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

Daniella Tola

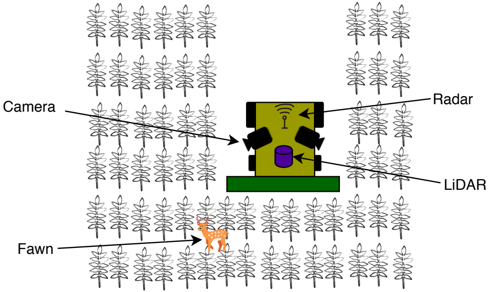
Master Thesis Defense, 18th June 2020

Agenda

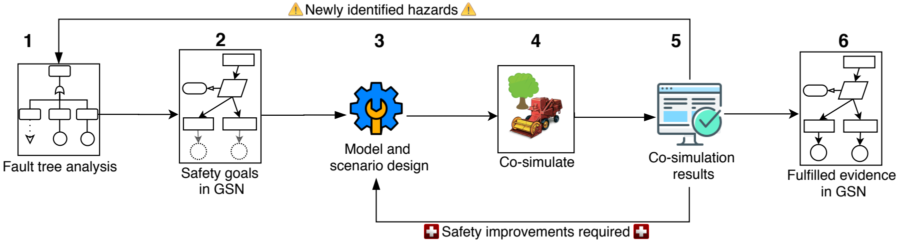
- Introduction
- Development Process
- Safety Case
- Producing Evidence using Co-simulation
- Discussion
- Conclusion
- Model Improvements
- Incorporating Humans in Co-simulation
- Model Validation

Introduction

Motivation and Case Study

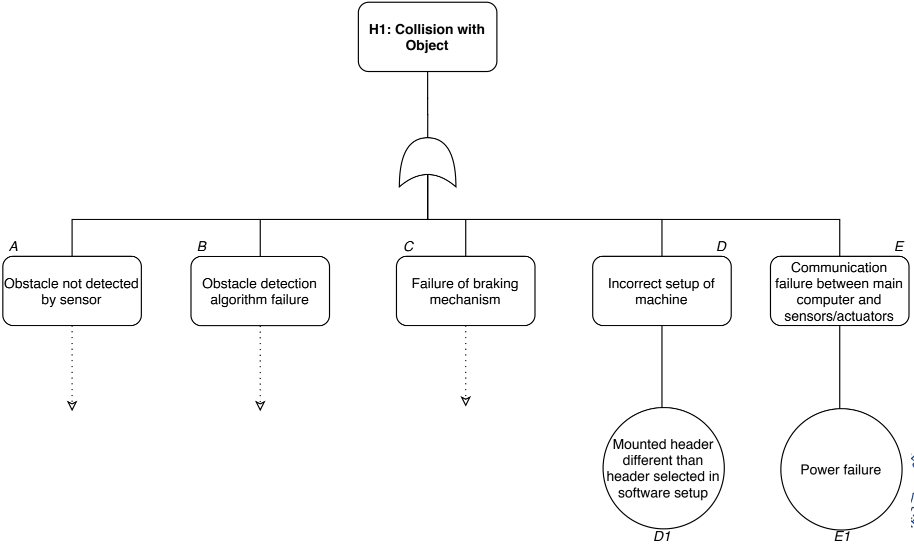


Development Process


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

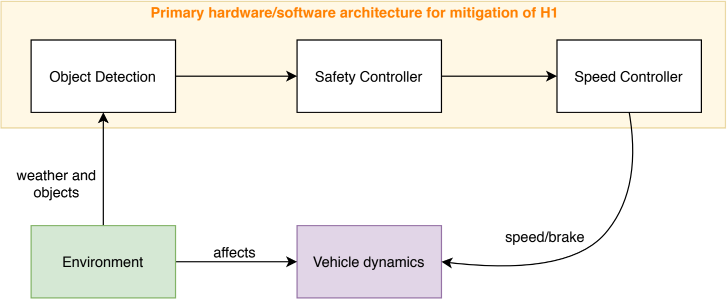
Safety Case

Hazard Analysis - Fault Tree


H1: Collision with Object
A
Obstacle not detected by sensor
B
Obstacle detection algorithm failure
C
Failure of braking mechanism
D
Incorrect setup of machine
E
Communication failure between main computer and sensors/actuators
Mounted header different than header selected in software setup
D1
Power failure
E1

