Hi-Drive – 1st Summer School, Porto Heli, Greece

Towards a Quantitative SOTIF Validation of Automated Driving Systems

Lina Putze
German Aerospace Center (DLR) e.V.
Institute of Systems Engineering for Future Mobility

DLR

How does the ISO 21448:2022 require or suggest performing a quantitative SOTIF validation?

How does the ISO 21448:2022 require or suggest performing a quantitative SOTIF validation?
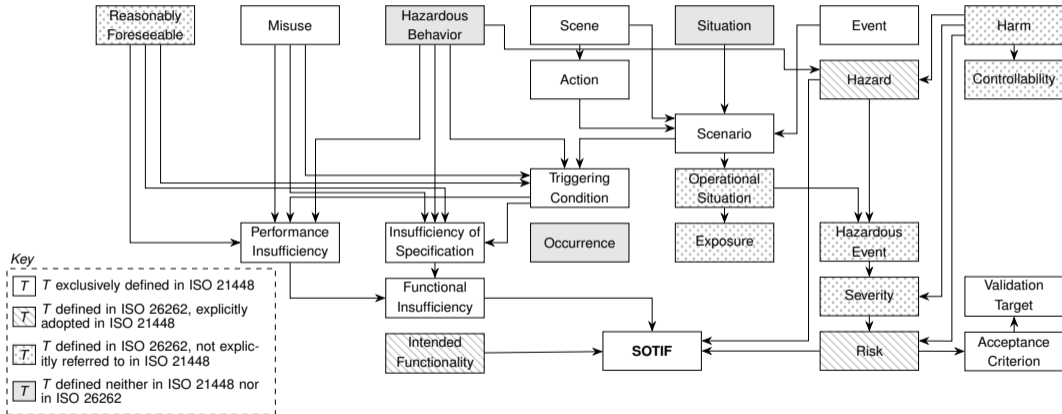
To answer this, we...

(1) study and adjust the ISO 21448's terminological risk framework

(2) examine the relevant normative and informative parts on SOTIF validation and provide constructive suggestions for improvement

> How does the ISO 21448:2022 require or suggest performing a quantitative SOTIF validation?
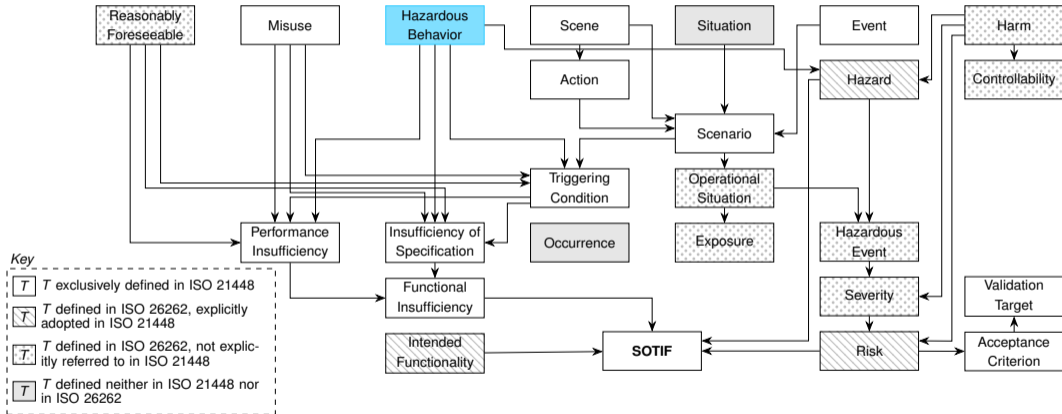
To answer this, we...

(1) study and adjust the ISO 21448's terminological risk framework

(2) examine the relevant normative and informative parts on SOTIF validation and provide constructive suggestions for improvement
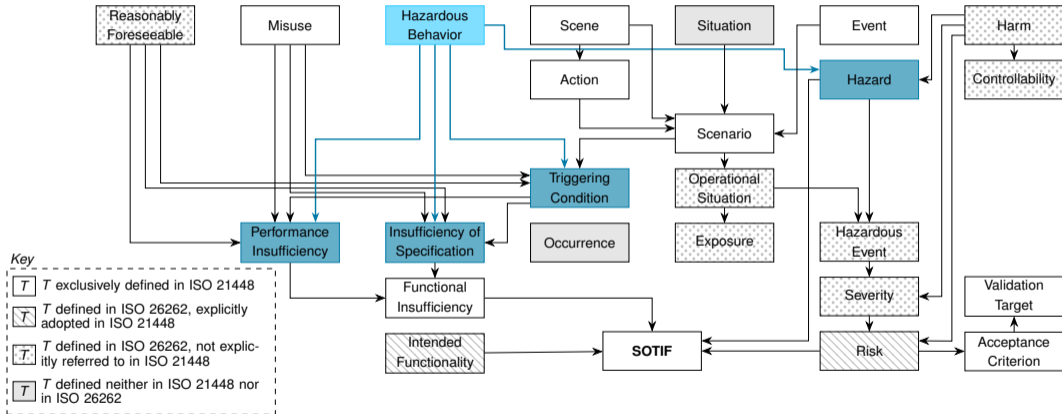
Lina Putze, Towards a Quantitative SOTIF Validation of Automated Driving Systems, 07.09.2023

```
Functional Insufficiency ◄─────────────── Hazardous Behavior ───► Hazard ◄─── Harm
                                    │
                                    ▼
                          Triggering Condition
```

Relations of Definitions

Hazardous Behavior

Functional Insufficiency

'limitation of the technical capability [. . .]' or 'spec-ification, possibly incom-plete, contributing to either a hazardous behavior or an inability to prevent or detect and mitigate a reasonably foresee-able indirect misuse when activated by one or more triggering con-ditions' [ISO 21448]

Triggering Condition

'specific condition of a scenario that serves as an initiator for a subse-quent system reaction contributing to either a hazardous behavior or an inability to prevent or detect and mitigate a reasonably foreseeable in-direct misuse' [ISO 21448]

Hazard

'potential source of harm caused by mal-functioning behavior of the item' [ISO 26262], '[. . .] caused by the hazardous behavior at the vehicle level' [ISO 21448]

Harm

'physical injury or dam-age to the health of persons' [ISO 26262]

DLR

Functional Insufficiency ← **Hazardous Behavior** ← **Hazard** ← **Harm**

'limitation of the technical capability [. . .]' or 'spec-ification, possibly incom-plete, contributing to either a <u>hazardous behavior</u> or an inability to prevent or detect and mitigate a reasonably foresee-able indirect misuse when activated by one or more triggering con-ditions' [ISO 21448]

