Softwareanforderungsanalyse

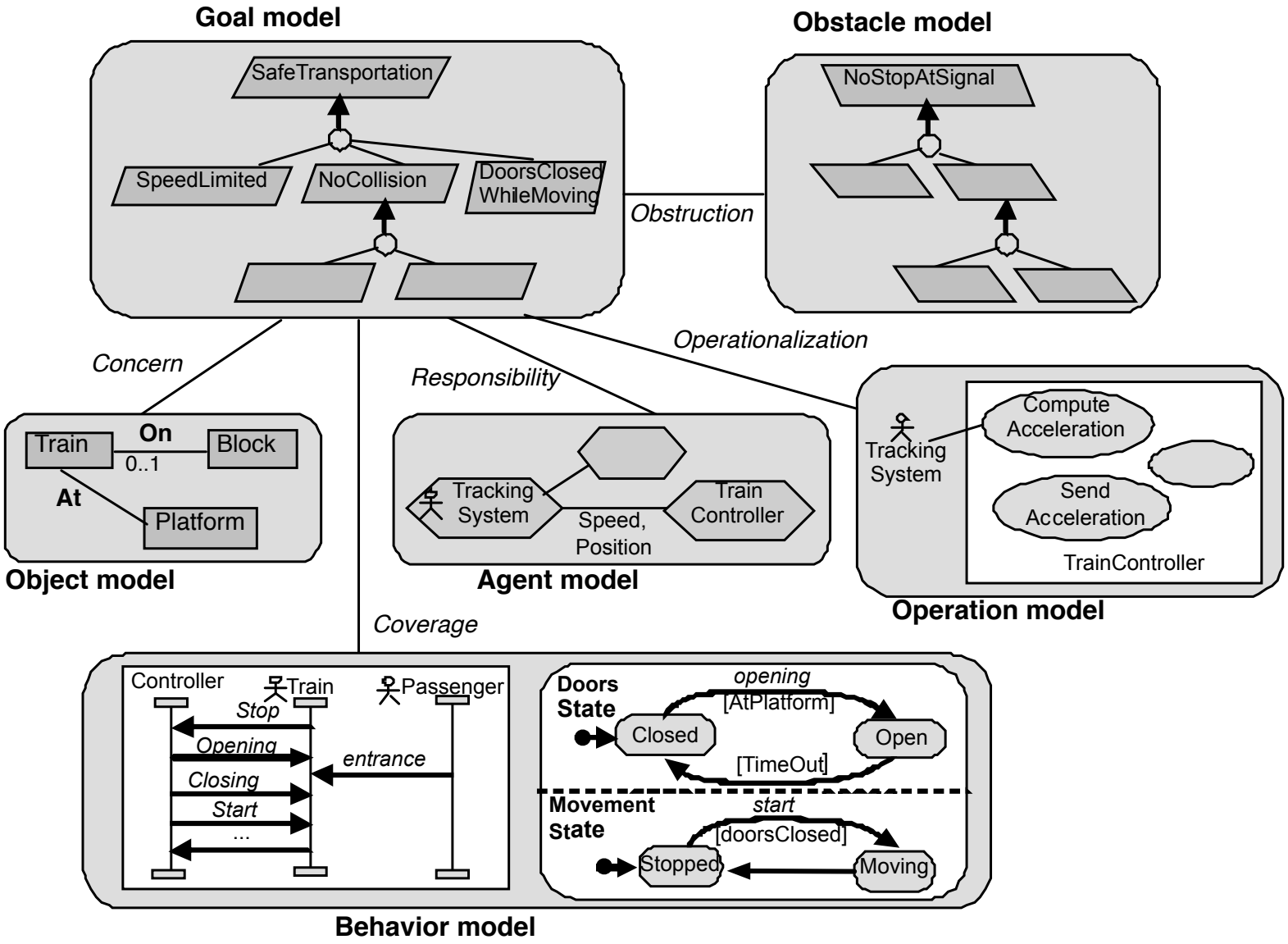
Risikoanalyse

Burkhardt Renz

THM, Fachbereich MNI

Wintersemester 2018/19

Das Hindernismodell im Kontext der Modellierung



Quelle: Lamsweerde, S. 291

Übersicht

- Risiken und Hindernisse
- Modellierung von Hindernissen
- Vorgehen bei der Risikoanalyse
- Sicherheitsanalyse

Risikoanalyse

Definition (Risiko)

Ein Risiko ist ein unsicherer Faktor, der dazu führen kann, dass ein Ziel nicht erreicht wird — in der Regel infolge unerwarteten Verhaltens eines Akteurs.

