Combining GSN and STPA for Safety Arguments

Celso Hirata (ITA, Brazil) and

Simin Nadjm-Tehrani

Linköping University, Sweden





Greetings from Celso!





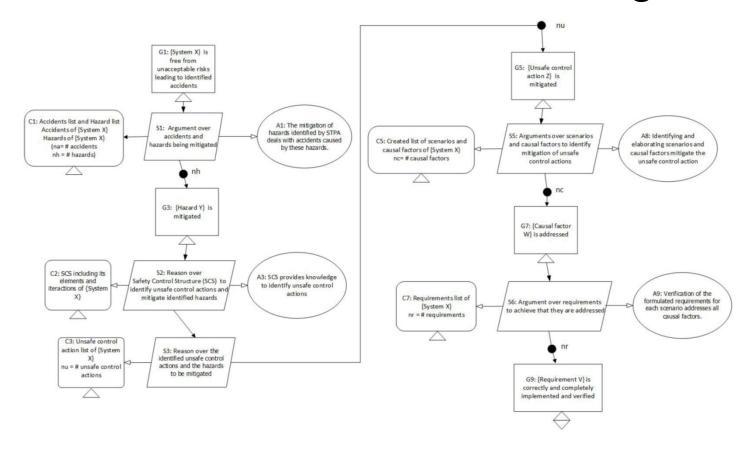
First the acronyms

• GSN: Goal Structuring Notation

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



Our contribution: Pattern for combining them



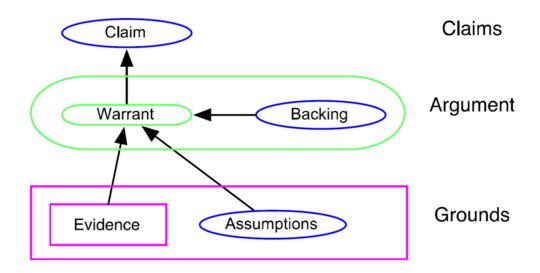


Motivation: Safety assurance



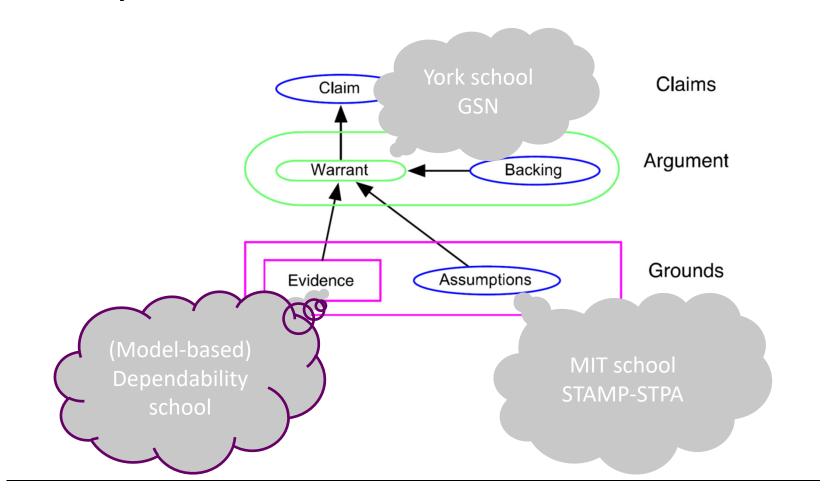
Safety assurance basics

• Formulated already in 1958!





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



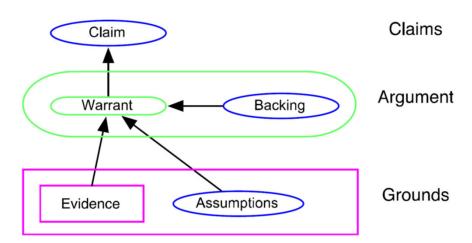


GSN in brief



Goal Structuring Notation (GSN)

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





GSN subset we used

SupportedBy Goal InContextOf Context Undeveloped element decorator Assumption Strategy



Hazard analysis with STPA



"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."

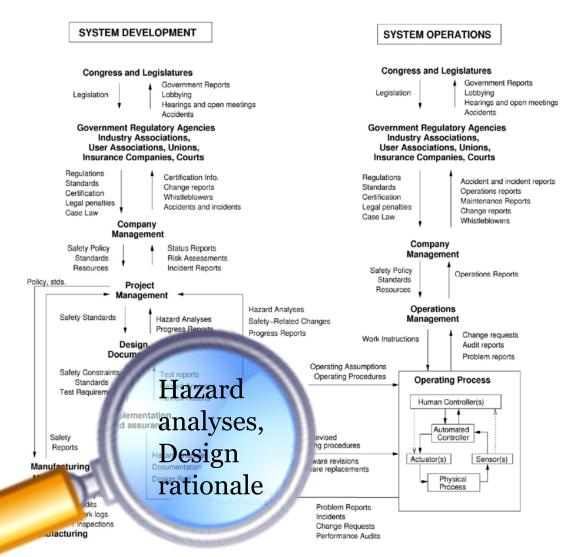
Leveson 2015

doi.org/10.1016/j.ress.2014.10.008



Safety is not just code!

