Uncertainty Representation with Extended Evidential Networks for Modeling Safety of the Intended Functionality (SOTIF)

Given Name Surname
dept. name of organization (of Aff.), City, Country E-mail: email address

Given Name Surname
dept. name of organization (of Aff.), City, Country E-mail: email address

Given Name Surname
dept. name of organization (of Aff.), City, Country E-mail: email address

Given Name Surname
dept. name of organization (of Aff.), City, Country E-mail: email address

Highly automated driving (HAD) vehicles are complex and safety critical systems. They are deployed in an intricate environment which undergoes continual changes. Complexity of these systems as well as sensing and understanding the operational environment results in uncertainties, which needs to be addressed for the safety of HAD vehicles. Ongoing standardization activities (ISO/PAS 21448) to provide Safety of the Intended Functionality (SOTIF) of HAD vehicles intend to address these issues.
As part of the SOTIF argumentation, we propose a novel modeling method to represent uncertainty of the system and the environment as well as the propagation of uncertainty through the system. Some authors classified three types of uncertainty, namely aleatory, epistemic and ontological for this purpose. In this paper, we provide multiple plausibility functions of Dempster-Shafer Theory to fully assimilate the representation of ontological uncertainty along with epistemic and aleatory. We implement our proposed method using a commercial Bayesian Network tool. We show the application of our method with a perception classification use case.

Keywords: SOTIF, autonomous vehicle safety, safety of the intended functionality, dependability, Dempster-Shafer Theory, Bayesian networks, Evidential networks

1. Introduction

Safety analysis of highly automated driving (HAD) vehicles is a major challenge. HAD vehicles operate in an environment that cannot be specified completely at design time, at least not at the necessary granularity level, due to inherent environmental complexity and continual ongoing changes in the environment. Together, these intricacies constitute *open context* [Burton et al. (2020); Chang et al. (2020)]. The open context nature results in uncertainties originating from the operational environment (e.g. a pedestrian takes a random turn not predicted by system perception), sensing (e.g. charge loses in shift registers of CCD camera), understanding the environment (e.g. machine learning algorithm used for classification) [Burton et al. (2020); Chang et al. (2020)] and complexity of the system (e.g. emergent behavior [Leveson and Thomas (2013)]). Ongoing standardization activities [ISO/PAS21448 (2019)] to provide Safety of the Intended Functionality (SOTIF) of HAD vehicles corroborate to the existence of these challenges. The goal of the SOTIF activity is to identify the performance limitations and triggering conditions that may lead to potentially hazardous behavior.
Gansch et al. presented a system theoretic approach of uncertainties, which help to quantify these performance limitation and triggering conditions. Uncertainties originating from various sources are traditionally categorized into two types [Gansch and Adee (2020)].

(i) Epistemic Uncertainty: lack of knowledge about the system model and the inexact encoding of physical system to models (Fig. 1)
(ii) Aleatory Uncertainty: randomness of a process represented by a system model (Fig. 1)

The authors introduced the concept of ontological uncertainty in addition to the two types mentioned earlier.

(iii) Ontological Uncertainty: condition of complete ignorance in the model of a relevant

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference.
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_"Uncertainty Representation with Extended Evidential Networks for Mo

aspect of the system (Fig. 1)

Consideration of ontological uncertainty as a separate artifact is valuable for safety analysis of HAD vehicles, as it requires different means of representation and mitigation [Gansch and Adee (2020)]. For HAD vehicles operating in the open context, this type of uncertainty can never be completely disregarded over the vehicle lifetime, e.g. a decade ago eScooters were not imagined to be part of road traffic. Even though epistemic and ontological uncertainties originate from lack of knowledge, a general distinction can be made between model parameters (epistemic) and model correctness (ontological) to segregate the two uncertainties (Fig. 1). In order to represent the ontological uncertainty in the system model, the notion of unknown state was introduced [Gansch and Adee (2020)]. However, the following issues have not been addressed so far.

