Epistemic parametric uncertainties in availability assessment of a Railway Signalling System using Monte Carlo simulation

Siqi Qiu[a], Mohamed Sallak[a], Walter Schön[a], Zohra Cherfi-Boulanger[b]

siqi.qiu@utc.fr

[a]UMR CNRS 7253 Heudiasyc
Compiegne University of Technology

[b]UMR CNRS 7337 Roberval
Compiegne University of Technology

October 1, 2013

ESREL 2013 - Amsterdam, Netherlands

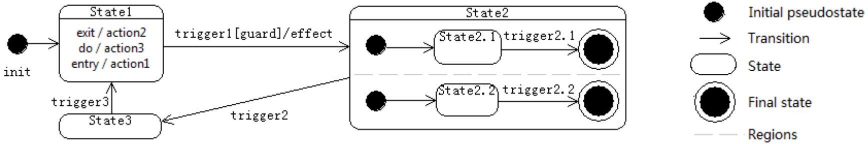
Outline

- Introduction
- Statecharts
- RAMS requirements
- Two-phase nested Monte Carlo simulation
- Application: ERTMS/ETCS Level 2
- Conclusion and perspective

Introduction

- Propose a dynamic model of ERTMS/ETCS Level 2 in Statecharts.
- Evaluate the instantaneous availability of ERTMS/ETCS Level 2.
- Study the influence of uncertain parameters.
  - Two kinds of uncertainties:
    - Aleatory uncertainty
    - Epistemic uncertainty
  - Epistemic parametric uncertainties (imprecision) are taken into account.

Statecharts



Two kinds of epistemic uncertainties may exist in Statecharts:

- Epistemic state uncertainty represents the imprecision of the states of the model.
- Epistemic parametric uncertainty represents the imprecision of the values of parameters (transition rates).

RAMS requirements

- RAMS are considered as fundamental characteristics of railway systems. Equipment should satisfy RAMS requirements to meet the service expectations and ensure the safety of railway systems.
- Some RAMS analysis methods:
  - Failure modes, effects and criticality analysis (FMECA)
  - Fault tree analysis (FTA)
  - Dependent failure assessment (common cause and common mode)
  - Reliability block diagrams (RBD) and Monte Carlo simulations

1998 EEIG ERTMS Users Group, "*ERTMS/ETCS RAMS Requirements Specification. Chapter 2 - RAM.*"

2009 UNISIG, "*Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2.*"

RAMS requirements

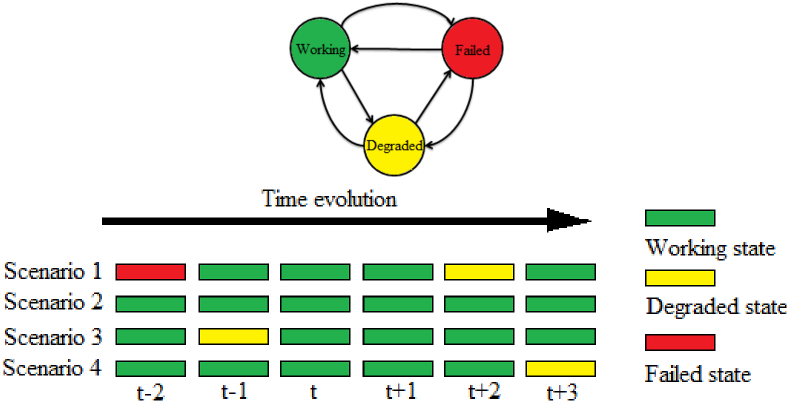
Some RAMS requirements of ERTMS:

Availability targets
Operational availability, due to all the causes of failure, shall be not less than 0.99973
Operational availability, due to hardware failures and transmission errors, shall be not less than 0.99984
Reliability targets
The Mean Time Between Immobilising hardware Failures $MTBF - I_{ONB}$, defined for Onboard equipment, shall be not less than $2.7 * 10^6$ hours.
The $MTBF - I_{TRK}$, defined for Trackside Centralised equipment, shall be not less than $3.5 * 10^8$ hours.

