 27-Nov, 2020).

[98] J. Morton, T. A. Wheeler, M. J. Kochenderfer, Closed-loop policies for operational tests of safety-critical systems, IEEE Transactions on Intelligent Vehicles 3 (3) (2018) 317–328.

[99] S. A. Seshia, D. Sadigh, S. S. Sastry, Towards verified artificial intelligence, arXiv preprint arXiv:1606.08514.

[100] S. A. Seshia, A. Desai, T. Dreossi, D. J. Fremont, S. Ghosh, E. Kim, S. Shivakumar, M. Vazquez-Chanlatte, X. Yue, Formal specification for

deep neural networks, in: International Symposium on Automated Technology for Verification and Analysis, Springer, 2018, pp. 20–34.

[101] J. Leike, M. Martic, V. Krakovna, P. A. Ortega, T. Everitt, A. Lefrancq, L. Orseau, S. Legg, Ai safety gridworlds, arXiv preprint arXiv:1711.09883.

[102] A. Nilim, L. El Ghaoui, Robust control of markov decision processes with uncertain transition matrices, Operations Research 53 (5) (2005) 780–798.

[103] D. Sadigh, A. Kapoor, Safe control under uncertainty with probabilistic signal temporal logic.

[104] A. Fawzi, O. Fawzi, P. Frossard, Analysis of classifiers' robustness to adversarial perturbations, Machine Learning 107 (3) (2018) 481–508.

[105] A. Nguyen, J. Yosinski, J. Clune, Deep neural networks are easily fooled: High confidence predictions for unrecognizable images, in: Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 427–436.

[106] S.-M. Moosavi-Dezfooli, A. Fawzi, P. Frossard, Deepfool: a simple and accurate method to fool deep neural networks, in: Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 2574–2582.

[107] I. J. Goodfellow, J. Shlens, C. Szegedy, Explaining and harnessing adversarial examples, arXiv preprint arXiv:1412.6572.

[108] S. Ghosh, D. Sadigh, P. Nuzzo, V. Raman, A. Donzé, A. L. Sangiovanni-Vincentelli, S. S. Sastry, S. A. Seshia, Diagnosis and repair for synthesis from signal temporal logic specifications, in: Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, 2016, pp. 31–40.

[109] L. A. Dennis, M. Fisher, N. K. Lincoln, A. Lisitsa, S. M. Veres, Practical verification of decision-making in agent-based autonomous systems, Automated Software Engineering 23 (3) (2016) 305–359.

[110] R. Alur, Formal verification of hybrid systems, in: Proceedings of the ninth ACM international conference on Embedded software, 2011, pp. 273–278.

[111] S. Chakraborty, D. J. Fremont, K. S. Meel, S. A. Seshia, M. Y. Vardi, Distribution-aware sampling and weighted model counting for sat, arXiv preprint arXiv:1404.2984.

[112] Y. Shoukry, P. Nuzzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, G. J. Pappas, P. Tabuada, Smc: Satisfiability modulo convex optimization, in: Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control, 2017, pp. 19–28.

[113] C. E. Tuncali, J. Kapinski, H. Ito, J. V. Deshmukh, Reasoning about safety of learning-enabled components in autonomous cyber-physical systems, in: Proceedings of the 55th Annual Design Automation Conference, 2018, pp. 1–6.

[114] S. Lee, S. Cha, D. Lee, H. Oh, Effective white-box testing of deep neural networks with adaptive neuron-selection strategy, in: Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis, 2020, pp. 165–176.

[115] K. Pei, Y. Cao, J. Yang, S. Jana, Deepxplore: Automated whitebox testing of deep learning systems, in: proceedings of the 26th Symposium on Operating Systems Principles, 2017, pp. 1–18.

[116] Y. Tian, K. Pei, S. Jana, B. Ray, Deeptest: Automated testing of deep-neural-network-driven autonomous cars, in: Proceedings of the 40th international conference on software engineering, 2018, pp. 303–314.

[117] M. Wicker, X. Huang, M. Kwiatkowska, Feature-guided black-box safety testing of deep neural networks, in: International Conference on Tools and Algorithms for the Construction and Analysis of Systems, Springer, 2018, pp. 408–426.

[118] J. Wang, G. Dong, J. Sun, X. Wang, P. Zhang, Adversarial sample detection for deep neural network through model mutation testing, in: 2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE), IEEE, 2019, pp. 1245–1256.

