Dependability Checking with StoCharts

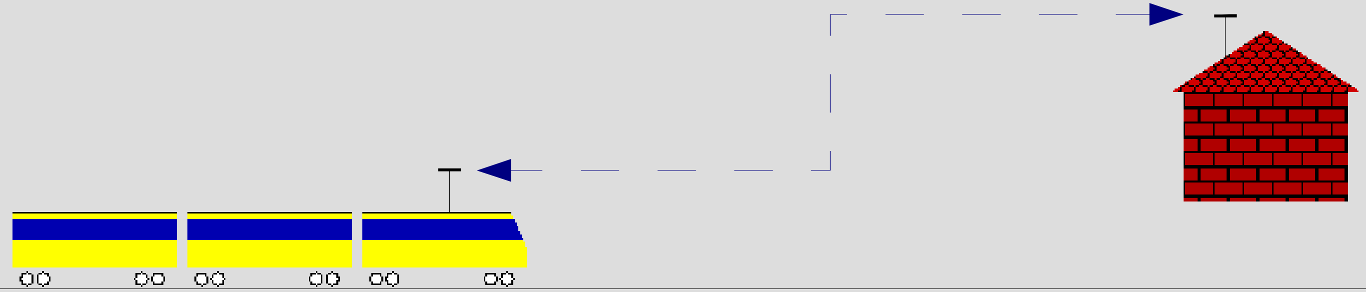
Is Train Radio Reliable Enough for Trains?

David N. Jansen
Holger Hermanns

QEST
September 30, 2004

Why train radio?

- European Train Control System
- a new standard for securing trains
- GSM-R radio communication
  between train and radio block centre



ETCS radio reliability

- **Q:** Can ETCS radio handle trains?
  - fast (300 km/h)
  - in dense traffic (headway ≈ 1 min)
  - with high reliability (99.95%)

ETCS radio reliability

- **Q:** Can ETCS radio handle trains?
  - fast (300 km/h)
  - in dense traffic (headway ≈ 1 min)
  - with high reliability (99.95%)

- **A:** Yes!

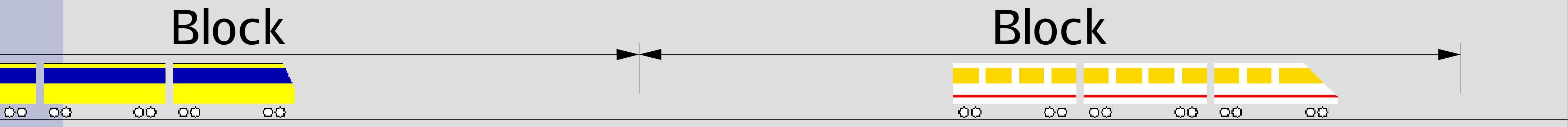
  details on the following slides

Overview

- More on securing trains and ETCS
- Our modelling language: StoCharts
- Our model
- Analysis
- Outlook

Securing Trains: Principles

- Block
  - exclusive access to a single train
  - train is not allowed to leave its block(s)
- Movement authority
  - allowance to enter a block
- Integrity check
  - make sure the complete train leaves a block



Securing Trains: Practice

- Signals show movement authorities to the driver
- Some protection against human error
  - Transmit passage of danger points electronically
  - different national systems

Interoperability

- One railway’s train runs on another railway’s track
- Mechanical interoperability is implemented
- Broken by different security systems

- ETCS standard intends to overcome this
  - specifies communication between train and track
  - does not specify internals of train
  - does not specify trackside aspects of policy

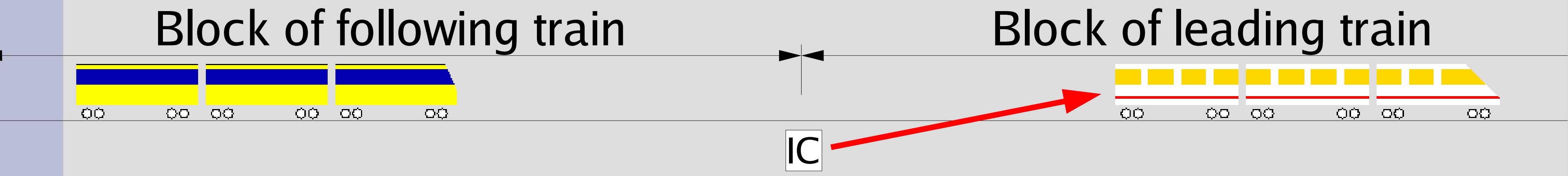
Securing Trains: New Ideas

- Exchange more information electronically
  - train characteristics
  - track information
  - complete movement authorities
- Cab signalling
- On-board integrity check