$$Operational\,availability = \frac{T_{op}}{T_{op} + T_{fault}}$$

T_{op}: Time of ERTMS correct operation
T_{fault}: Time of ERTMS fault condition

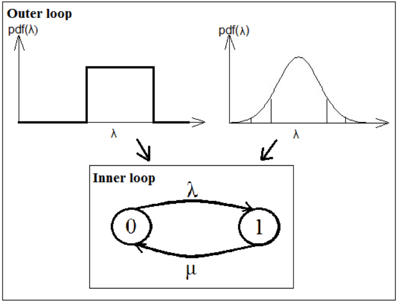
Instantaneous availability



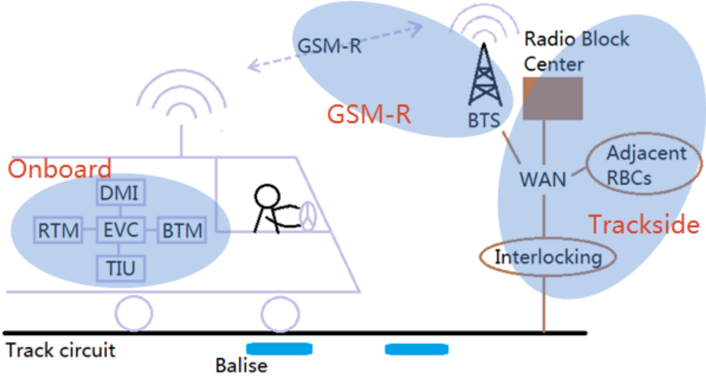
Instantaneous availability = $\frac{\textit{number of working and degraded scenarios}}{\textit{number of operational scenarios}}$ at each sampling instant.

Two-phase nested Monte Carlo simulation

- Outer loop: uncertain parameters are sampled
  - Epistemic uncertainties in parameters (transition rates) are characterized by probability distributions.
  - Two kinds of probability distributions are considered:
    - Uniform distribution
    - Normal distribution : 95% confidence interval and 99% confidence interval
- Inner loop: the model of the system is executed



ERTMS/ETCS Level 2



RTM: Radio Transmission Module
BTM: Balise Transmission Module
TIU: Train Interface Unit
DMI: Driver Machine Interface
EVC: European Vital Computer

Previous ERTMS models

2005 "*From StoCharts to MoDeST : a comparative reliability analysis of train radio communications*"

Published in: "Proceedings of the 5th international workshop on Software and performance"

2010 "*Performance assessment of european railway signalling system superposed of the french system in the presence of failures*" (Coloured Petri Nets)

Published in: "Lamda-Mu'2010"

Previous ERTMS models

2011 "*Mechanising the Validation of ERTMS Requirements and New Procedures*" (UML diagrams)

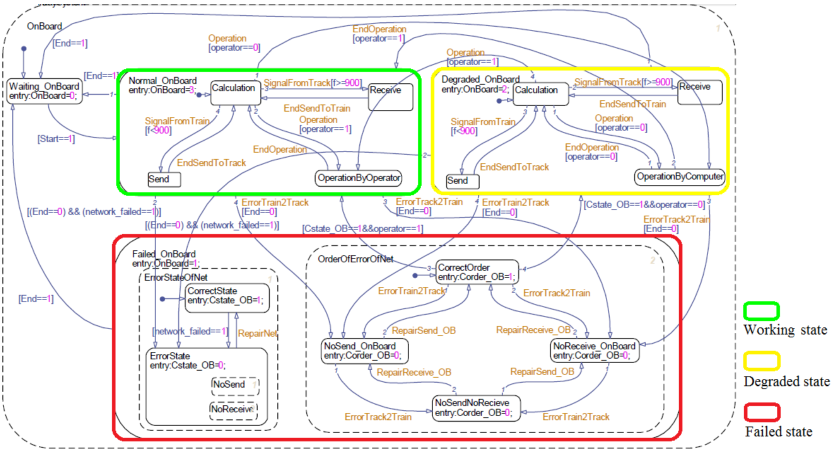
Published in: "9th World Congress on Railway Research"

2011 "*Modeling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks*" (UML diagrams)

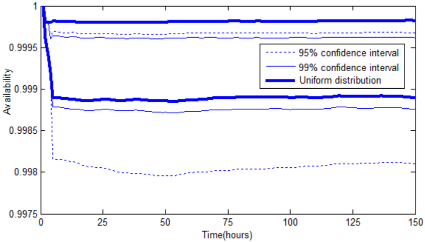
Published in: "Proceedings of the 15th European Safety and Reliability Conference"

There isn't a complete model which takes all the constituents of ERTMS and its dynamic behavior into account.

