A Co-Simulation Based Approach for Developing Safety-Critical Systems

Daniella Tola Peter Gorm Larsen

Aarhus University, Department of Engineering

7th December 2020
The 18th Overture Workshop

Agenda

- Background
- Development Process
- Demo
- Discussion & Conclusion

Background

Definitions:

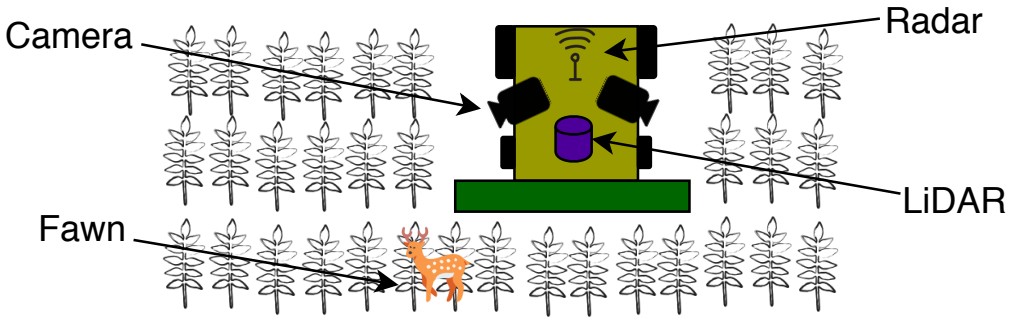
- Safety-critical system
- Safety case

Motivation:

- Systems are becoming more complex
- Time-consuming
- Avoid large system re-designs

Background

Case Study



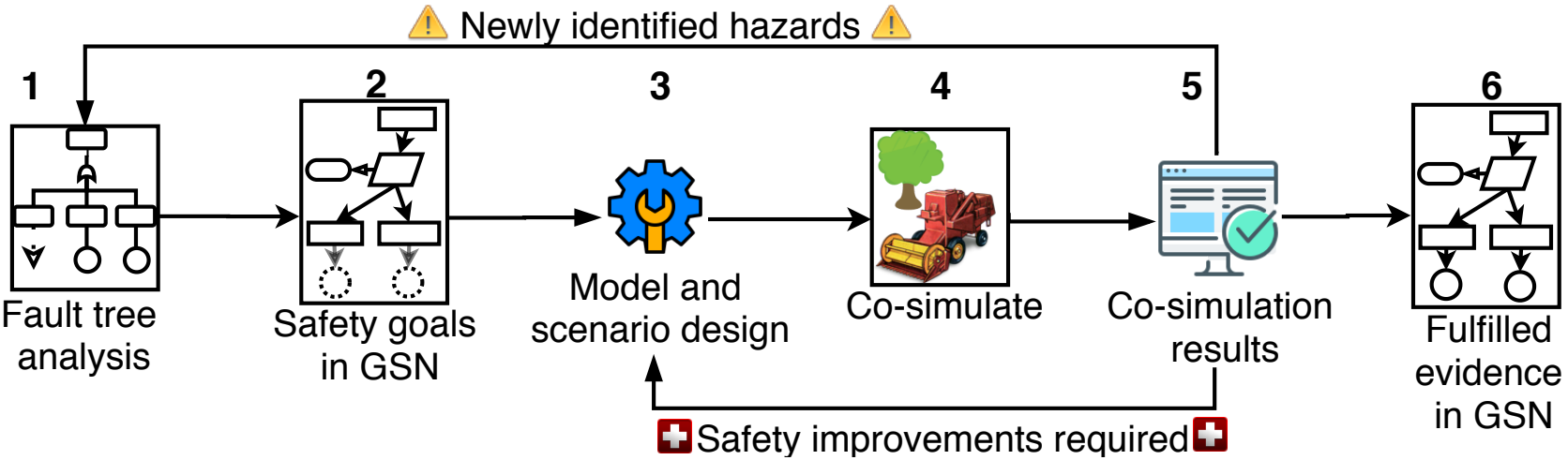
- Expensive to perform physical tests
- Uncontrollable environment
- Unethical tests

Background

Case Study

https://www.theguardian.com/world/2014/apr/25/german-drones-protect-young-deer-combine-harvesters