- ETCS supports these features

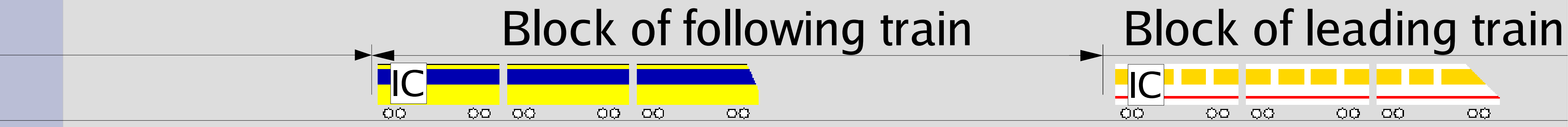
Moving Block Operation

- Enabled by on-board integrity check
- Each part of the block is freed immediately after the train has passed...
- ... and can be reserved for the next train without delay
- shorter headway ⇒ better track utilisation



Moving Block Operation

- Enabled by on-board integrity check
- Each part of the block is freed immediately after the train has passed...
- ... and can be reserved for the next train without delay
- shorter headway ⇒ better track utilisation



Speaking technically

- Eurobalise
  - trackside transceiver
  - transmit movement authorities etc. and position

Speaking technically

- Eurobalise
  - trackside transceiver
  - transmit movement authorities etc. and position

Level 1

- GSM-R
  - a variant of GSM
  - transmit movement authorities etc.

Level 2+3

- Cab signalling and on-board integrity check
  - train internal – only a few aspects specified

Level 3

Modelling Language: StoCharts

- Statecharts
- + Probabilistic choice

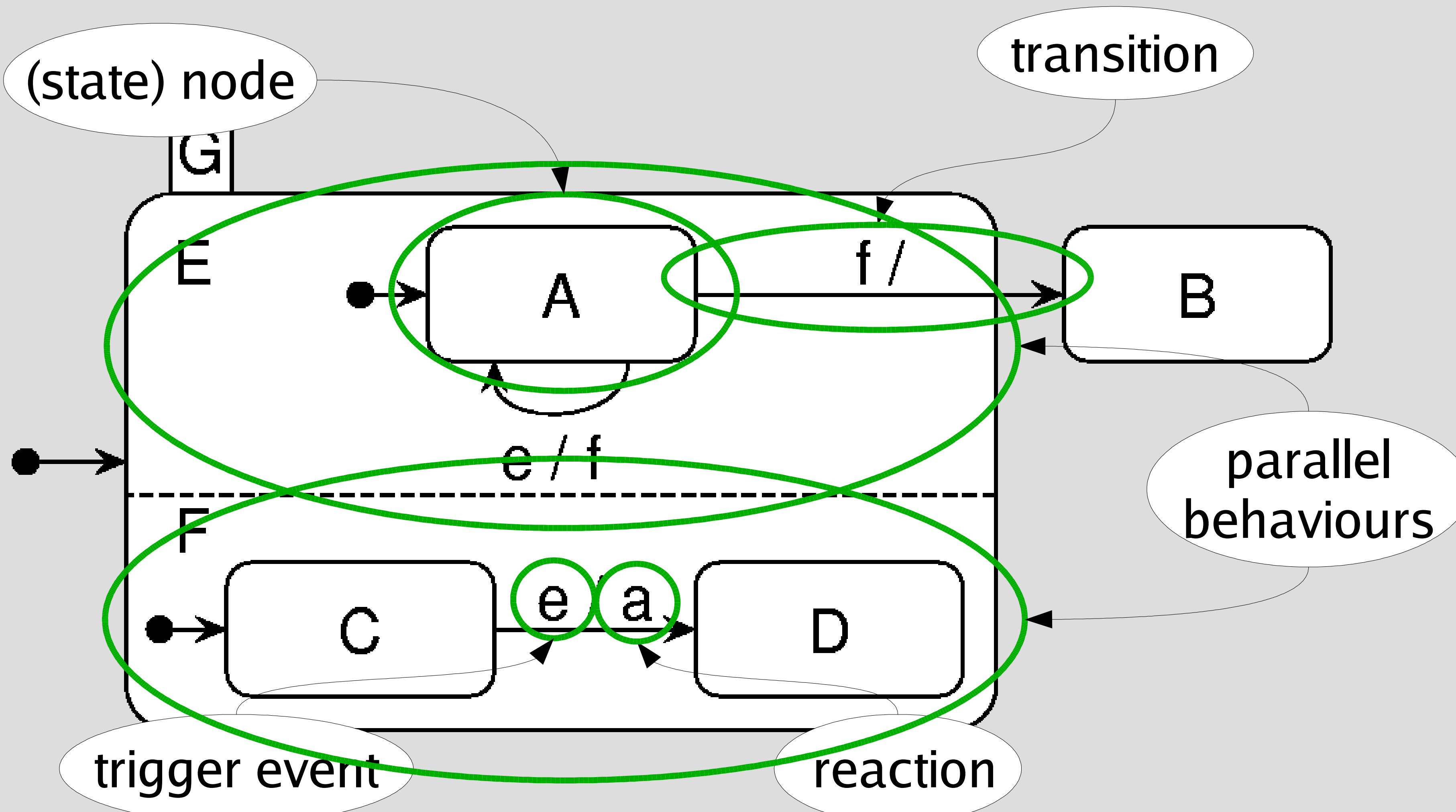
  e. g. with probability 10^{-4}, a message is lost
- + Stochastic timing