Definition (Hindernis)

Ein Hindernis ist eine Vorbedingung, die dazu führt, dass ein Ziel nicht erreicht wird.

Definition (Risikoanalyse)

In der Risikoanalyse wird das Zielemodell systematisch auf Hindernisse hin untersucht um ggf. Gegenmaßnahmen einzuführen.

Kategorien von Risiken/Hindernissen

- Bedrohung der Betriebssicherheit
- Bedrohung der Sicherheit, d.h. von Vertraulichkeit, Integrität oder Verfügbarkeit
- Requests können nicht (rechtzeitig) erfüllt werden
- Fehlinformationen
- Ungenaue Daten
- Fehler durch Mängel in der Softwareergonomie
- ...

Übersicht

- Risiken und Hindernisse
- Modellierung von Hindernissen
- Vorgehen bei der Risikoanalyse
- Sicherheitsanalyse

Modellierung von Hindernissen

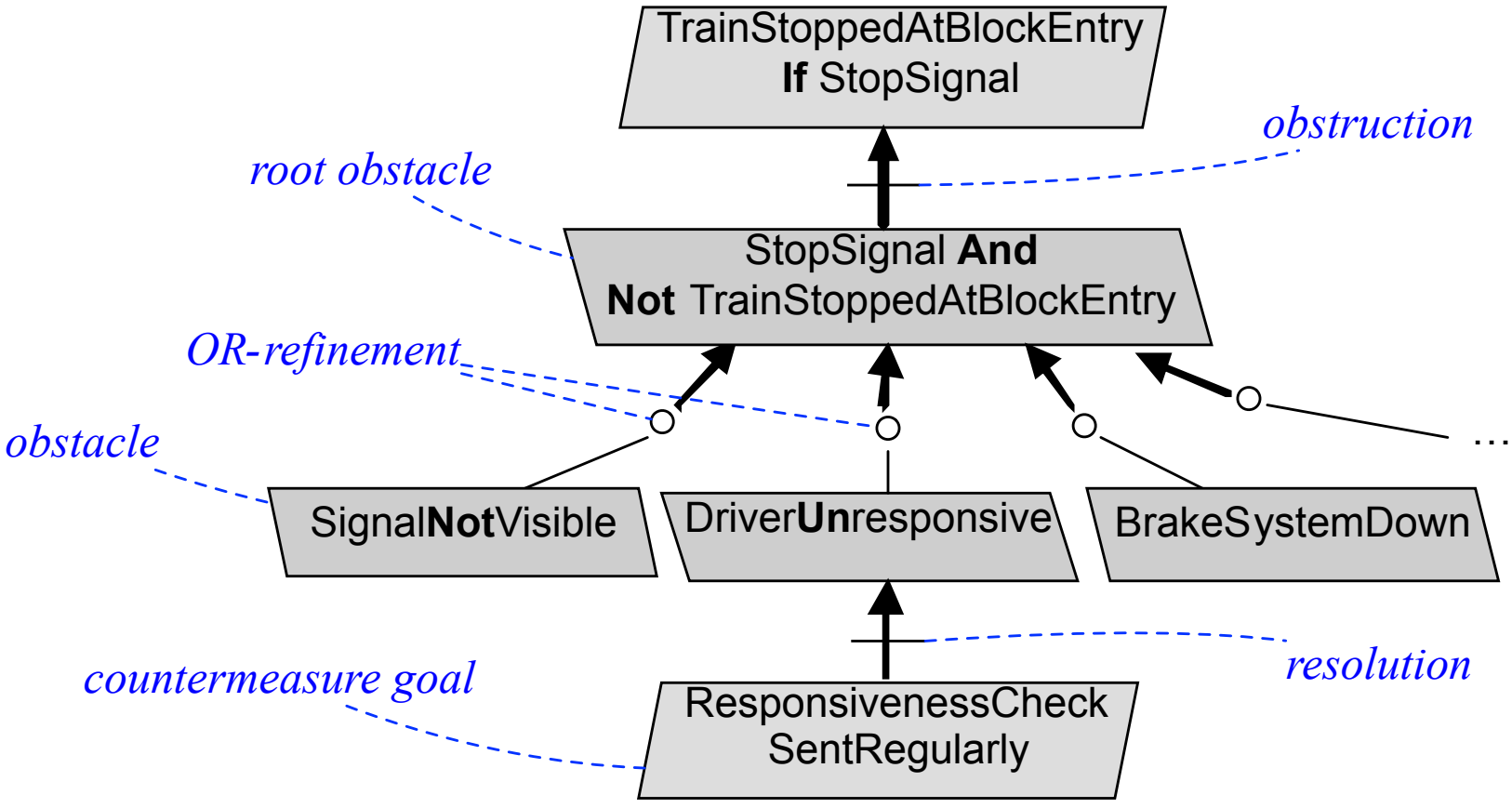
Definition (Hindernisdiagramm)

