Lessons-learned from Applying STAMP Safety and Security Analysis on AEB for L4 Autonomous Driving

Shefali Sharma[1], Adan Flores[1], Carlos Moreno[1] , Chris Hobbs[2] , Jeff Stafford [3], Kamal Lamichhane[1], Waleed Khan[1] and Sebastian Fischmeister[1]

[1] University of Waterloo, Waterloo, ON, Canada

[2]QNX Software Systems Limited, Kanata, ON, Canada

[3]Renesas Electronics America Inc., Farmington Hills, MI, USA

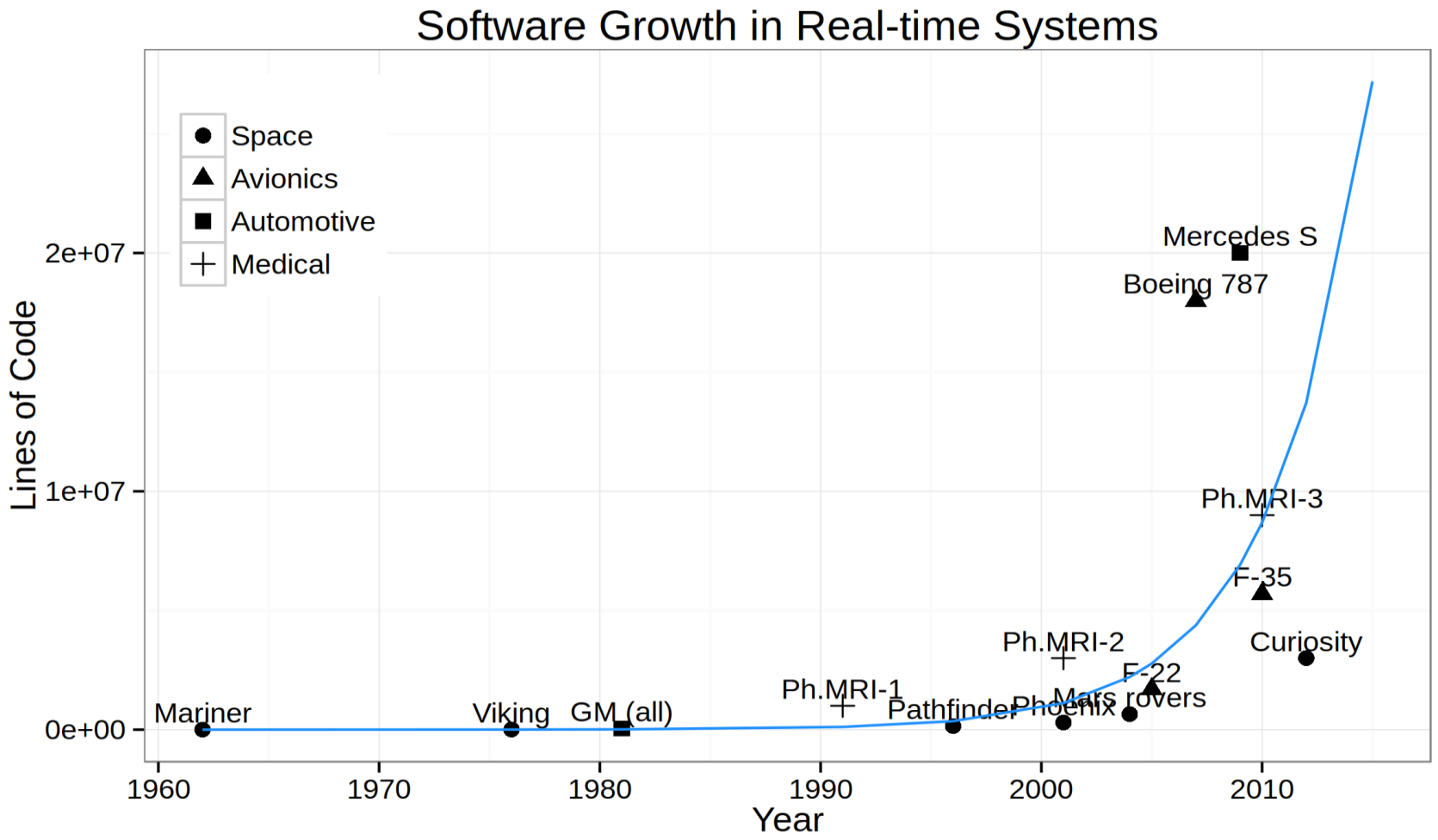