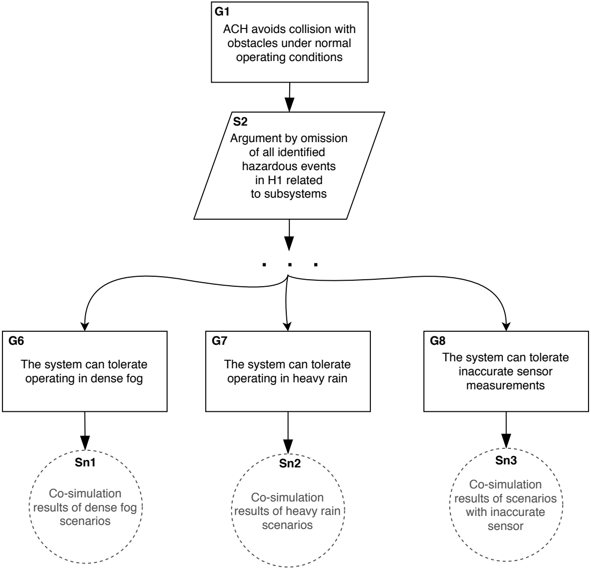
Safety Case

Hazard Analysis - Components



Safety Case

Goal Structuring Notation



G1
ACH avoids collision with obstacles under normal operating conditions

S2
Argument by omission of all identified hazardous events in H1 related to subsystems

. . .

G6
The system can tolerate operating in dense fog

G7
The system can tolerate operating in heavy rain

G8
The system can tolerate inaccurate sensor measurements

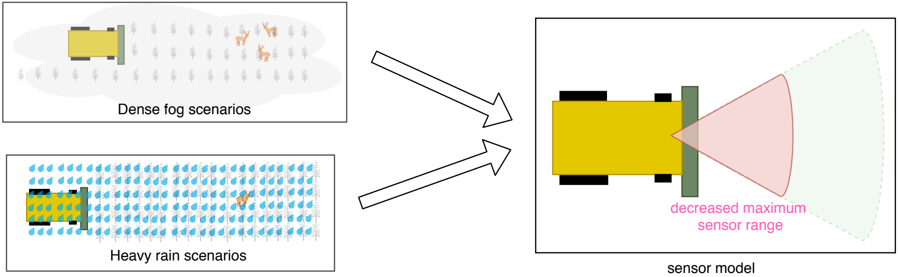
Sn1
Co-simulation results of dense fog scenarios

Sn2
Co-simulation results of heavy rain scenarios

Sn3
Co-simulation results of scenarios with inaccurate sensor

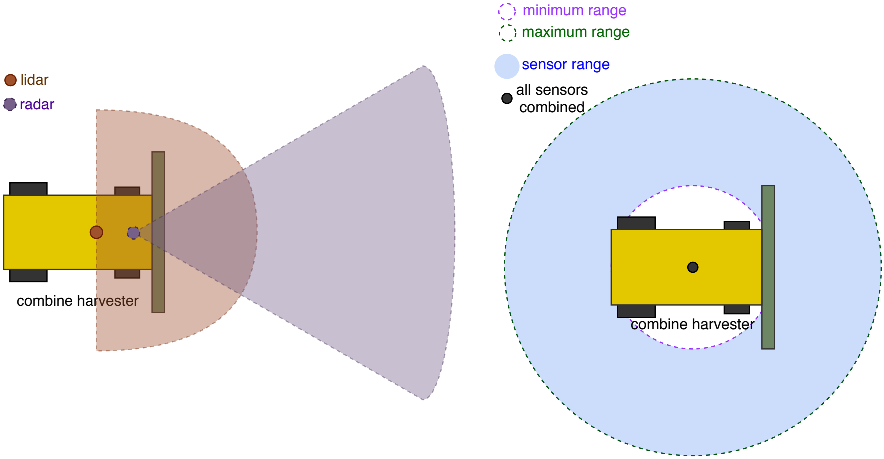
Producing Evidence using Co-simulation

Defining and Modelling Scenarios



Producing Evidence using Co-simulation

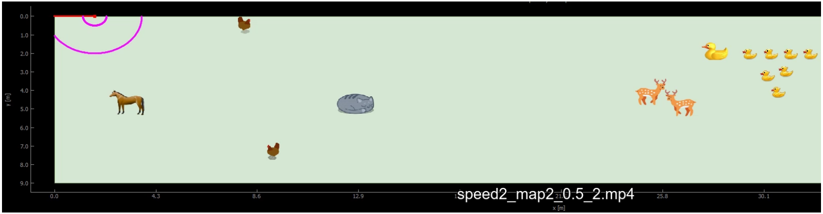
Modelling Sensors



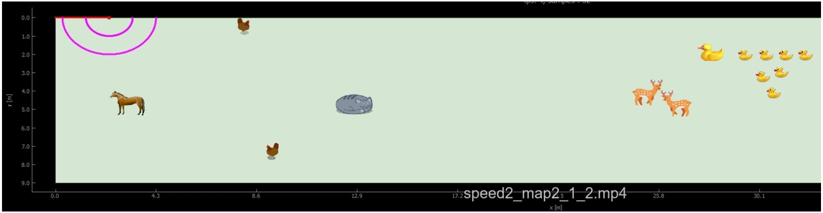
Producing Evidence using Co-simulation

Demo

Speed: 2 m/s, Range: [0.5 ; 2]:

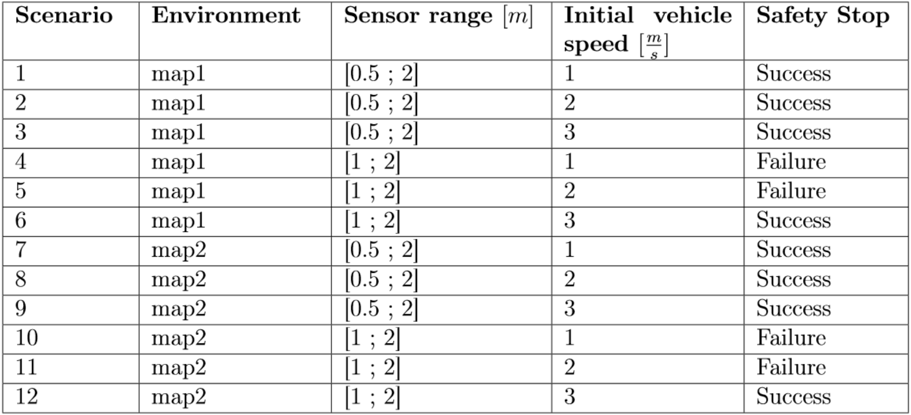


Speed: 2 m/s, Range: [1 ; 2]:



Producing Evidence using Co-simulation

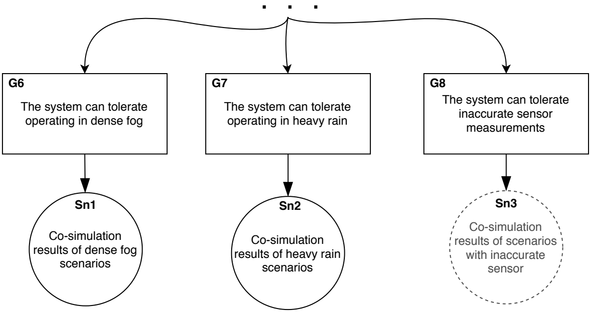
Co-simulation Results



Scenario	Environment	Sensor range $[m]$	Initial vehicle speed $[\frac{m}{s}]$	Safety Stop
1	map1	[0.5 ; 2]	1	Success
2	map1	[0.5 ; 2]	2	Success
3	map1	[0.5 ; 2]	3	Success
4	map1	[1 ; 2]	1	Failure
5	map1	[1 ; 2]	2	Failure
6	map1	[1 ; 2]	3	Success
7	map2	[0.5 ; 2]	1	Success
8	map2	[0.5 ; 2]	2	Success
9	map2	[0.5 ; 2]	3	Success
10	map2	[1 ; 2]	1	Failure
11	map2	[1 ; 2]	2	Failure
12	map2	[1 ; 2]	3	Success

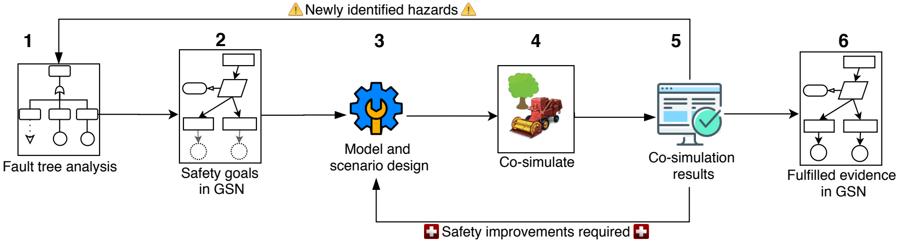
Producing Evidence using Co-simulation

Safety Case Overview



. . .
G6
The system can tolerate operating in dense fog
G7
The system can tolerate operating in heavy rain
G8
The system can tolerate inaccurate sensor measurements
Sn1
Co-simulation results of dense fog scenarios
Sn2
Co-simulation results of heavy rain scenarios
Sn3
Co-simulation results of scenarios with inaccurate sensor

