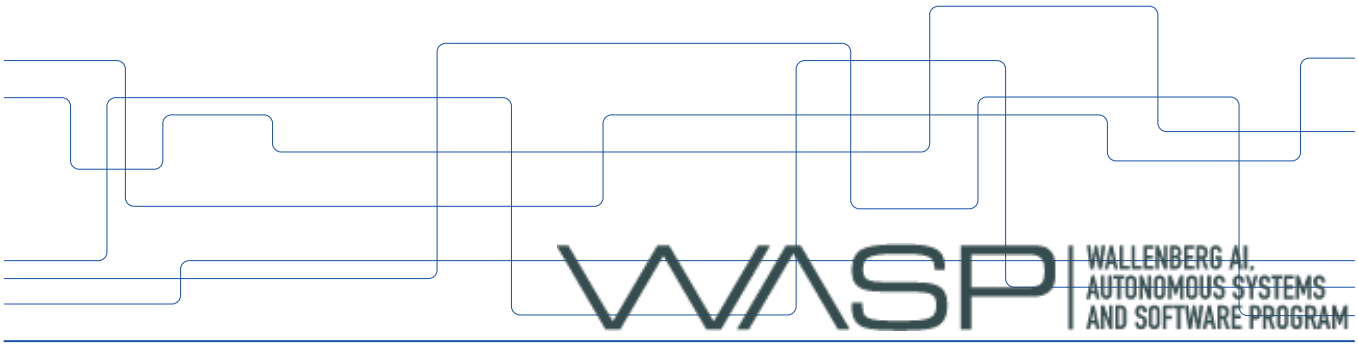
High-Confidence Formal Verification of Real Cyber-Physical Systems: from Models to Machine Code