[119] L. Ma, F. Zhang, J. Sun, M. Xue, B. Li, F. Juefei-Xu, C. Xie, L. Li, Y. Liu, J. Zhao, et al., Deepmutation: Mutation testing of deep learning systems, in: 2018 IEEE 29th International Symposium on Software Reliability Engineering (ISSRE), IEEE, 2018, pp. 100–111.

[120] Y. Sun, M. Wu, W. Ruan, X. Huang, M. Kwiatkowska, D. Kroening, Concolic testing for deep neural networks, in: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, 2018, pp. 109–119.

[121] L. Ma, F. Juefei-Xu, F. Zhang, J. Sun, M. Xue, B. Li, C. Chen, T. Su, L. Li, Y. Liu, et al., Deepgauge: Multi-granularity testing criteria for deep learning systems, in: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, 2018, pp. 120–131.

[122] Y. Sun, X. Huang, D. Kroening, J. Sharp, M. Hill, R. Ashmore, Testing deep neural networks, arXiv preprint arXiv:1803.04792.

[123] T. Byun, S. Rayadurgam, Manifold for machine learning assurance, arXiv preprint arXiv:2002.03147.

[124] F. Harel-Canada, L. Wang, M. A. Gulzar, Q. Gu, M. Kim, Is neuron coverage a meaningful measure for testing deep neural networks?, in: Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2020, pp. 851–862.

[125] T. Dreossi, A. Donzé, S. A. Seshia, Compositional falsification of cyber-physical systems with machine learning components, Journal of Automated Reasoning 63 (4) (2019) 1031–1053.

[126] C. E. Tuncali, G. Fainekos, H. Ito, J. Kapinski, Simulation-based adversarial test generation for autonomous vehicles with machine learning components, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 1555–1562.

[127] S. Dutta, S. Jha, S. Sanakaranarayanan, A. Tiwari, Output range analysis for deep neural networks, arXiv preprint arXiv:1709.09130.

[128] R. Ehlers, Formal verification of piece-wise linear feed-forward neural networks, in: International Symposium on Automated Technology for Verification and Analysis, Springer, 2017, pp. 269–286.

[129] X. Huang, M. Kwiatkowska, S. Wang, M. Wu, Safety verification of deep neural networks, in: International Conference on Computer Aided Verification, Springer, 2017, pp. 3–29.

[130] G. Katz, C. Barrett, D. L. Dill, K. Julian, M. J. Kochenderfer, Reluplex: An efficient smt solver for verifying deep neural networks, in: International Conference on Computer Aided Verification, Springer, 2017, pp. 97–117.

[131] X. Sun, H. Khedr, Y. Shoukry, Formal verification of neural network controlled autonomous systems, in: Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control, 2019, pp. 147–156.

[132] M. Fazlyab, M. Morari, G. J. Pappas, Probabilistic verification and reachability analysis of neural networks via semidefinite programming, in: 2019 IEEE 58th Conference on Decision and Control (CDC), IEEE, 2019, pp. 2726–2731.

[133] W. Xiang, T. T. Johnson, Reachability analysis and safety verification for neural network control systems, arXiv preprint arXiv:1805.09944.

[134] R. Ivanov, J. Weimer, R. Alur, G. J. Pappas, I. Lee, Verisig: verifying safety properties of hybrid systems with neural network controllers, in:

Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control, 2019, pp. 169–178.

[135] M. Akintunde, A. Lomuscio, L. Maganti, E. Pirovano, Reachability analysis for neural agent-environment systems., in: KR, 2018, pp. 184–193.

[136] R. Ivanov, T. J. Carpenter, J. Weimer, R. Alur, G. J. Pappas, I. Lee, Case study: verifying the safety of an autonomous racing car with a neural network controller, in: Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control, 2020, pp. 1–7.

[137] L.-H. Hoang, M. A. Hanif, M. Shafique, Ft-clipact: Resilience analysis of deep neural networks and improving their fault tolerance using clipped activation, in: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, 2020, pp. 1241–1246.

[138] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus, Intriguing properties of neural networks, arXiv preprint arXiv:1312.6199.

[139] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Šrndić, P. Laskov, G. Giacinto, F. Roli, Evasion attacks against machine learning at test time, in: Joint European conference on machine learning and knowledge discovery in databases, Springer, 2013, pp. 387–402.

[140] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, A. Swami, Practical black-box attacks against machine learning, in: Proceedings of the 2017 ACM on Asia conference on computer and communications security, 2017, pp. 506–519.