  e. g. the response time is distributed exponentially with average 0.5 sec

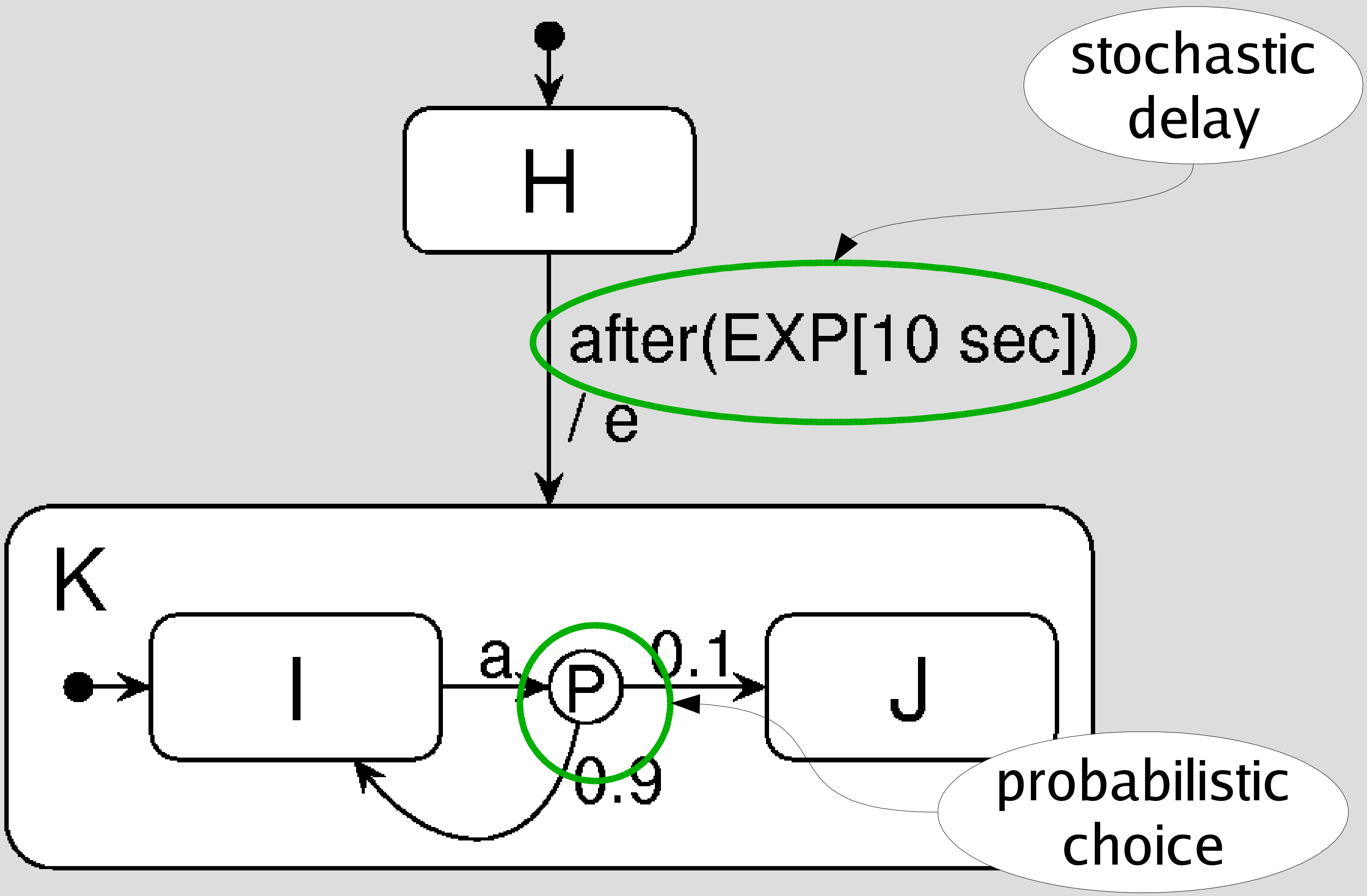
Prob(response time $\leq t$)
$= 1 - e^{-t / 0.5}$

Statecharts

- Hierarchical extension of automata



Example StoChart



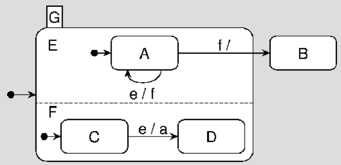
StoChart Definition

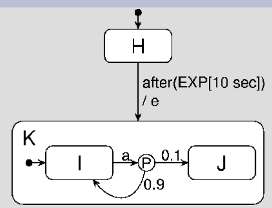
- Nodes
  - with a tree structure
- Events
  - includes pseudoevent after(*stochastic delay*)
- P-Edge
  - P = probabilistic
  - trigger: source node(s), (pseudo)event, guard
  - reaction: probability space over
    actions and destination node(s)