- Separate representation of epistemic and ontological uncertainty in the outcome of safety analyses so that relevant steps such as design modification (model refinement, model rediscovery etc.) can be duly taken.
- Utilization of uncertainties to support SOTIF analysis of a system model.

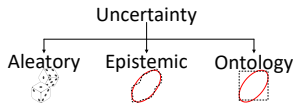


Fig. 1. Uncertainty categorization: Aleatory uncertainty depicts the inherent randomness of the process depicted by the system model. Epistemic uncertainty represents lack of knowledge about the system model and the inexact representation of physical system to models while ontological uncertainty depicts condition of complete ignorance in the model of a relevant aspect of the system.

To this end, we summarize our contribution as follows.

- We introduce Extended Evidential Network (EEN), that represent epistemic, ontological as well as mixed epistemic and ontological uncertainties distinctly.
- We demonstrate the application of EEN for SOTIF analysis.
- We demonstrate and evaluate the applicability of the proposed method by applying it to a perception function case study.
- We also demonstrate how EEN can help in decision making through our case study.

The remainder of the publication is structured as follows: Sec. 2 summarizes the related work and provides an overview of DST. Sec. 3 presents the proposed methodology. Sec. 4 provides the application process of EEN for SOTIF. An application of the proposed methodology on the case study is shown in Sec. 5. Conclusive remarks on this work and future directions are provided in Sec. 6.

2. Related Work

In order to incorporate uncertainties in safety analysis, probabilities traditionally provide the mathematical structure [Hacking (2006); Bernstein and Bernstein (1996); Shafer (1976); Helton (2011)] while directed acyclic graphs (DAGs), e.g. Bayesian networks [Pearl (2014)], provide comprehensible graphical representations [Simon and Weber (2009); Liu et al. (2018); Luxhoj (2013); Cai et al. (2016)]. Use of Bayesian Network (BN) is an established method for dependability applications [Weber et al. (2012); Cai et al. (2018)]. BN uses nodes to represent propositions (random variables), arcs to define direct dependencies between the linked propositions. The strength of these dependencies are quantified by conditional probability values between $[0, 1]$. The directed arc runs from $parent$ to $child$. As depicted in Fig. 2, $X5$ is the parent node of $X6$ with two functioning states $(fail, success)$, one epistemic state $(fail\ or\ success)$ and one ontological state $(unknown)$. When a node is a root (no influence), an a priori probability table is defined. Probability theory and BN are considered sufficient to represent aleatory uncertainty [Simon et al. (2007)]. However, sufficiency of probability theory to represent epistemic uncertainty has been challenged by some authors [Ferson et al. (2015)].
The Dempster-Shafer Theory (DST) or Evidence Theory (ET) is a mathematical theory that structures phenomenon by degree of beliefs (belief masses) on events or states [Dempster (1968); Shafer (1976)]. Conceptually, DST can be viewed as a generalized Bayesian Model [Smets (1993)]. This characteristic increases its applicability on the safety analyses, where BN algorithms are used [Simon et al. (2008)]. DST comprises of the following three attributes.

1. Frame of Discernment Consider the multi-state analysis outcome with n mutually exclusive and exhaustive states. The frame of discernment Ω is the finite set of such elements

$$\Omega = \{y_1, y_2, \ldots, y_n\} \tag{1}$$

In DST, the basic belief assignment (BBA) is calculated on the power set of frame of discernment.

$$2^{\Omega} = \{\emptyset, \{y_1\}, \{y_2\}, \ldots, \{y_n\}, \ldots, \{y_1, y_2\}, \ldots, \{y_1, \ldots, y_n\}\} \tag{2}$$

2. Basic Belief Assignment Information on the outcome states (power set) is assigned by belief

$m(A)$ with the following properties $m : 2^{\Omega} \rightarrow [0, 1]$ and

$$m(\emptyset) = 0 \tag{3}$$

$$\sum_{A \in 2^{\Omega}} m(A) = 1 \tag{4}$$

where A is the subset of the power set of frame of discernment. BBA can be seen as an alternative to probabilities. In this publication we use the term BBA and belief mass for DST, EN and EEN and probabilities for Bayesian Network (BN) parameters. The subsets fulfilling $\{A \in 2^{\Omega} : m(A) > 0\}$ are called focal elements. Full knowledge can be represented by assigning masses to singleton sets of Eq. 2, while assigning mass $m(\Omega) = 1$ represents total ignorance [Aguirre et al. (2013)]. Eq. 3 constrains the outcome elements to the closed world assumption [Reiter (1981)].

