www.pegasusprojekt.de

Anforderungen & Rahmenbedingung – Stand 8

HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

PEGASUS

Von der Testmethode zum Sicherheitsnachweis.

Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

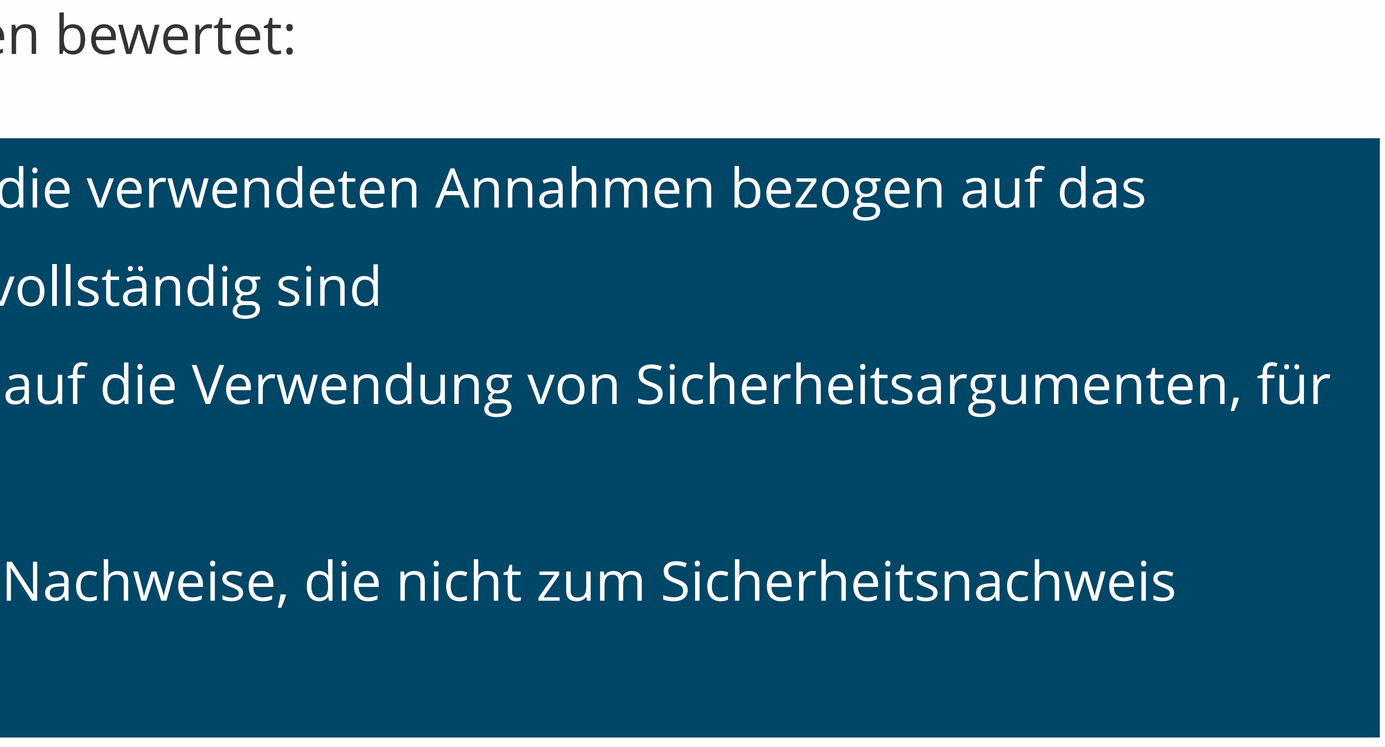
Pegasus erarbeitet ein methodisches Vorgehen zur Ableitung, Durchführung und Auswertung von Testfällen, um den Nachweis zu erbringen, dass HAF mindestens so gut ist, wie der menschliche Fahrer. Die Besonderheit dieser Testmethodik besteht in der Kombination observierter Szenen mit Systemwissen, sodass ein szenarienbasiertes Testen von HAF möglich wird. Um der Frage nachzugehen, wie belastbar/tragfähig die daraus resultierenden Sicherheitsnachweise sind, wurde die Gesamtheit der Testmethodik unter Verwendung der nachfolgenden Kriterien bewertet:

