Combining GSN and STPA for Safety Arguments

Celso Hirata (ITA, Brazil)

and

Simin Nadjm-Tehrani

Linköping University, Sweden

LINKÖPING UNIVERSITY

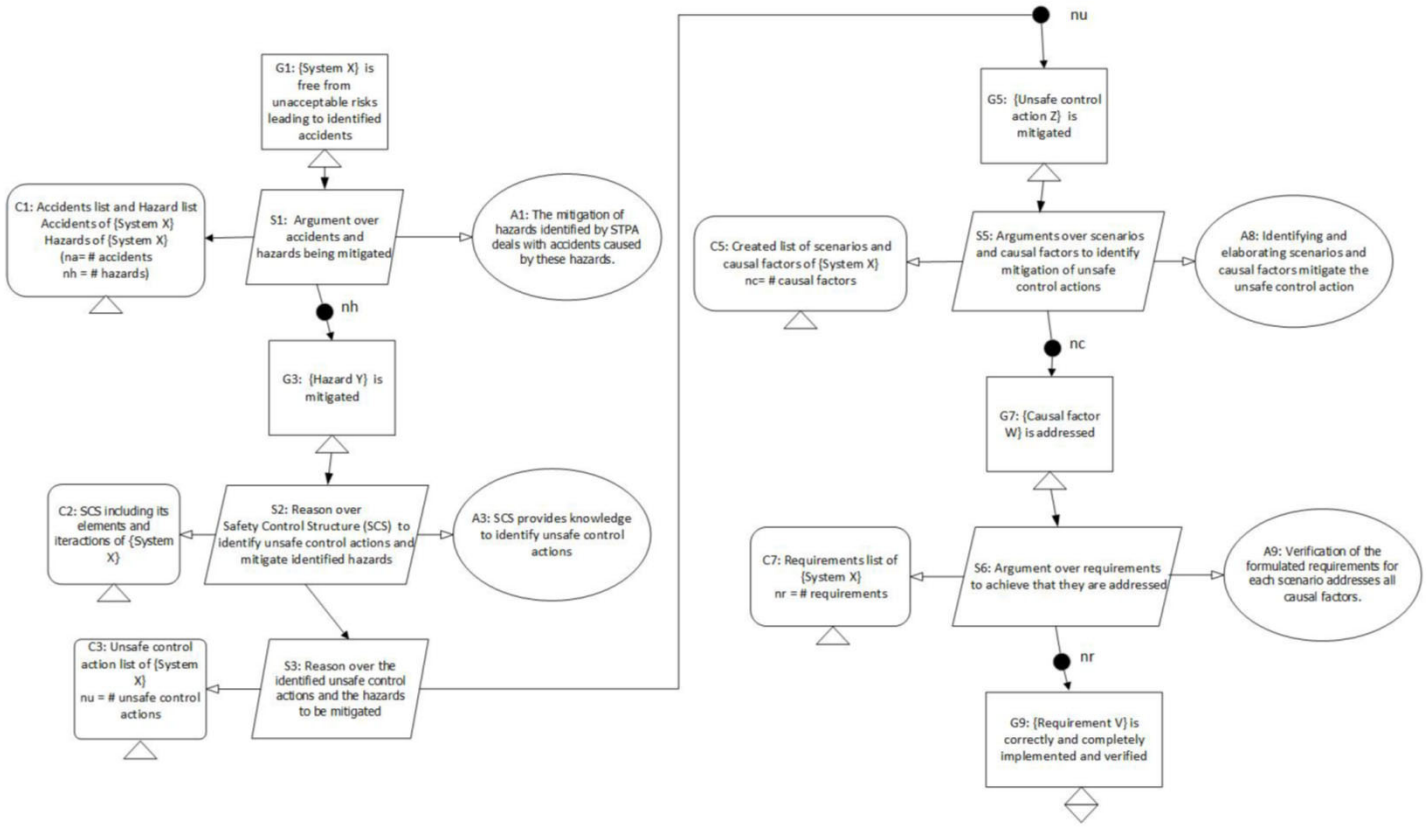
Greetings from Celso!

First the acronyms

- GSN: Goal Structuring Notation

- STAMP: System-Theoretic Accident Model and Processes
- STPA: System Theoretic Process Analysis