27th March, 2018

UNIVERSITY OF WATERLOO
FACULTY OF ENGINEERING

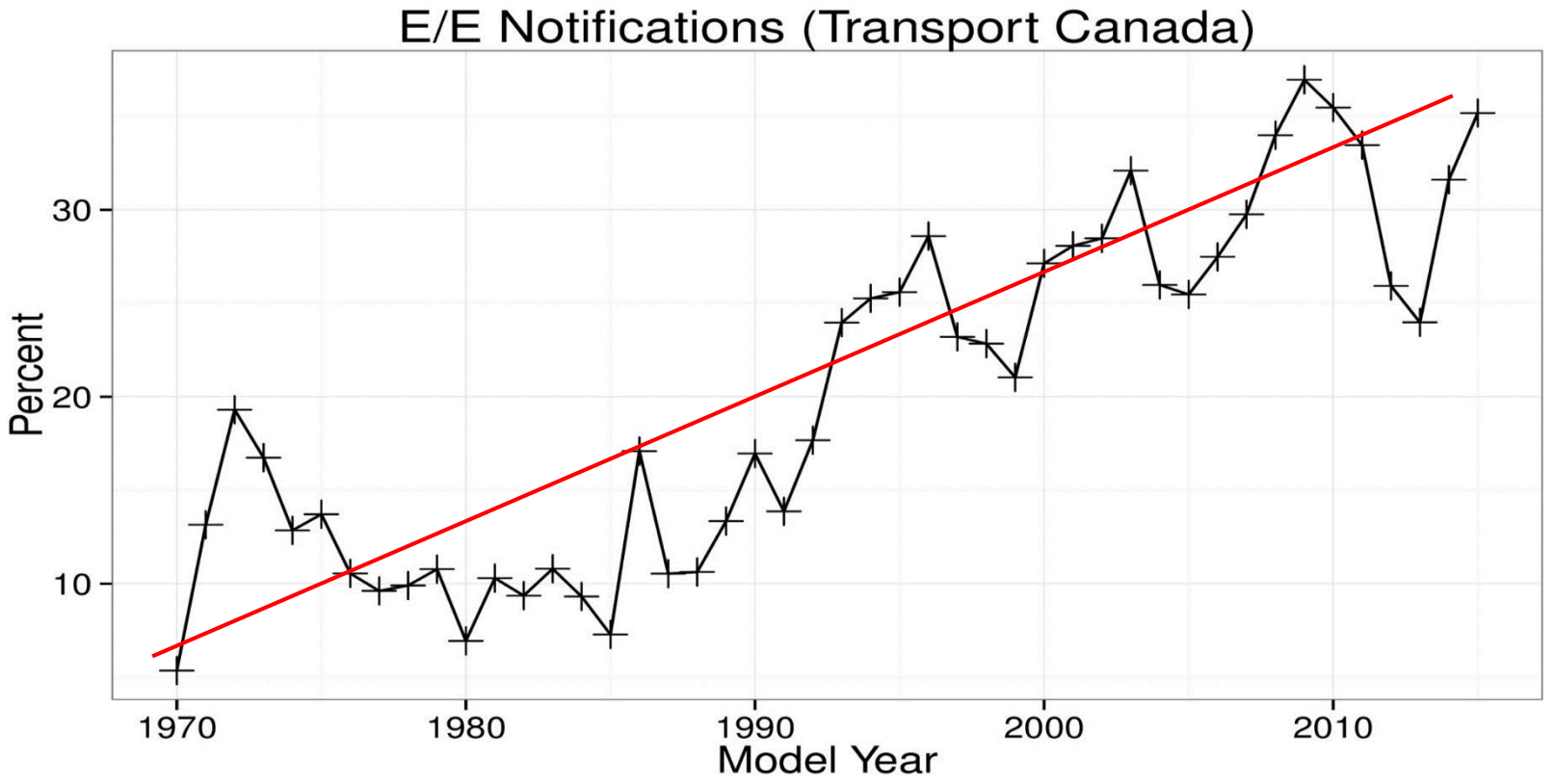
QNX™

RENESAS

Code Complexity is Increasing



Recalls Are Increasing



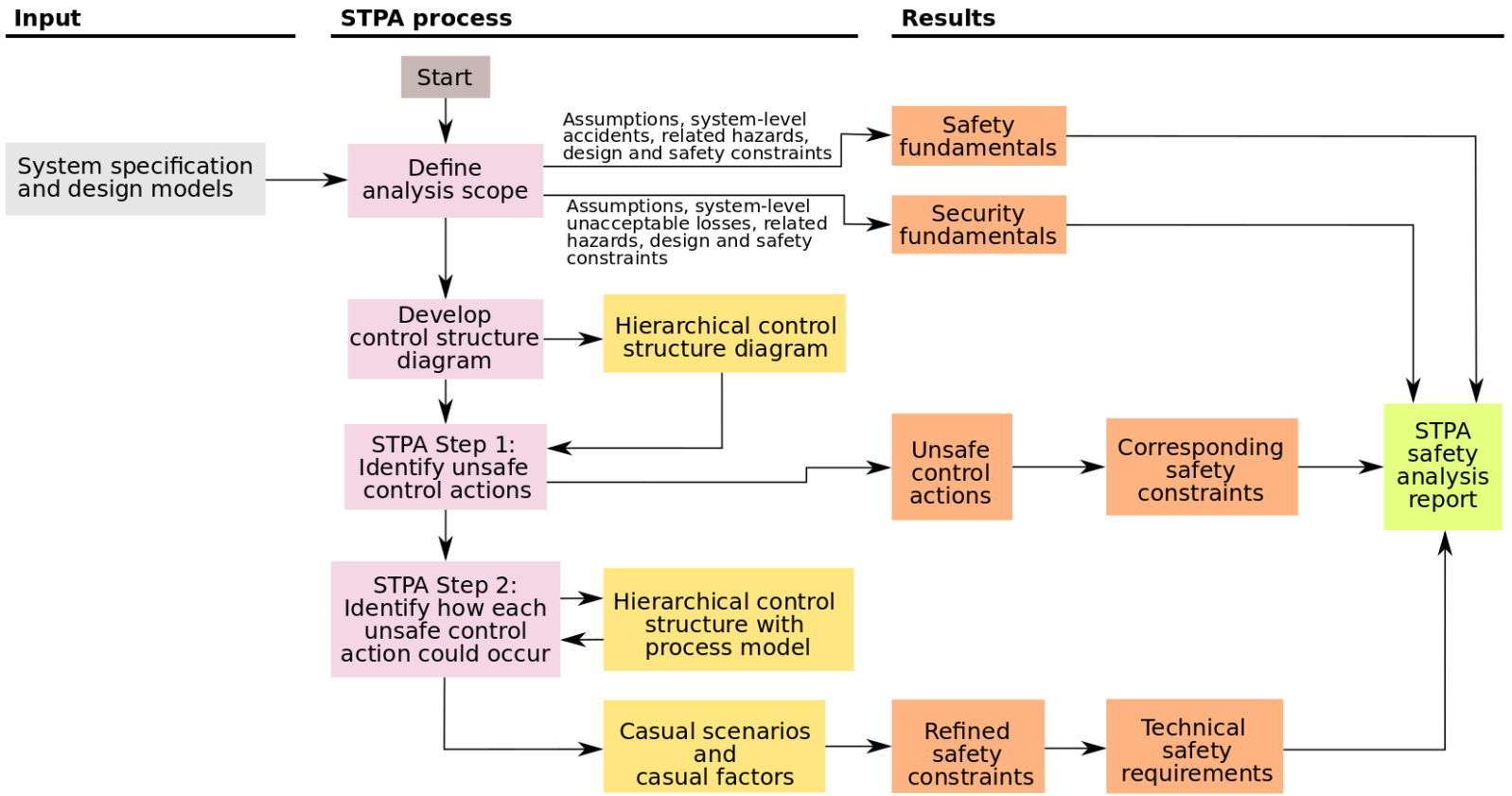
Source: Johnson, T. T., R. Gannamaraju, and S. Fischmeister, "A Survey of Electrical and Electronic (E/E) Notifications for Motor Vehicles", 24th International Technical Conference on the Enhanced Safety of Vehicles (ESV), Gothenburg, Sweden, pp. 1--15, 2015.