1. **Assumption coverage** – gibt an, ob die verwendeten Annahmen bezogen auf das intendierte Design hinreichend und vollständig sind
2. **Unfounded evidence** – bezieht sich auf die Verwendung von Sicherheitsargumenten, für die kein Nachweis erbracht wurde
3. **Unused evidence** – bezieht sich auf Nachweise, die nicht zum Sicherheitsnachweis beitragen

II. Bewerten der Elemente mittels Kriterien

	betrachtete Elemente
1	Informationsbasis
2	Ontologie
3	Kritikalität
4	Assoziation
5	Relation
6	Variation

III. Reflektieren der Tragfähigkeit der Testmethodik



I. Identifizieren von Elementen, die den Sicherheitsnachweis beeinträchtigen können

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Anforderungen & Rahmenbedingung – Stand 8

HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

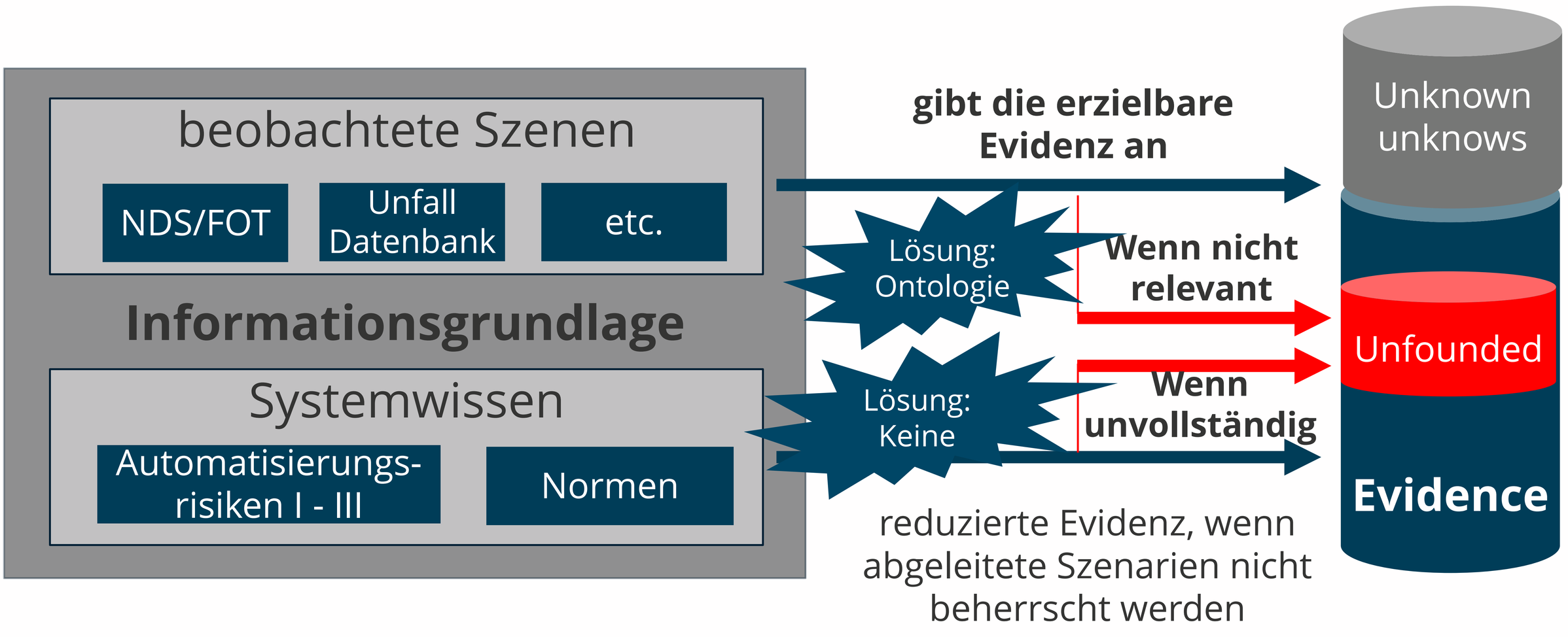
PEGASUS

Von der Testmethode zum Sicherheitsnachweis.

Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

1. **Informationsgrundlage**

- dient der Bereitstellung von Referenzdaten für die Durchführung eines Sicherheitsnachweises
- mit der Folge, dass der Umfang und die Repräsentativität der verwendeten Referenzdaten zu einer limitierten „Assumption Coverage“ führen. Immer dann, wenn diesen Referenzdaten eine Repräsentativität unterstellt wird, ohne diese nachzuweisen, muss zusätzlich eine „unfounded evidence“ unterstellt werden.