Development Process: Methodology

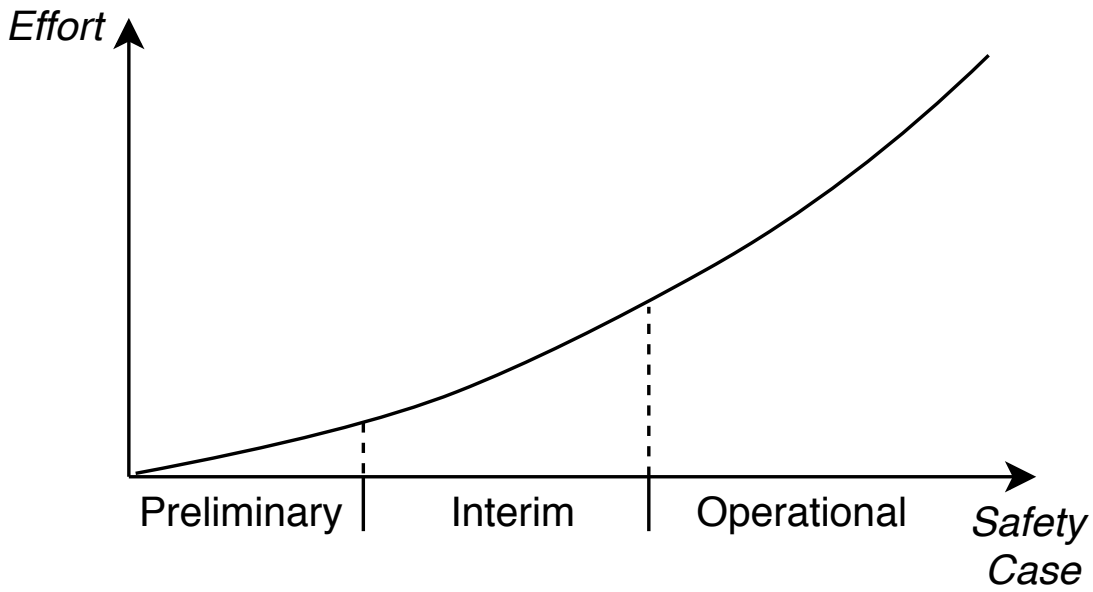


Development Process: Safety Case

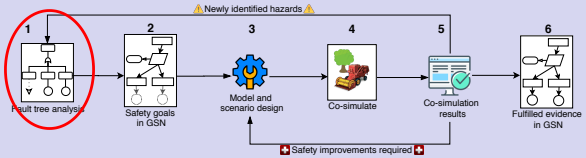
Phased Safety Case

Three main phases:

- Preliminary
- Interim
- Operational

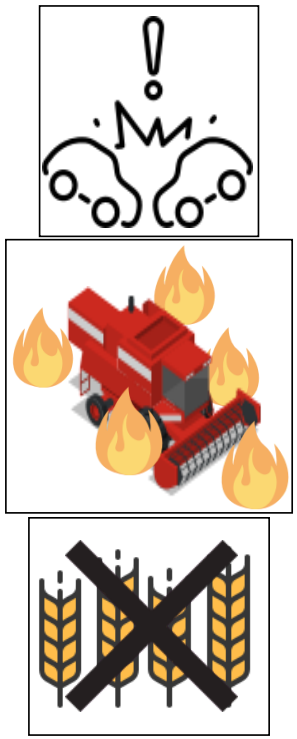


Development Process: Safety Analysis

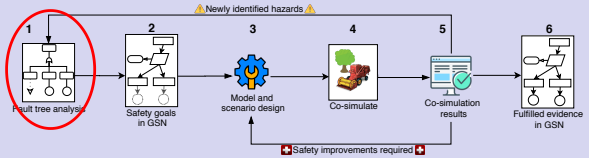


Hazard Analysis

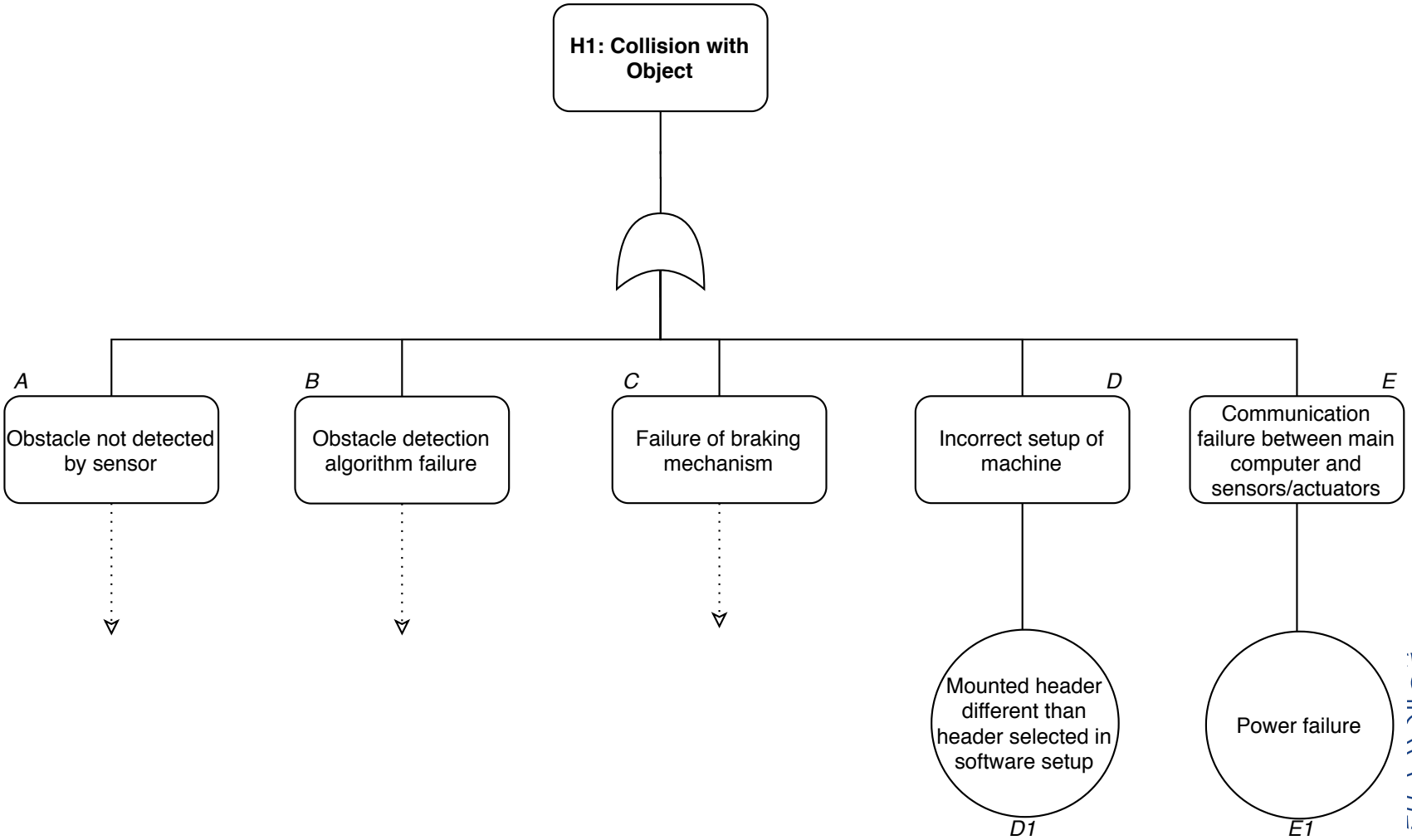
- H1: Collision with object.
- H2: Damage to unharvested crops.
- H3: Fire ignition.
- H4: Damage to harvesting machinery.
- H5: Contamination of harvested crops.