Behavior of the func-tionality which can lead to a hazard

Triggering Condition

'specific condition of a scenario that serves as an initiator for a subse-quent system reaction contributing to either a <u>hazardous behavior</u> or an inability to prevent or detect and mitigate a reasonably foreseeable in-direct misuse' [ISO 21448]

'potential source of harm caused by mal-functioning behavior of the item' [ISO 26262], '[. . .] caused by the <u>hazardous behavior</u> at the vehicle level' [ISO 21448]

'potential source of harm' [ISO/IEC Guide 51]

'physical injury or dam-age to the health of persons' [ISO 26262]

Hazardous Event

'combination of
a <u>hazard</u> and an
<u>operational situation</u>'
[ISO 26262]

Relations of Definitions

Hazardous Event

Event	'combination of a <u>hazard</u> and an <u>operational situation</u>' [ISO 26262]	Hazard
'occurrence at a point in time' [ISO 21448]		

Hazard
+
'scenario containing conditions in which the hazard can lead to harm'
Hazardous Event
[ISO 21448, Figure 12]

Relations of Definitions

Hazardous Event

Event		Hazard

Event

'occurrence at a point in time' [ISO 21448]

'combination of a hazard and an operational situation' [ISO 26262]

Hazard

+

Hazardous Event

'scenario containing conditions in which the hazard can lead to harm'

[ISO 21448, Figure 12]

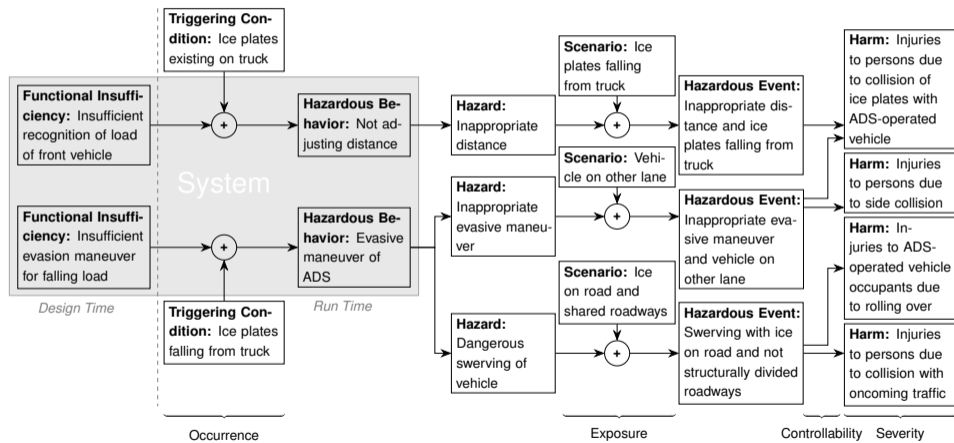event that is a combination of a hazard and a scenario containing conditions in which the hazard can lead to harm

How does the ISO 21448:2022 require or suggest performing a quantitative SOTIF validation?

To answer this, we...

(1) study and adjust the ISO 21448's terminological risk framework

(2) examine the relevant normative and informative parts on SOTIF validation and provide constructive suggestions for improvement

How does the ISO 21448:2022 require or suggest performing a quantitative SOTIF validation?

To answer this, we...

(1) study and adjust the ISO 21448's terminological risk framework

(2) examine the relevant normative and informative parts on SOTIF validation and provide constructive suggestions for improvement

DLR

Relevant clauses within the normative part:

Relevant clauses within the normative part:

Clause 6: Identification and evaluation of hazards

Relevant clauses within the normative part:

Clause 6: Identification and evaluation of hazards

Clause 7: Identification and evaluation of potential functional insufficiencies and potential triggering conditions

Relevant clauses within the normative part:

Clause 6: Identification and evaluation of hazards

Clause 7: Identification and evaluation of potential functional insufficiencies and potential triggering conditions

Clause 9: Definition of the verification and validation strategy

Relevant clauses within the normative part:

Clause 6: Identification and evaluation of hazards

Clause 7: Identification and evaluation of potential functional insufficiencies and potential triggering conditions

Clause 9: Definition of the verification and validation strategy

Remark: The normative part of the ISO 21448 is rather sparse with requirements compared to other standards

Clause 6: Identification and evaluation of hazards

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains

DLR

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains
    - severity, controllability: treated as binary variables

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains
  - severity, controllability: treated as binary variables
  - exposure: not considered

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains
    - severity, controllability: treated as binary variables
    - exposure: not considered
    - ✗ general reasoning why this simplification of the ASIL classification should be sufficient is missing

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains
    - severity, controllability: treated as binary variables
    - exposure: not considered
    - ✗ general reasoning why this simplification of the ASIL classification should be sufficient is missing
- acceptance criteria must be formulated for SOTIF-related hazardous events

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains
    - severity, controllability: treated as binary variables
    - exposure: not considered
    - ✗ general reasoning why this simplification of the ASIL classification should be sufficient is missing
- acceptance criteria must be formulated for SOTIF-related hazardous events
    - both qualitative <u>and</u> quantitative acceptance criteria are permitted

Clause 6: Identification and evaluation of hazards

- no ASIL classification required unlike in the ISO 26262
- idea of considering severity, exposure and controllability remains
  - severity, controllability: treated as binary variables
  - exposure: not considered
  - ✗ general reasoning why this simplification of the ASIL classification should be sufficient is missing
- acceptance criteria must be formulated for SOTIF-related hazardous events
  - both qualitative <u>and</u> quantitative acceptance criteria are permitted
  - quantitative acceptance criteria are exclusively mentioned: GAMAB, PRB, ALARP, MEM

Clause 7: Identification and evaluation of potential functional insufficiencies and potential triggering conditions

Clause 7: Identification and evaluation of potential functional insufficiencies and potential triggering conditions

- systematic qualitative or quantitative analysis of potential functional insufficiencies and associated triggering conditions demanded

DLR

Clause 7: Identification and evaluation of potential functional insufficiencies and potential triggering conditions

- systematic qualitative or quantitative analysis of potential functional insufficiencies and associated triggering conditions demanded
- for scenarios containing identified triggering conditions SOTIF-achievability needs to be demonstrated

Clause 9: Definition of the verification and validation strategy

Clause 9: Definition of the verification and validation strategy

- validation targets should be derived to argue that the acceptance criteria are fullfilled