Ein Hindernisdiagramm ist ein AND-OR-Graph, der ein Hindernis (die Negation eines Ziels) und seine Verfeinerung (Ursachen) darstellt.

Definition (Hindernismodell)

Das Hindernismodell ist eine Menge von (annotierten) Hindernisdiagrammen verknüpft mit Zielen in einem Zielemodell sowie mit Gegenmaßnahmen.

Beispiel Hindernisdiagramm



Quelle: Lamsweerde S.340

Annotationen im Hindernisdiagramm

- Name = eindeutige Bezeichnung
- Def = präzise textuelle Beschreibung

optional

- Category
- Likelihood = wie wahrscheinlich?
- Criticality = wie schwerwiegend?
- Issue = Fragen, Probleme?
- FormalSpec = formale Spezifikation

Beispiel Annotationen zu Hindernis

Name DriverUnresponsive
Def *Situation of a train driver failing to react to a command and take appropriate action according to that command.*
Category Hazard
Likelihood likely
Criticality catastrophic
FormalSpec $\Diamond \exists$ dr: Driver, tr: Train, cd: Command
Drives (dr, tr) $\wedge$ $\neg$ Reacts (dr, cd)

Quelle: Lamsweerde S.343

Übersicht

- Risiken und Hindernisse
- Modellierung von Hindernissen
- Vorgehen bei der Risikoanalyse
- Sicherheitsanalyse

Vorgehen bei der Risikoanalyse

1. Identifizieren von Hindernisse - systematisch durch die Negation von Blättern im Zielediagramm
2. Analysieren der Hindernisse
3. Entschärfen durch Gegenmaßnahmen oder alternative Lösung im Zielemodell

Techniken für Gegenmaßmahmen

- Alternative Verfeinerung im Zielemodell, die Hindernis umgeht
- Anderen, zuverlässigeren Akteur finden
- Hindernis `O` vermeiden durch neues Ziel `Avoid[O]` und dessen Subziele und verantwortliche Akteure
- Abschwächen des ursprünglichen Ziels
- Wahrscheinlichkeit des Eintretens des Hindernisse verkleinern
- ...

Übersicht

- Risiken und Hindernisse
- Modellierung von Hindernissen
- Vorgehen bei der Risikoanalyse
- Sicherheitsanalyse