Aufgrund der Tatsache, dass der Umfang, sowie die Repräsentativität der verwendeten Informationsgrundlage sowohl für einen szenariobasierten, als auch für das „Black-Box Testen“ limitierend auf die „Assumption Coverage“ wirken, ist dieser Einfluss als generelle Herausforderung zu werten.

Im Kontext der Verwendung von Systemwissen für den Sicherheitsnachweis bringt der szenarienbasierte Ansatz den Nachteil mit sich, dass dieses Wissen zum einen identifiziert und zum anderen in Form eines Szenarios dargestellt werden muss. Im Vergleich dazu bietet der „Black-Box Test“ den Vorteil, dass das Systemwissen inhärent in den observierten Szenarien enthalten ist und keine zusätzliche Identifikation, sowie Abbildung erforderlich ist. Folglich kann von der Verwendung eines szenariobasierten Ansatzes eine „unfounded evidence“ ausgehen, aufgrund der Tatsache, dass das Systemwissen eines HAF potentiell als unbekannt/unterspezifiziert gilt.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Anforderungen & Rahmenbedingung – Stand 8

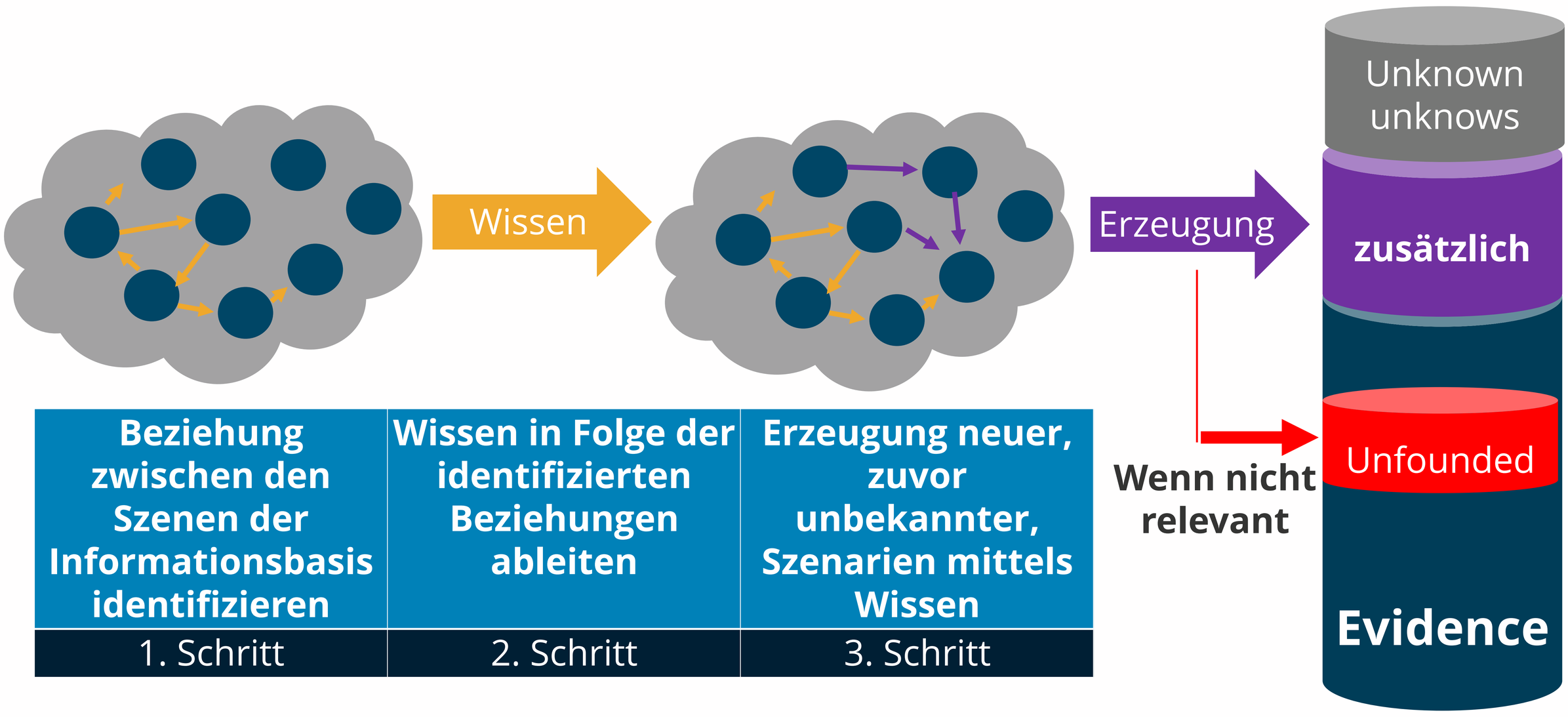
HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

