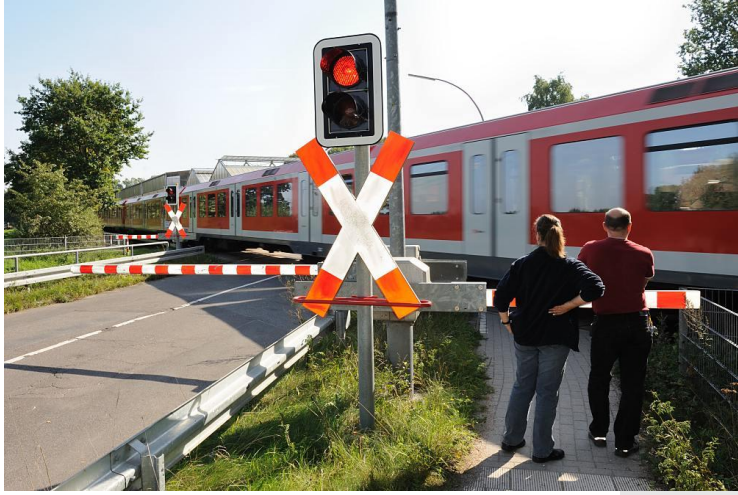
TU Clausthal



# Some Issues on Formal Safety Analysis and Verification in Industrial Practice


Michaela Huhn[1]

Joint work with Sara Bessling[1], Ilays Daskaya[2], and Stefan Milius[2]

[1]Clausthal University of Technology, Department of Informatics

[2]Braunschweig University of Technology, Institute of Theoretical Computer Science

# Motivation

- „Formal methods, notably formal verification, are an adequate means in development of safety critical systems.“
- But still a gap between research-driven success stories and industrial practice.
- Questions (in the context of SCADE Suite)
  - What does it need to make formal verification an every day task?
  - What building blocks can be used in safety cases and certification?
- Industrial case studies at hand: Pacemaker and Level crossing control