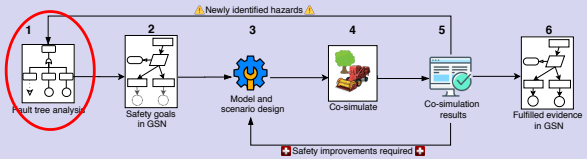
Development Process: Safety Analysis



Hazard Analysis - Fault Tree Analysis



Development Process: Safety Analysis

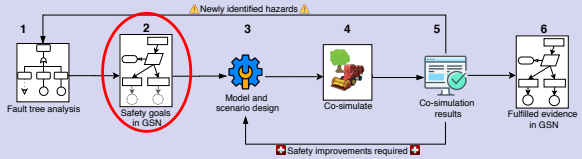


Risk Assessment

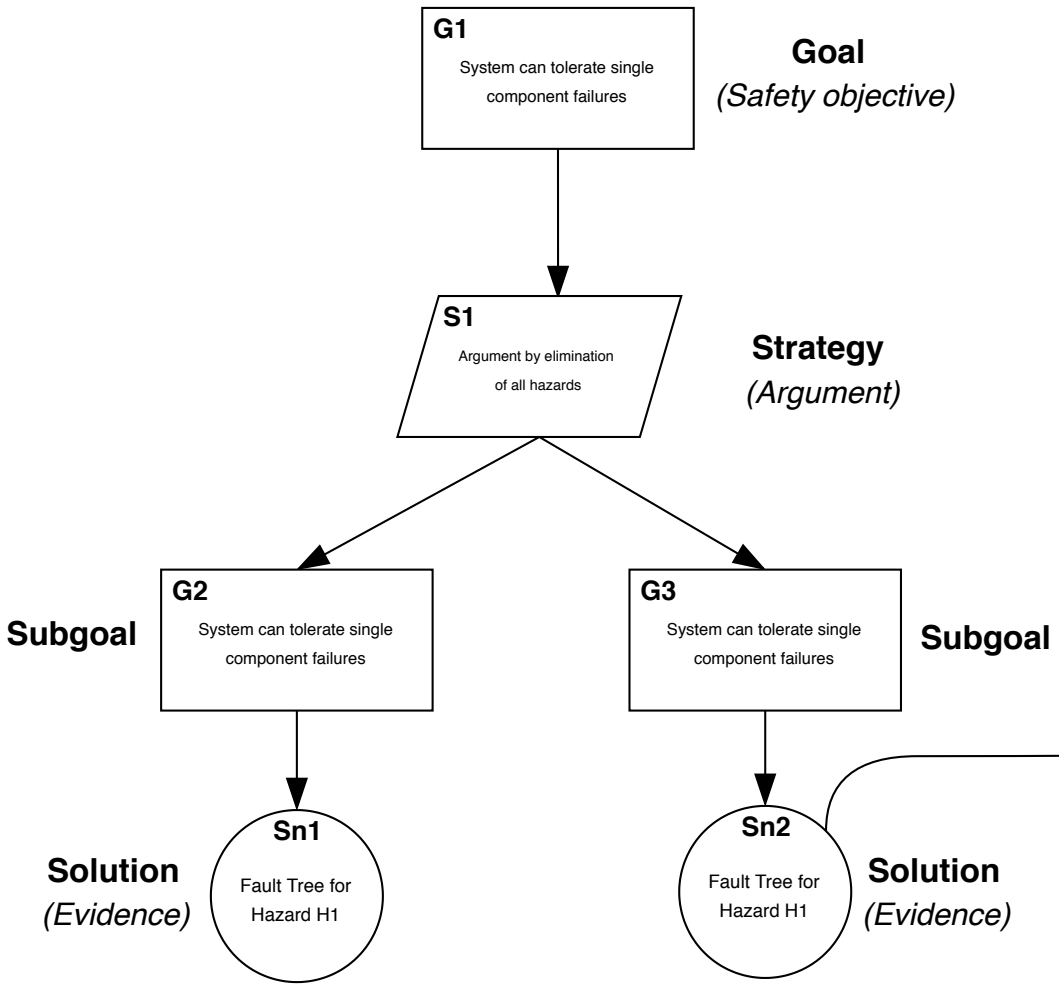
Identified Hazard	**Hazard probability**	**Accident severity**	**Estimated risk**	**Acceptability**
H1: Collision with object	Medium	High	High	Intolerable
H2: Damage to unharvested crops	Low	Medium	Medium	ALARP
H3: Fire ignition	Low	High	High	Intolerable
H4: Damage to harvesting machinery	Low	Medium	Medium	ALARP
H5: Contamination of harvested crops	Low	Medium	Medium	ALARP