StoChart Semantics

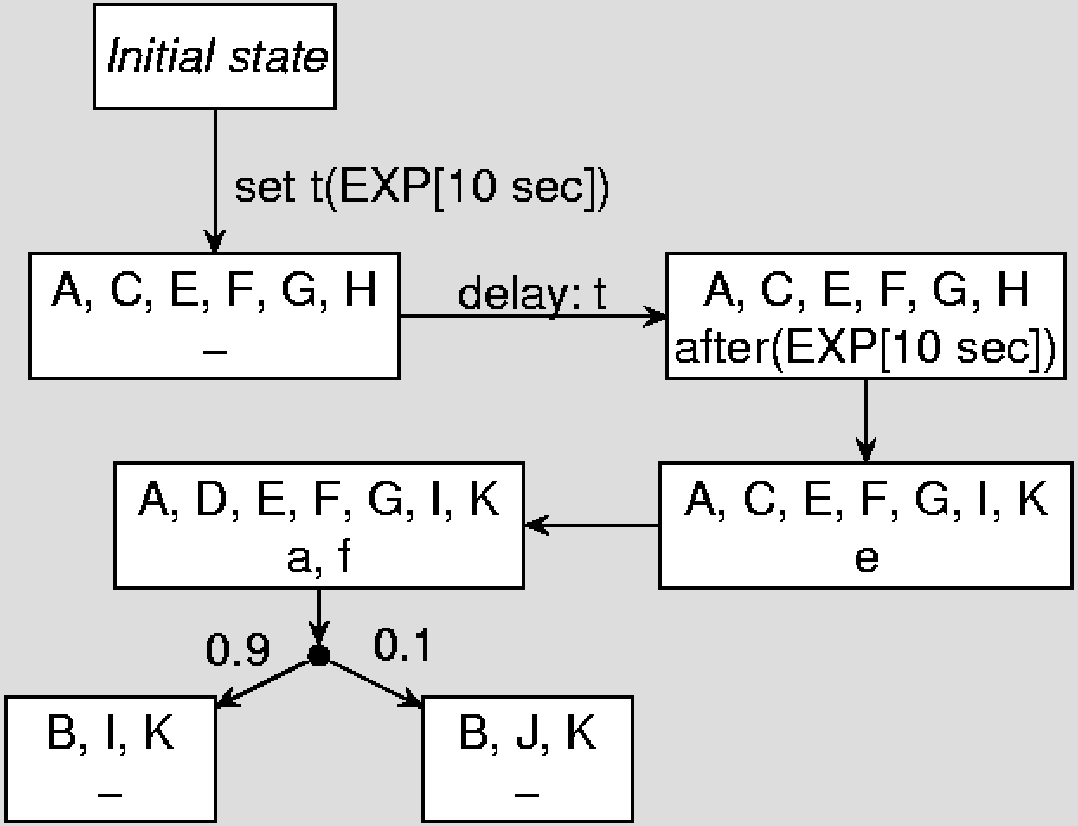
- Maps on 'Stochastic Timed I/O Automata'
- Random timers model stochastic delays
  - initialised to a sample from probability distribution
  - run down to 0
  - then trigger the corresponding edge