Clause 9: Definition of the verification and validation strategy

- validation targets should be derived to argue that the acceptance criteria are fullfilled
- strategy to provide evidence that validation targets are met must be provided

Clause 9: Definition of the verification and validation strategy

- validation targets should be derived to argue that the acceptance criteria are fullfilled

- strategy to provide evidence that validation targets are met must be provided

- an example for deriving a validation target from a given quantitative acceptance criterion is given in Annex C.2 leading to the following decomposition

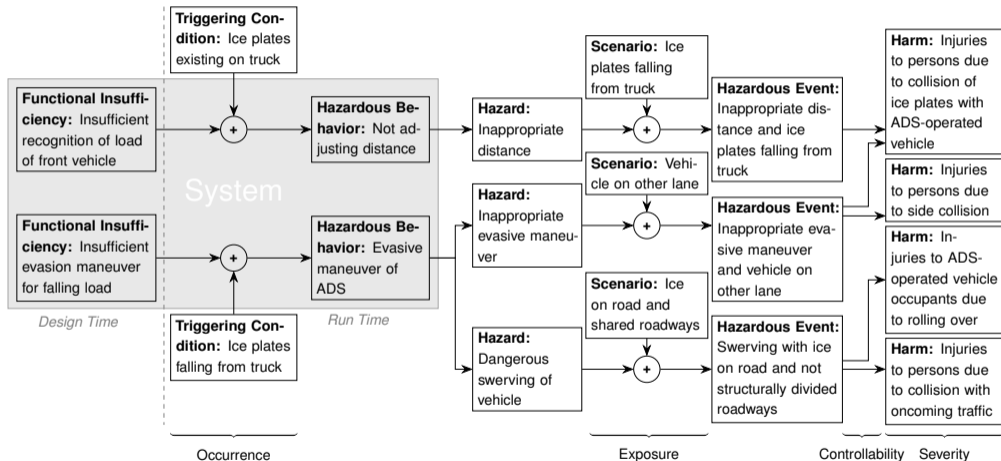$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

DLR

Clause 9: Definition of the verification and validation strategy

- validation targets should be derived to argue that the acceptance criteria are fullfilled

- strategy to provide evidence that validation targets are met must be provided

- an example for deriving a validation target from a given quantitative acceptance criterion is given in Annex C.2 leading to the following decomposition

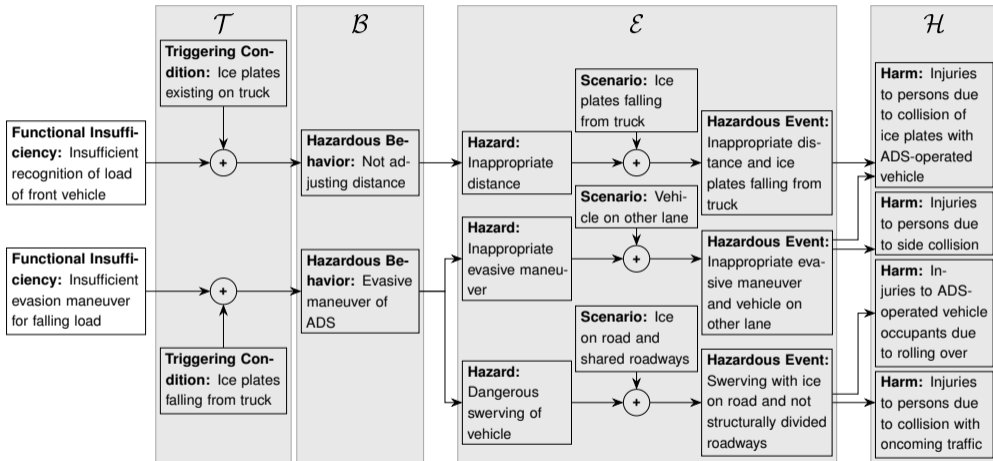$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

✗ deficient use of conditional probabilities

Clause 9: Definition of the verification and validation strategy

- validation targets should be derived to argue that the acceptance criteria are fullfilled

- strategy to provide evidence that validation targets are met must be provided

- an example for deriving a validation target from a given quantitative acceptance criterion is given in Annex C.2 leading to the following decomposition

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

    ✗ deficient use of conditional probabilities

    ✗ probabilities are claimed to be known from field data

DLR

Clause 9: Definition of the verification and validation strategy

- validation targets should be derived to argue that the acceptance criteria are fullfilled

- strategy to provide evidence that validation targets are met must be provided

- an example for deriving a validation target from a given quantitative acceptance criterion is given in Annex C.2 leading to the following decomposition

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

- ✗ deficient use of conditional probabilities

- ✗ probabilities are claimed to be known from field data

- ✗ 1-to-1 relation between hazardous behavior and harm is implicitly assumed

Validation of the SOTIF using Quantitative Acceptance Criteria

$\mathcal{T}$

Triggering Condition: Ice plates existing on truck

Functional Insufficiency: Insufficient recognition of load of front vehicle

Functional Insufficiency: Insufficient evasion maneuver for falling load

Triggering Condition: Ice plates falling from truck

$\mathcal{B}$

Hazardous Behavior: Not adjusting distance

Hazardous Behavior: Evasive maneuver of ADS

$\mathcal{E}$

Hazard: Inappropriate distance

Scenario: Ice plates falling from truck

Hazardous Event: Inappropriate distance and ice plates falling from truck

Hazard: Inappropriate evasive maneuver

Scenario: Vehicle on other lane

Hazardous Event: Inappropriate evasive maneuver and vehicle on other lane

Hazard: Dangerous swerving of vehicle

Scenario: Ice on road and shared roadways

Hazardous Event: Swerving with ice on road and not structurally divided roadways

$\mathcal{H}$

Harm: Injuries to persons due to collision of ice plates with ADS-operated vehicle