Our contribution: Pattern for combining them

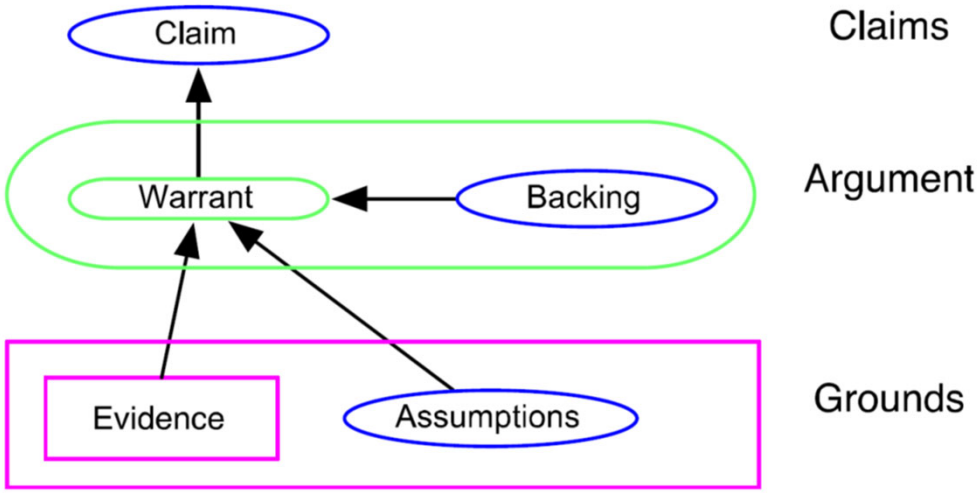


Motivation: Safety assurance

LINKÖPINGS UNIVERSITET

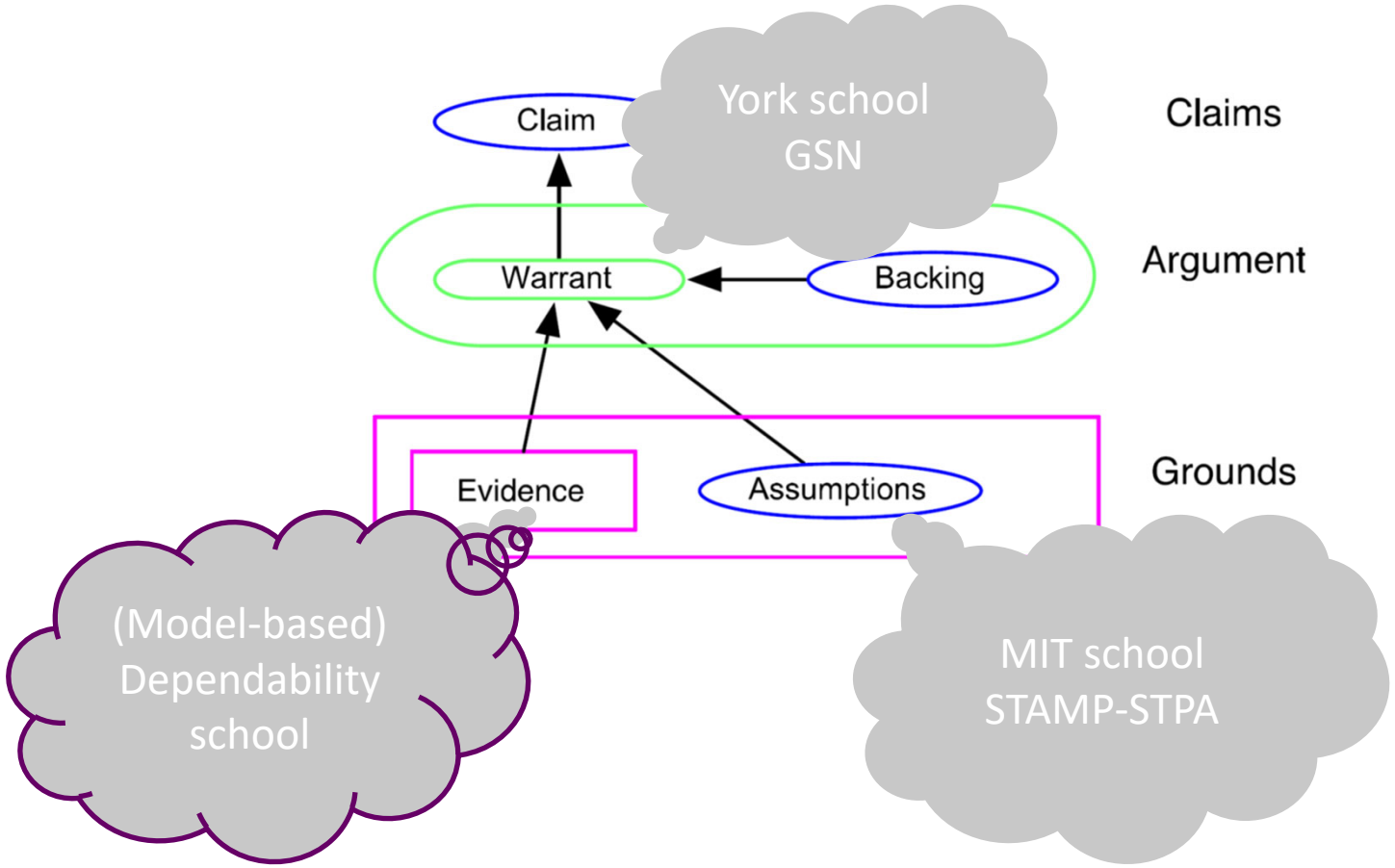
Safety assurance basics

- Formulated already in 1958!



Bloomfield et al. 2013
doi.org/10.1007/978-3-642-40894-6_2

Safety assurance methods



Overview

- Safety assurance driven dependability analysis
  - What is GSN?
  - What is STPA?

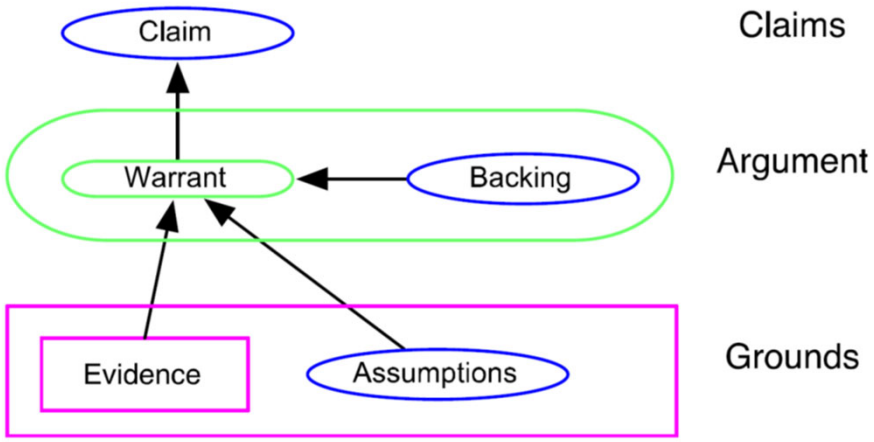
- How to combine their benefits?
  - Running case as example: Train door controller system