StoChart Semantics

- IOSA(

|| 

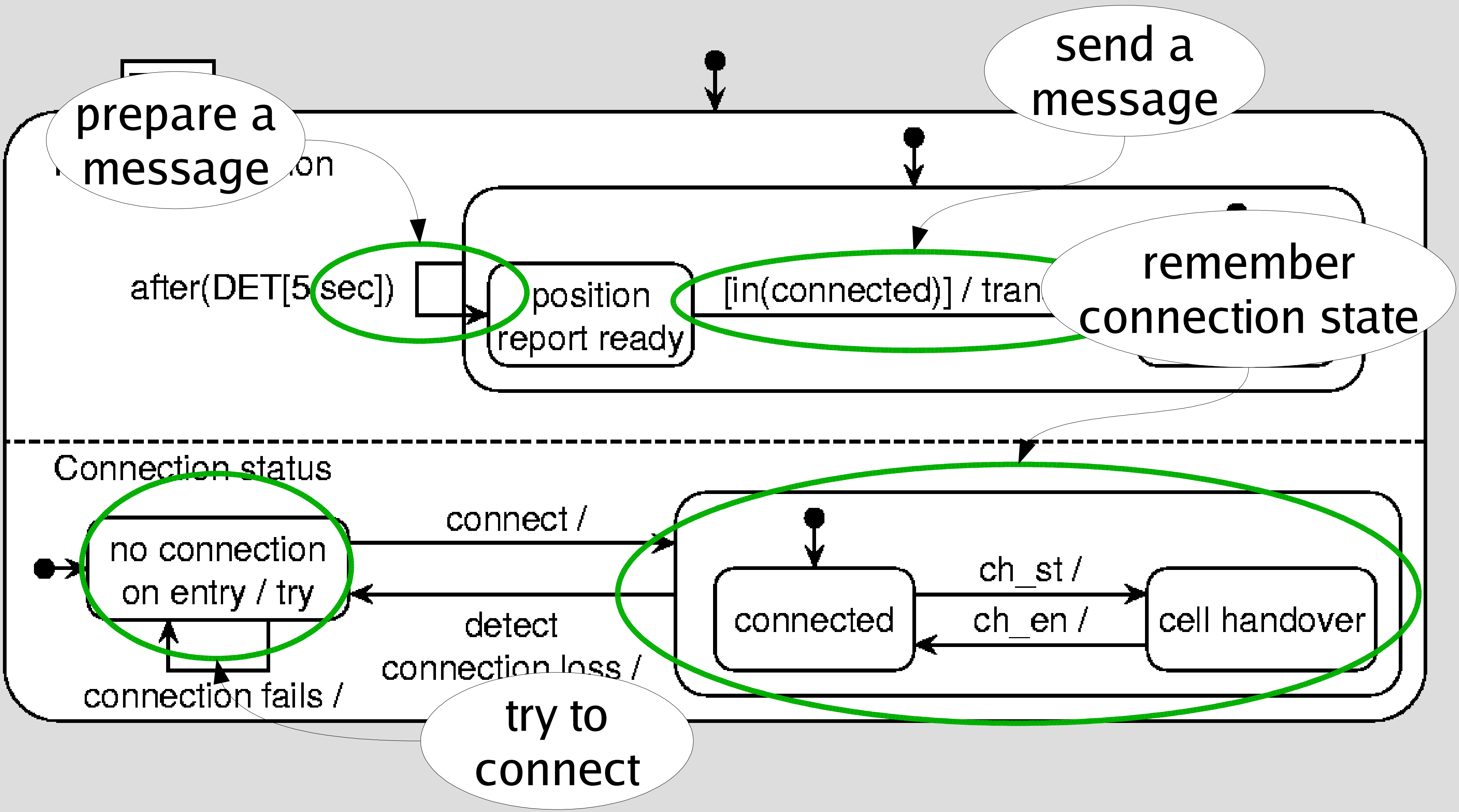
) =



Assumptions and Guarantees

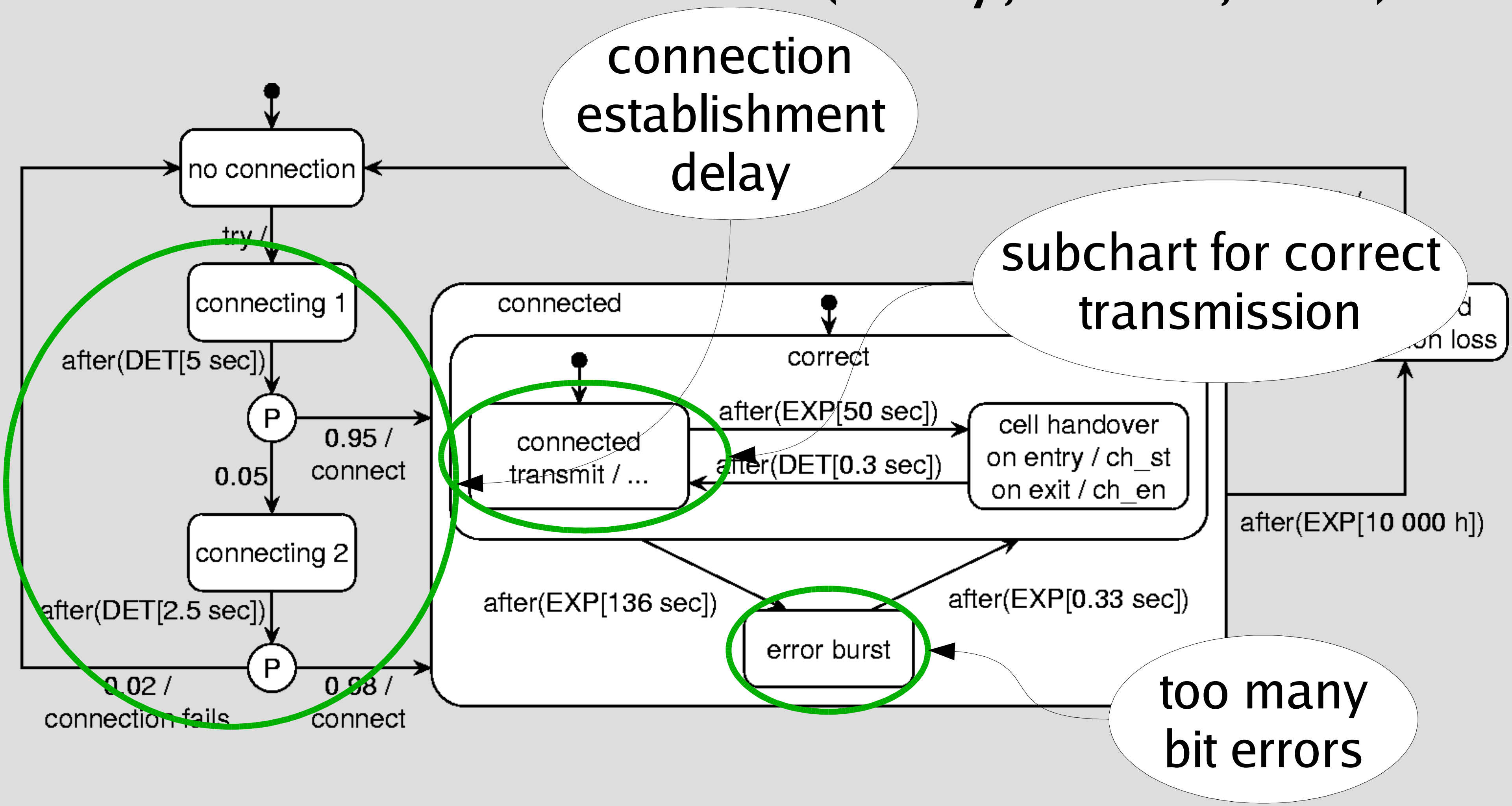
- “Design by Contract” paradigm
- If the environment keeps the assumptions, the system is guaranteed to fulfil its duty.
- Our assumptions: GSM-R works as specified
  - e. g. a GSM-R connection is established within 5 sec with 95% probability.
- Our guarantees: ETCS radio is as dependable as specified
  - e. g. the communication succeeds with 99.95% probability.