PEGASUS

Von der Testmethode zum Sicherheitsnachweis.

Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

2. **Ontologie**
- dient der Erzeugung von zusätzlichen Szenarien auf Grundlage bereits observierter Szenen,
- mit der Folge, dass eine Erhöhung der „Assumption Coverage“ erzielt werden kann, sofern diese Szenarien auch für die Sicherheitsaussage relevant sind. Andernfalls ist der Verwendung einer Ontologie eine „unfounded evidence“ zu unterstellen.



Beziehung zwischen den Szenen der Informationsbasis identifizieren	Wissen in Folge der identifizierten Beziehungen ableiten	Erzeugung neuer, zuvor unbekannter, Szenarien mittels Wissen
1. Schritt	2. Schritt	3. Schritt

Der Einsatz einer Ontologie zur Erzeugung neuer Szenarien bringt die Herausforderung mit sich, zusätzliche Szenarien zu erzeugen, die zum einen neu und zum anderen für die Sicherheitsargumentation relevant sind. Da die Relevanz eines Szenarios im Allgemeinen erst nach dessen auftreten als nachgewiesen gilt, muss den neu generierten Szenarien folglich eine „unfounded evidence“ unterstellt werden, weil ein Nachweis ohne zugehörige Sicherheitsargumentation erbracht wird. Zur Vermeidung dieser Problematik wird zum gegenwärtigen Zeitpunkt die Verwendung des Systemwissens zur Argumentation der Relevanz von erzeugten Szenarien vorgeschlagen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Anforderungen & Rahmenbedingung – Stand 8

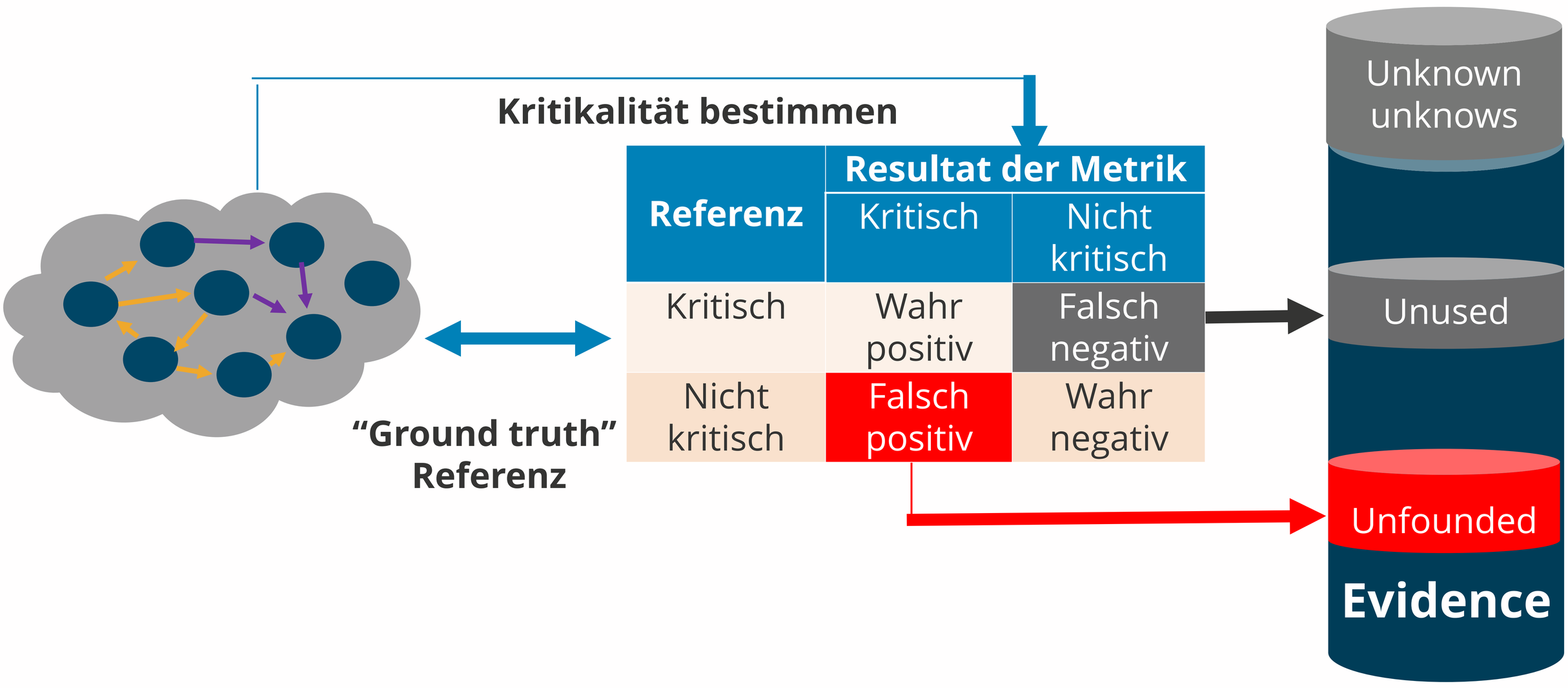
HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