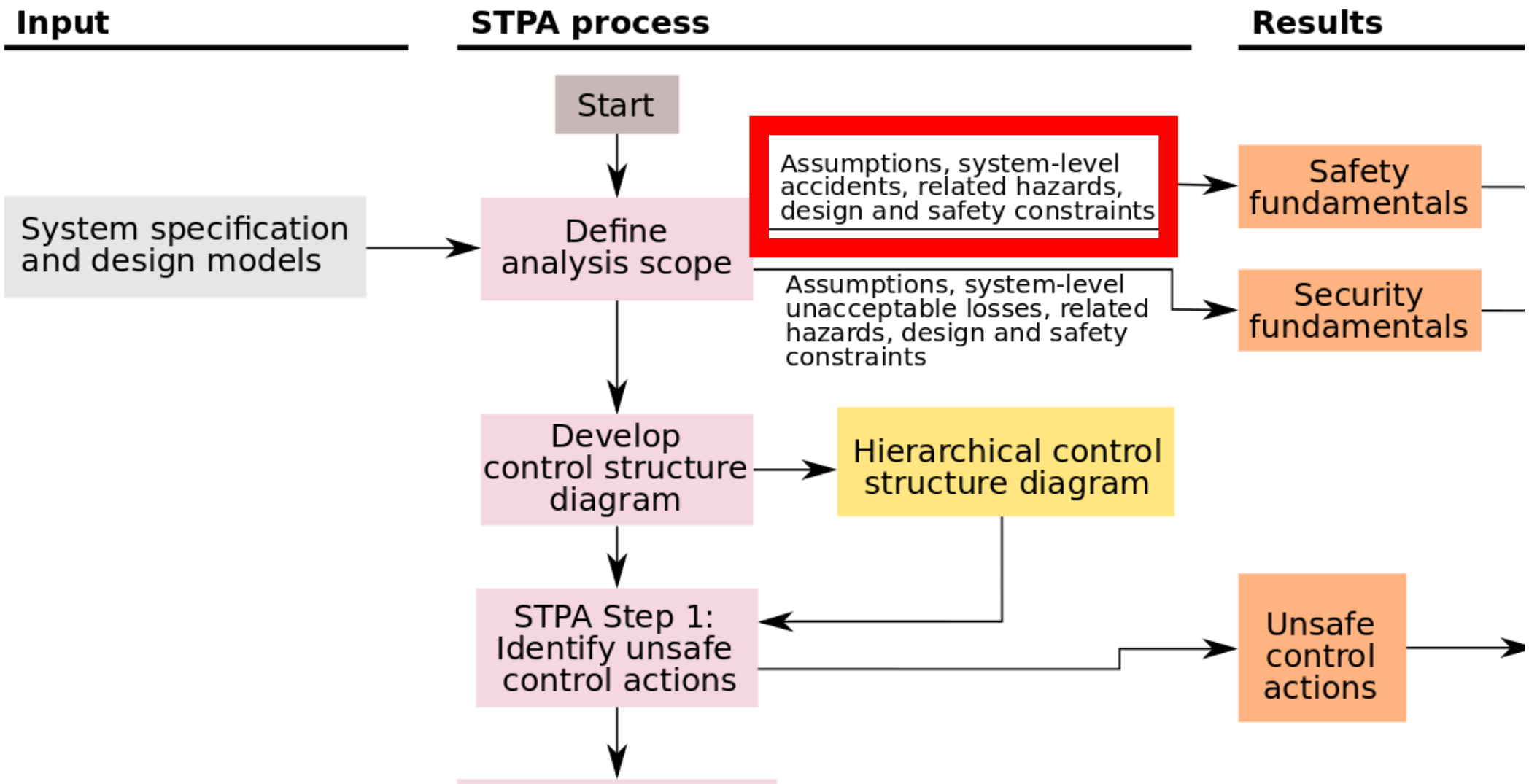
Scope & Purpose

- *Scope* – A safety and security analysis on existing L4 architecture
- *Purpose* – To improve the design of L4 vehicle based on the requirements that resulted in the analysis
- Why Autonomous Emergency Braking (AEB)?
- Security analysis is limited to impact on functional safety

Methodology

The methodology used combined safety and security analysis.