Sender Model

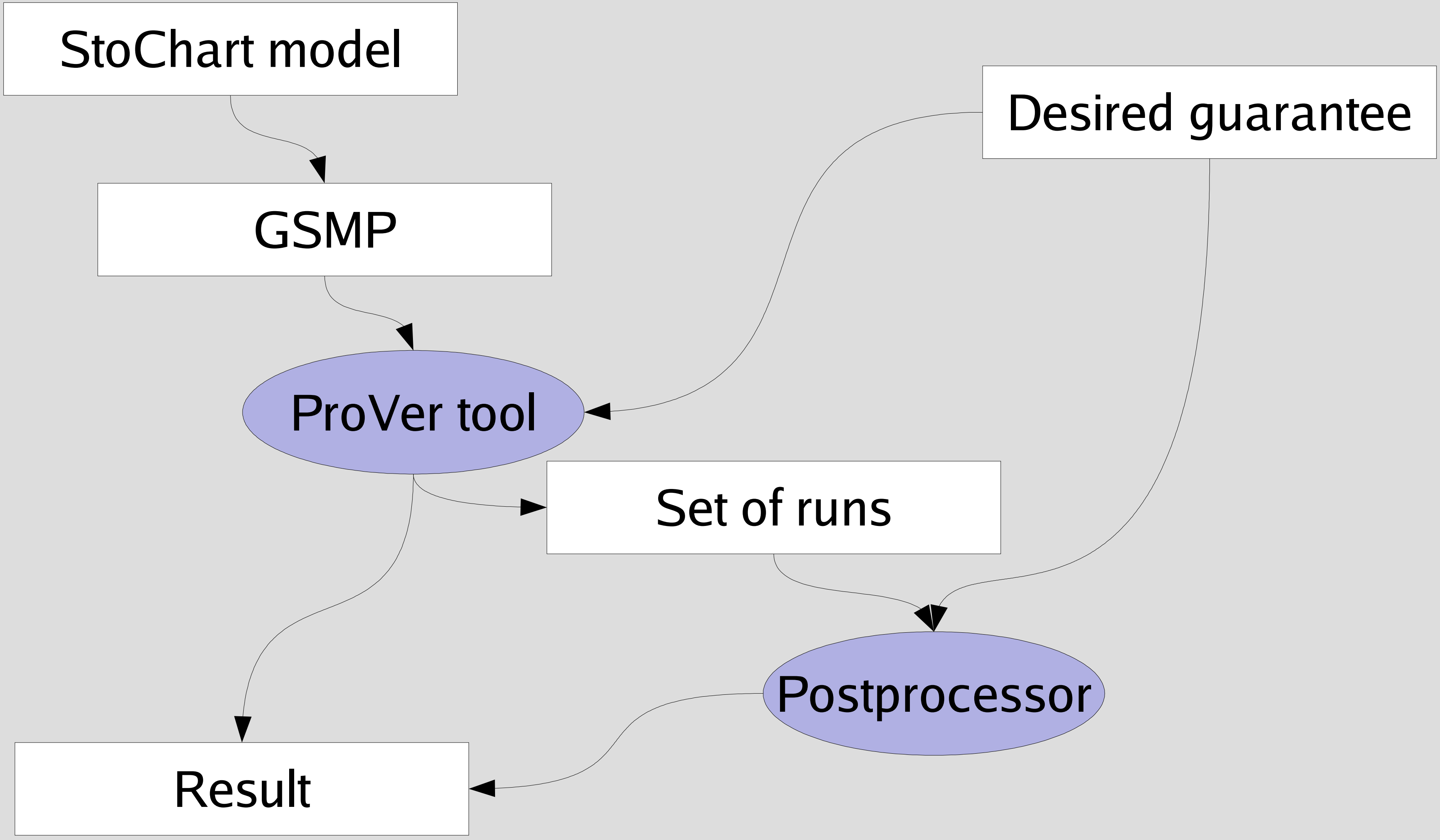


Receiver Model

- includes channel model (delay, errors, loss)