Harm: Injuries to persons due to side collision

Harm: Injuries to ADS-operated vehicle occupants due to rolling over

Harm: Injuries to persons due to collision with oncoming traffic

Lina Putze, Towards a Quantitative SOTIF Validation of Automated Driving Systems, 07.09.2023
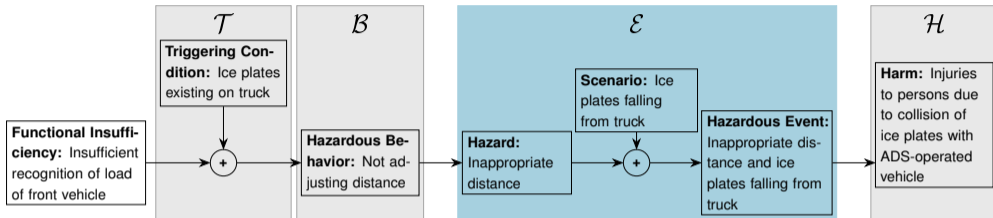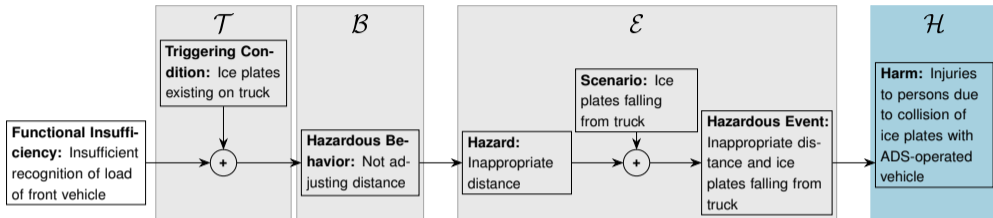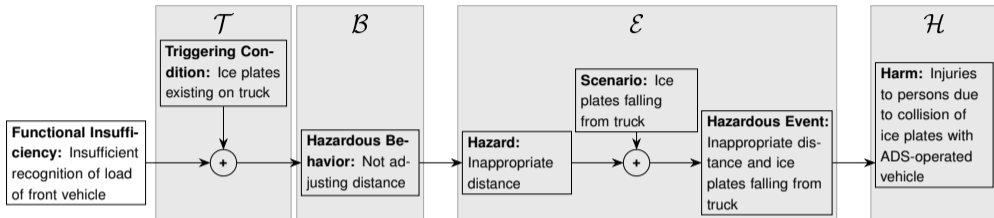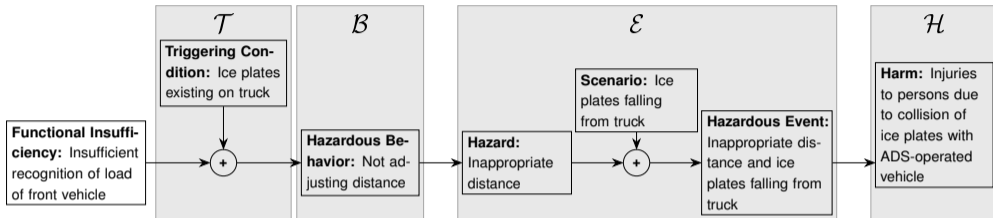
Validation of the SOTIF using Quantitative Acceptance Criteria

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$
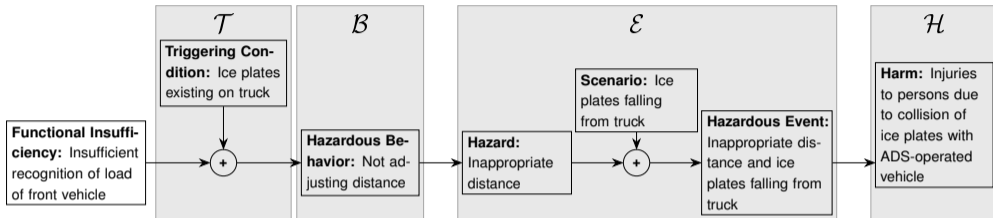
- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T}) P(\mathcal{B}|\mathcal{T}) P(\mathcal{E}|\mathcal{B}, \mathcal{T}) P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T})$$

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$
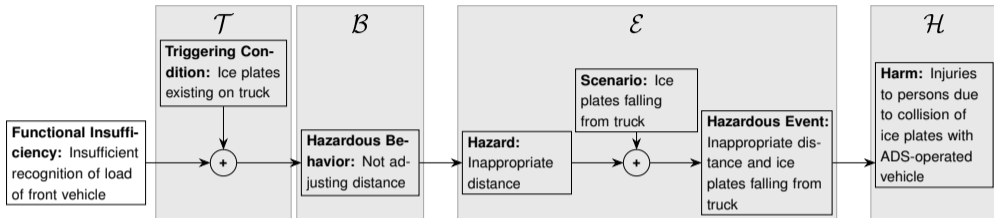
DLR

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T}) P(\mathcal{B}|\mathcal{T}) P(\mathcal{E}|\mathcal{B}, \mathcal{T}) P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T})$$

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$

Validation of the SOTIF using Quantitative Acceptance Criteria
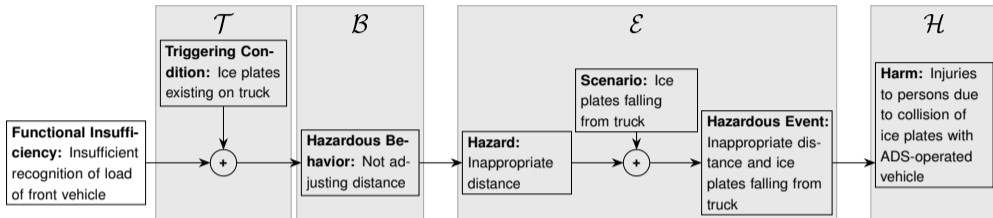

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$

- Probability of occurrence of a given harm $\mathcal{H}$ in combination with a severity level $\mathcal{S}$:

$$P(\mathcal{H},\mathcal{S}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})P(\mathcal{S}|\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$$

Validation of the SOTIF using Quantitative Acceptance Criteria

- Probability of occurrence of a given harm $\mathcal{H}$:

$$P(\mathcal{H}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$$

- Probability of occurrence of a given harm $\mathcal{H}$ in combination with a severity level $\mathcal{S}$:

$$P(\mathcal{H},\mathcal{S}) \leq \sum_{\mathcal{E},\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B},\mathcal{T})P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})P(\mathcal{S}|\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$$