3. Belief and Plausibility Measures provide upper and lower bounds on the BBA in DST with the following mathematical structures.

$$bel(B) = \sum_{A|A \subseteq B} m(A) \tag{5}$$

$$pl(B) = \sum_{A|A \cap B \neq \emptyset} m(A) \tag{6}$$

where B is the subset of the power set of frame of discernment. The difference between plausibility and belief function provides a notion of epistemic uncertainty [Agarwal et al. (2004); Simon and Weber (2009); Rakowsky (2007)]. $bel(B)$ can be seen as sum of BBA of all the subsets of Ω that are *fully* in agreement with B, while $pl(B)$ can be regarded as sum of BBA of all the subsets of Ω that are *fully or partially* in agreement with B [Aguirre et al. (2013)]. For singleton subsets of frame of discernment Ω, where BBA and belief functions are same, plausibility functions can model the lack of knowledge postulation. However, when categorized into ontological and epistemic, it becomes challenging to comprehend which uncertainty among epistemic and ontological is represented by the difference of unique plausibility and belief function.

Evidential Network are also DAGs which represent uncertainties as randomness (aleatory) and lack of knowledge (epistemic) [Simon et al. (2008)]. Instead of probability theory, they incorporate evidence theory [Dempster (1968); Shafer (1976)]. They use nodes to represent random variables, arcs to define direct dependence between nodes and conditional belief mass to quantify dependency. When a node is a root, an a priori belief mass table is defined. Moreover, distinction is made for leaf node by providing belief and plausibility measures (Fig. 2). The dashed arrows signifies the fact that there is no influence involved in those connection.

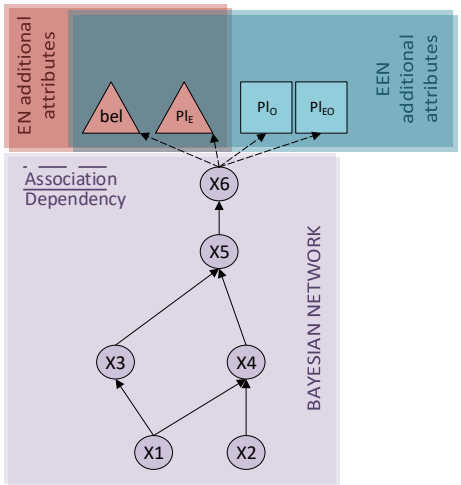
3. Proposed Approach for Extended Uncertainty Representation

In this section, we propose an approach that extends the representation of uncertainties using DST by incorporating ontological uncertainty. We also extend evidential networks to incorporate both epistemic and ontological uncertainties separately through *extended evidential network (EEN)*. We redefine the DST attributes for our approach as follows.

3.0.1. *1. Frame of Discernment*

Consider the multi-state analysis outcome with the inclusion of ontological uncertainty through state u [Gansch and Adee (2020)]. The state u refers to all those states that may not have been considered during system design/ analysis. Eq. 1 can be rewritten as

$$\Omega = \{y_1, y_2, \ldots, y_n, u\} \tag{7}$$



X5	X6= Fail	X6= Success	X6=Fail or Success	X6= Unknown
Fail	0.7	0.1	0.15	0.05
Success	0.5	0.3	0.1	0.1
Fail or Success	0.2	0.6	0.2	0
Unknown	0.05	0.05	0.2	0.7

Fig. 2. Example of Bayesian network: Directed acyclic graph with nodes (X1,. . . ,X6) and arcs represented by arrows. Evidential network adds two additional nodes of belief and plausibility. Extended evidential network adds further nodes to represent notion of ontological uncertainty. Exemplary conditional probability table for X6 given.