Model Analysis



ProVer tool

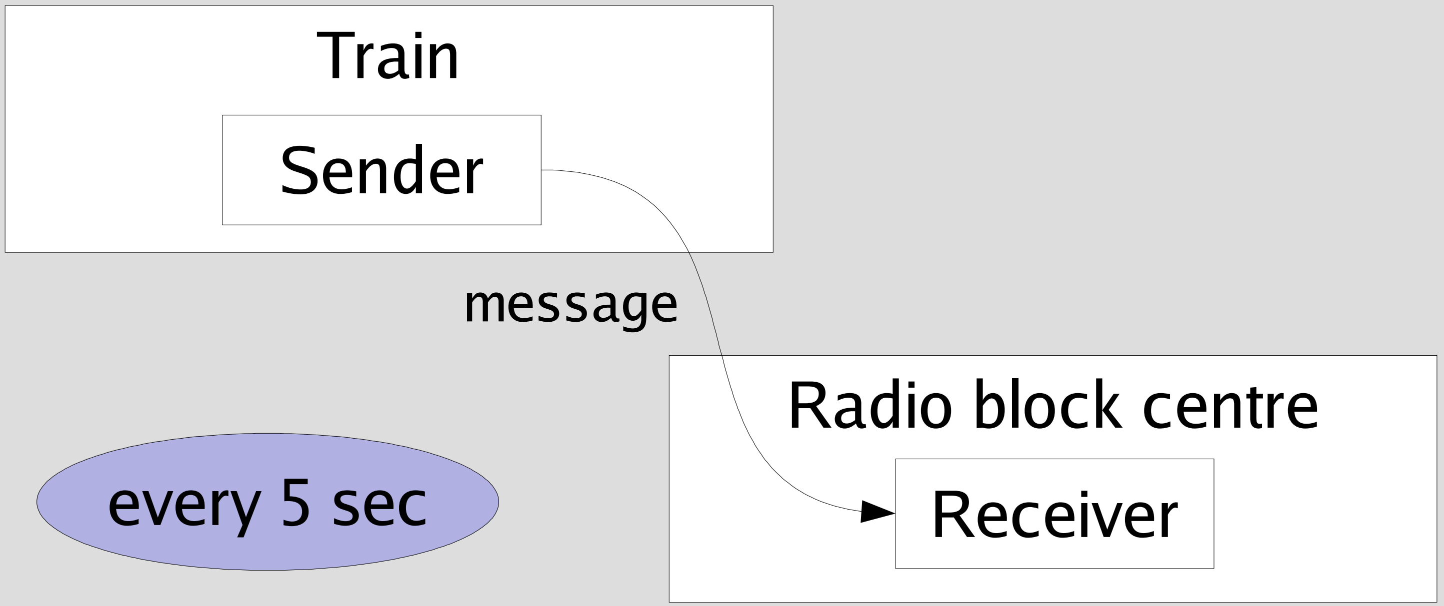
- simulation tool
- model checker like: estimates whether a probabilistic property is satisfied
  - e. g.: Is the probability of a failure less than 1%?
  - Possible answer: Yes, with confidence 0.99.
- tailored to GSMPs
- developed at CMU by Håkan Younes

Communication Reliability

- Is the communication reliable enough?
- Required by the spec is 99.95%

Communication Reliability

- Is the communication reliable enough?
- Required by the spec is 99.95%



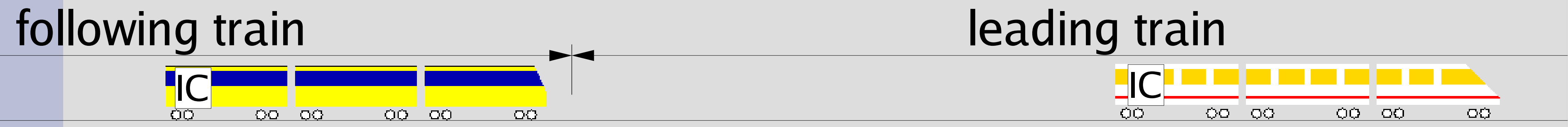
Communication Reliability

- 99.95% requirement is ambiguous:
  No time bound for communication provided
- Analysed directly using ProVer
- Time until first message arrives — Probability