GSN in brief

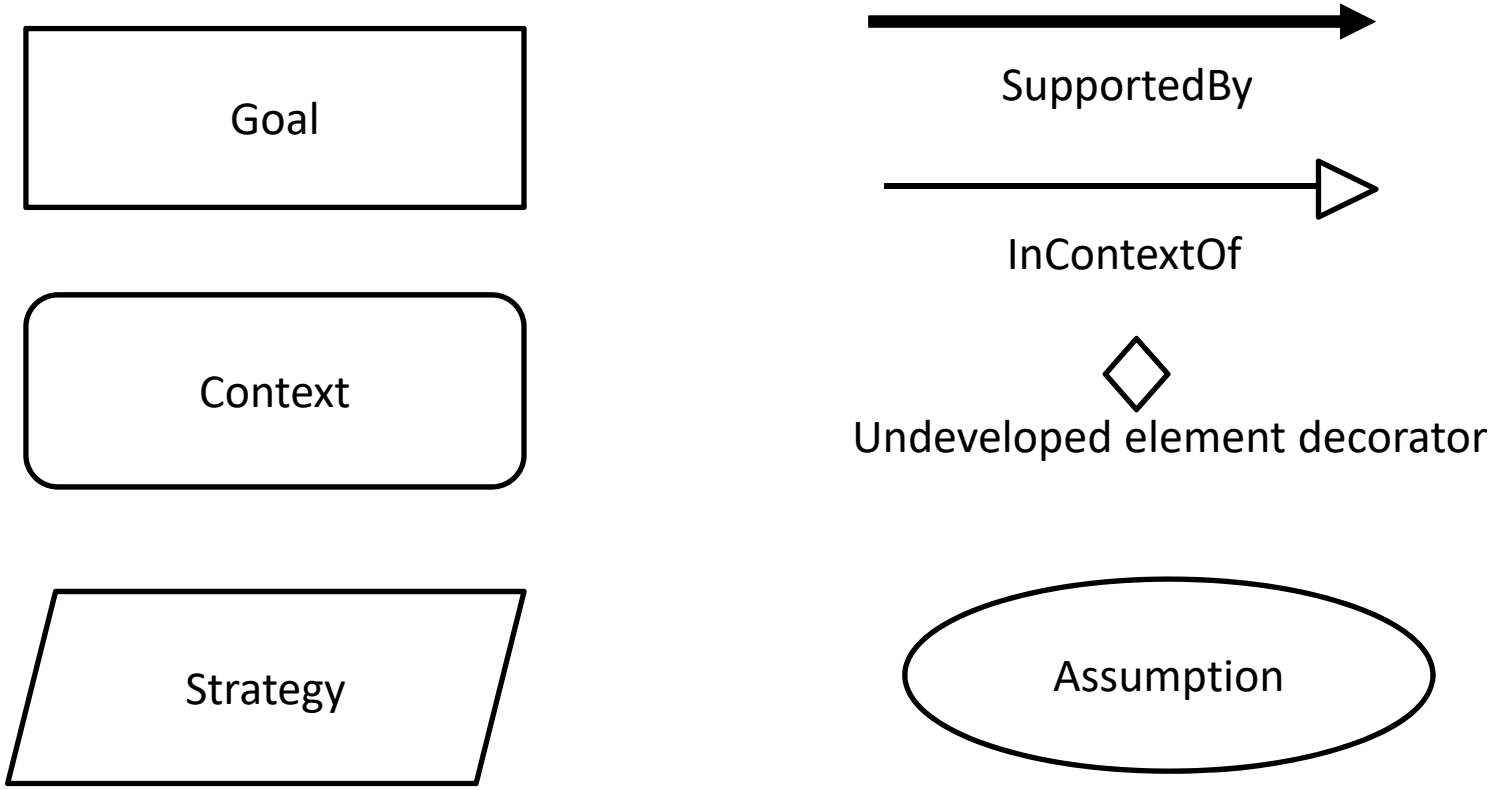
LINKÖPINGS UNIVERSITET

Goal Structuring Notation (GSN)

- Corresponding elements:
  - Goals = Claims
  - Strategies = Arguments
  - Solutions = Evidence



GSN subset we used



Hazard analysis with STPA

LINKÖPINGS UNIVERSITET

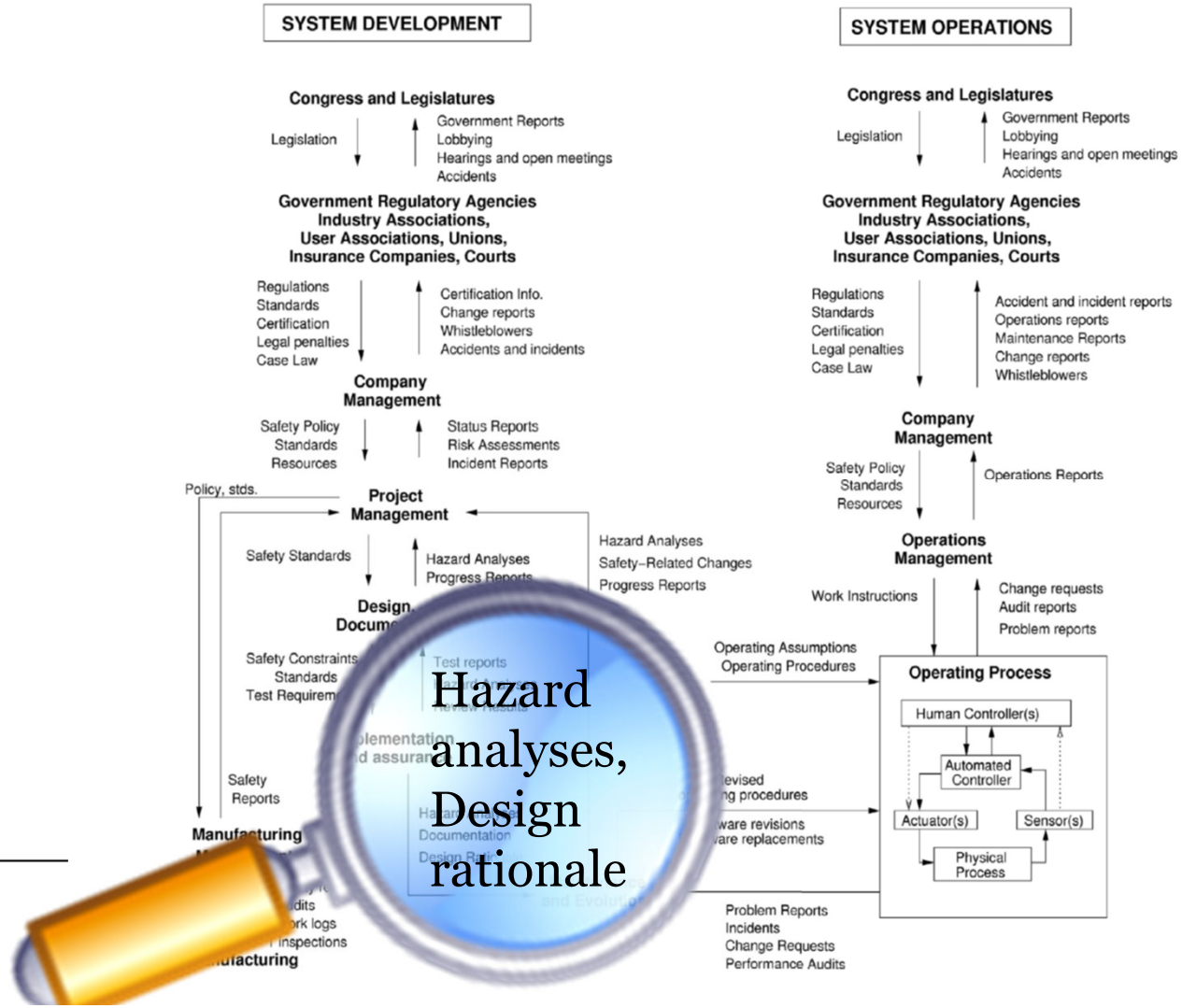
"Control is provided not only by engineered systems and direct management intervention, but also indirectly by policies, procedures, shared values, and other aspects of the organizational culture, sometimes called the "safety culture."