Validation of the SOTIF using Quantitative Acceptance Criteria
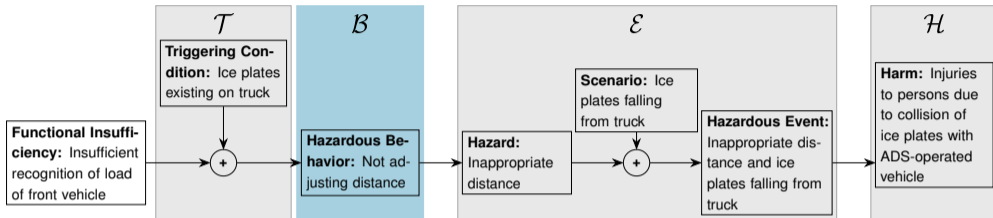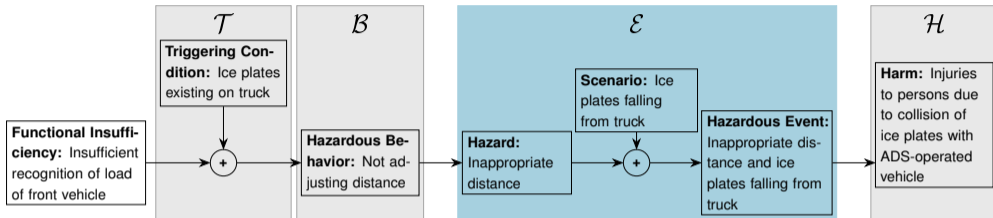

✗ Decomposition given in the Annex C.2 of the ISO 21448:

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

✓ Approach proposed:

$$P(\mathcal{H}, \mathcal{S}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T}) P(\mathcal{B}|\mathcal{T}) P(\mathcal{E}|\mathcal{B}, \mathcal{T}) P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T}) P(\mathcal{S}|\mathcal{H}, \mathcal{E}, \mathcal{B}, \mathcal{T})$$
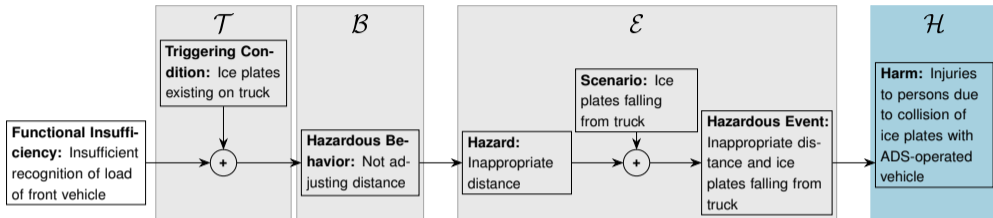
✗ Decomposition given in the Annex C.2 of the ISO 21448:

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

✓ Approach proposed:

$$P(\mathcal{H}, \mathcal{S}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T}) P(\mathcal{B}|\mathcal{T}) P(\mathcal{E}|\mathcal{B}, \mathcal{T}) P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T}) P(\mathcal{S}|\mathcal{H}, \mathcal{E}, \mathcal{B}, \mathcal{T})$$
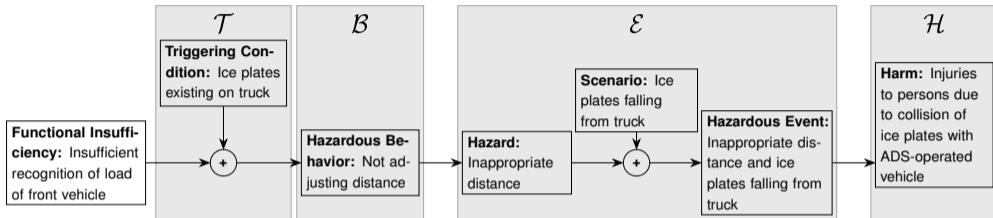
✗ Decomposition given in the Annex C.2 of the ISO 21448:

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

✓ Approach proposed:

$$P(\mathcal{H}, \mathcal{S}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{E}|\mathcal{B}, \mathcal{T})P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T})P(\mathcal{S}|\mathcal{H}, \mathcal{E}, \mathcal{B}, \mathcal{T})$$

Validation of the SOTIF using Quantitative Acceptance Criteria

✗ Decomposition given in the Annex C.2 of the ISO 21448:

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

✓ Approach proposed:

$$P(\mathcal{H}, \mathcal{S}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T}) P(\mathcal{B}|\mathcal{T}) P(\mathcal{E}|\mathcal{B}, \mathcal{T}) P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T}) P(\mathcal{S}|\mathcal{H}, \mathcal{E}, \mathcal{B}, \mathcal{T})$$

Validation of the SOTIF using Quantitative Acceptance Criteria
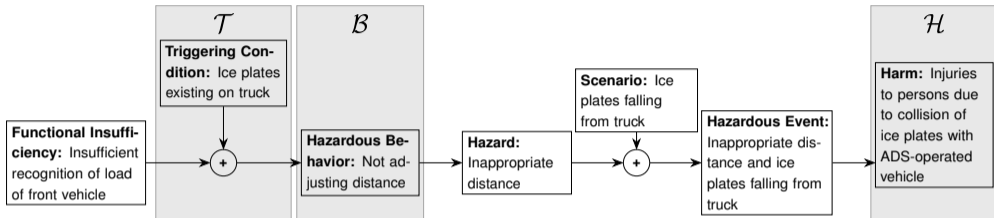

✗ Decomposition given in the Annex C.2 of the ISO 21448:

$$A_H = R_{HB} \cdot P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}$$

✓ Approach proposed:

$$P(\mathcal{H}, \mathcal{S}) \leq \sum_{\mathcal{E}, \mathcal{B}, \mathcal{T}} P(\mathcal{T}) P(\mathcal{B}|\mathcal{T}) P(\mathcal{E}|\mathcal{B}, \mathcal{T}) P(\mathcal{H}|\mathcal{E}, \mathcal{B}, \mathcal{T}) P(\mathcal{S}|\mathcal{H}, \mathcal{E}, \mathcal{B}, \mathcal{T})$$

Validation of the SOTIF using Quantitative Acceptance Criteria

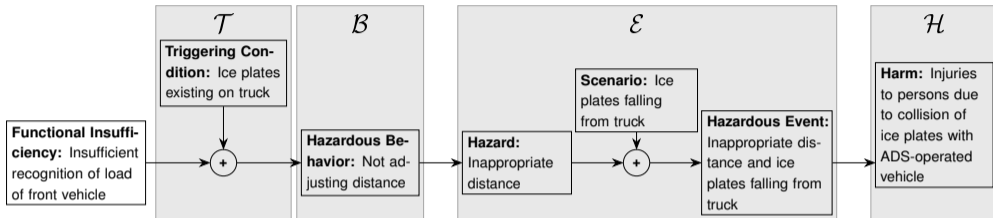- Other discretizations are also conceivable, for example:

$$P(\mathcal{H}) \leq \sum_{\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{H}|\mathcal{B},\mathcal{T})$$