In DST, the BBA is performed on the power set of frame of discernment.

$$2^{\Omega} = \{\emptyset, \{y_1\}, \{y_2\}, \ldots, \{y_n\}, \{u\}, \ldots, \{y_1, y_2\}, \ldots, \{y_1, \ldots, y_n, u\}\} \quad (8)$$

We also define three subsets of Eq. 8.

$$E = \{\{y_1, y_2\}, \{y_1, y_3\}, \ldots \{y_1, y_n\}, \ldots, \{y_2, y_3\}, \ldots \{y_1, \ldots, y_n\}\} \quad (9)$$

$$O = \{\{u\}\} \quad (10)$$

$$EO = \{\{y_1, u\}, \{y_2, u\}, \ldots \{y_1, y_2, u\}, \ldots \{y_1, \ldots, y_n, u\}\} \quad (11)$$

Here Eq. 9, 10 and 11 represent the epistemic, ontological and mixed epistemic and ontological uncertainty sets respectively. Mixed epistemic and ontological set (Eq. 11) includes the outcome states which are epistemic and ontological uncertain.

3.0.2. *2. Belief and Plausibility Measures*

As we discussed in the previous section, belief measure $bel(B)$ can be viewed as sum of BBA of all the subsets of Ω that are fully in agreement with B and do not contribute to uncertainties, hence belief measure bel (Eq. 6) remains the same in our proposed approach. We define the following presumptions about the Eq. 8 before defining plausibility functions.

(1) All singleton subsets are considered exempted from the uncertainty except u.
(2) Element u is considered as ontological uncertainty (O).
(3) Non-singular subsets not containing u are considered epistemic uncertainty of the system model (E).
(4) Non-singular subsets containing u are considered mixed ontological and epistemic uncertainty of the system (EO).

Based on the above presumptions and Eq. (9-11), we define the multiple plausibility functions to individually characterize uncertainties in the analysis outcome. $\{\forall B : B \subset 2^{\Omega} \wedge |B| = 1\}$

$$bel(B) = \sum_{A|A \subseteq B} m(A) \quad (12)$$

$$pl_E(B) = bel(B) + \sum_{\substack{A|A \cap B \neq \emptyset \\ \wedge \ A \in E}} m(A) \quad (13)$$

$$pl_O(B) = bel(B) + \sum_{\substack{A|A \cap B \neq \emptyset \\ \wedge \ A \in O}} m(A) \quad (14)$$

$$pl_{EO}(B) = bel(B) + \sum_{\substack{A|A \cap B \neq \emptyset \\ \wedge \ A \in EO}} m(A) \quad (15)$$

The method we present here is applicable on the quantification of plausibility functions of the original frame of discernment "Ω" states only. Separate representation of epistemic and ontological uncertainty in EEN can assist in choosing the right improvement measure. For example, model refinement (changing model parameters) and model rediscovery (changing the model altogether) can be associated to epistemic and ontological uncertainty, respectively. Mixed epistemic and ontological uncertainty may serve the case where both model refinement and rediscovery require improvement. In other words, this categorization in the safety analysis may assist in the improvement measures by indicating the aspect to be improved (e.g. better parameterization of a model or redesigning a model all together).
Having provided with the approach to discriminate between epistemic and ontological uncertainties, we now provide the definition of Extended Evidential Network.

Definition 3.1. Extended Evidential Networks (EENs) are Directed Acyclic Graphs (DAGs). They represent uncertainties as randomness (aleatory), lack of knowledge (epistemic) and state of complete ignorance (ontological). They use nodes to represent random variables, arcs to define direct dependence between nodes and conditional belief mass to quantify dependency. When a node is a root, an a priori belief mass table is defined. Leaf node represents the query of the network. Moreover, leaf nodes are distinct as belief and *multiple plausibility measures* are provided (Fig. 2).