Input
STPA process
Results
Start
System specification and design models
Define analysis scope
Assumptions, system-level accidents, related hazards, design and safety constraints
Safety fundamentals
Assumptions, system-level unacceptable losses, related hazards, design and safety constraints
Security fundamentals
Develop control structure diagram
Hierarchical control structure diagram
STPA Step 1: Identify unsafe control actions
Unsafe control actions

Lessons learned

- *Assumptions:*

  Limiting conditions that act as a basis for the analysis

- *Accident section:*

  Identification of accidents lacks a systematic approach

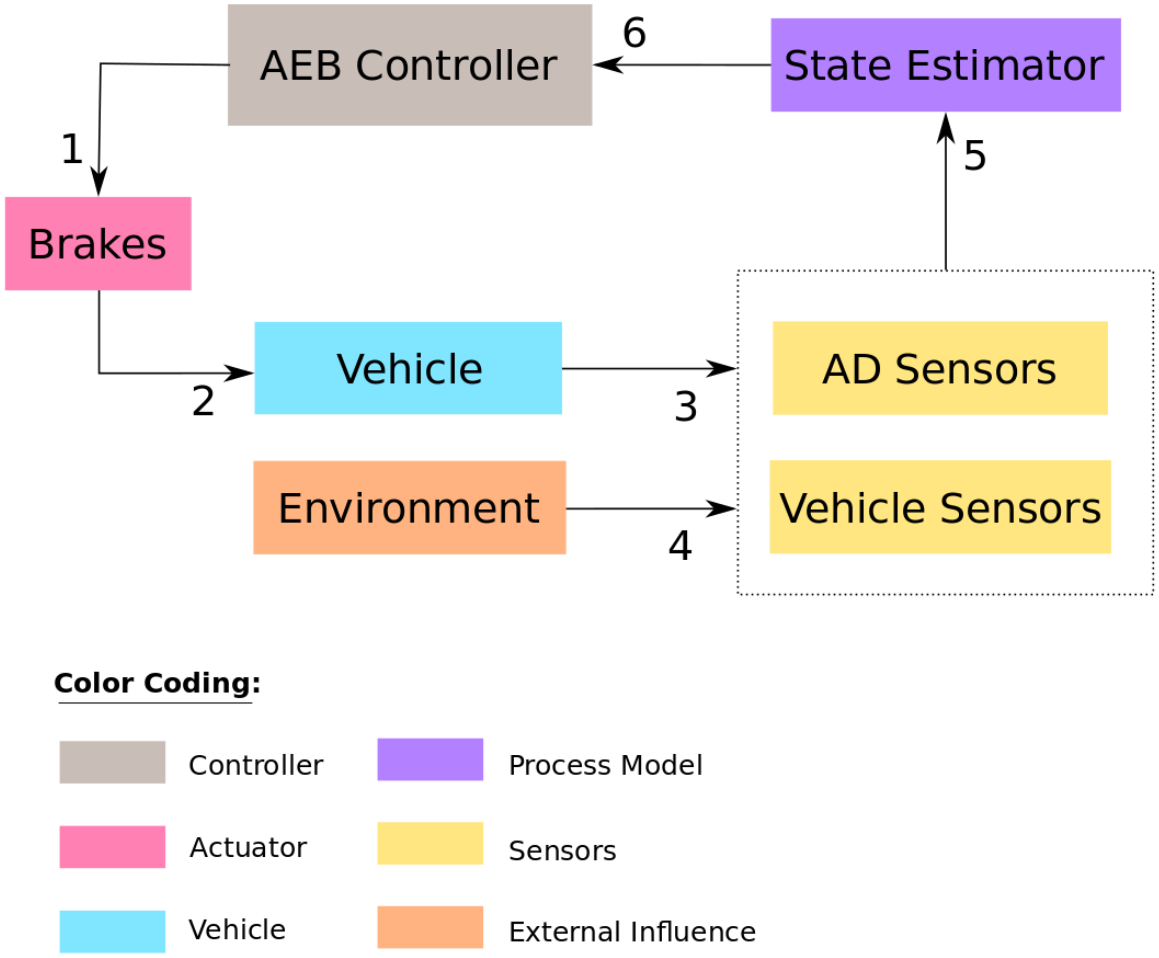
- *Hazard section:*

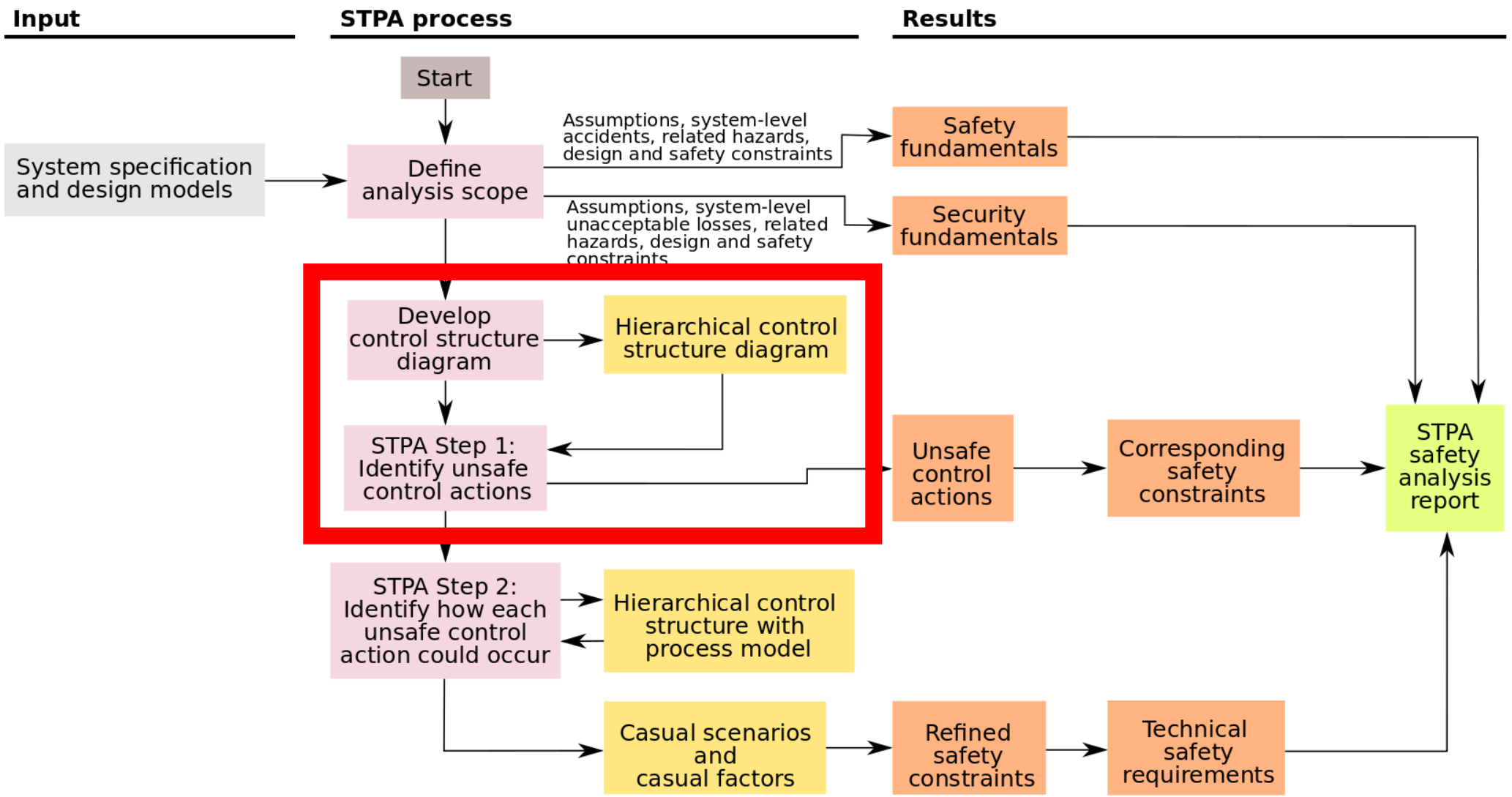
  Integrated safety and safety related security hazards in a single report

Control loop structure

Unsafe Control Actions (UCA) consider two states:

- Braking Force Command (BFC) disengaged
- BFC engaged (modulated engagement ranging from 0%-100%)




Input
STPA process
Results
Start
System specification and design models
Define analysis scope
Assumptions, system-level accidents, related hazards, design and safety constraints
Assumptions, system-level unacceptable losses, related hazards, design and safety constraints
Safety fundamentals
Security fundamentals
Develop control structure diagram
Hierarchical control structure diagram
STPA Step 1: Identify unsafe control actions
Unsafe control actions
Corresponding safety constraints
STPA safety analysis report
STPA Step 2: Identify how each unsafe control action could occur
Hierarchical control structure with process model
Casual scenarios and casual factors
Refined safety constraints
Technical safety requirements