Leveson 2015

doi.org/10.1016/j.ress.2014.10.008

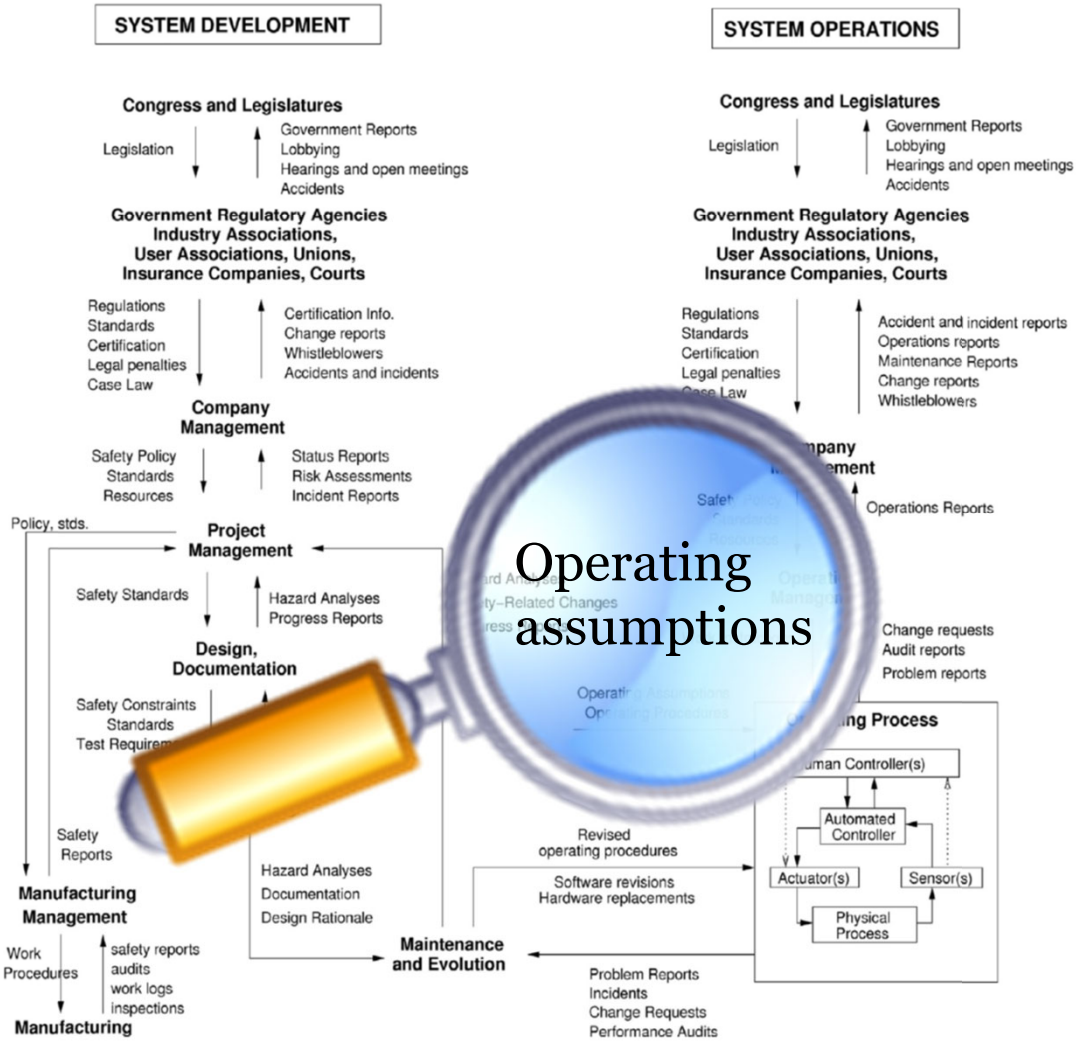
Safety is not just code!

Leveson 2015



Safety is not only code!

Leveson 2015



LINKÖPING UNIVERSITY

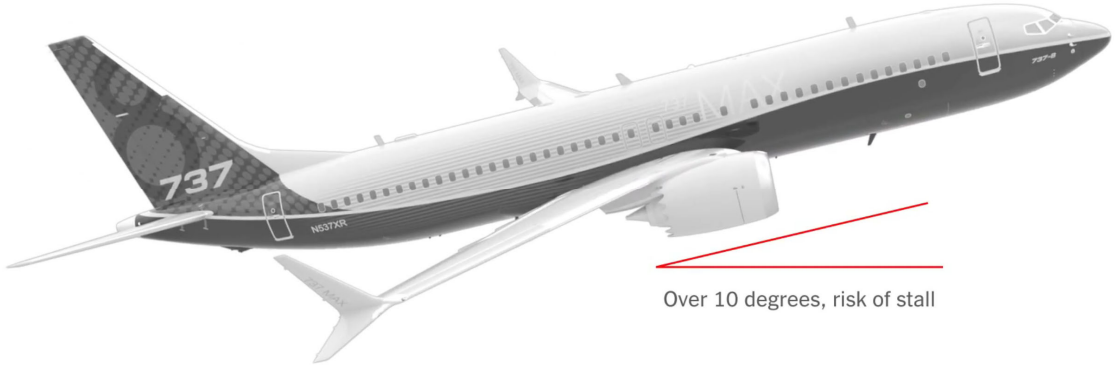
"Hazards that the engineers thought were eliminated or prevented should, of course, never occur. If they do, this event is an indication of flaws in the engineering process or perhaps in the assumptions made about the operational system, such as assumptions about pilot or air traffic controller behavior. It is not just enough to fix the technical process. The holes in the development process that allowed hazardous behaviour to occur need to be fixed."

Leveson 2015

Well, that's where we are!

- B737M accidents 2018-19

https://www.nytimes.com/interactive/2019/03/29/business/boeing-737-max-8-flaws.html

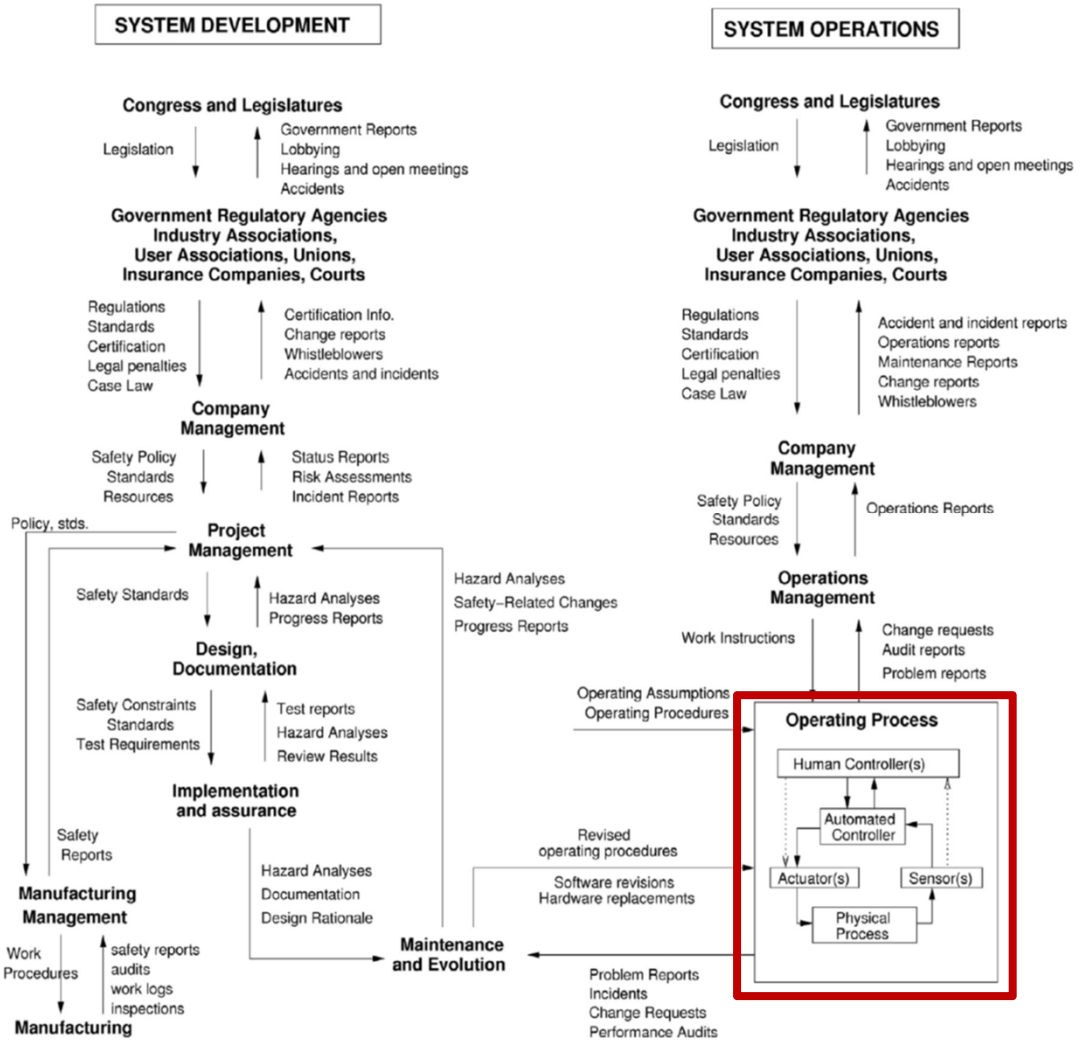


STPA: System-Theoretic Process Analysis

- *Define the Purpose of the Analysis* aims to identify **accidents**, **hazards**, and the system boundary
- ***Model the Control Structure*** captures functional relationships and interactions using STAMP
- *Identify Unsafe Control Actions* - identifies the potentially **Unsafe Control Actions** (UCA) and associated safety constraints
- *Identify Loss Scenarios* - reveals potential causes of issuing UCAs and generate **safety requirements**

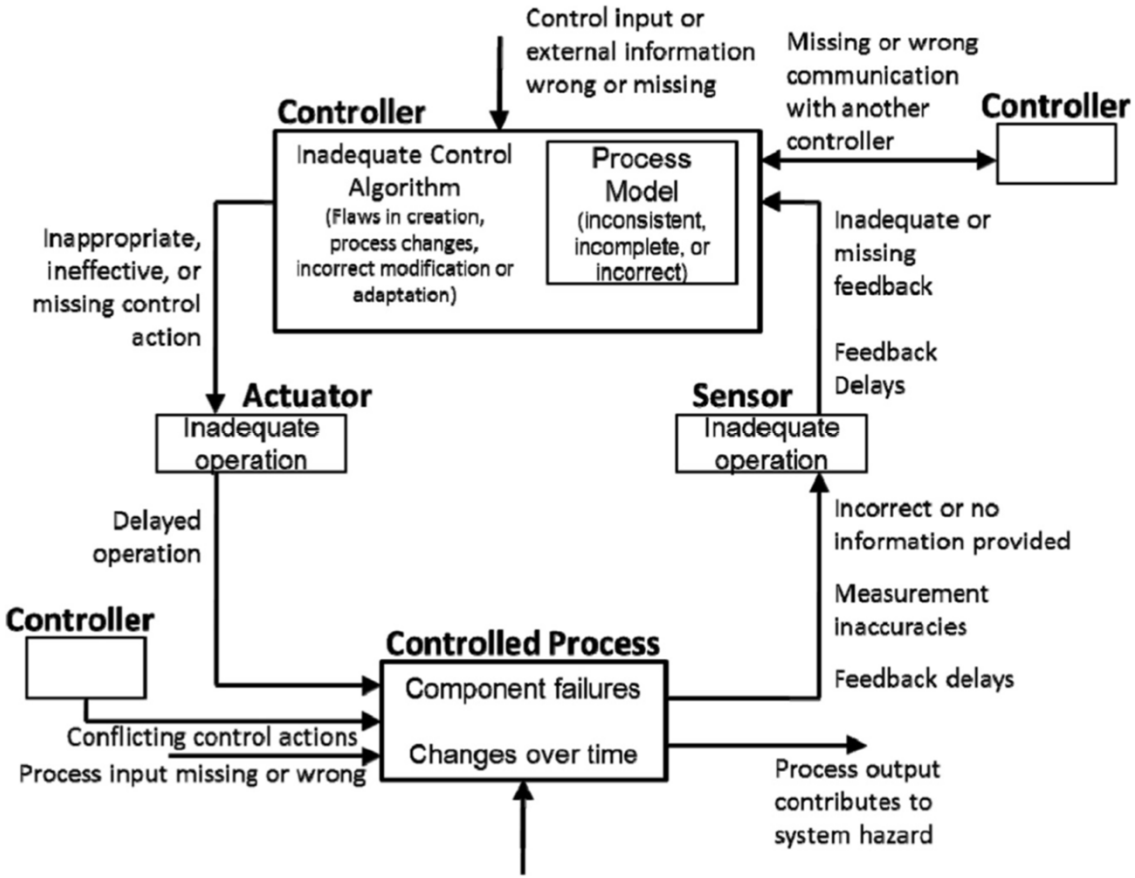
Safety is not just code!