4. Method Application Process on SOTIF

As defined in ISO/ PAS 21448, SOTIF analysis focuses on situational awareness. The situational

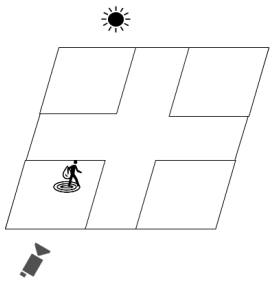


Fig. 3. Scenario: A low sun inclination is faced by a front facing camera, while a pedestrian crosses the road along side a puddle

awareness is derived from complex sensors and processing algorithms, which may not be able to comprehend all the situations at all times as termed as functional insufficiencies and performance limitation [ISO/PAS21448 (2019)].
A sound understanding of the nominal function including its operational environment is essential for the application of the methodology. The system function can be decomposed to perception, control and actuation functions [ISO/PAS21448 (2019)]. We apply the safety analysis method in accordance with the clause 7, clause 8, annex B and annex D of the SOTIF standard [ISO/PAS21448 (2019)] using the following steps.

(1) **Hazardous Behavior:** Potential hazardous behavior caused by the intended functionality is gathered. This may include but not limited to the following.
   (a) The inability of the function to correctly comprehend the situation and operate safely; this also includes functions that use machine learning algorithms.
   (b) Insufficient robustness of the function, system, or algorithm with respect to sensor input variations, heuristics used for fusion, or diverse environmental conditions.

   The hazardous behavior may or may not lead to a harm.
(2) **Scenario Level Triggering Condition:** Triggering conditions aggravate the occurrence of SOTIF hazardous behavior. All those conditions at scenario level that may lead to triggering conditions are listed. This also include environmental effects and foreseeable misuse [ISO/PAS21448 (2019)]. Some of the triggering conditions may include the following.
   (a) Road/ traffic conditions
   (b) Weather conditions
   (c) Other triggering conditions
(3) **Insufficiencies of specification and performance limitation** that may contribute to occurrence of SOTIF hazardous behavior are defined at system, sub system and component level. Some examples for such insufficiencies and limitations are
   (a) System level detection mismatch e.g.
      i. The mismatch of radar-based obstacle and visual (front camera) based obstacle for AEB system.
   (b) Sensor performance limitation e.g.
      i. Incomplete perception of the scene
   (c) Algorithm accuracy e.g.
      i. Insufficiency of the decision algorithm
      ii. Insufficient training data

   We neither claim nor provide an exhaustive list of triggering conditions, insufficiencies of specification and performance limitation.
(4) **Extended Evidential Network:** An EEN model is constructed out of the information from previous steps. The steps further taken are as follows.
   (a) Hierarchal dependency between hazardous behavior, triggering conditions and insufficiencies of specifications and performance limitations is established.
   (b) A BN is constructed i.e. nodes representing hazardous behavior, triggering condition and insufficiencies of specifications and performance limitations and arcs representing the dependency.
   (c) Belief masses for root nodes and conditional belief tables (CBT) for intermediate nodes are assigned to quantify the extent of dependency.
   (d) Belief masses of the leaf node is calculated by propagation.
   (e) bel, pl_E, pl_O and pl_{EO} functions are calculated (Eqs. 12-15) for the leaf node states, thus constructing the EEN.
(5) **Uncertainty Calculation:** Calculation for epistemic, ontological and mixed epistemic and ontological uncertainty is then performed.

$$Un_X = pl_X - bel \tag{16}$$

   where X represents E, O or OE and Un represent epistemic, ontological and mixed epistemic and ontological uncertainty respectively.
(6) **Risk & Uncertainty Analysis:** Resulting model and uncertainties calculated can be used for SOTIF improvement measures e.g. decision about design improvement (e.g. model refinement (epistemic) and model rediscovery (ontological)), residual risk calculation and runtime analysis and adaptation. We provide a brief account on the design improvement measures examples in the next section.

5. Scenario Modeling and Case Study for SOTIF

In order to illustrate our methodology, we consider a perception function. We take a simple scenario in which a low inclined sun faces the camera used for perception. A neural network classifier is used for classification. A water puddle besides human who intends to cross the road, can **occlude** the camera function resulting in wrong/miss classification (Fig. 3). We apply the steps from the previous section.

(1) **Hazardous Behavior:** In the given scenario, **incorrect perception** may lead to unwanted

Table 1. Example for calculating belief and plausibility functions for perception node (Fig. 4).

Perception $A \subseteq 2^{\Omega}$	belief bel(A)	plausibility pl_E(A)	plausibility pl_O(A)	plausibility pl_{EO}(A)
{Human}	0.5051	0.6334	0.5051	0.6698

Table 2. Improvement measures in accordance with ISO/ PAS 21448 based on the predicted uncertainties

Uncertainty Type	SOTIF Improvement Measure
Epistemic (Un_E)	Improved sensor calibration
	Improved computing power
	Additional information for better training of the model
Ontological (Un_O)	New sensors inclusion for sensing
	Different model altogether
Mixed (Un_{EO})	Any combination of epistemic and ontological

acceleration or deceleration which in turn can potentially lead to a harm. Thus perception is the SOTIF hazardous behavior in this study

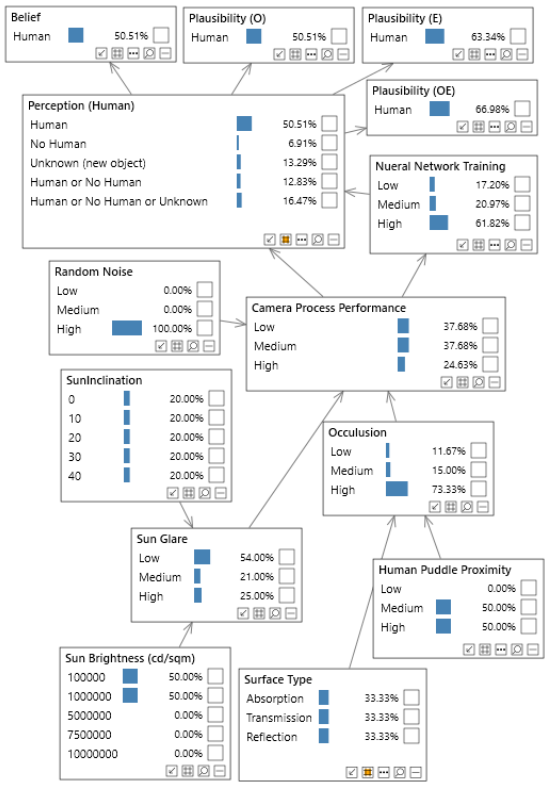


Fig. 4. Extended Evidential Network of the scenario shown in Fig. 3

(Fig. 4). At state level of perception node, we define the following states.

(a) Human
(b) No human
(c) Unknown object
(d) human or no human
(e) human or no human or unknown object

The frame of discernment of the perception node contains the states human H, no human NH and unknown object U and mathematically represented as follows.

$$\Omega = \{H, NH, U\} \tag{17}$$

A frame of discernment with 3 elements results in 8 combinatorial elements, , three of which are considered mixed epistemic and ontological combinatorial states. We define the set of focal element as

$$2^{\Omega}_{focal} = \{\{H\}, \{NH\}, \{U\}, \{H, NH\}, \{H, NH, U\}\} \tag{18}$$

Moreover, set Eqs. 9-11 for the perception node states are.

$$E = \{\{H, NH\}\} \tag{19}$$

$$O = \{\{U\}\} \tag{20}$$

$$EO = \{\{H, NH, U\}\} \tag{21}$$

(2) **Scenario Level Triggering Condition:** Scenario level triggering conditions relevant to hazardous behavior in the case study are as follows.

(a) Low Sun inclination, directly facing in the camera lens
(b) Clear sky increasing the brightness (decreasing contrast)
(c) Highly reflective road surface
(d) Human and puddle proximity

(3) **Insufficiencies of specification and performance limitation:** This study considers camera for situational awareness, hence the only listed component level insufficiencies of specification and performance limitation are.
   (a) Performance limitation
      i. We include occlusion and random noise of the camera process as the main factors of sensor performance limitation
   (b) Insufficiencies of the specification
      i. Insufficient provision of training data in which human is in the proximity of puddle as training example for the neural network classifier.