ALARP: As Low as Reasonably Possible

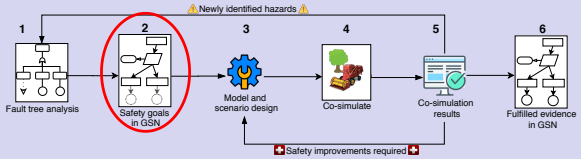
Development Process: Safety Analysis



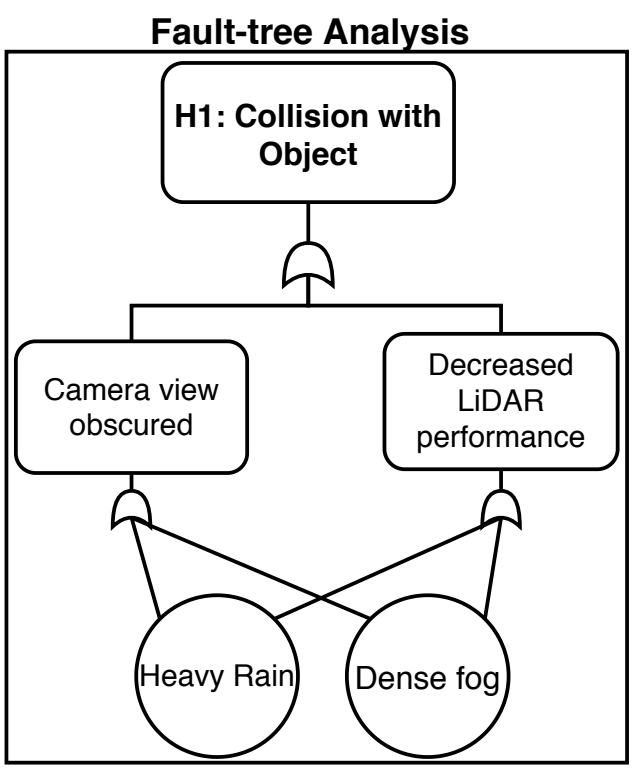
Goal Structuring Notation (GSN)

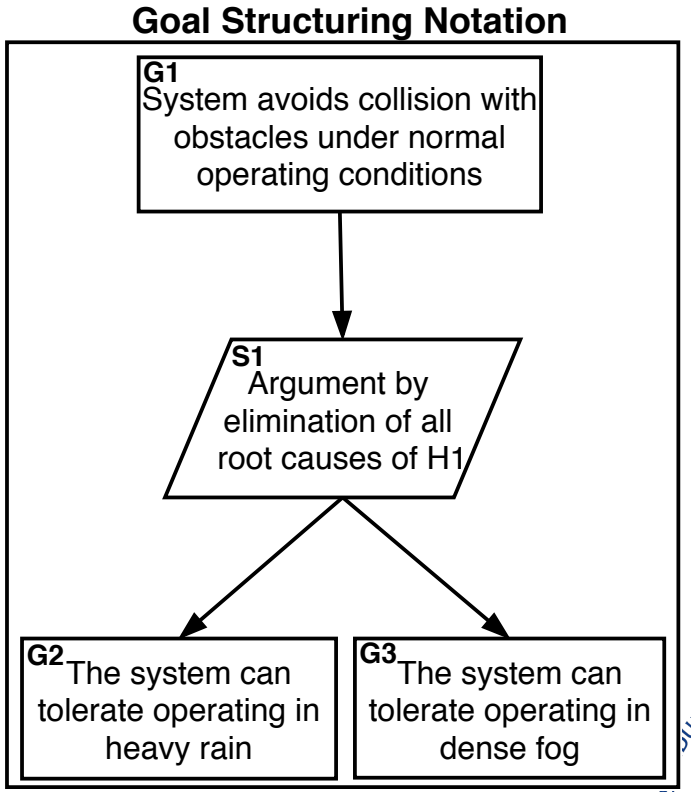


Development Process: Safety Analysis

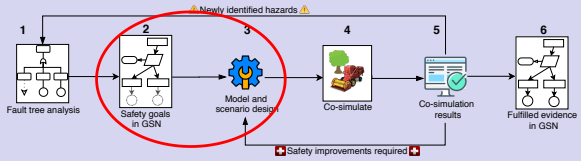


Formalizing Safety Goals





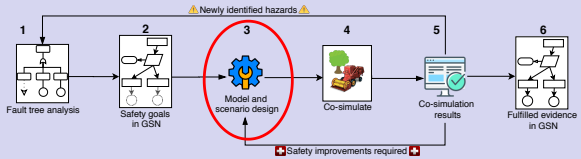
Development Process: Producing Evidence using Co-simulation



When to use co-simulation for producing evidence?

Hazard	H1	H3
Root causes	• software/hardware failure • dense fog, heavy rain • dust/materials on sensors • swarm of insects blocking sensor view	• friction of knife in cutter bar • oil or fuel leakage • residue inside high temperature areas of machinery • extreme wind, high temperatures, and low humidity

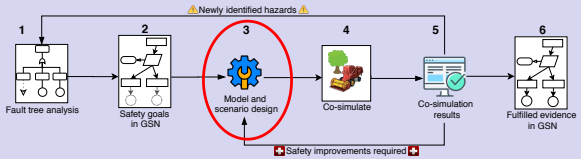
Development Process: Producing Evidence using Co-simulation



Scenario Construction

Hazardous event	**Vehicle speed**	**Initial distance to obstacle**
Dense fog	{1,2,3} [m/s]	>1 meter
Heavy rain	{1,2,3} [m/s]	>1 meter
Inaccurate sensor	{1,2,3} [m/s]	>1 meter

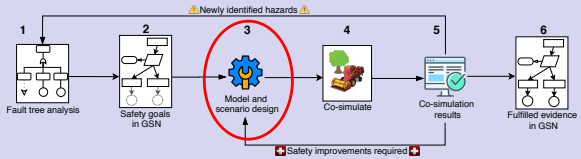
Development Process: Producing Evidence using Co-simulation