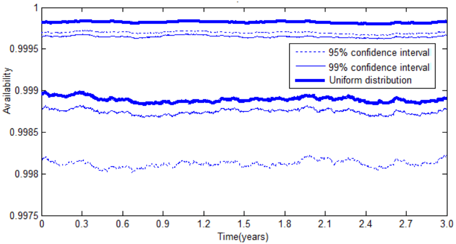
Statechart of the Onboard system



Results: Instantaneous availability

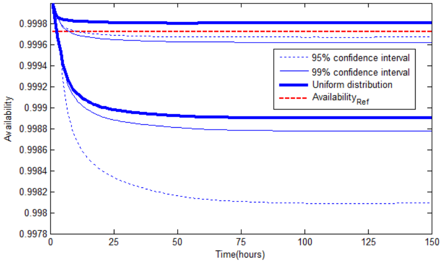


In the short term

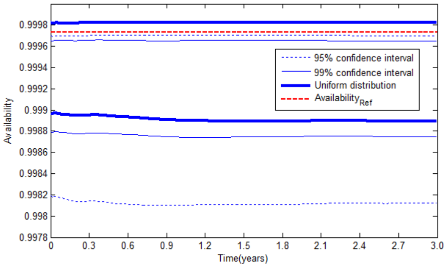


In the long term

Results: Operational availability



In the short term



In the long term

Sensitivity Analysis

- Aim: estimate which kind of probability distribution of epistemic uncertainties has the most significant influence on the availability of ERTMS/ETCS Level 2.
- This influence is measured by the distance between the minimum of the upper bound and the maximum of the lower bound of the instantaneous availability interval when the two bounds tend to remain constant:
  - Uniform distribution : 0.00081
  - Normal distribution
    - 95% confidence interval : 0.00144
    - 99% confidence interval : 0.00080

Conclusion

- Model ERTMS/ETCS Level 2 in Statecharts
- Propose a methodology based on two-phase Monte Carlo simulation to evaluate the instantaneous availability of ERTMS under uncertainty
- Study the influence of the type of epistemic uncertainties' distribution on the availability of systems.

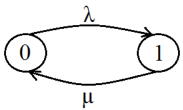
Perspective

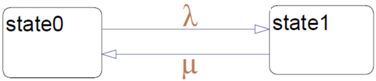
- Model ERTMS/ETCS Level 2 in Valuation-Based Systems and analyze epistemic uncertainty by belief functions theory

Thank you for your attention

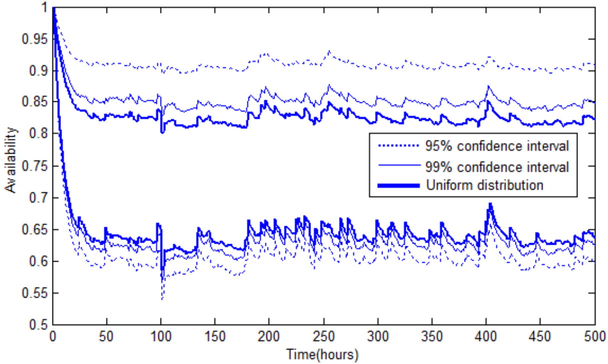
siqi.qiu@utc.fr

Example: a binary component





Epistemic uncertainty exists in the failure rate → $\lambda \in [\underline{\lambda}, \overline{\lambda}]$



Epistemic uncertainties in the transition rates

Epistemic uncertainties exist in four transition rates:

- The failure rate from the working state to the failed state "**ErrorStateOfNet**" λ_{n1} and its corresponding repair rate μ_{n1}.
  - $\lambda_{n1} \in [\underline{\lambda_{n1}}, \overline{\lambda_{n1}}]$ and $\mu_{n1} \in [\underline{\mu_{n1}}, \overline{\mu_{n1}}]$
- The failure rate from the working state to the failed state "**OrderOfErrorOfNet**" λ_{n2} and its corresponding repair rate μ_{n2}.
  - $\lambda_{n2} \in [\underline{\lambda_{n2}}, \overline{\lambda_{n2}}]$ and $\mu_{n2} \in [\underline{\mu_{n2}}, \overline{\mu_{n2}}]$