PEGASUS

Von der Testmethode zum Sicherheitsnachweis.

Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

3. **Kritikalität**
- dient der Identifikation von Szenen mit einem Potential für einen nicht unfallfreien Ausgang,
- mit der Folge, dass im Falle einer falsch positiven Bewertung eine „unfounded evidence“ und im Falle einer falsch negativen Bewertung eine „unused evidence“ resultiert.



Die Herausforderung der Kritikalitätsbestimmung besteht im Abwägen zwischen einer zu konservativen beziehungsweise einer zu aggressiven Auslegung der Metriken, anhand derer eine Szene als kritisch gilt. Sind diese zu aggressiv (falsch positiv) festgelegt, wird eine Szene als kritisch bezeichnet, obwohl von diesen Szenen kein erhöhtes Potential für einen Unfall ausgeht, mit der Folge, dass eine „unfounded evidence“ in den Sicherheitsnachweis eingeht, da ein Nachweis für unkritische Szenarien erbracht wird, dieser aber als Nachweis eines kritischen Szenarios in den Sicherheitsnachweis einfließt. Im Gegensatz dazu verbleiben Evidenzen ungenutzt, zum Beispiel, wenn die Kritikalität einer Szene zu konservativ (falsch negativ) bewertet wird und somit auf einen Sicherheitsnachweis verzichtet wird, obwohl er zu erbringen wäre. Folglich wird bei einer zu konservativen Auslegung auf einen verfügbaren Sicherheitsnachweis verzichtet, während bei einer zu aggressiven Auslegung der resultierende Nachweis überbewertet wird.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Anforderungen & Rahmenbedingung – Stand 8