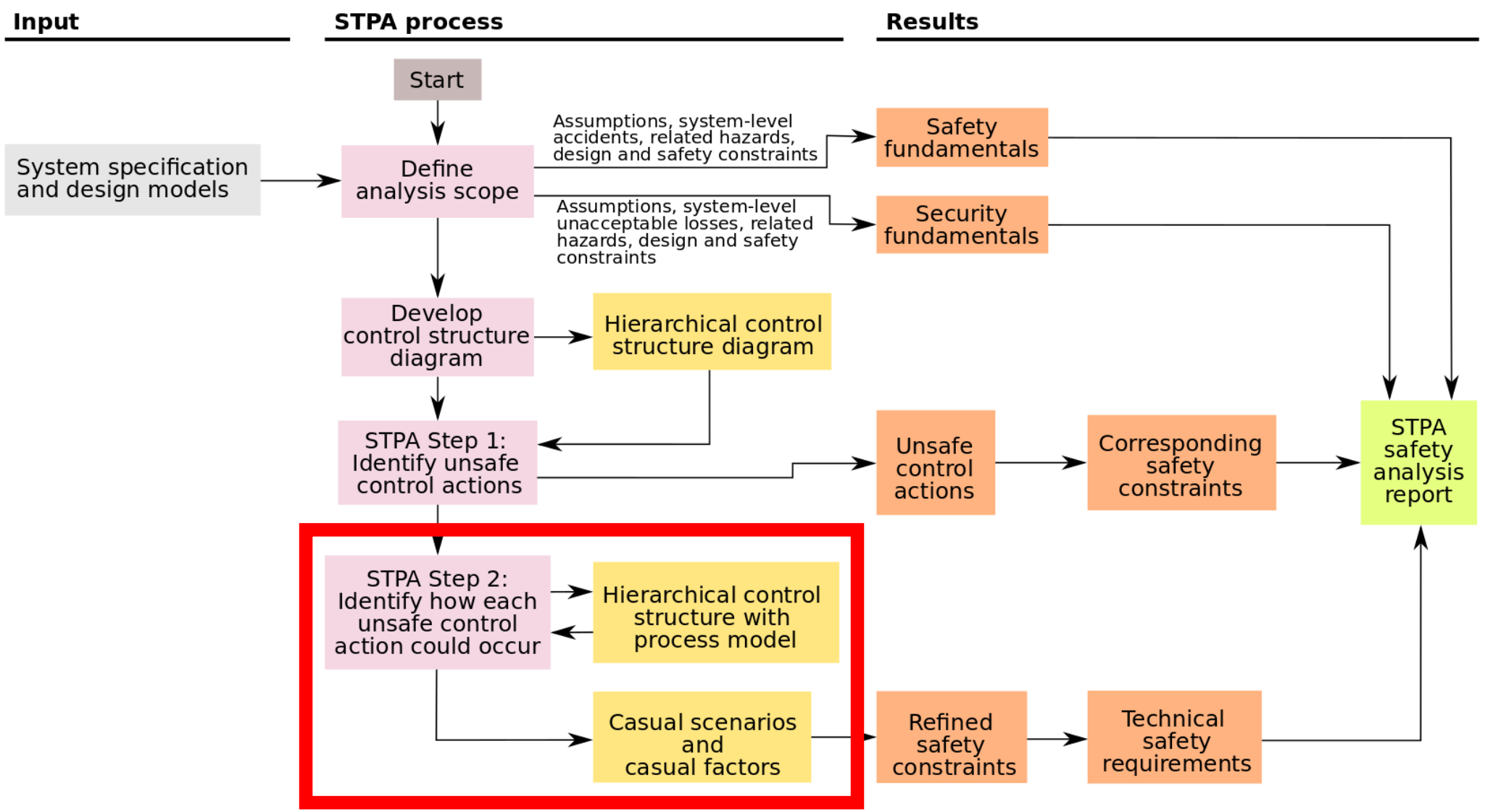
Lessons learned

- *From control diagram:*

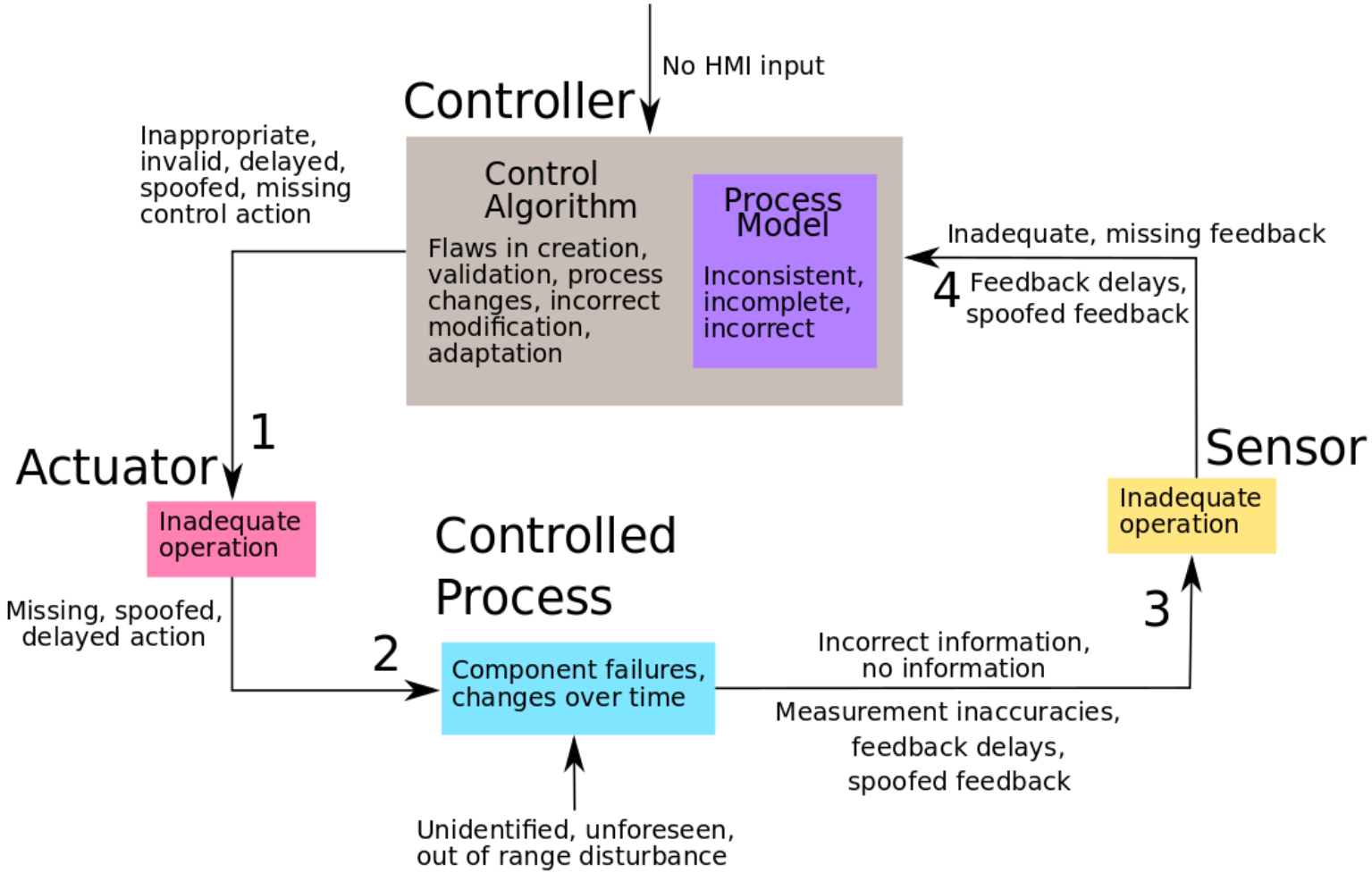
  The control diagram must represent the basic blocks with generic functionalities and terms