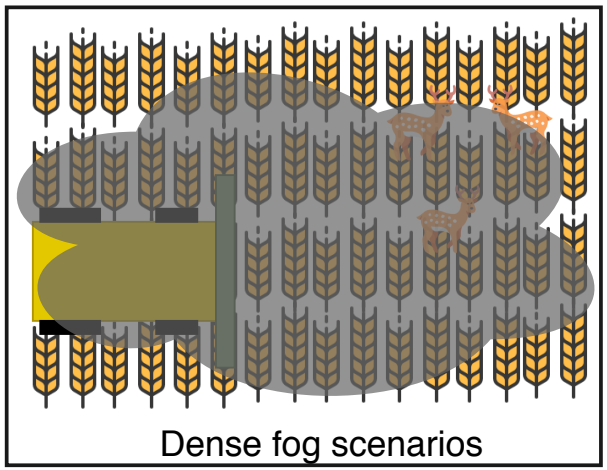
Identify Models

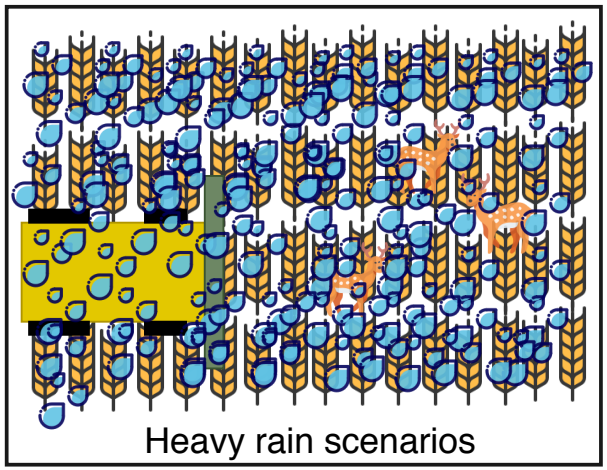
FMU	**Tool**
Controller	Overture
Vehicle	20-sim
Environment	PyFMU
Sensor	PyFMU
Supervisory Controller	PyFMU
Monitor	PyFMU

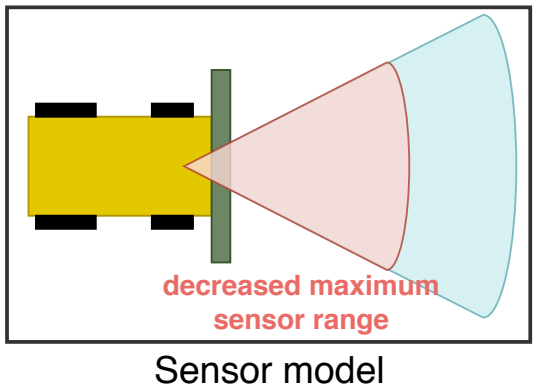
Development Process: Producing Evidence using Co-simulation



