

Erlaubter Raum

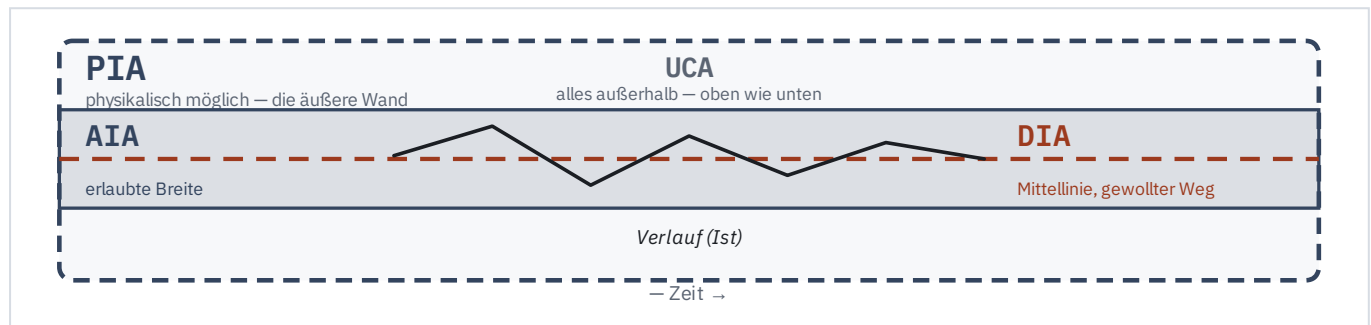
Referenzkarte

Ausg. 09/2026

Verlauf, Schlauch, Deckung — eine Erweiterung von STPA

Ein System hat nie einen Zustand, nur einen Verlauf, der sich ständig bewegt — Stillstand gibt es nicht. Man legt einen Schlauch daneben: Mittellinie (gewollter Weg) plus Breite (erlaubte Abweichung), über die Zeit. Eine Prüfung — liegt der Verlauf im Schlauch? — ersetzt drei bisher getrennte Aufgaben: Betrieb überwachen, Ziele auf Machbarkeit prüfen, Sicherheitsanalyse nach STPA (Leveson).

DER SCHLAUCH — VIER KLASSEN JEDER EINWIRKUNG



PIA

PHYSICALLY POSSIBLE

Die äußere Wand: alles, was auf einem Kanal physisch ankommen kann.

AIA

ALLOWED

Die Breite: was stören darf, ohne dass der Schlauch verlassen wird.

DIA

DESIRED

Die Mittellinie: was das Ziel verändern darf.

UCA

UNSAFE/UNWANTED

Der Rest — PIA minus (AIA u DIA). Nie erfunden, nur berechnet.

1

BETRIEB

Läuft es? Bleibt der Ist-Verlauf im Schlauch?

FALLE

Eine Momentaufnahme kann eine Deckung nie bestätigen — sie zeigt einen Punkt, nicht die Bahn (Aliasing).

FÜR DICH

☐ Beobachte die Reserve — den Abstand zur Schlauchwand — nicht nur, ob die Wand schon berührt ist. Schrumpfende Reserve ist das früheste Signal.

2

AUFTRAG

Kann das System das überhaupt? Gewollte Rate $\leq$ real mögliche Rate.

FALLE

Den Auftrag trotzdem erteilen und hoffen, obwohl die Zeitkonstanten es nicht hergeben.

FÜR DICH

☐ Scheitert die Prüfung: genau drei ehrliche Auswege — Mittellinie verlangsamen, Schlauch verbreitern, oder das System ändern.

3

KOMPOSITION

Passt es zusammen? Was A abgibt, muss B als AIA/DIA erlauben.

FALLE

Jede Komponente einzeln geprüft, das Zusammenspiel nie — komponentenweise gedeckt ist nicht systemweit sicher.

FÜR DICH

☐ Schnittstelle für Schnittstelle: liegt die Ausgabe-Schwankung von A innerhalb dessen, was B deklariert hat?

WAS DIESE ERWEITERUNG NICHT KANN

- Nur so vollständig wie die Deklaration — ein nicht deklarierter Kanal bleibt ein blinder Fleck.
- Ersetzt Levesons Systemsicht nicht — komponentenweise gedeckt ist nicht systemweit sicher, jede Ebene braucht ihren eigenen Schlauch.
- Entwirft nichts — sagt nur, was unerreichbar oder unverträglich ist, nicht was gebaut wird.

Ausführliche Herleitung mit Belegen unter thomasarends.de

Teil einer Reihe von Referenzkarten: Lebensfähigkeit (privat/Firma) · ADRA · Universeller Graph · FMEA

Thomas Arends · September 2026