Summary



⚠ Newly identified hazards ⚠

1 Fault tree analysis

2 Safety goals in GSN

3 Model and scenario design

4 Co-simulate

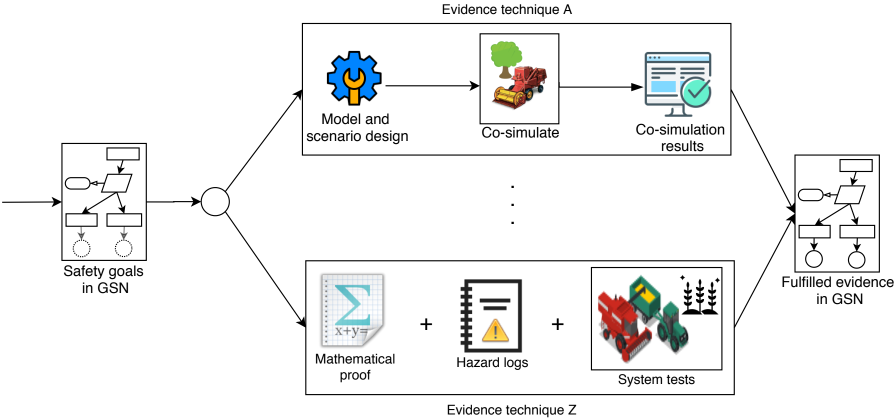
5 Co-simulation results

6 Fulfilled evidence in GSN

🟥 Safety improvements required 🟥

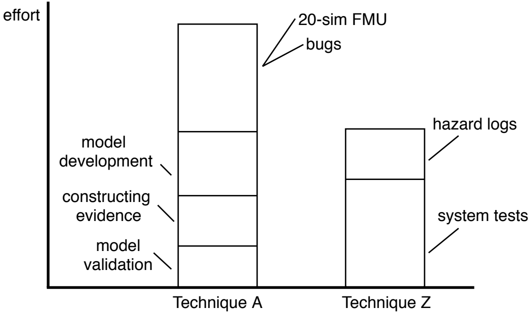
Discussion

When to use this technique?



Discussion

Practical Limitations



Conclusion and Future Work

Conclusion:

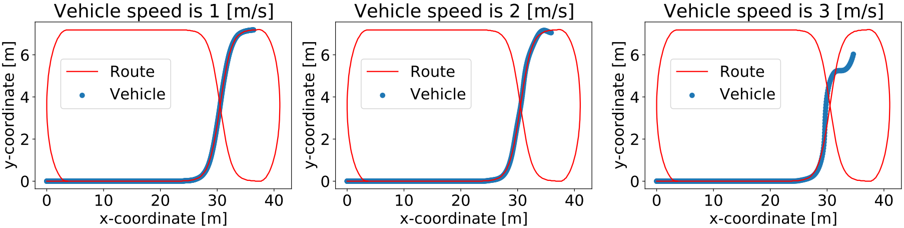
- Case study
- Complex interactions

Future Work:

- Complete safety case
- Medical systems

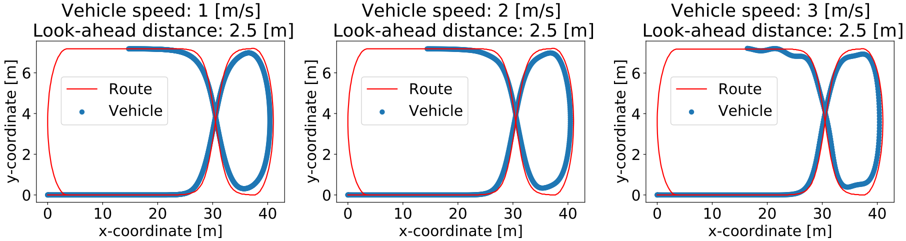
Model Improvements

Issues - Look-Ahead Distance of 0.4m



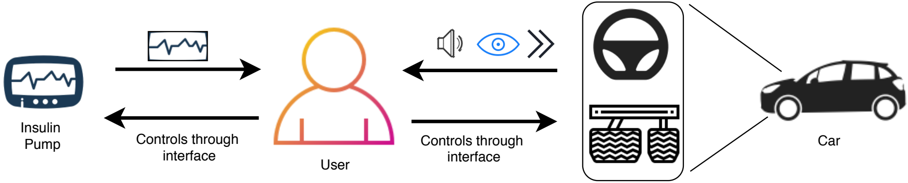
Model Improvements

Improvement - Look-Ahead Distance of 2.5m



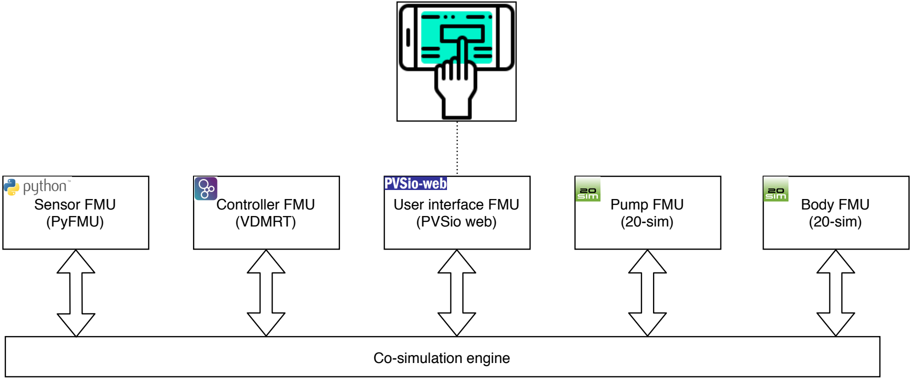
Incorporating Humans in Co-simulation

Humans operating Cyber-Physical Systems



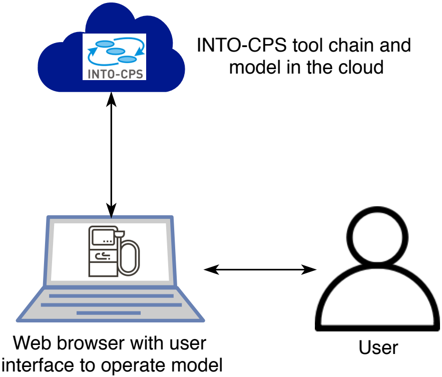
Incorporating Humans in Co-simulation

Co-simulation



Incorporating Humans in Co-simulation

Usability



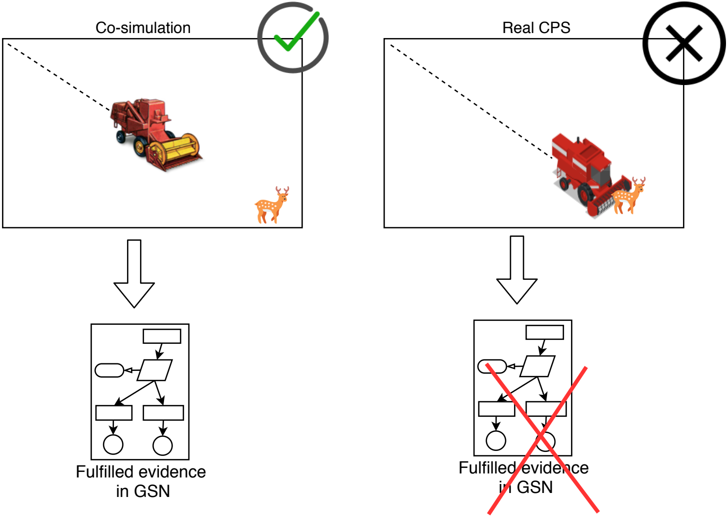
INTO-CPS tool chain and model in the cloud

Web browser with user interface to operate model

User

Model Validation

Why do we need to validate the model?



Co-simulation

Real CPS

Fulfilled evidence in GSN

Fulfilled evidence in GSN

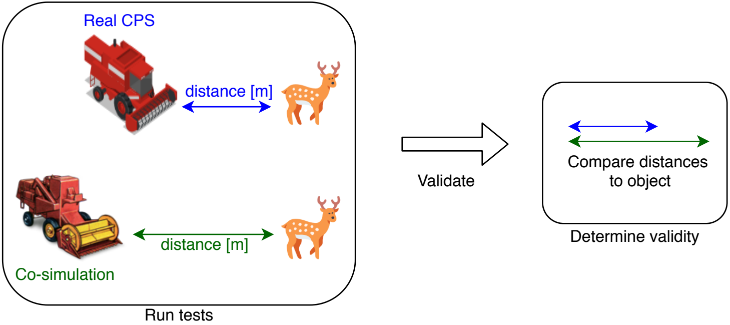
Model Validation

How to validate?

- Purpose of model
- Calibration (non-linear)
- Define expected accuracy: e.g. range
- Define experimental sets

Model Validation

Case study


Real CPS
distance [m]
distance [m]
Co-simulation
Run tests
Validate
Compare distances to object
Determine validity