David Broman
Associate Professor
KTH

Magnus Myreen
Associate Professor
Chalmers



Application Areas

Automotive

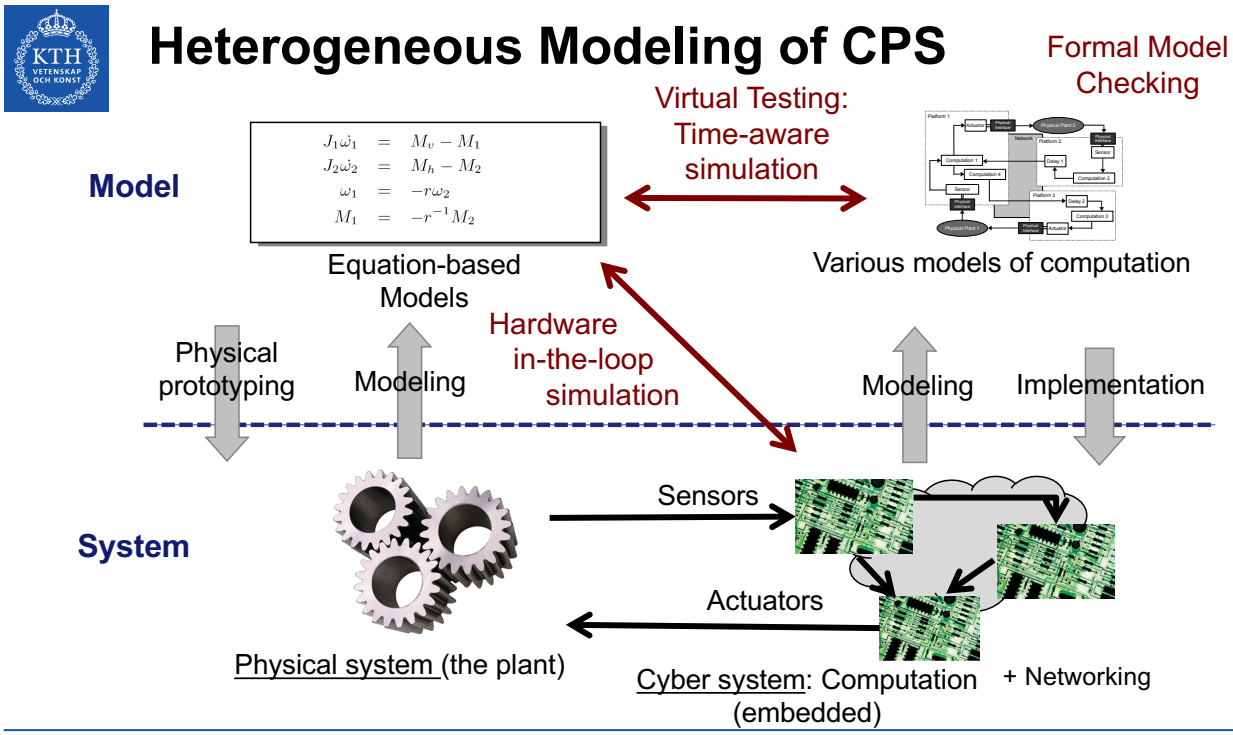
Aircraft

Cyber-Physical Systems (CPS)

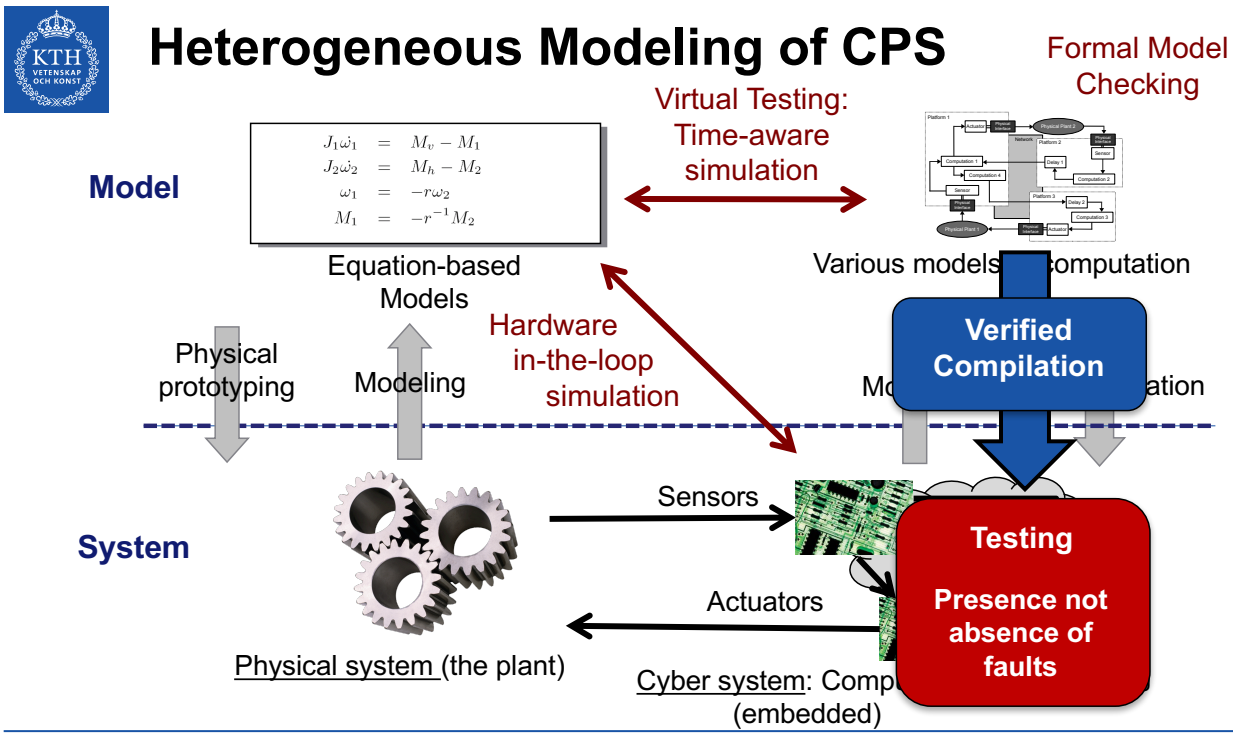
Satellites

Container Automation

Heterogeneous Modeling of CPS



Heterogeneous Modeling of CPS



Research Challenges

Model Checking
- UPPAAL
- Verified LTL model checker (Esparza, 2013)
- Verified Timed automata in Isabelle (Wimmer, 2018)