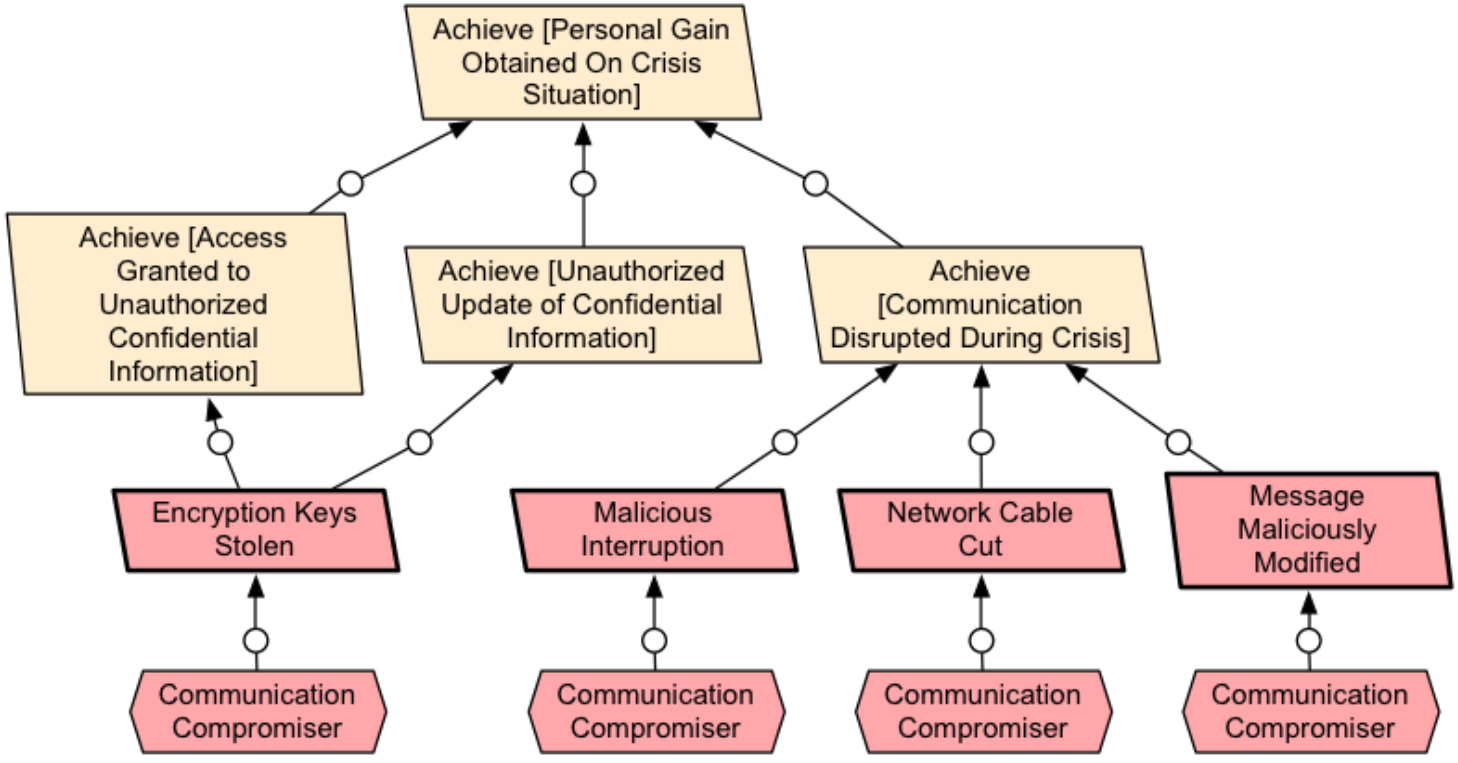
Anti-Ziele

- Sicherheitsfragen spielen in aktuellen Anwendungen eine immer größere Rolle – oft verteilt, oft über Internet erreichbar
- Für die Anforderungsanalyse: eher Gefahren auf der Anwendungsebene im Vordergrund des Interesses, weniger auf Protokollebene
- zu berücksichtigen:
  - unabsichtliche Gefahr $\rightarrow$ Fehler in der Anwendung
  - absichtlicher Angriff $\rightarrow$ Angreifer macht eine Attacke
- In KAOS: Gefahren sind Hindernisse für Sicherheitsziele
  - unabsichtliche Gefahren $\rightarrow$ Anforderungen, die Fehler vermeiden
  - absichtliche Angriffe $\rightarrow$ Neue Art Akteur: Angreifer

Vorgehen

1. Identifizieren von Anti-Zielen
2. Identifizieren von Angreifern und Ermitteln ihrer Fähigkeiten
3. Angriffs-Graph der Anti-Ziele bilden
4. Gegenmaßnahmen herleiten und als neue Anforderungen formulieren

Beispiel für Sicherheitsanalyse



aus „Modeling Car Crash Management with KAOS“ von Antoine Cailliau, Christophe Damas, Bernard Lambeau und Axel van Lamsweerde