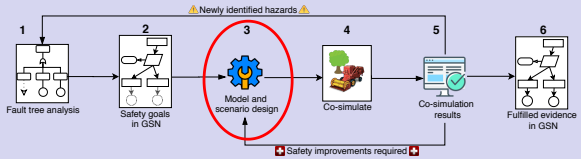
Modelling Scenarios



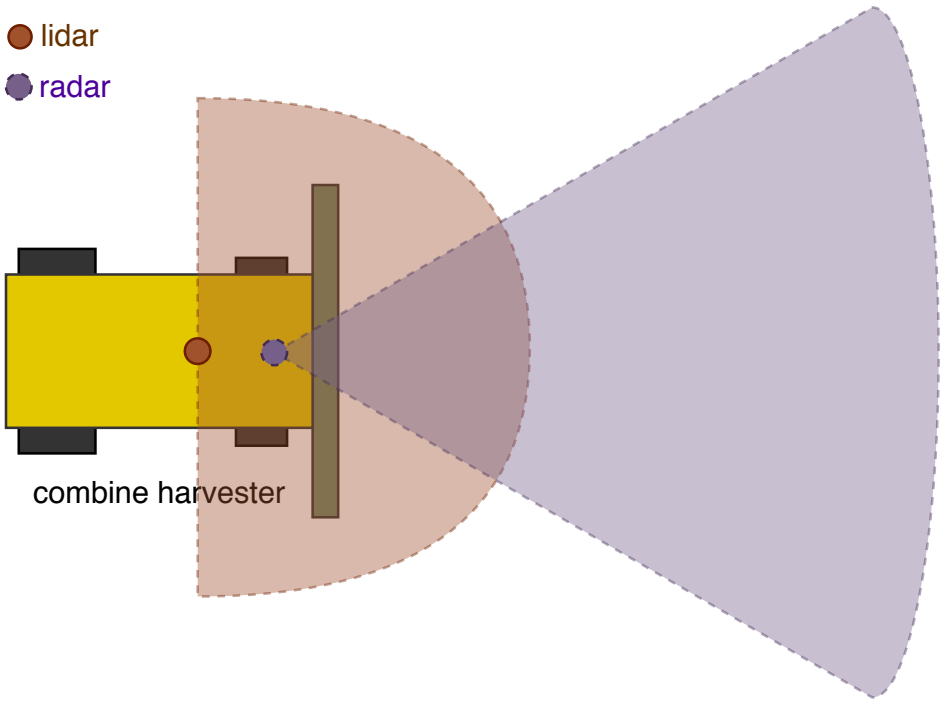


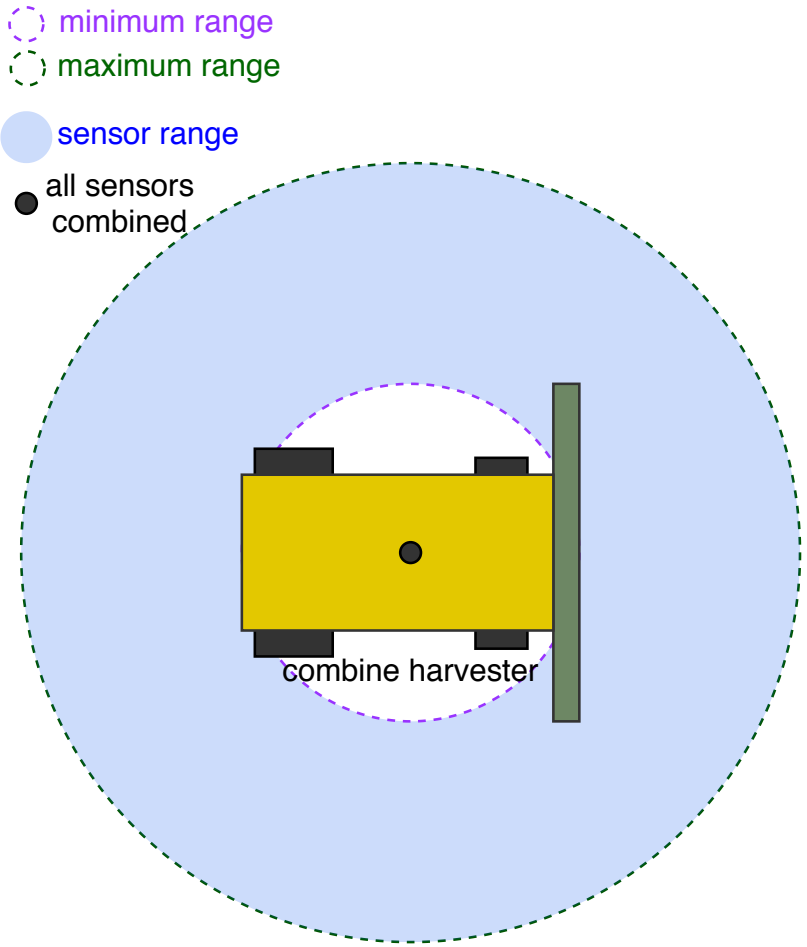


Development Process: Producing Evidence using Co-simulation

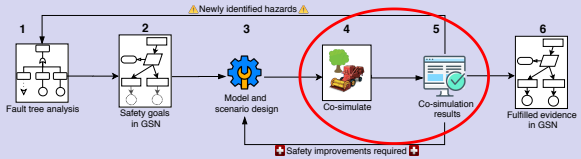


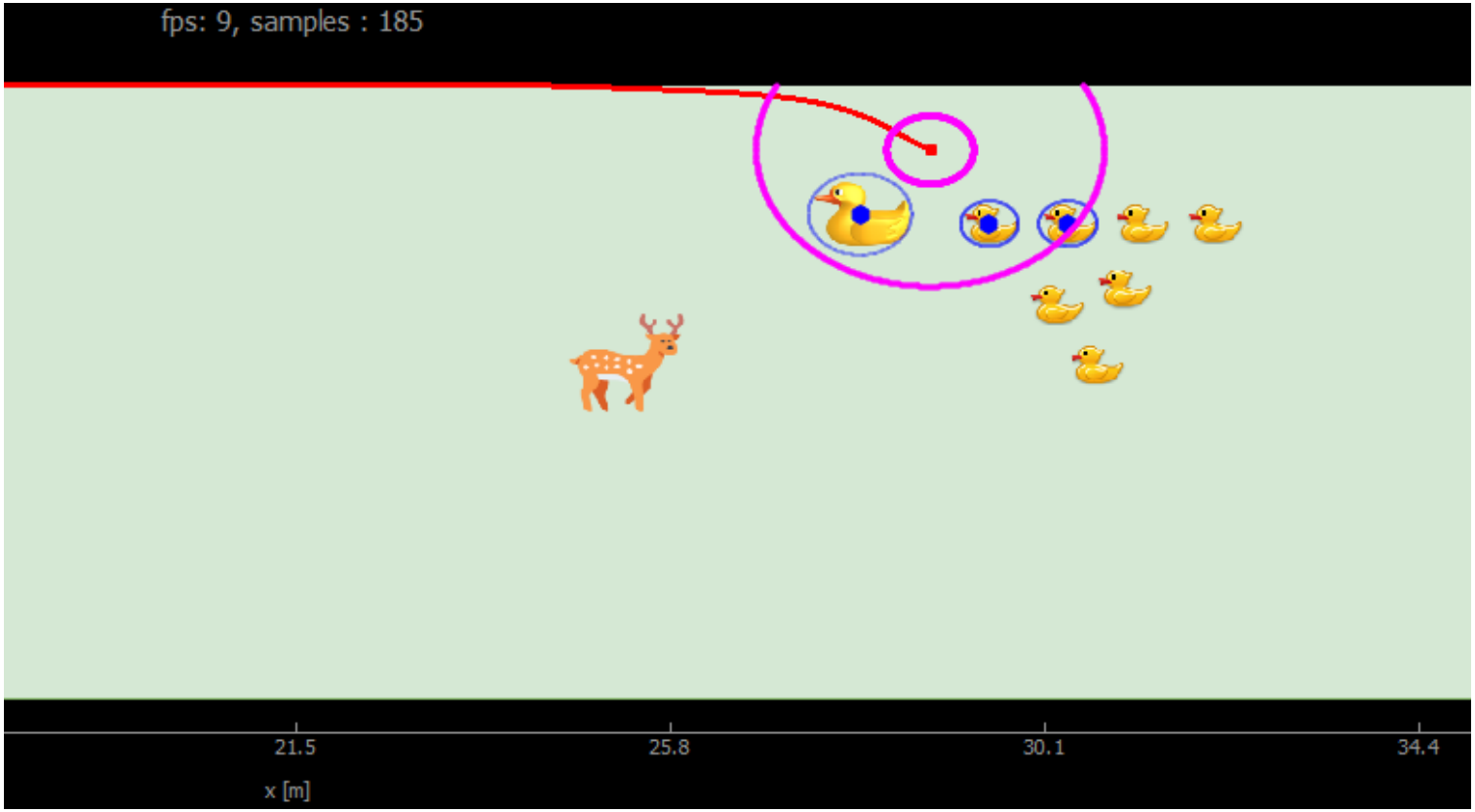
Sensor Model