(4) **Extended Evidential Network:** As a first step towards derivation of EEN, we establish hierarchal dependencies between hazardous behavior, triggering conditions, insufficiencies of specification and performance limitations e.g. the proposition $p1$: $low\ sun\ inclination\ may\ potentially\ causes\ occlusion\ and\ sun\ glare$, their strength being dependent on sun inclination. We then construct BN with arcs representing the dependencies and nodes representing the hazardous behavior, triggering conditions, insufficiencies of specification and performance limitations e.g., the proposition $p1$ is modeled as explicit nodes i.e., $sun\ inclination$, $sun-glare$ and $occlusion$ (Fig. 4). We provide arbitrary values to belief masses and CBTs to represent the extent of the dependency as the aim of this study is to demonstrate the application of the proposed method. However, these CBTs can be constructed using different methods [Perkusich et al. (2013); Nunes et al. (2018); Chin et al. (2009)]. Moreover, sensor values and other data streams can be used as input for root nodes at runtime, thus using EEN as a safety supervisor at runtime.
In this analysis $Perception : Human$ value defines the belief on the nominal functionality. The deviation from nominal functionality (incorrect perception) is quantified by the belief and plausibility functions using Eq. 12-15 (Table. 1).

(5) **Uncertainty Calculation:** Based on difference between plausibility and belief functions (Table 1), we calculate epistemic, ontological and mixed epistemic and ontological uncertainties categories for the state of interest of the hazardous behavior node.

(6) **Risk & Uncertainty Analysis:** Table 1 summarizes the result of uncertainty based safety analysis that we propose in this publication. We provide some examples as design improvement steps for SOTIF (Table 2) that can applied based on the calculated uncertainties. For example, the system modeler may select $improved\ sensor\ calibration$ and $training\ new\ model\ for\ classification$ based on the results, since mixed epistemic and ontological uncertainty is the most influential for this use case.

6. Conclusion and Future Work

Providing dependability assessment to safety of the intended functionality (SOTIF) is an important aspect in the overall safety argumentation of highly automated driving. Uncertainty based safety analysis provide a promising direction to provide SOTIF argumentation. We proposed a novel approach for SOTIF analysis through uncertainty modeling. The proposed method provides multiple plausibility functions in order to accommodate representation of ontological uncertainty through evidence theory and assists in SOTIF oriented improvement measures to be taken.
The proposed method was supported with an application on a use case, in accordance with the propositions from SOTIF standard. SOTIF oriented improvement measures were also provided, based on the analysis results.
We believe that EEN can be used as a tool to perform runtime reconfiguration of highly automated driving functions, using the uncertainty values of EEN provided at runtime. In future, we intend to assess the applicability of the EENs on runtime analysis and adaptation of HAD functions, e.g. adaptive cruise control.
A prodigious problem associated to larger BN (or EEN) is the exponential growth of conditional probability tables (CPTs) parameters. We intend to use expert elicitation based semi automated techniques for CPT elicitation in future.

Acknowledgement

The research leading to these results has received funding from the X research and innovation program under Y agreement.

References

Agarwal, H., J. E. Renaud, E. L. Preston, and D. Padmanabhan (2004). Uncertainty quantification using evidence theory in multidisciplinary design optimization. *Reliability Engineering & System Safety 85*(1-3), 281–294.

Aguirre, F., M. Sallak, W. Schön, and F. Belmonte (2013). Application of evidential networks in quantitative analysis of railway accidents. *Proceedings of the Institution of Mechanical En-*

gineers, Part O: Journal of Risk and Reliability 227(4), 368–384.

Bernstein, P. L. and P. L. Bernstein (1996). *Against the gods: The remarkable story of risk*. Wiley New York.

Burton, S., I. Habli, T. Lawton, J. McDermid, P. Morgan, and Z. Porter (2020). Mind the gaps: Assuring the safety of autonomous systems from an engineering, ethical, and legal perspective. *Artificial Intelligence 279*, 103201.

