Towards Enabling Reuse in the Context of Safety- critical Product Lines

Barbara Gallina
School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
name.surname@mdh.se

19th May 15, 5th International Workshop on PLEASE (Product LinE Approaches in Software Engineering)

Context

- Safety-critical systems
- Safety certification/self assessment
- Safety cases
  - Process-based arguments
  - Product-based arguments

Time consuming and costly!

Dilemma

- Re-invent not-to-reinvent the wheel

- Standardization framework:
  - Reusable Software Components
  - Safety Element out of Context

Challenges

- Economical
  - How reuse could be enabled? →time/cost reduction!
  - How unnecessary repetitive actions could be reduced/eliminated?
- Societal
  - How safer products could be achieved?

Talk outline

- Background
  - Product lines
  - Safety-oriented process lines
  - Safety case lines
- Anti-Sisyphus
- Related work
- Conclusion and future work

Safety-critical product lines

- We are surrounded by families of products
  - Intra-domain products at micro-level
    - Fuel level estimation and display systems
  - Intra-domain products at macro-level
    - Trucks
  - Inter-domain products
    - Operating systems

Safety-oriented Process Lines (SoPL)

- Families of (safety-oriented) processes
  - (partial)commonalities
  - variabilities

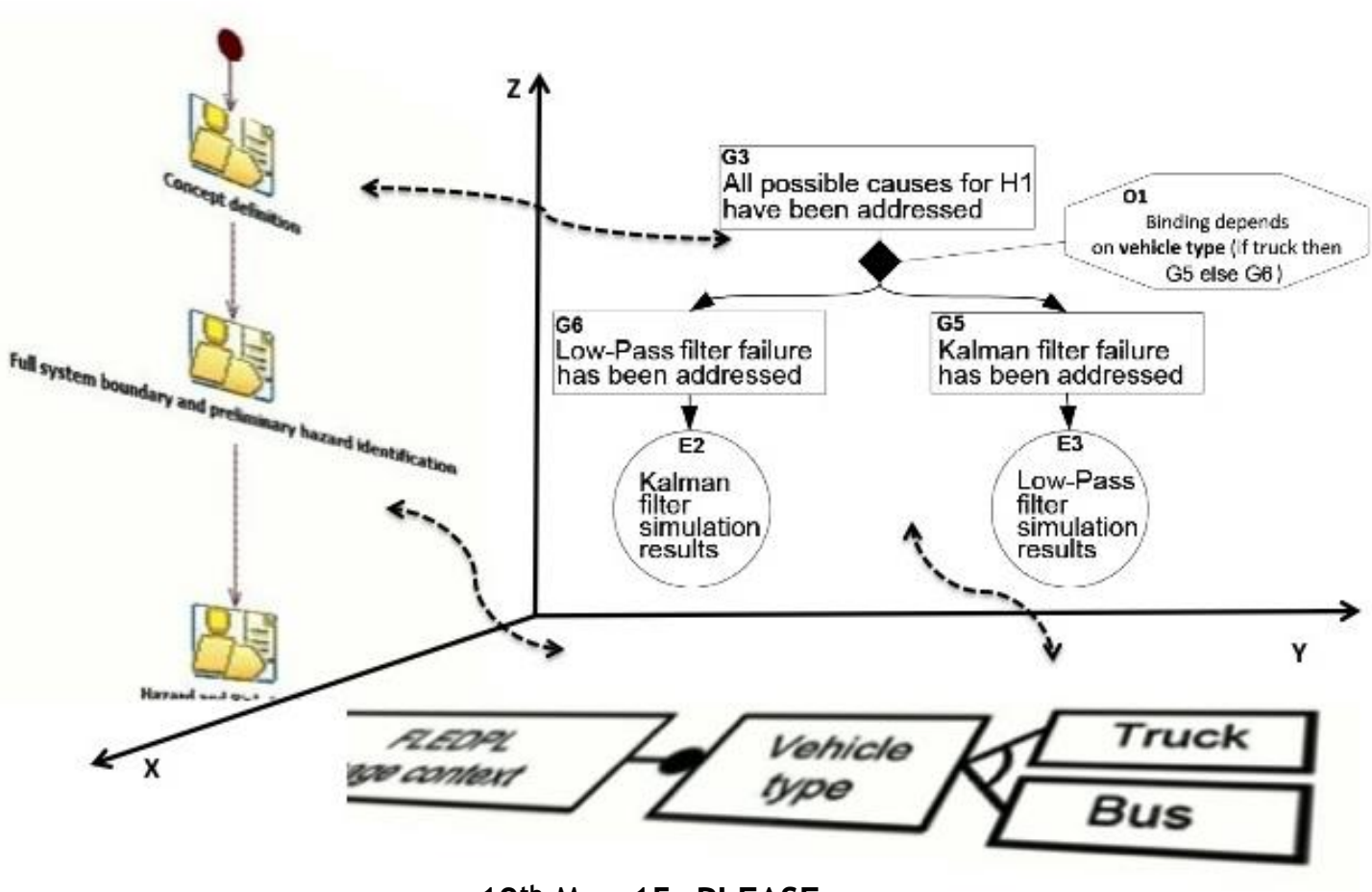
Safety case lines

- Families of safety cases
  - (partial)commonalities
  - variabilities

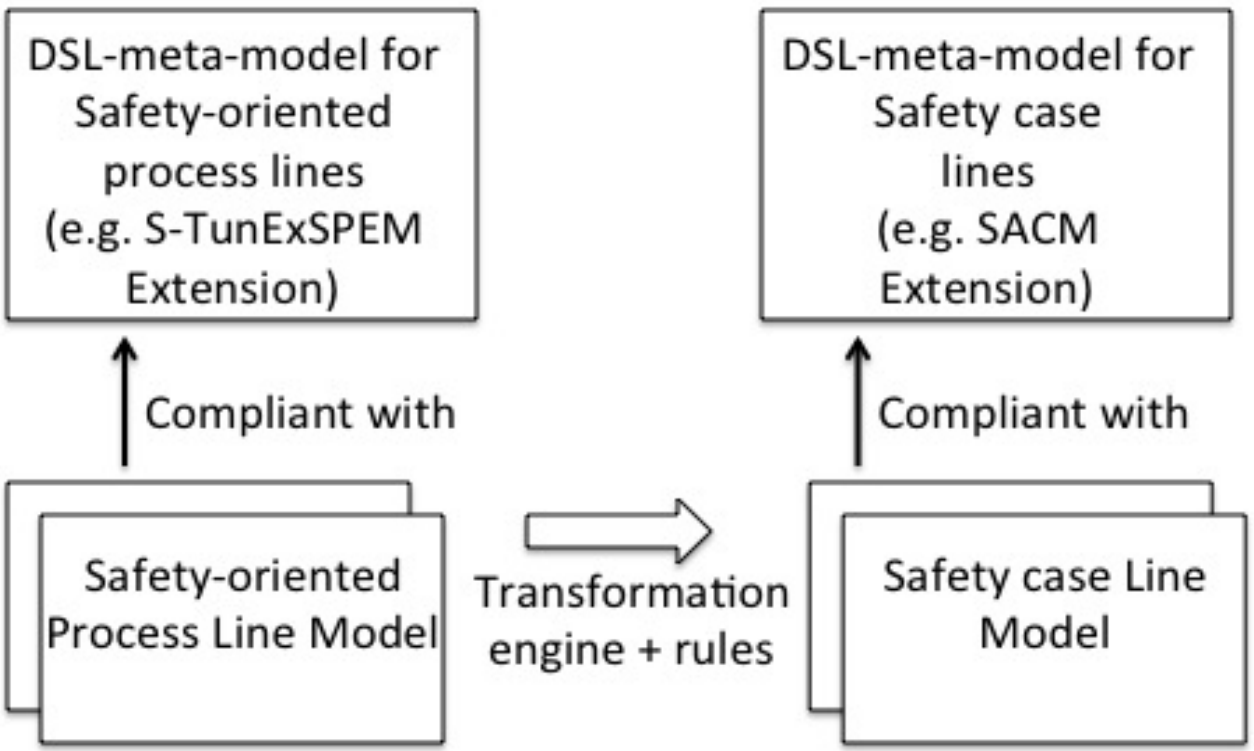
Talk outline

- Background
- Anti-Sisyphus
- Conclusion and future work

Anti-Sisyphus



Towards-Anti-Sisyphus



THRUST & MDSafeCer

Conclusion and future work

- Anti-Sisyphus: a novel methodological framework aimed at avoiding unnecessary repetitive actions while building safety cases for safety-critical product lines
  - 3D reuse-based approach
    - Safety-oriented process lines
    - Safety-critical product lines
    - Safety case lines
    - Model-driven safety certification
- Provision of intra/cross-quadrant modeling means
- Model transformations enabling generation of reusable safety-case fragments
- Prototype tool support

Thank you for your attention!

Discussion time…
Dating time!