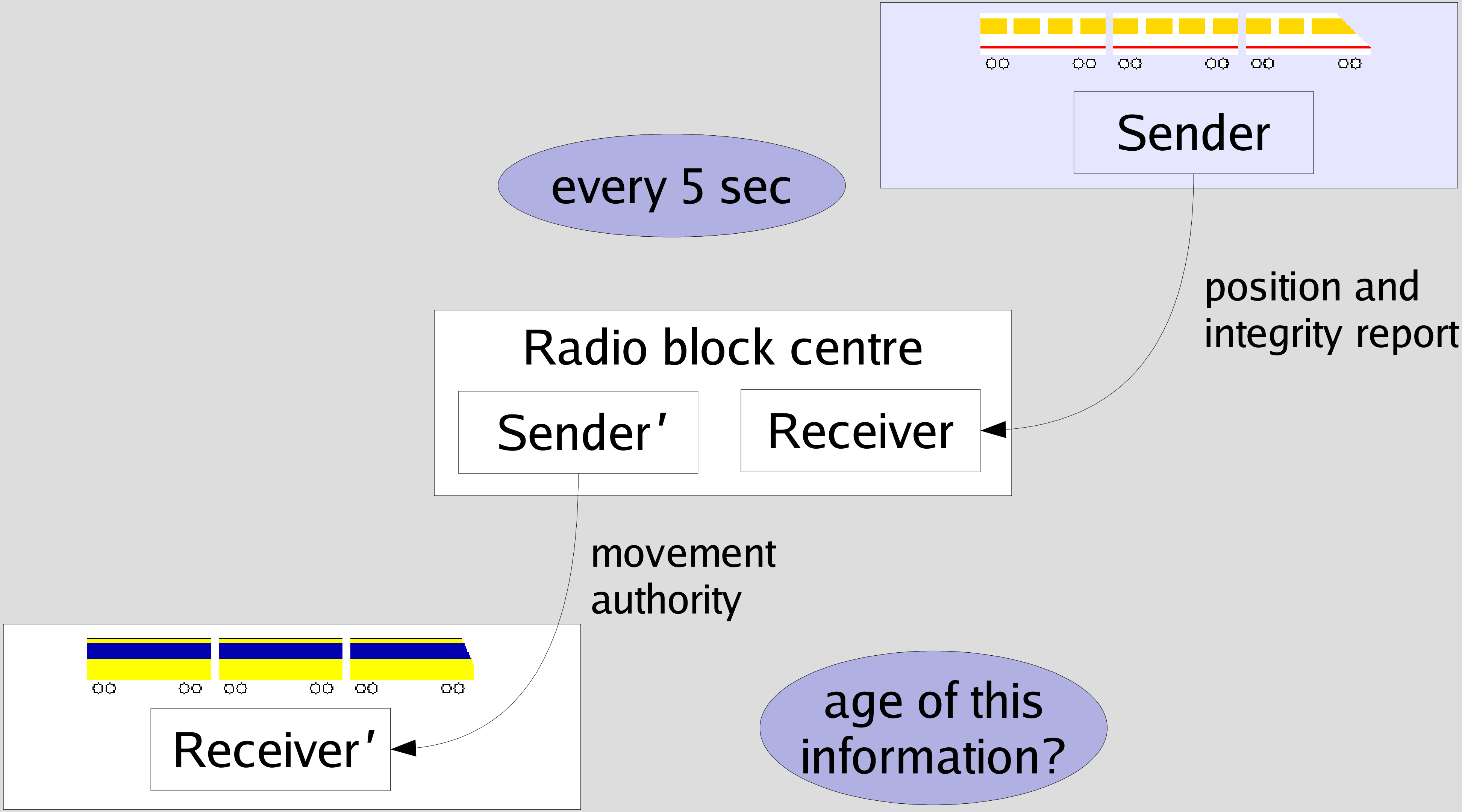
Time until first message arrives	Probability
10 sec	0.98267
15 sec	0.999700
20 sec	0.9999944

Delayed Trains

- How often do GSM-R failures cause delays?
- Challenging scenario:
  Two trains at minimal distance
  - for a full trip (~ 1 hour)
  - at maximum speed (300 km/h)
  - with moving block operation



Delayed Trains



Delayed Trains

- Age of the information cannot be measured directly
- Measure an upper bound
-

Headway	Probability to brake at least once
57.4 sec	0.9562
62.4 sec	0.101
67.4 sec	0.0036
72.4 sec	0.00034

4 train pairs per hour $\Rightarrow$
< 1 train per month delayed

Related Work

- Our work is inspired by work of [Zimmmermann/Hommel 2003]
  - use stochastic Petri nets (general distributions)
  - numerical solution, not simulation
  - slightly different model
  - entirely different results

Related Work

- Assumptions of Zimmermann/Hommel
  - “deadline” corresponds to a headway ~ 54 sec
  - no multiple failures
  - almost only exponential distribution

Outlook

- Recommendation for reliability
  - Is this service needed always?
    Otherwise, a cheaper solution
    (= weaker assumptions) could be enough.
- Work in progress:
  Analysis with the Möbius tool (via MoDeST)
  - expect easier translation to MoDeST
  - first results are promising: similar outcomes