Leveson 2015



LINKÖPING UNIVERSITY

STAMP/STPA: High-level control structure



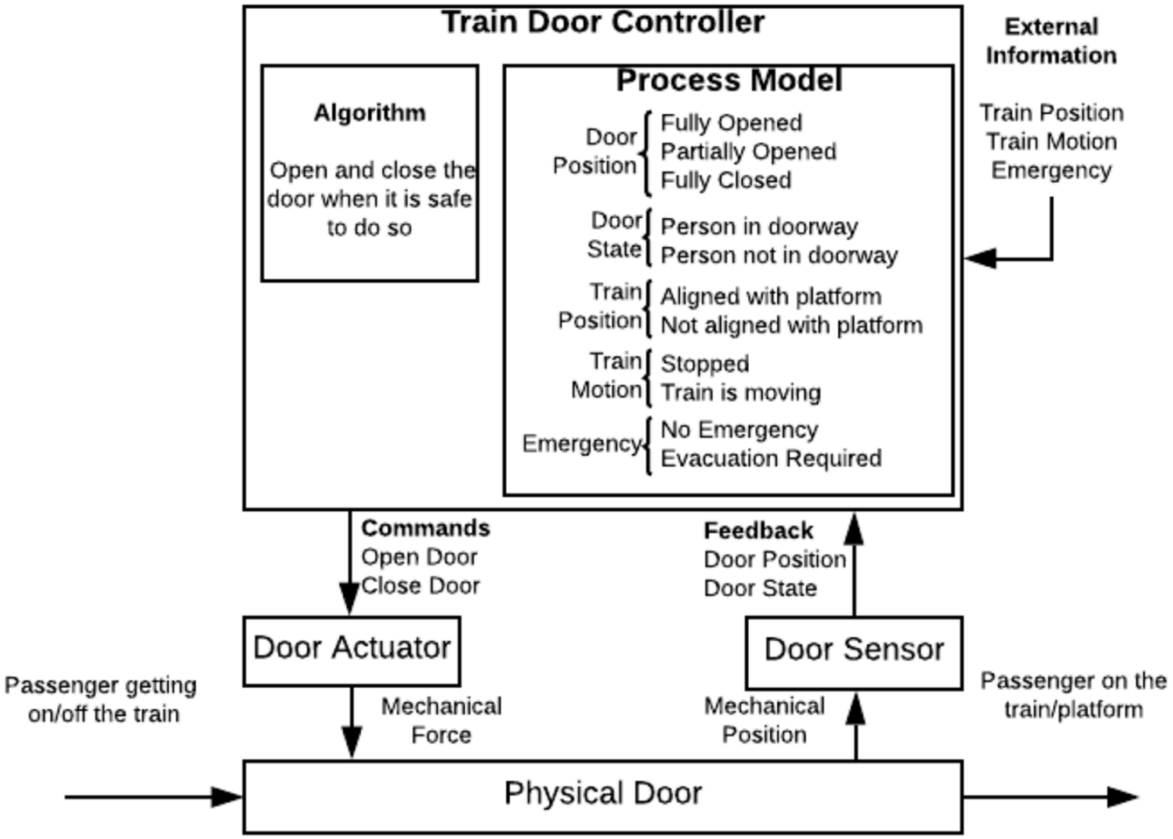
STPA: System-Theoretic Process Analysis

- Define the Purpose of the Analysis aims to identify accidents, hazards, and the system boundary
- Model the Control Structure captures functional relationships and interactions using STAMP
- *Identify Unsafe Control Actions* - identifies the potentially **Unsafe Control Actions** (UCA) and associated safety constraints
- *Identify Loss Scenarios* - reveals potential causes of issuing UCAs and generate **safety requirements**