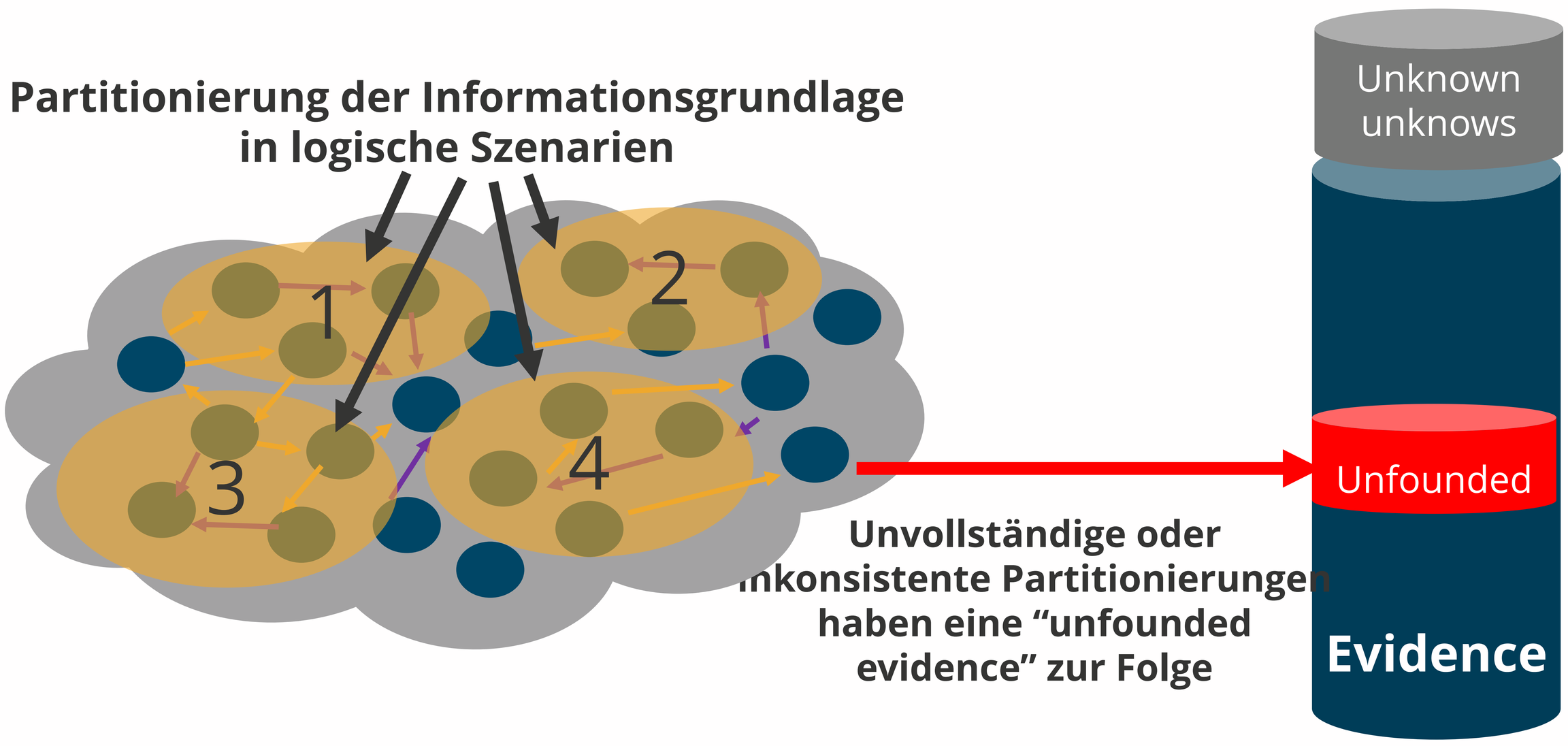
HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

PEGASUS

Von der Testmethode zum Sicherheitsnachweis.

Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

4. **Assoziation**
- dient der Partitionierung der observierten Szenen in logische Szenarien,
- mit der Folge, dass möglicherweise eine „unfounded evidence“ aufgrund einer Vereinfachung der observierten Verkehrsdynamik im Rahmen der Abbildung von der Szene auf das Szenario auftreten kann.



Die Assoziationsproblematik resultiert aus einer Vereinfachung der observierten Verkehrsdynamik durch deren Partitionierung in logische Szenarien. Diese Vereinfachung kann zur Folge haben, dass ein HAF System den abgeleiteten Testfall besteht, aber nicht in der Lage ist, die eingangs partitionierte Szene zu beherrschen. Folglich wird Sicherheit argumentiert, ohne den dafür notwendigen Sicherheitsnachweis zu erbringen. Solange nicht nachgewiesen wurde, dass mögliche Vereinfachungen zu vernachlässigen sind, muss einem Szenario-basierten Ansatz eine „unfounded evidence“ unterstellt werden.