- *From UCA:*

  Repeated refinement resulted in additional scenarios and causal factors


Input
STPA process
Results
Start
System specification and design models
Define analysis scope
Assumptions, system-level accidents, related hazards, design and safety constraints
Assumptions, system-level unacceptable losses, related hazards, design and safety constraints
Safety fundamentals
Security fundamentals
Develop control structure diagram
Hierarchical control structure diagram
STPA Step 1: Identify unsafe control actions
Unsafe control actions
Corresponding safety constraints
STPA safety analysis report
STPA Step 2: Identify how each unsafe control action could occur
Hierarchical control structure with process model
Casual scenarios and casual factors
Refined safety constraints
Technical safety requirements

Potential control flaws



Systematic approach for causal factors

- Actions regarding data considered per block in the control structure:
  - Missing
  - Inadequate
  - Incorrect
  - Delayed

- Reasons for unsafe actions:
  - Spoofing
  - Component failure
  - Electrical requirements not met
  - Communication failure

Blocks	Actions	Reasons
Sensors(EPS, Localization data, Vehicle speed, Local planner, object identification sensor)		
Controller		
Actuator		
Controlled process		

Lessons learned

- *Causal scenarios:*

  Depending on the type of functionality under consideration, the approach needs to be modified

- *Causal factors:*

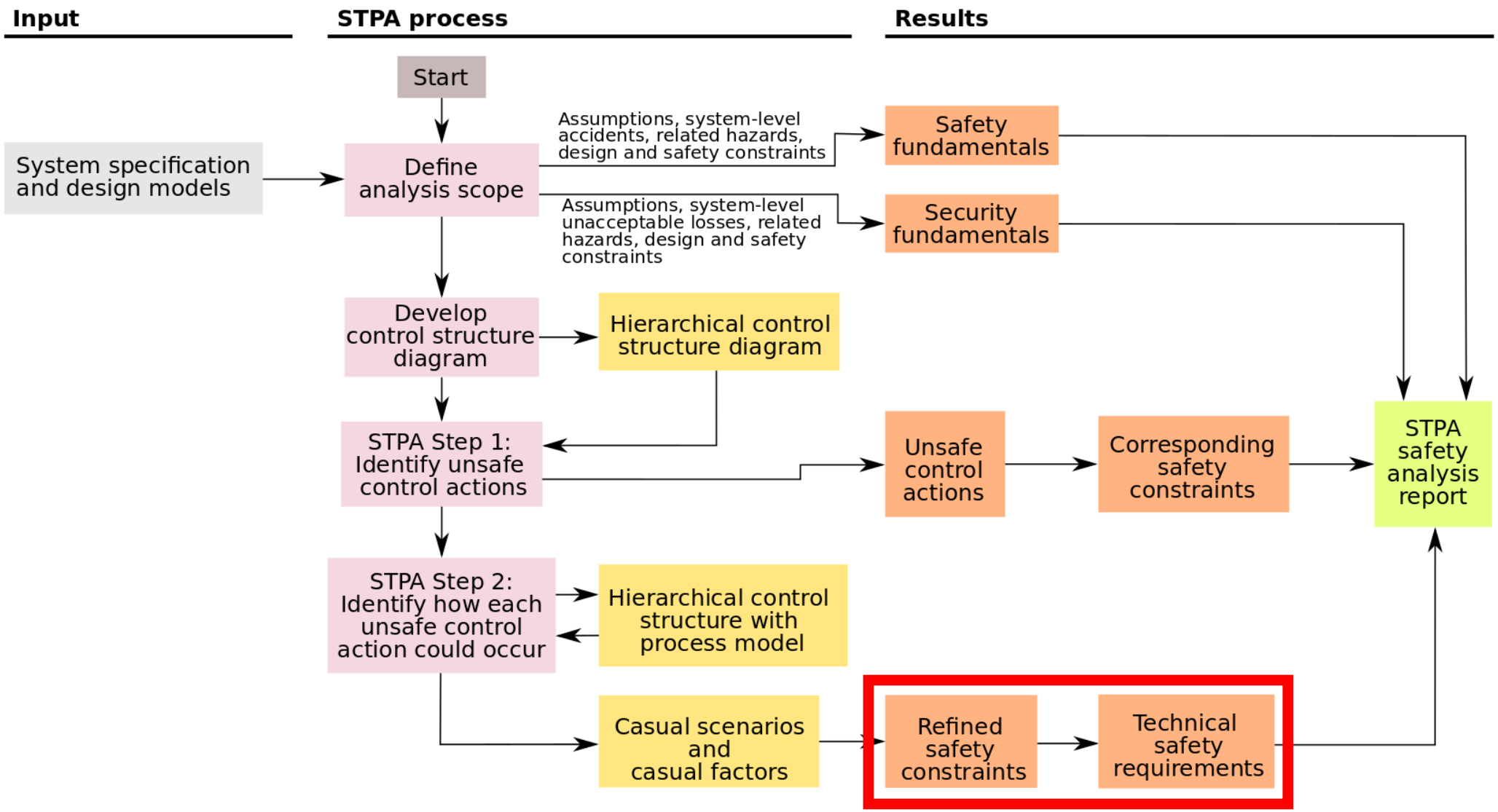
  Current approach is more systematic and avoids mental exercise