Verified Compilers
- CompCert (Leroy, 2009)
- CakeML (Kiam Tan et al., 2016)
- Véluz (Bourke et al, 2017)

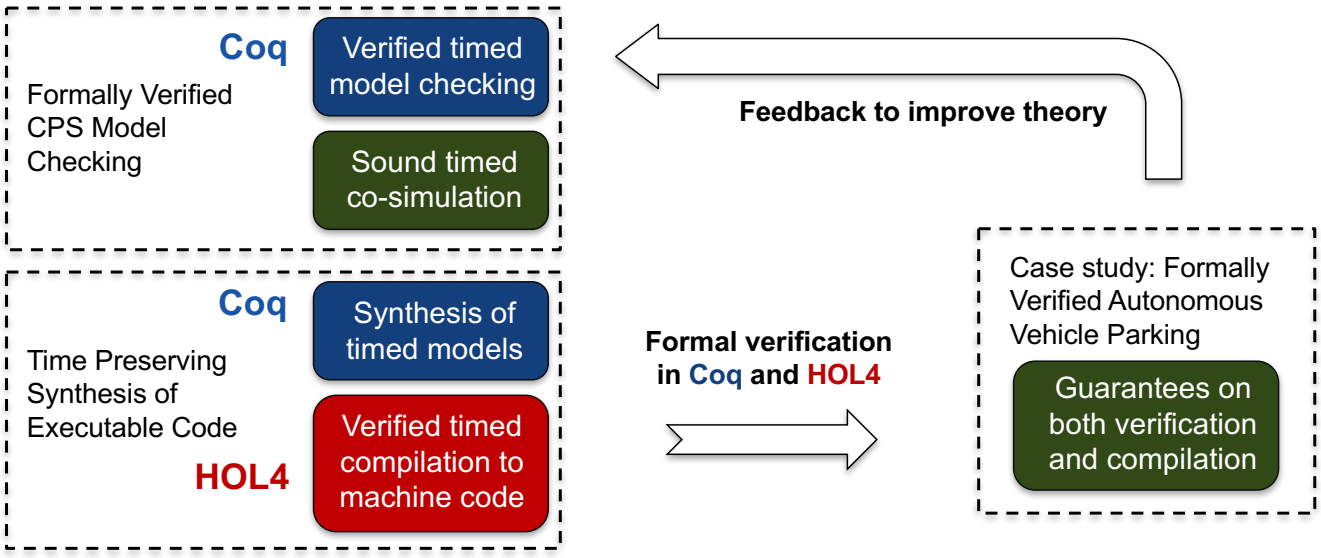
Challenge 2:
Formally verify the verifier and transfer proof

Challenge 1:
Both functional and temporal constraints

The overall research goal of this project is to

*develop a new theoretical foundation of **formally verified** cyber-physical domain-specific model compilation, **from high-level real system models down to machine code**, satisfying both **functional and temporal constraints.***

Project Overview



Team

David Broman, Assoc. Prof., KTH
Modeling languages, CPS,
real-time systems, and co-sim

Magnus Myreen, Assoc. Prof., Chalmers
Programming languages and
interactive theorem proving

Elias Castegren
Postdoc, KTH
Prog. languages, Coq

Mauricio Chimento
Postdoc, KTH
Formal methods, Coq

Hira Taqdees Syeda,
Postdoc, Chalmers
Formal methods, HOL4

Expedition Vision