Im Gegensatz dazu ist die beschriebene Vereinfachungsproblematik im Kontext eines „Black-box Tests“ nicht zu erwarten, weil Szenen getestet werden, ohne diese zu modifizieren.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Anforderungen & Rahmenbedingung – Stand 8

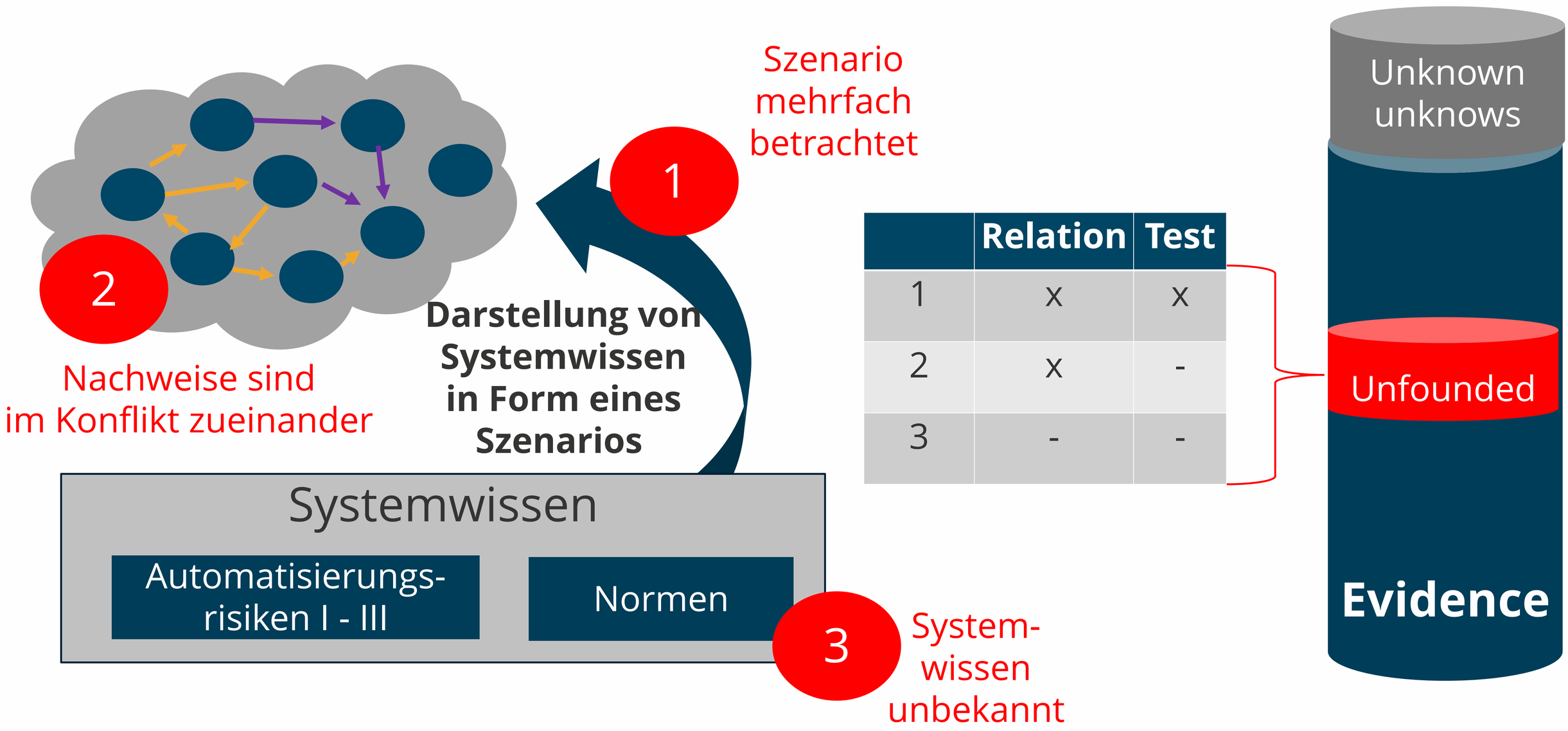
HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

PEGASUS

Von der Testmethode zum Sicherheitsnachweis.

Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

5. **Relation**
- dient der Darstellung eines Automatisierungsrisikos in Form eines Szenarios,
- mit der Folge, dass möglicherweise eine “unfounded evidence” aus einem mehrfach erbrachten Sicherheitsnachweis für ein und dasselbe Szenario resultieren kann.