$$P(\mathcal{H},\mathcal{S}) \leq \sum_{\mathcal{B},\mathcal{T}} P(\mathcal{T})P(\mathcal{B}|\mathcal{T})P(\mathcal{H}|\mathcal{B},\mathcal{T})P(\mathcal{S}|\mathcal{H},\mathcal{B},\mathcal{T})$$
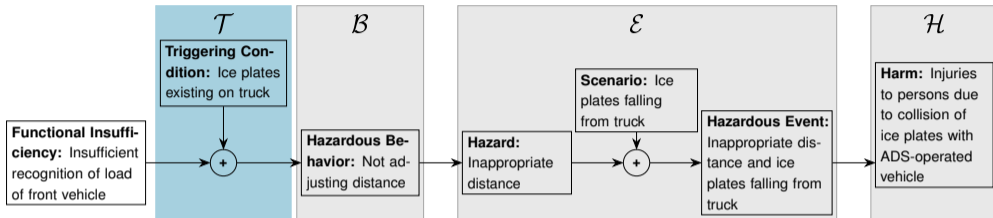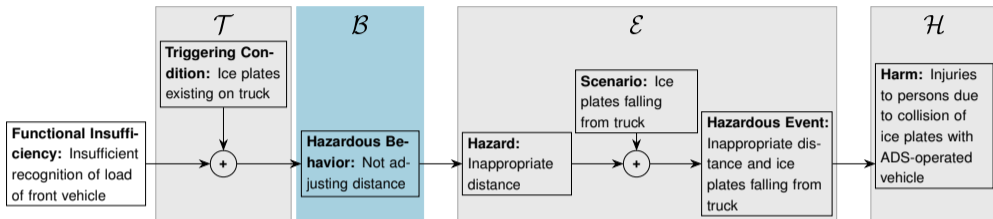
	$P(\mathcal{T})$	$P(\mathcal{B}\vert\mathcal{T})$	$P(\mathcal{E}\vert\mathcal{B},\mathcal{T})$	$P(\mathcal{H}\vert\mathcal{E},\mathcal{B},\mathcal{T})$	$P(\mathcal{S}\vert\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$
Traffic Data					
Proving Ground					
Simulation					

Validation of the SOTIF using Quantitative Acceptance Criteria

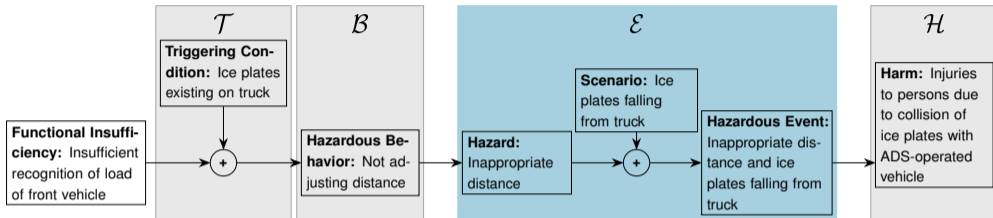|	$P(\mathcal{T})$	$P(\mathcal{B}|\mathcal{T})$	$P(\mathcal{E}|\mathcal{B},\mathcal{T})$	$P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$	$P(\mathcal{S}|\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$
Traffic Data	✗				
Proving Ground	✗				
Simulation	✗				

DLR

	$P(\mathcal{T})$	$P(\mathcal{B}|\mathcal{T})$	$P(\mathcal{E}|\mathcal{B},\mathcal{T})$	$P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$	$P(\mathcal{S}|\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$
Traffic Data	✗	✗			
Proving Ground	✗	✓			
Simulation	✗	✓			

Validation of the SOTIF using Quantitative Acceptance Criteria
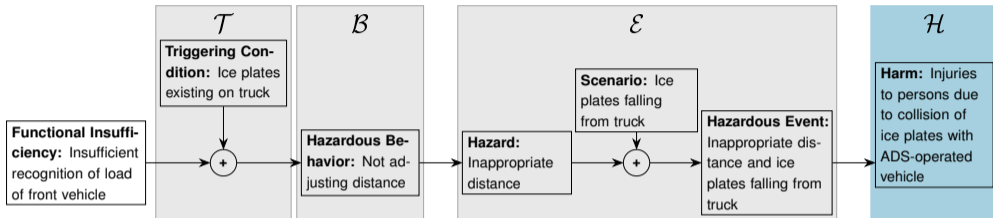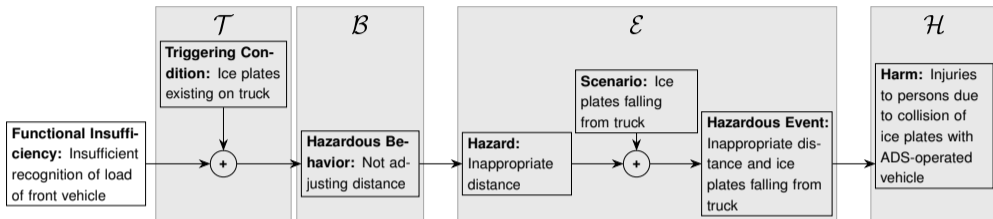

	$P(\mathcal{T})$	$P(\mathcal{B}|\mathcal{T})$	$P(\mathcal{E}|\mathcal{B},\mathcal{T})$	$P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$	$P(\mathcal{S}|\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$
Traffic Data	✗	✗	✓		
Proving Ground	✗	✓	(✗)		
Simulation	✗	✓	(✗)		

Validation of the SOTIF using Quantitative Acceptance Criteria

	$P(\mathcal{T})$	$P(\mathcal{B}\vert\mathcal{T})$	$P(\mathcal{E}\vert\mathcal{B},\mathcal{T})$	$P(\mathcal{H}\vert\mathcal{E},\mathcal{B},\mathcal{T})$	$P(\mathcal{S}\vert\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$
Traffic Data	✗	✗	✓	(✓)	
Proving Ground	✗	✓	(✗)	✓	
Simulation	✗	✓	(✗)	✓	

DLR

	$P(\mathcal{T})$	$P(\mathcal{B}|\mathcal{T})$	$P(\mathcal{E}|\mathcal{B},\mathcal{T})$	$P(\mathcal{H}|\mathcal{E},\mathcal{B},\mathcal{T})$	$P(\mathcal{S}|\mathcal{H},\mathcal{E},\mathcal{B},\mathcal{T})$
Traffic Data	✗	✗	✓	(✓)	(✓)
Proving Ground	✗	✓	(✗)	✓	✓
Simulation	✗	✓	(✗)	✓	✓

Discussion

DLR

- Are there some general rules to derive a suitable decomposition of the risk?