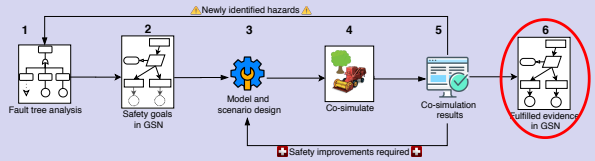


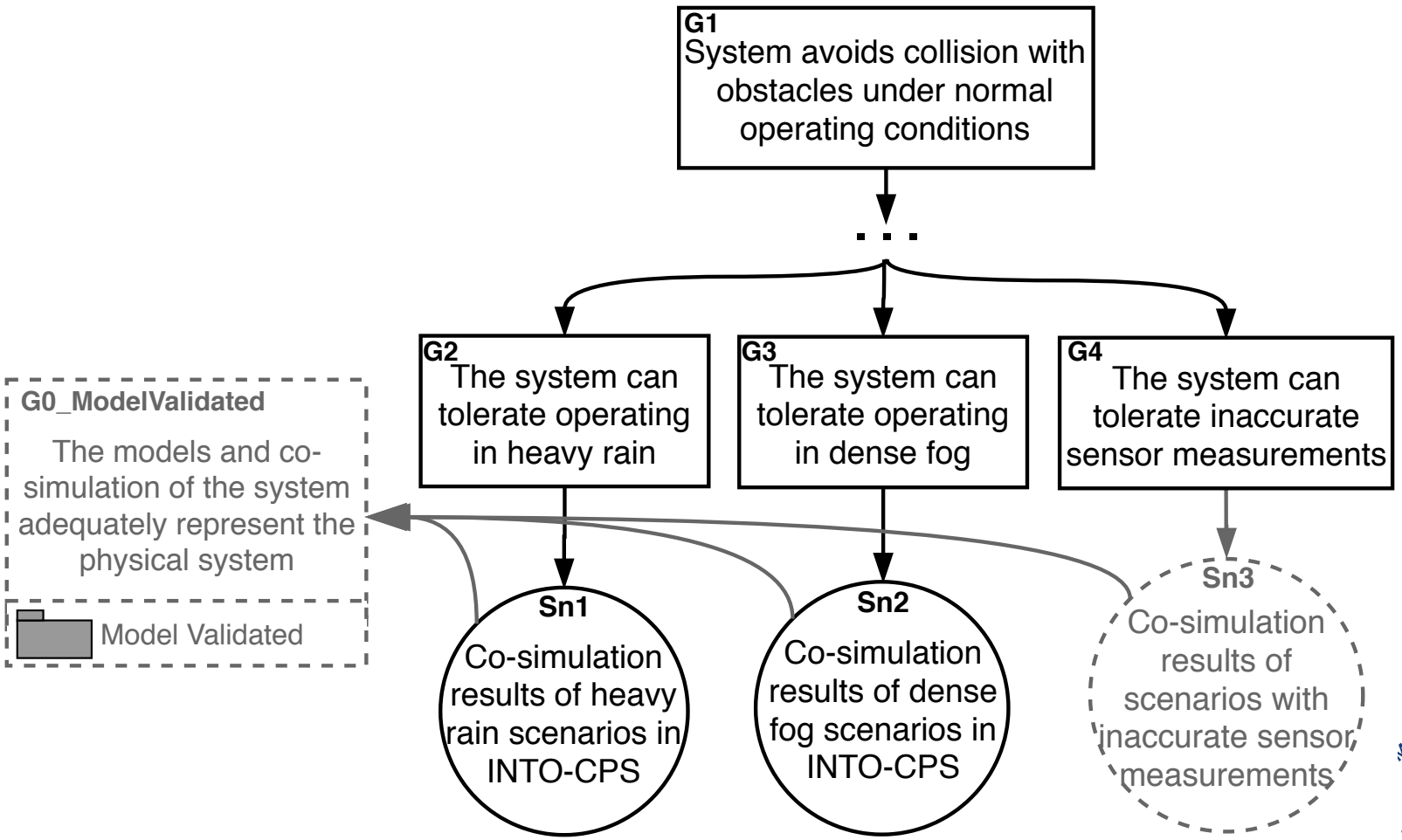
Demo


Newly identified hazards
1
Fault tree analysis
2
Safety goals in GSN
3
Model and scenario design
4
Co-simulate
5
Co-simulation results
6
Fulfilled evidence in GSN
Safety improvements required


fps: 9, samples : 185
21.5
25.8
30.1
34.4
x [m]