Die Darstellung des Systemwissens in Form eines Szenarios bringt die Herausforderung mit sich, mögliche Automatisierungsrisiken durch spezifische Szenarien anzuregen. Dieser Abbildung ist eine „unfounded evidence“ zu unterstellen, zum Beispiel, wenn das Systemwissen unvollständig identifiziert oder inkorrekt auf ein Szenario abgebildet wurde (siehe 3). Aber auch, wenn die Identifikation und Darstellung des Systemwissens korrekt durchgeführt wird, muss eine „unfounded evidence“ unterstellt werden, aufgrund der Tatsache, dass möglicherweise multiple Nachweise für ein und dieselbe Sicherheitsargumentation (siehe 1&2) erbracht werden. Im Gegensatz dazu kann keines dieser Probleme unter Verwendung eines „Black-Box Tests“ auftreten, da die Trigger Ereignisse für ein Automatisierungsrisiko inhärent in einer observierten Szene enthalten sind. Dennoch gibt es keine Garantie, dass durch besonders exzessives „Black-box Testing“ diese Trigger auftreten, was wiederum ein Argument für das Szenario-basierte Testen darstellt, welches es ermöglicht, Automatisierungsrisiken reproduzierbar zu testen, sofern diese in Form eines Szenarios dargestellt wurden.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Anforderungen & Rahmenbedingung – Stand 8

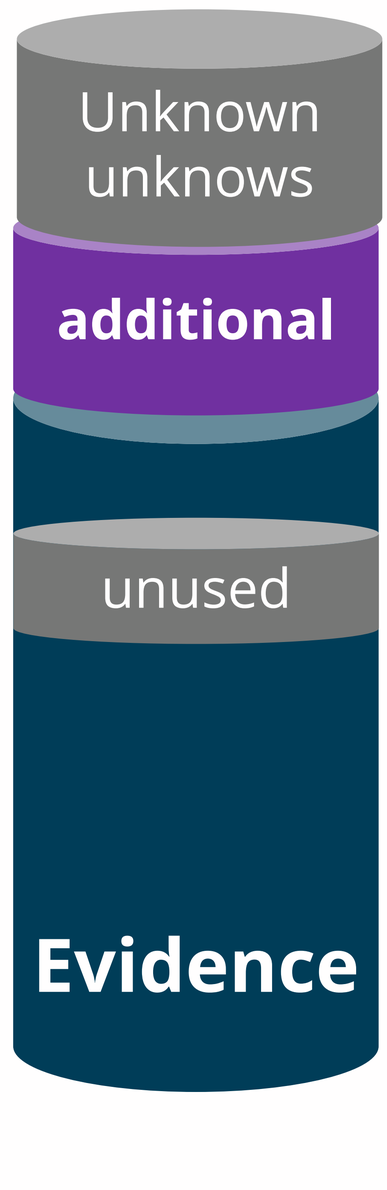
HERAUSFORDERUNGEN EINES SZENARIEN-BASIERTEN ANSATZES

PEGASUS

Von der Testmethode zum Sicherheitsnachweis.
Wie tragfähig sind die Nachweise eines Szenarien-basierten Ansatzes, Stützen diese Nachweise die Sicherheitsargumentation?

6. **Variation**
- dient der Variation von Parametern zum Nachweis der Systemstabilität,
- mit der Folge, dass eine erhöhte „assumption coverage“ erwartet werden darf, sofern das Variationsresultat für den Sicherheitsnachweis relevant ist.

relevant	**erhöht die “assumption coverage”, da Szenarien getestet werden können, die bisher unbekannt waren**	**erbringt Nachweise für bekannte aber bisher nicht getestete Szenarien, so dass die „unused evidence“ reduziert werden kann**
nicht relevant	Szenarien ohne Relevanz leisten grundsätzlich keinen Beitrag zur Sicherheitsargumentation können aber zur Stabilitätsverifikation des „System under Test“ getestet werden	
	neu	**nicht neu**
	Szenarien infolge der Variation	



Die Herausforderung der Variation besteht darin, die Testspezifikation in einer Art und Weise zu variieren, sodass zum einen neue Szenarien daraus hervorgehen und zum anderen diese für die Sicherheitsargumentation auch relevant sind. Sollte den variierten Szenarien eine nicht nachgewiesene Repräsentativität unterstellt werden, dann folgt aus der Verwendung dieser Szenarien für einen Sicherheitsnachweis eine „unfounded evidence“. Diese Problematik lässt sich möglicherweise in Analogie zur Ontologie durch den Einsatz von Systemwissen vermeiden. Abschließend gilt festzuhalten, dass variierte aber nicht-relevante Szenarien keinen Beitrag für die Sicherheitsargumentation leisten und bestenfalls zum Stabilitätsnachweis des HAF Systems herangezogen werden können.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages