Formale Verifikation - RaSTA

Student: Heinrich Sporys
Betreuer: Prof. Dr.-Ing. habil. Matthias Werner
M.Sc. Billy Naumann

Rail Safe Transport Application - RaSTA

- DIN EN 50159 (VDE 0831-159) 01.06. 2015
- Sicheres Kommunikationsprotokoll
- Beschreibt Sicherheits-, Sendewiederholungs- und Redundanzschicht

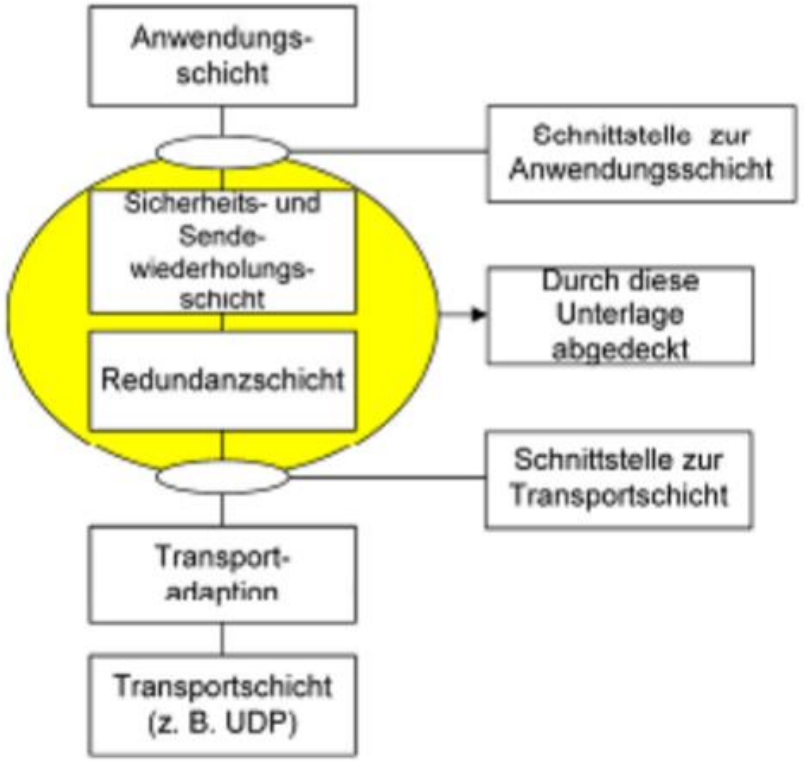


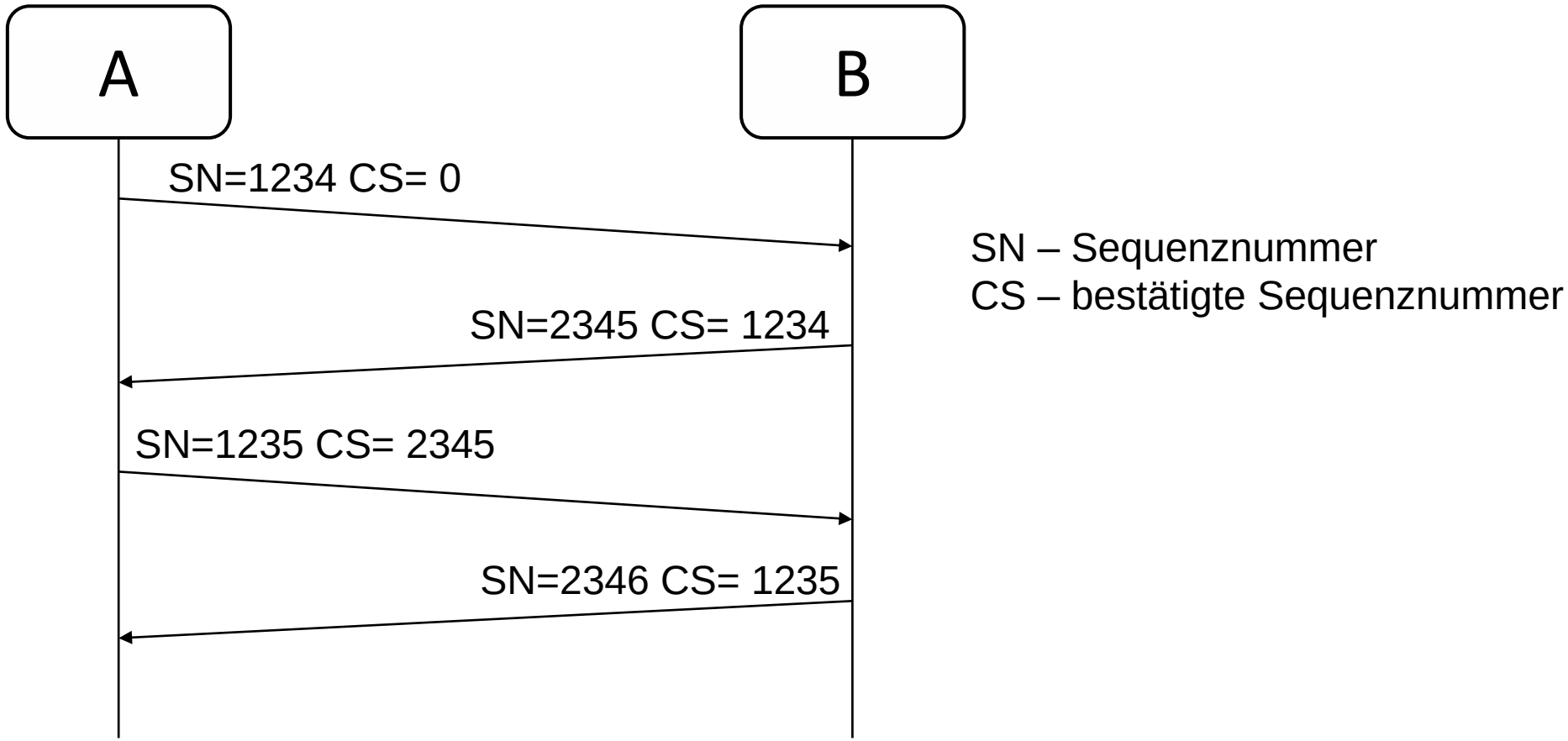
Bild 1 – Einordnung und Abgrenzung der Spezifikation

Quelle [1]

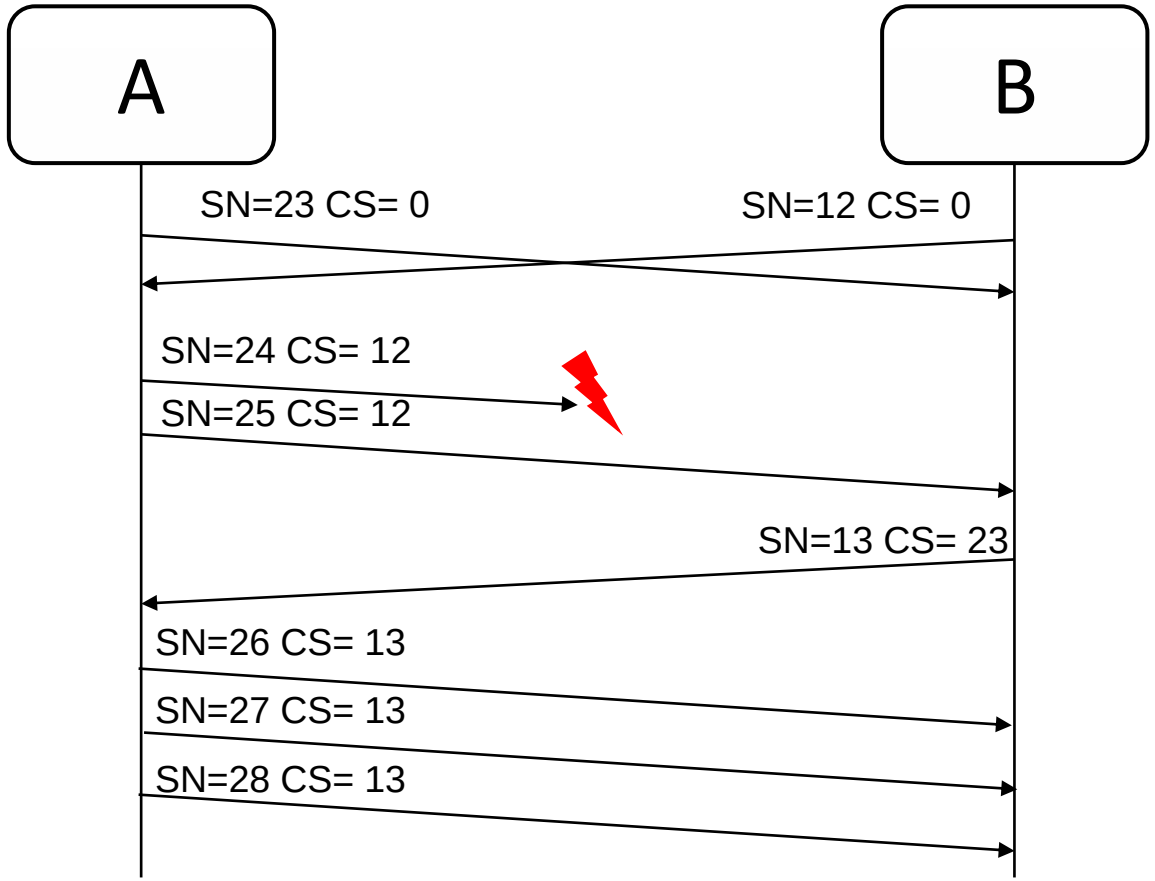
Nachrichtensequenz

- „Die Verwendung einer Sequenznummer schützt vor Wiederholung, Wiederabspielen, Auslassung, Verlust, Einfügung und Resequenzierung von Protokolldateneinheiten.“ [1]
- Sequenznummer:
  - 4 Bytes unsigned Int
  - jeder Nachricht beigelegt
- Bestätigte Sequenznummer:
  - 4 Byte unsigned Int
  - letzte empfangene Sequenznummer
  - enthalten in jeder Antwort
- Bei Überlauf auf 0 zurückgesetzt

Sequenznummerverlauf bei Verbindungsaufbau



Sequenznummerverlauf bei Fehlübertragung



SN – Sequenznummer
CS – bestätigte Sequenznummer

Sequenznummerprüfung

Sequenznummern

- $0 <= SN_{PDU} - SN_{R} <= N_{sendmax} * 10$
- $SN_{R} = SN_{PDU}$

Bestätigte Sequenznummern

- $0 <= CS_{PDU} - CS_{R} < SN_{T} - CS_{R}$

- Prüfung Abhängig von Nachrichtentyp

Wozu formal modellieren und verifizieren?

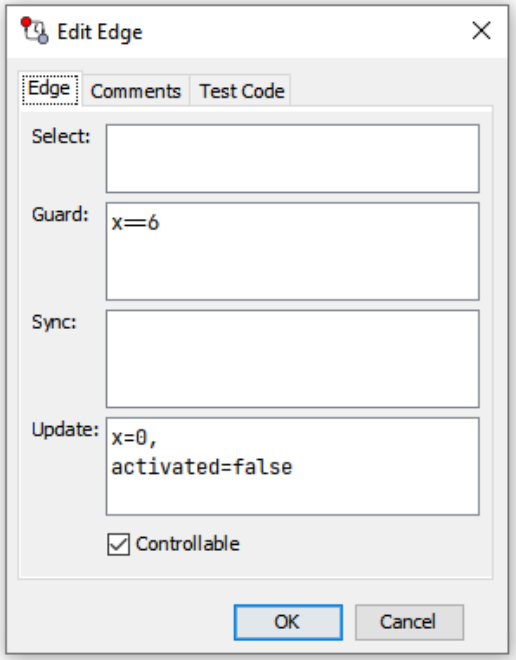
- „Sequenznummern können nur größer werden.“
- Diese Aussage basiert auf mehreren Annahmen:
  - Nachrichten können sich auf der Redundanzschicht nicht überholen
  - Sequenznummern können nicht verändert werden
  - Sequenznummern werden richtig inkrementiert
- Diese Annahmen sind meist nicht explizit aufgelistet, können aber durch ein Modell abgeleitet werden
- Eigenschaften sind in Modellen leichter nachweisbar als in der Implementation
- Zusätzliche Eigenschaften können formuliert werden z.B.:
  - Maximale/Minimale Queuelänge

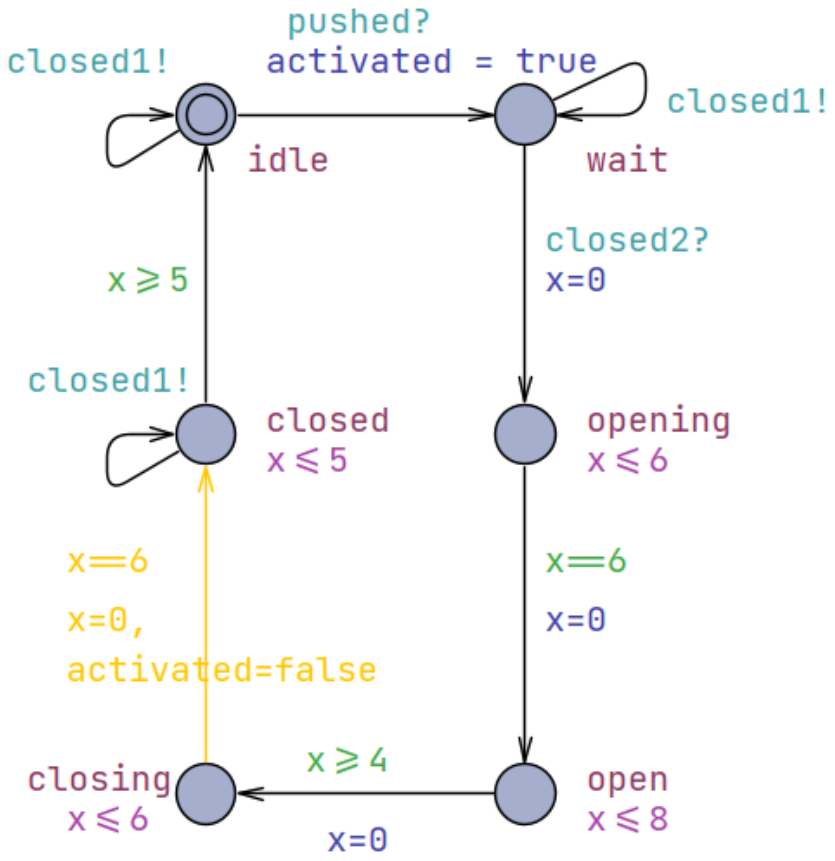
Formale Verifikation - RaSTA

UPPAAL

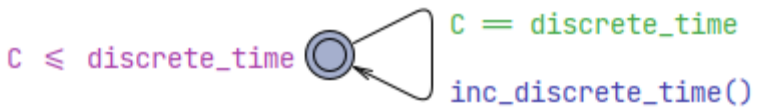
- Von **Upp**sala University und **Aal**borg University entwickelt
- Tool zur Erstellung und Verifizierung von Echtzeitsystemen durch zeitgesteuerte Automaten