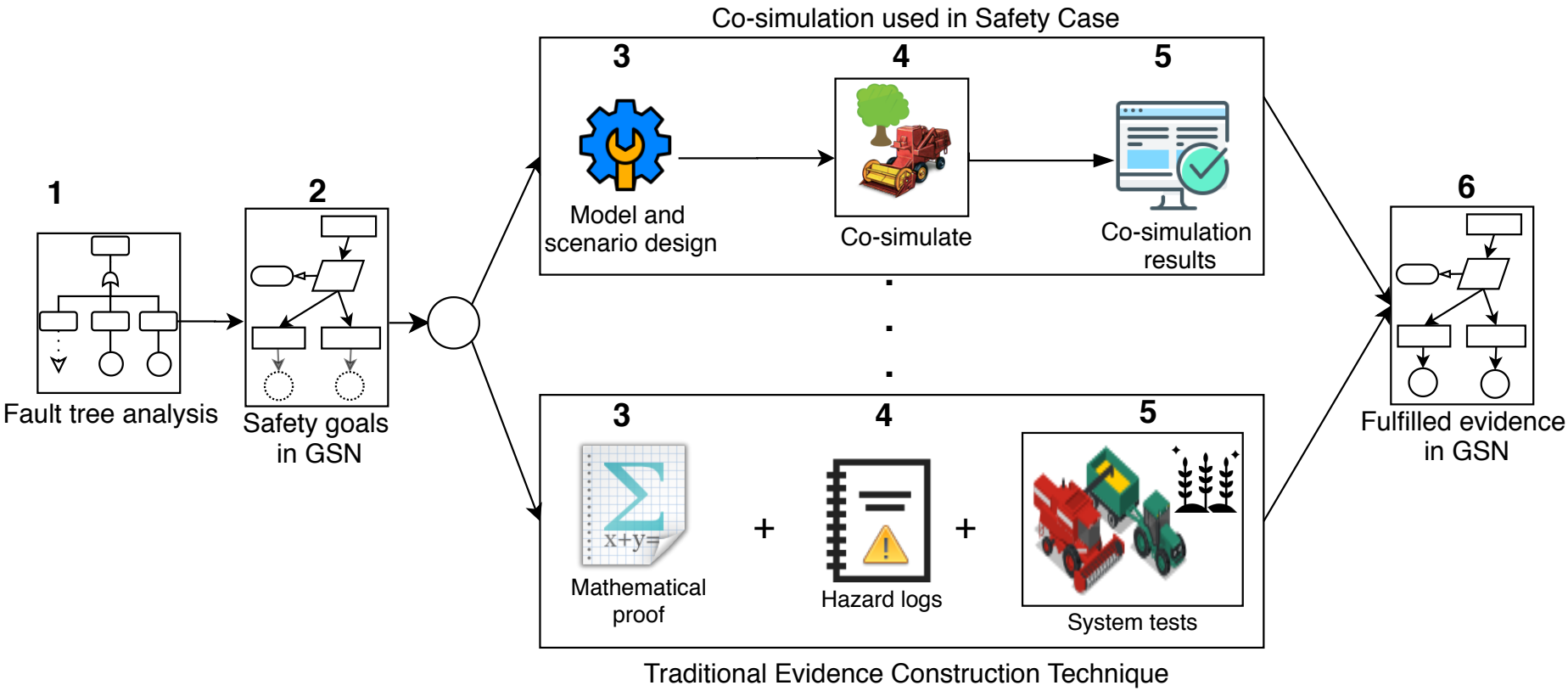
Results


Newly identified hazards
1
Fault tree analysis
2
Safety goals in GSN
3
Model and scenario design
4
Co-simulate
5
Co-simulation results
6
Fulfilled evidence in GSN
Safety improvements required


G1
System avoids collision with obstacles under normal operating conditions
G2
The system can tolerate operating in heavy rain
G3
The system can tolerate operating in dense fog
G4
The system can tolerate inaccurate sensor measurements
G0_ModelValidated
The models and co-simulation of the system adequately represent the physical system
Model Validated
Sn1
Co-simulation results of heavy rain scenarios in INTO-CPS
Sn2
Co-simulation results of dense fog scenarios in INTO-CPS
Sn3
Co-simulation results of scenarios with inaccurate sensor measurements

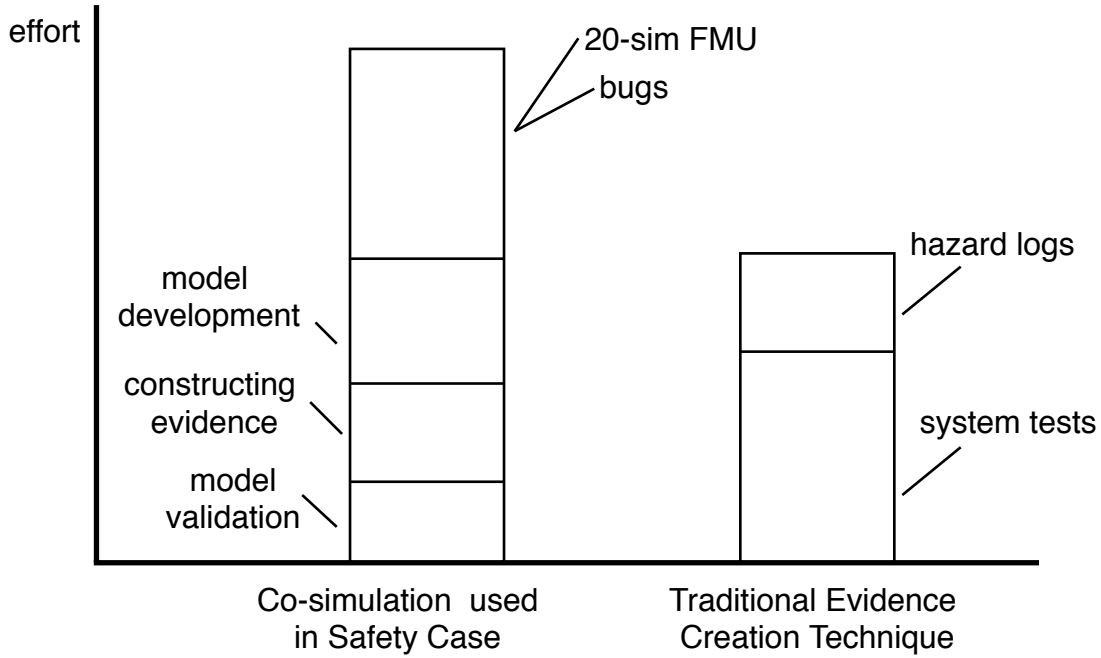
Discussion

When to use this technique?



Discussion

Practical Limitations



Conclusion and Future Work

Conclusion:

- Complex software and hardware interactions
- Visualize results

Future Work:

- Interim and Operational
- Amount of parameters per scenario
- Model validation
- Evaluate on other systems, e.g. medical devices

Acknowledgements

Thank you to Martin Peter Christensen from AGCO for the discussions about the challenges of an autonomous combine harvester.

And thank you to the anonymous reviewers of the paper for the detailed feedback.

AARHUS UNIVERSITY