Discussion

- Are there some general rules to derive a suitable decomposition of the risk?
- Does a scenario-based approach (sufficiently) reduce the validation effort?

Discussion

DLR

- Are there some general rules to derive a suitable decomposition of the risk?
- Does a scenario-based approach (sufficiently) reduce the validation effort?
- Is a quantitative risk assessment possible before deployment?

Discussion

- Are there some general rules to derive a suitable decomposition of the risk?
- Does a scenario-based approach (sufficiently) reduce the validation effort?
- Is a quantitative risk assessment possible before deployment?
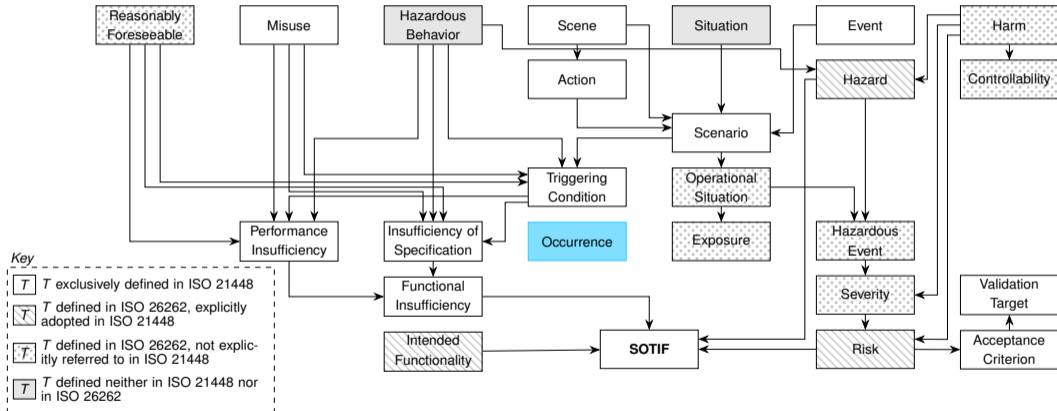- How to deal with updates – even post deployment?
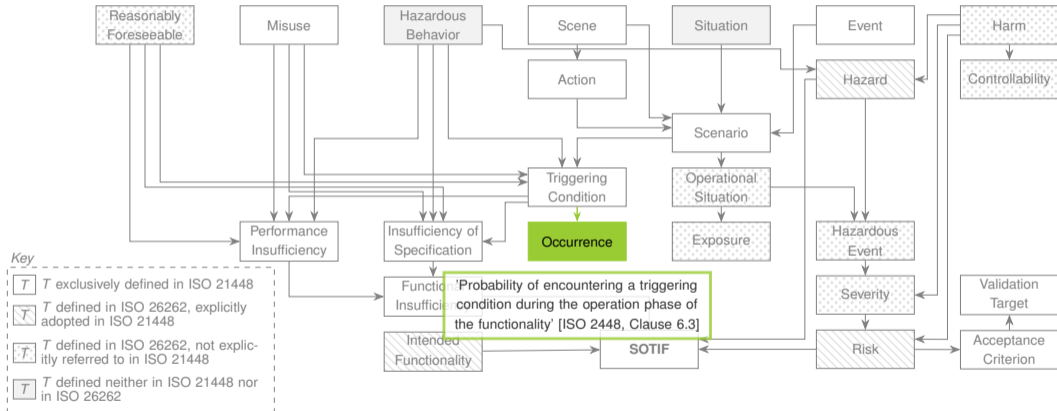
Thank you for the attention.

Contact:

Lina Putze, M.Sc.
German Aerospace Center (DLR) e.V.
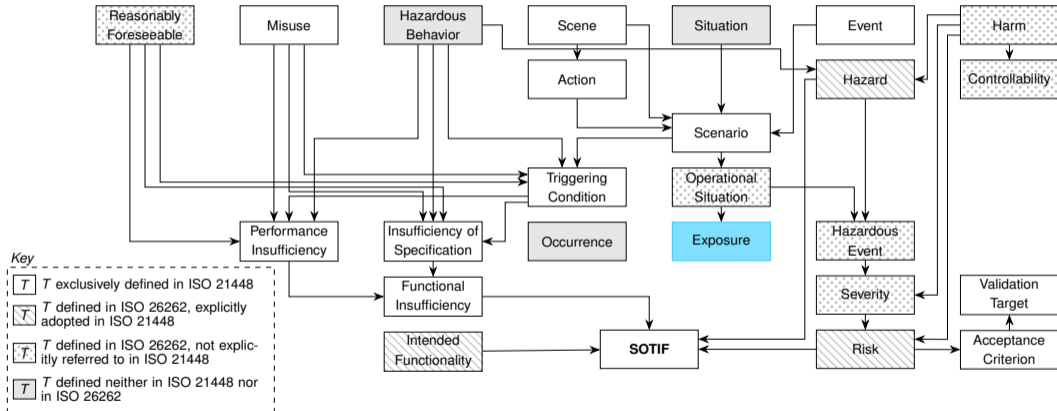Institute of Systems Engineering for Future Mobility
lina.putze@dlr.de

Definition Occurrence

Definition Exposure

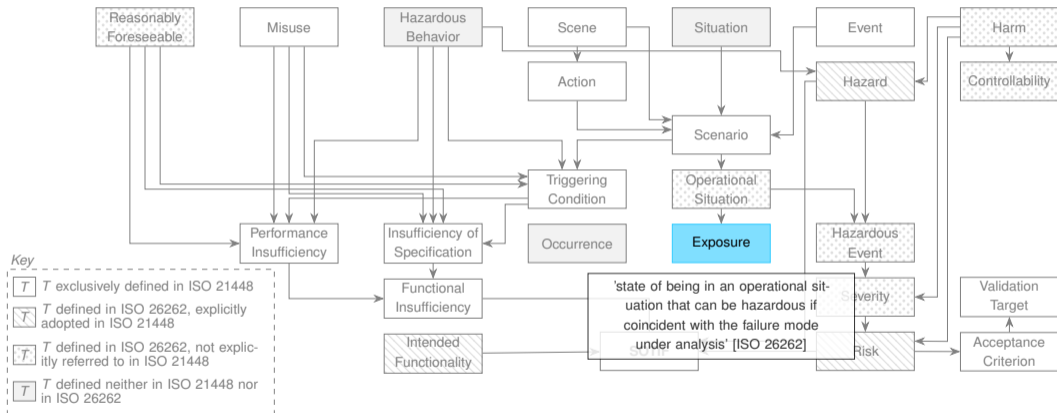Lina Putze, Towards a Quantitative SOTIF Validation of Automated Driving Systems, 07.09.2023