UPPAAL - Aufbau

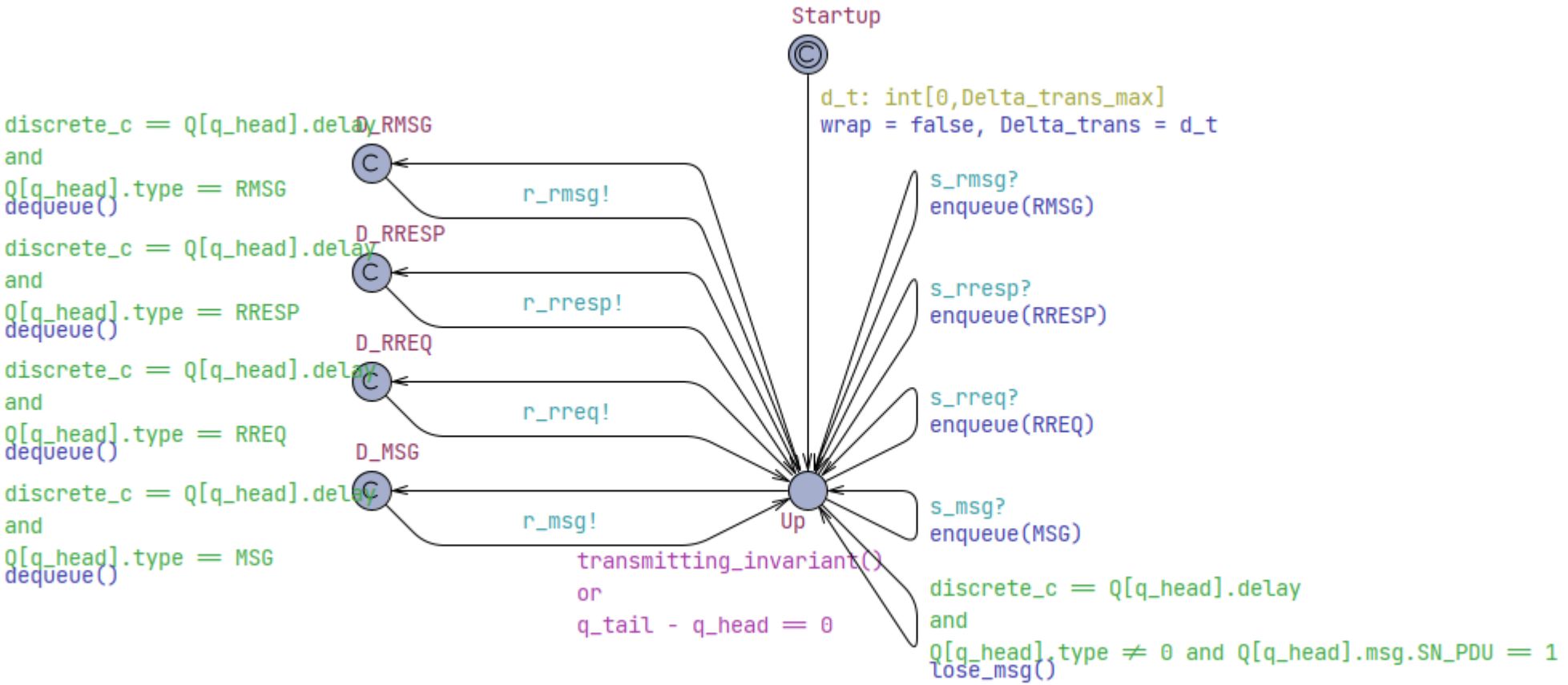




UPPAAL - RaSTA

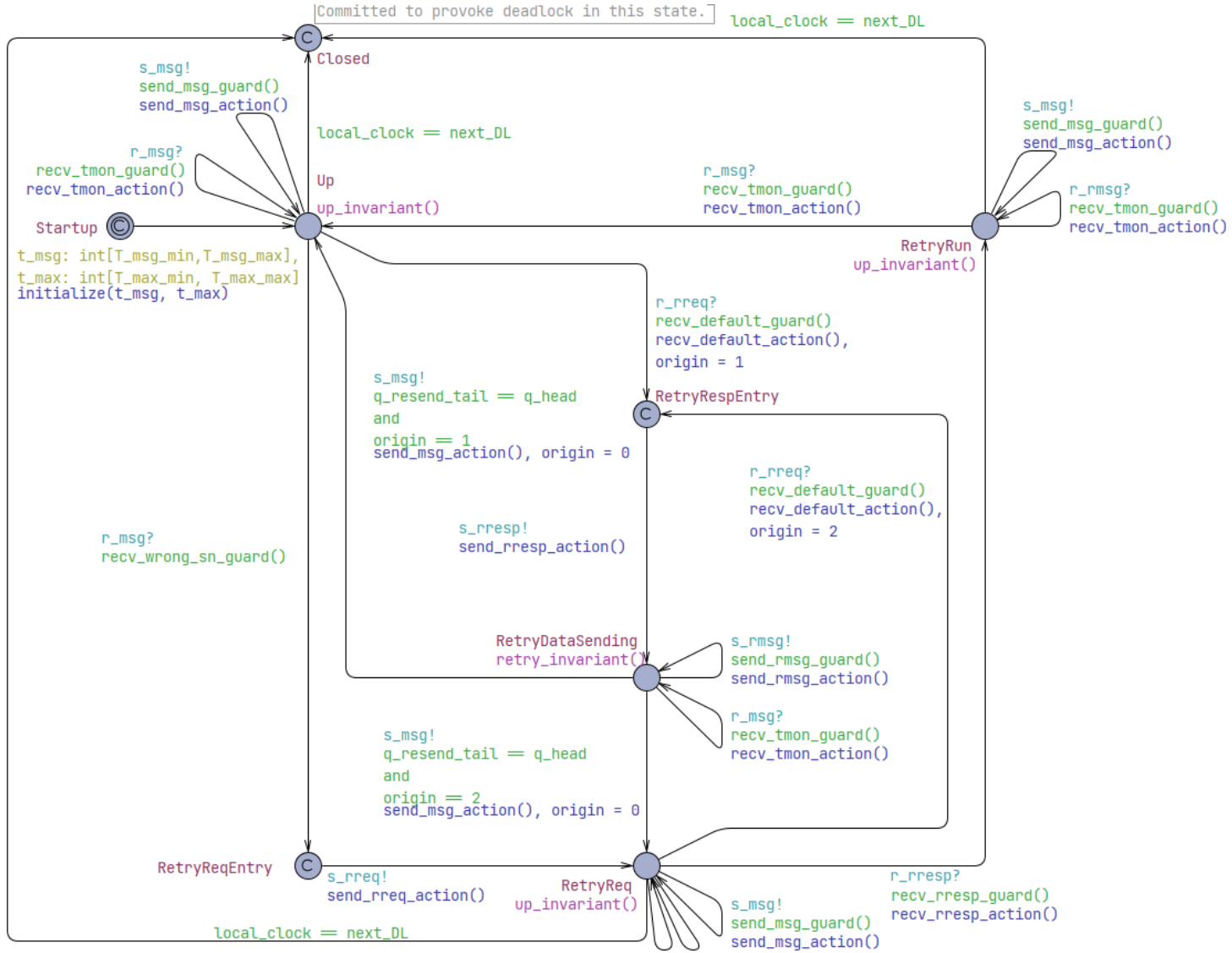


UPPAAL - RaSTA



Formale Verifikation - RaSTA

UPPAAL - RaSTA



Ausblick

- Großes Modell abstrahieren und auf Nachrichtensequenz spezialisieren
- Eigenschaften verifizieren:
  - Sequenznummern sind fortlaufend
  - Sequenznummerprüfung wird richtig durchgeführt
  - Sequenzwiederherstellung nach Packtverlust
  - …
- Anhand des Models implizite Eigenschaften ableiten

Quellen

[1] Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (Hrsg.): Elektrische Bahn-Signalanlagen – Teil 200: Sicheres Übertragungsprotokoll RaSTA nach DIN EN 50159 (VDE 0831-159). DIN VDE V 0831-200, Juni 2015.

[2] https://uppaal.org/