Cai, B., X. Kong, Y. Liu, J. Lin, X. Yuan, H. Xu, and R. Ji (2018). Application of bayesian networks in reliability evaluation. *IEEE Transactions on Industrial Informatics 15*(4), 2146–2157.

Cai, B., H. Liu, and M. Xie (2016). A real-time fault diagnosis methodology of complex systems using object-oriented bayesian networks. *Mechanical Systems and Signal Processing 80*, 31–44.

Chang, W., S. Burton, C.-W. Lin, Q. Zhu, L. Gauerhof, and J. McDermid (2020). Intelligent and connected cyber-physical systems: A perspective from connected autonomous vehicles. In *Intelligent Internet of Things*, pp. 357–392. Springer.

Chin, K.-S., D.-W. Tang, J.-B. Yang, S. Y. Wong, and H. Wang (2009). Assessing new product development project risk by bayesian network with a systematic probability generation methodology. *Expert Systems with Applications 36*(6), 9879–9890.

Dempster, A. P. (1968). A generalization of bayesian inference. *Journal of the Royal Statistical Society: Series B (Methodological) 30*(2), 205–232.

Ferson, S., V. Kreinovich, L. Grinzburg, D. Myers, and K. Sentz (2015). Constructing probability boxes and dempster-shafer structures. Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Gansch, R. and A. Adee (2020). System theoretic view on uncertainties. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1345–1350. IEEE.

Hacking, I. (2006). *The emergence of probability: A philosophical study of early ideas about probability, induction and statistical inference*. Cambridge University Press.

Helton, J. C. (2011). Quantification of margins and uncertainties: Conceptual and computational basis. *Reliability Engineering & System Safety 96*(9), 976–1013.

ISO/PAS21448 (2019). ISO/PAS 21448:2019 Road vehicles – Safety of the intended functionality. pp. 54.

Leveson, N. and J. Thomas (2013). An stpa primer. *Cambridge, MA*.

Liu, Q., A. Tchangani, F. Pérès, and V. Gonzalez-Prida (2018). Object-oriented bayesian network for complex system risk assessment. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 232*(4), 340–351.

Luxhoj, J. T. (2013). Predictive analytics for modeling uas safety risk. *SAE International Journal of Aerospace 6*(2013-01-2104), 128–138.

Nunes, J., M. Barbosa, L. Silva, K. Gorgônio, H. Almeida, and A. Perkusich (2018). Issues in the probability elicitation process of expert-based bayesian networks. In *Enhanced Expert Systems*. IntechOpen.

Pearl, J. (2014). *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Elsevier.

Perkusich, M., A. Perkusich, and H. O. de Almeida (2013). Using survey and weighted functions to generate node probability tables for bayesian networks. In *2013 BRICS Congress on Computational Intelligence and 11th Brazilian Congress on Computational Intelligence*, pp. 183–188. IEEE.

Rakowsky, U. K. (2007). Fundamentals of the dempster-shafer theory and its applications to reliability modeling. *international journal of Reliability, Quality and Safety Engineering 14*(06), 579–601.

Reiter, R. (1981). On closed world data bases. In *Readings in artificial intelligence*, pp. 119–140. Elsevier.

Shafer, G. (1976). *A mathematical theory of evidence*, Volume 42. Princeton university press.

Simon, C. and P. Weber (2009). Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge. *IEEE Transactions on Reliability 58*(1), 69–87.

Simon, C., P. Weber, and A. Evsukoff (2008). Bayesian networks inference algorithm to implement dempster shafer theory in reliability analysis. *Reliability Engineering & System Safety 93*(7), 950–963.

Simon, C., P. Weber, and E. Levrat (2007). Bayesian networks and evidence theory to model complex systems reliability.

Smets, P. (1993). Belief functions: the disjunctive rule of combination and the generalized bayesian theorem. *International Journal of approximate reasoning 9*(1), 1–35.

Weber, P., G. Medina-Oliva, C. Simon, and B. Iung (2012). Overview on bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence 25*(4), 671–682.