Definition Exposure

Lina Putze, Towards a Quantitative SOTIF Validation of Automated Driving Systems, 07.09.2023

Definition Exposure

state of being in a scenario containing conditions in which the hazard can lead to harm if coincident with the hazardous behavior under analysis

Key

- T exclusively defined in ISO 21448
- T defined in ISO 26262, explicitly adopted in ISO 21448
- T defined in ISO 26262, not explicitly referred to in ISO 21448
- T defined neither in ISO 21448 nor in ISO 26262
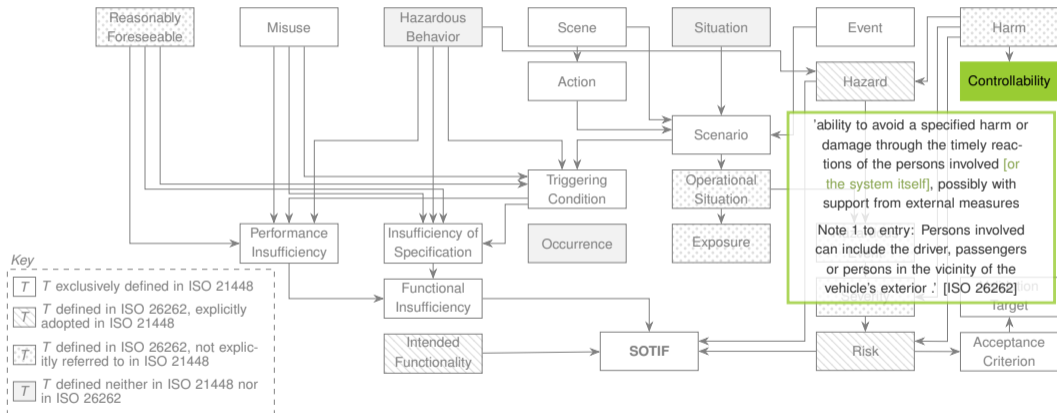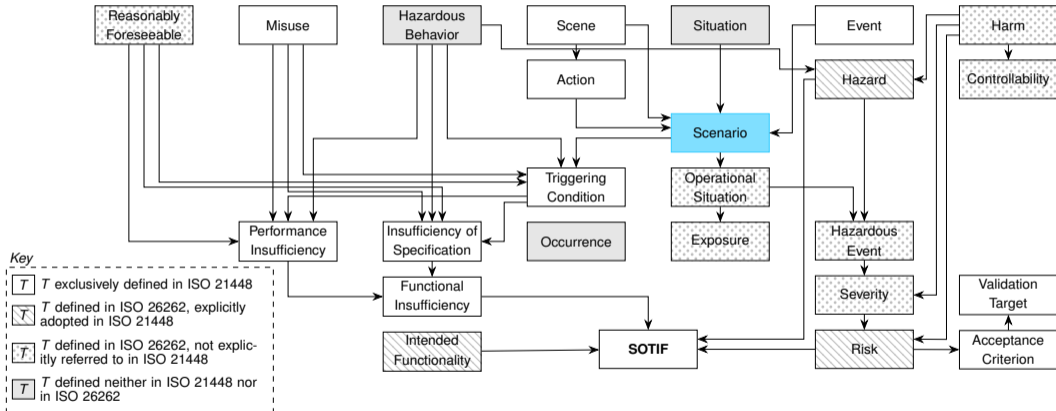
Definition Controllability

Definition Controllability

Definition Scenario

Lina Putze, Towards a Quantitative SOTIF Validation of Automated Driving Systems, 07.09.2023

'description of the temporal relationship between several scenes in a sequence of scenes, with goals and values within a specified situation, influenced by actions and events' [ISO 21448]

Key

- T T exclusively defined in ISO 21448
- T T defined in ISO 26262, explicitly adopted in ISO 21448
- T T defined in ISO 26262, not explicitly referred to in ISO 21448
- T T defined neither in ISO 21448 nor in ISO 26262

Definition Scenario

'temporal development between several scenes in a sequence of scenes. Every scenario starts with an initial scene. Actions & events as well as goals & values may be specified to characterize this temporal development in a scenario. Other than a scene, a scenario spans a certain amount of time.' [Ulbrich et al.]

Key

- T T exclusively defined in ISO 21448
- T T defined in ISO 26262, explicitly adopted in ISO 21448
- T T defined in ISO 26262, not explicitly referred to in ISO 21448
- T T defined neither in ISO 21448 nor in ISO 26262
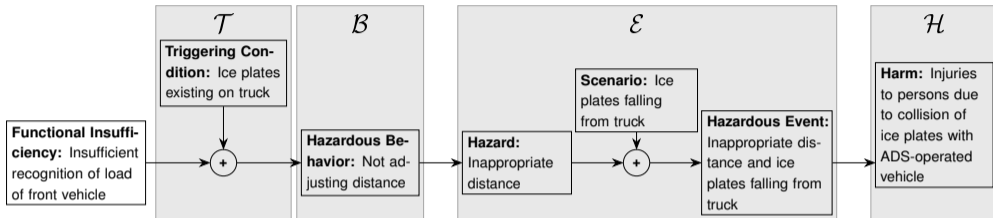
Derivation of Validation Targets

- Suggestion given in the Annex C.2 of the ISO 21448

Derivation of Validation Targets

- Suggestion given in the Annex C.2 of the ISO 21448
  - Solving the factorization of the acceptance criterion A_H for R_{HB}:

$$R_{HB} = \frac{A_H}{P_{E|HB} \cdot P_{C|E} \cdot P_{S|C}}$$

  - Estimation of a validation target τ that is sufficent for A_H with confidence level α:

$$\tau = -\ln(1 - \alpha)/R_{HB}$$

[ISO 21448]   International Organization for Standardization, "ISO 21448: Road vehicles –
                       Safety of the intended functionality," 2022.

[ISO 26262]   International Organization for Standardization, "ISO 26262: Road vehicles –
                       Functional safety," 2018.

[ISO/IEC Guide 51]   International Organization for Standardization, "ISO/IEC Guide 51: Safety
                       aspects — Guidelines for their inclusion in standards," 2014.

[Ulbrich et al.]   S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer, "Defining and
                       substantiating the terms scene, situation, and scenario for automated driv-
                       ing," in *2015 IEEE 18th international conference on intelligent transportation
                       systems*. IEEE, 2015, pp. 982–988.