Lessons learned

- *Rationale table:*

- Lists the logic behind the causal factors
- Works as a reference table for further steps

Group	Causal factor	Rationale
Controller (group 1)		
Actuator (group 2)		
Controlled process (group 3)		
B6/B7 Sensors (group 4)		


Input
STPA process
Results
Start
System specification and design models
Define analysis scope
Assumptions, system-level accidents, related hazards, design and safety constraints
Assumptions, system-level unacceptable losses, related hazards, design and safety constraints
Safety fundamentals
Security fundamentals
Develop control structure diagram
Hierarchical control structure diagram
STPA Step 1: Identify unsafe control actions
Unsafe control actions
Corresponding safety constraints
STPA safety analysis report
STPA Step 2: Identify how each unsafe control action could occur
Hierarchical control structure with process model
Casual scenarios and casual factors
Refined safety constraints
Technical safety requirements

Lessons learned

- *Technical safety requirements:*

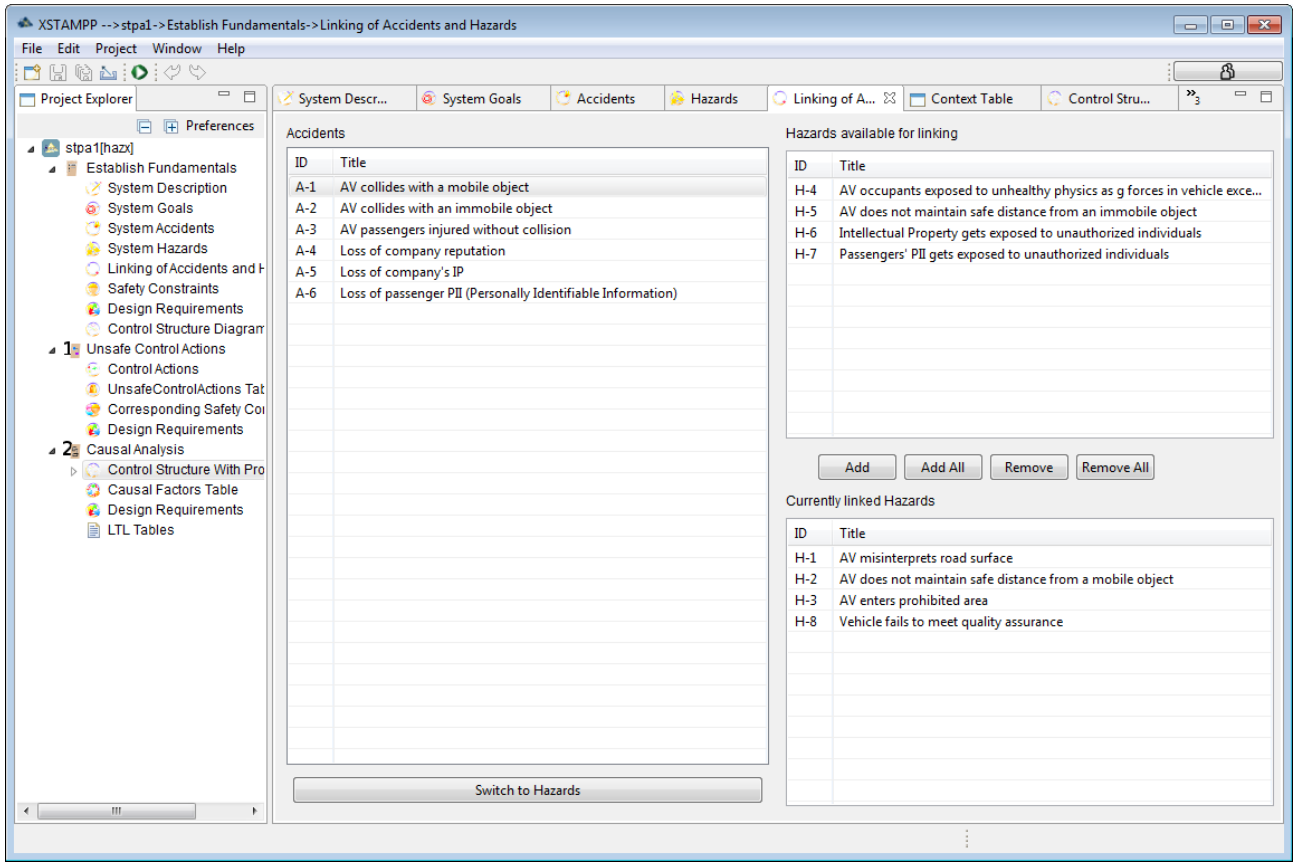
  Trade off between too specific and too generic to allow some flexibility for the designer

- *Gap analysis:*

  Using a generic approach — more extensive applications possible

Additional Lessons

- *Residual risks:* Some risks which are present in our system that can be accepted.
- *XSTAMPP Experiment:* Tried XSTAMPP tool (version 2.5.0) but abandoned due to inflexibility



Threats to validity of our analysis

- We are neither AEB, L4 experts, nor security experts (*but we are safety experts*)
- We used STPA for the first time (*but we have experience with other safety standards*)
- The security analysis is heavy on spoofing, but light on other attacks
- Is the analysis general for AEB or wherever applied?
- No formal verification completed
- No implementation has been done

Summary

- Analyzed AEB of an L4
- Learned lessons
- Valuable experience
- Applicability

Future Work:

- Comparative study, comparing the analysis with standard ISO 26262
- Can be expanded to cover the complete functionality of AV potentially


UNIVERSITY OF WATERLOO
FACULTY OF ENGINEERING
Thank you! Questions?
shefali.sharma@uwaterloo.ca