Some Issues on Formal Safety Analysis and Verification in Industrial Practice

Michaela Huhn¹

Joint work with Sara Bessling¹, Ilays Daskaya², and Stefan Milius²

¹Clausthal University of Technology, Department of Informatics
²Braunschweig 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