[141] K. Grosse, N. Papernot, P. Manoharan, M. Backes, P. McDaniel, Adversarial perturbations against deep neural networks for malware classification, arXiv preprint arXiv:1606.04435.

[142] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, A. Swami, The limitations of deep learning in adversarial settings, in: 2016 IEEE

European symposium on security and privacy (EuroS&P), IEEE, 2016, pp. 372–387.

[143] O. Bastani, Y. Ioannou, L. Lampropoulos, D. Vytiniotis, A. Nori, A. Criminisi, Measuring neural net robustness with constraints, in: Advances in neural information processing systems, 2016, pp. 2613–2621.

[144] M. Naseer, M. F. Minhas, F. Khalid, M. A. Hanif, O. Hasan, M. Shafique, Fannet: formal analysis of noise tolerance, training bias and input sensitivity in neural networks, in: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, 2020, pp. 666–669.

[145] S. Huang, N. Papernot, I. Goodfellow, Y. Duan, P. Abbeel, Adversarial attacks on neural network policies, arXiv preprint arXiv:1702.02284.

[146] S. Gu, L. Rigazio, Towards deep neural network architectures robust to adversarial examples, arXiv preprint arXiv:1412.5068.

[147] U. Shaham, Y. Yamada, S. Negahban, Understanding adversarial training: Increasing local stability of neural nets through robust optimization, arXiv preprint arXiv:1511.05432.

[148] T. Hazan, G. Papandreou, D. Tarlow, Adversarial perturbations of deep neural networks.

[149] N. Carlini, D. Wagner, Towards evaluating the robustness of neural networks, in: 2017 ieee symposium on security and privacy (sp), IEEE, 2017, pp. 39–57.

[150] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, C.-J. Hsieh, Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models, in: Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, 2017, pp. 15–26.

[151] A. Kurakin, I. Goodfellow, S. Bengio, Adversarial examples in the physical world, arXiv preprint arXiv:1607.02533.

[152] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, W. Zhou, Hidden voice commands, in: 25th {USENIX} Security Symposium ({USENIX} Security 16), 2016, pp. 513–530.

[153] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song, Robust physical-world attacks on deep learning visual classification, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 1625–1634.

[154] R. Palin, D. Ward, I. Habli, R. Rivett, Iso 26262 safety cases: Compliance and assurance.

[155] L. Gauerhof, P. Munk, S. Burton, Structuring validation targets of a machine learning function applied to automated driving, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2018, pp. 45–58.

[156] Y. Matsuno, F. Ishikawa, S. Tokumoto, Tackling uncertainty in safety assurance for machine learning: Continuous argument engineering with attributed tests, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2019, pp. 398–404.

[157] E. Denney, G. Pai, I. Habli, Dynamic safety cases for through-life safety assurance, in: 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Vol. 2, IEEE, 2015, pp. 587–590.

[158] C. Picardi, R. Hawkins, C. Paterson, I. Habli, A pattern for arguing the assurance of machine learning in medical diagnosis systems, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2019, pp. 165–179.

[159] C. Picardi, I. Habli, Perspectives on assurance case development for retinal disease diagnosis using deep learning, in: Conference on Artificial Intelligence in Medicine in Europe, Springer, 2019, pp. 365–370.

[160] M. Brundage, S. Avin, J. Wang, H. Belfield, G. Krueger, G. Hadfield, H. Khlaaf, J. Yang, H. Toner, R. Fong, et al., Toward trustworthy ai development: mechanisms for supporting verifiable claims, arXiv preprint arXiv:2004.07213.

[161] L. E. Lwakatare, A. Raj, J. Bosch, H. H. Olsson, I. Crnkovic, A taxonomy of software engineering challenges for machine learning systems: An empirical investigation, in: International Conference on Agile Software Development, Springer, Cham, 2019, pp. 227–243.

[162] K. R. Varshney, On mismatched detection and safe, trustworthy machine learning, in: 2020 54th Annual Conference on Information Sciences and Systems (CISS), IEEE, 2020, pp. 1–4.

[163] P. Koopman, Practical experience report: Automotive safety practices vs. accepted principles, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2018, pp. 3–11.

[164] X. Zhou, Y. Jin, H. Zhang, S. Li, X. Huang, A map of threats to validity of systematic literature reviews in software engineering, in: 2016 23rd Asia-Pacific Software Engineering Conference (APSEC), IEEE, 2016, pp. 153–160.