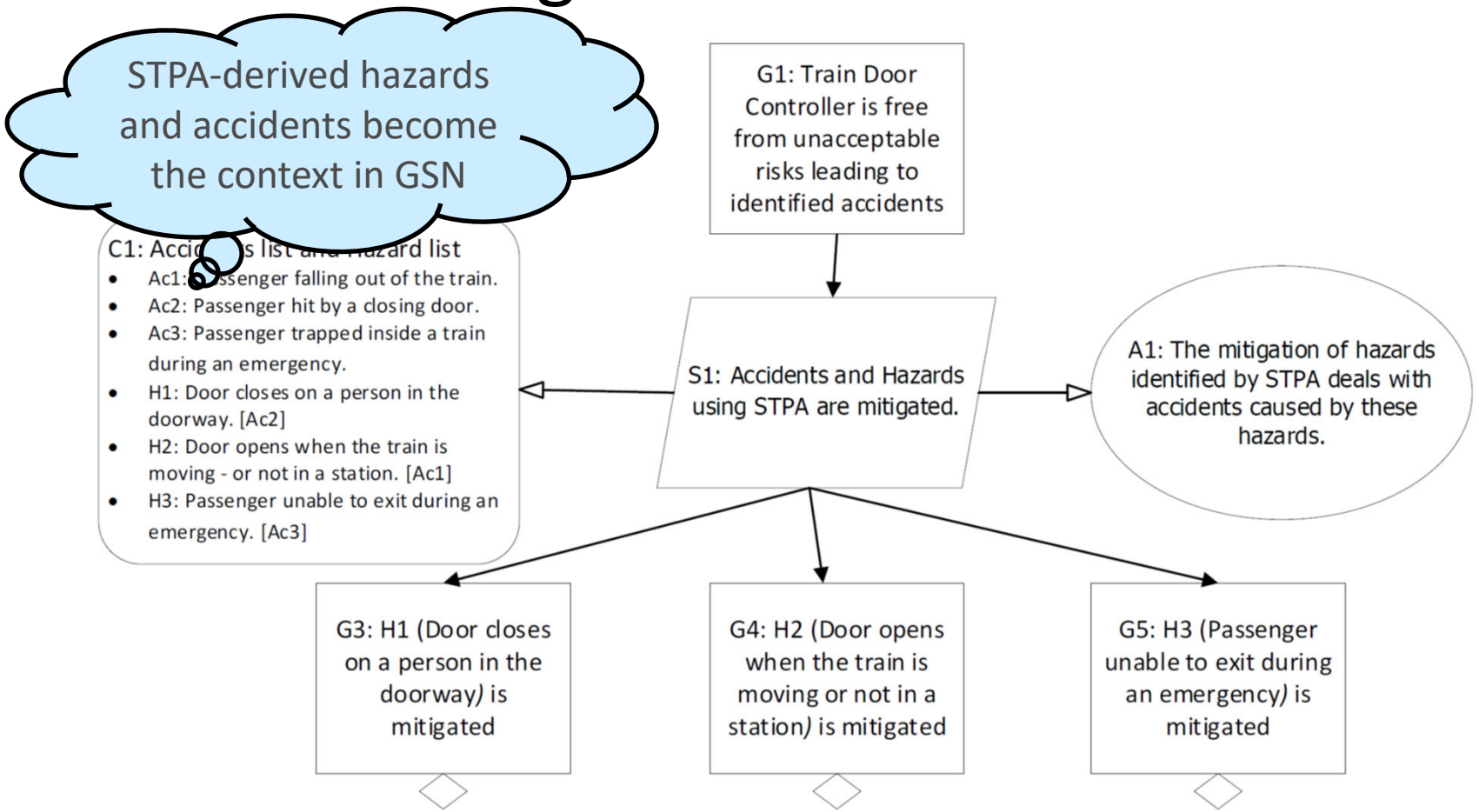
Arguing for GSN claims using STPA

LINKÖPINGS UNIVERSITET

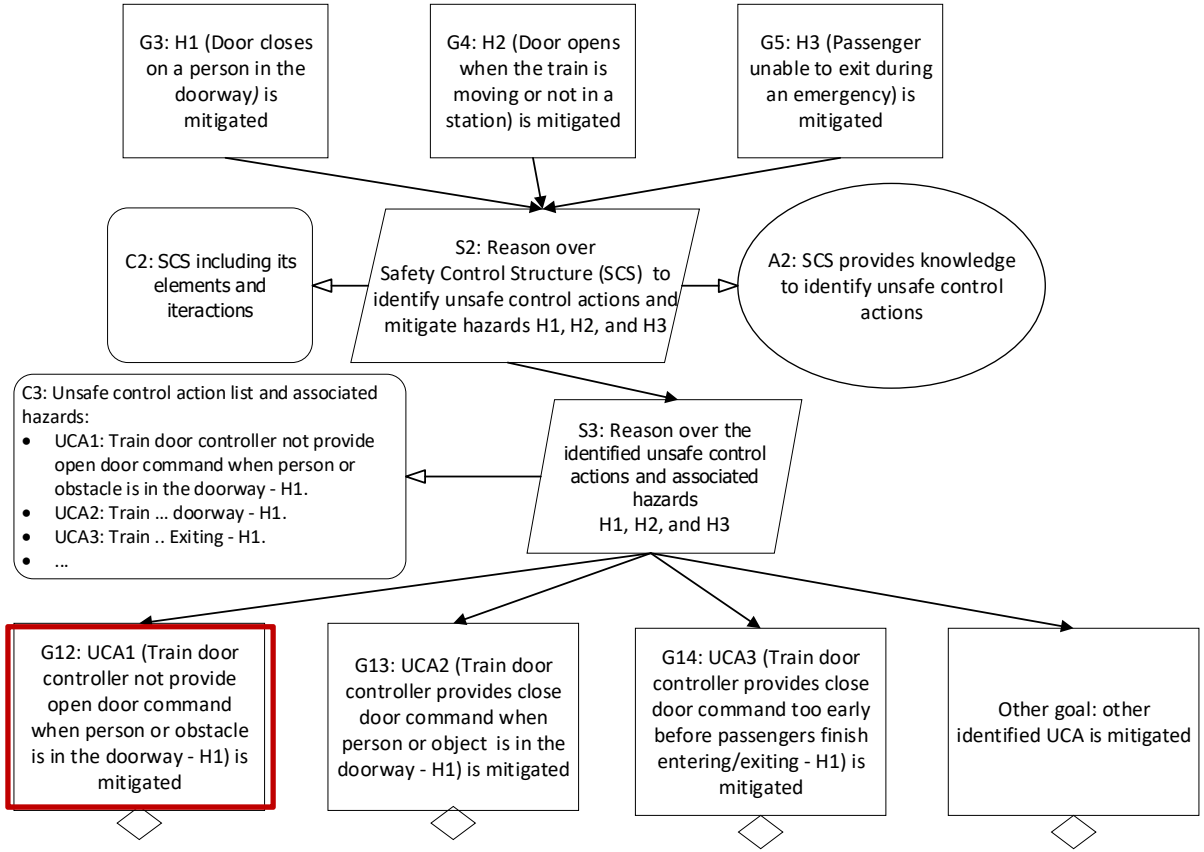
Example: Train door controller system



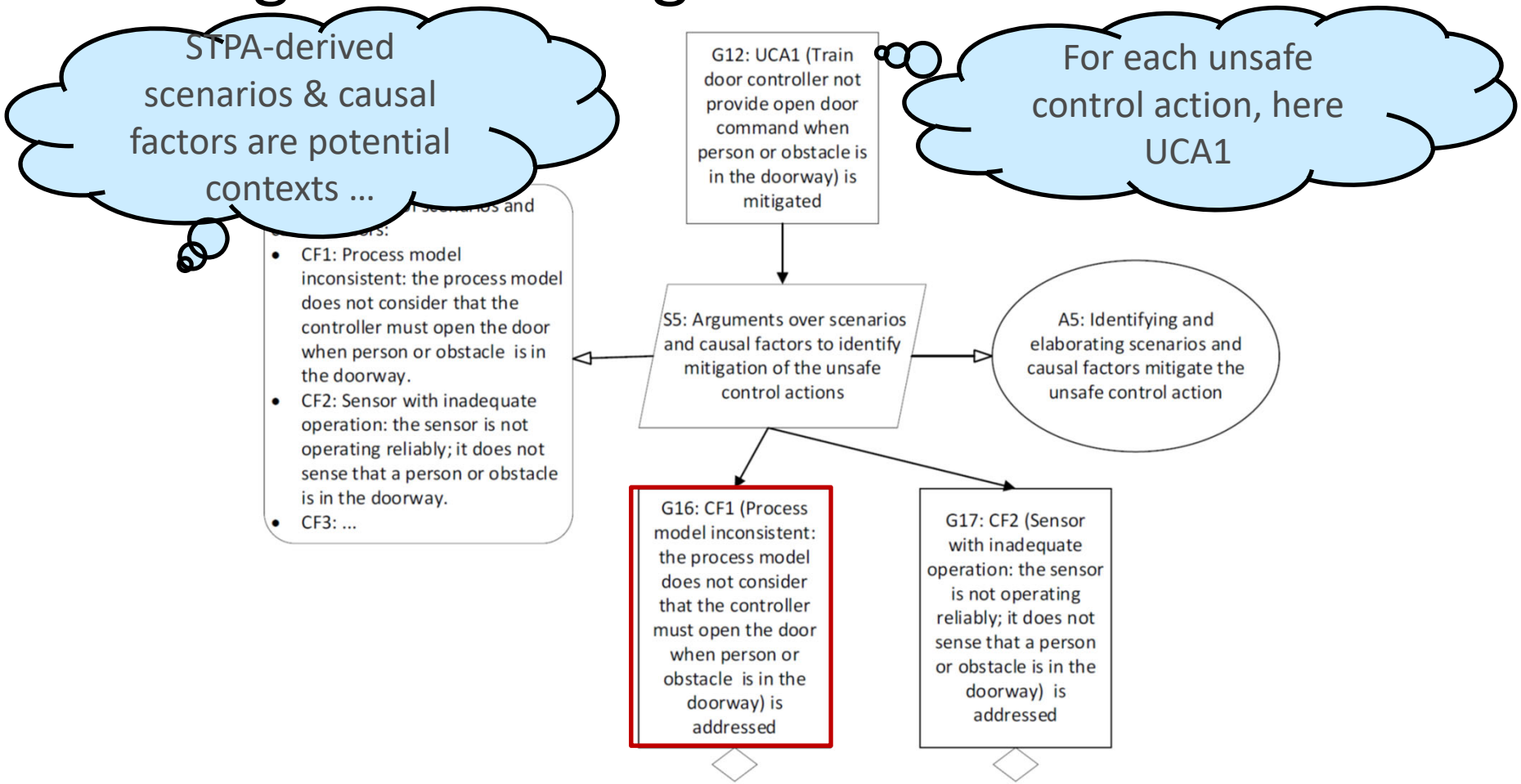
Documenting reliance on STPA



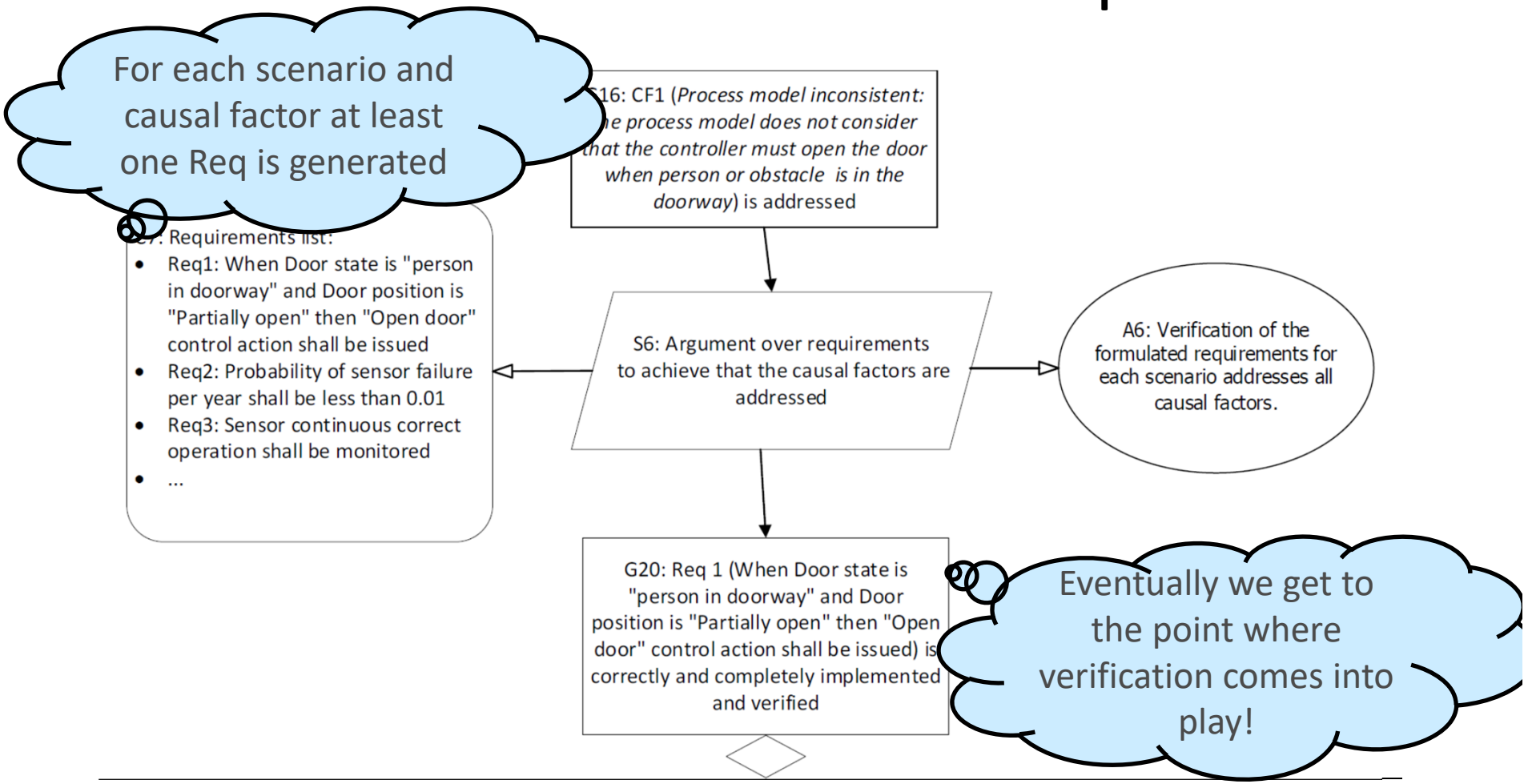
Mitigation of hazards



Using STPA for argument construction



From causes of accidents to Reqs



For the TDC example

- We constructed:
  - 3 accidents, 3 hazards
  - 13 unsafe control actions
  - 112 requirements (numbers of scenarios and causal factors are less)

- Perhaps the limit of what one can do manually without tool support!

Conclusions

- This work attempts to bring together seemingly isolated islands of work on safety analysis and assurance
- Model-based dependability analysis can then use the requirements
  - Systematically support the safety case
- The generic STPA+GSN template should be applicable to real systems
  - Documenting a natural work flow

Ongoing and future works

- The STPA generation of Hazards, Accidents, Scenarios, Causal factors, Requirements needs to be supported by tools
  - Our work in that direction uses ontologies – also considering impact of security on safety doi.org/10.1016/j.jisa.2019.05.014
  - WebSTAMP tool for STPA under development doi.org/10.1051/matecconf/201927302010

    (currently at: http://webstamp.herokuapp.com/)

Questions?

https://www.ida.liu.se/labs/rtslab/publications/