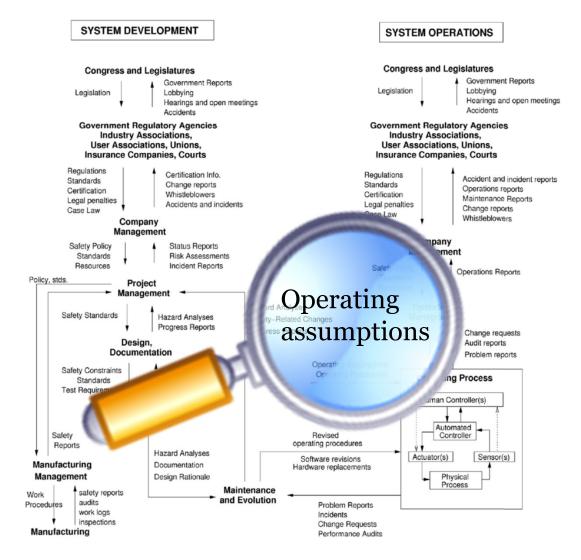
Leveson 2015





Safety is not only code!

Leveson 2015





"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."



Well, that's where we are!

• B737M accidents 2018-19

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





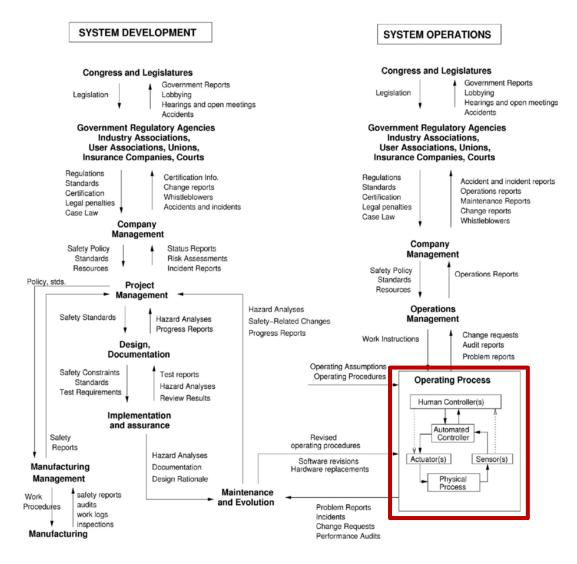
STPA: System-Theoretic Process Analysis

- 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**



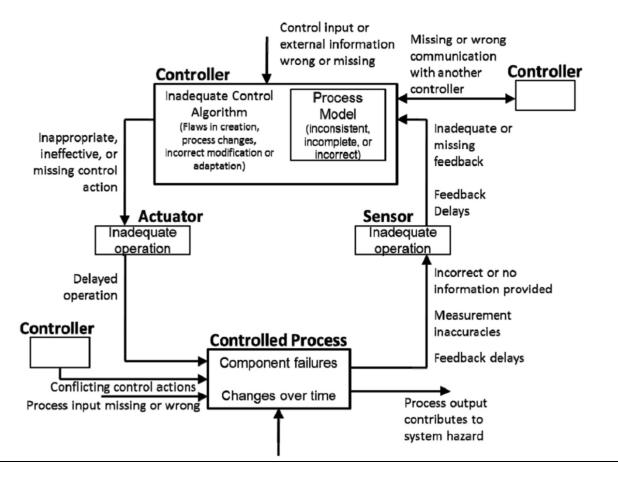
Safety is not just code!

Leveson 2015





STAMP/STPA: High-level control structure





STPA: System-Theoretic Process Analysis

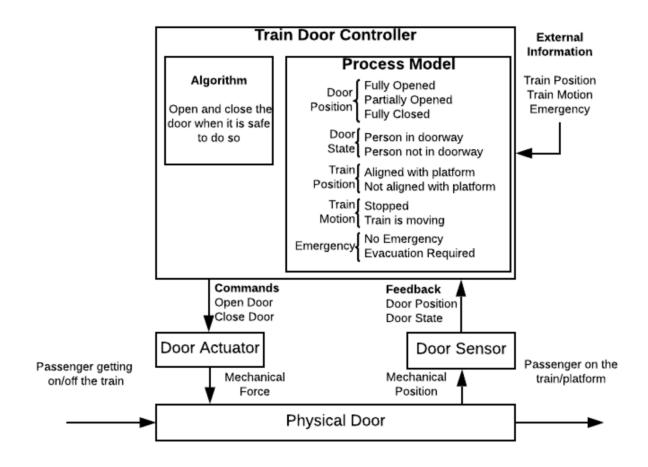
- Define the Purpose of the Analysis aims to identify accidents, hazards, and the system boundary
- Model the Control Structure captures functional relationships and interactions using STAMP
- Identify Unsafe Control Actions identifies the potentially **Unsafe Control Actions** (UCA) and associated safety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



Arguing for GSN claims using STPA

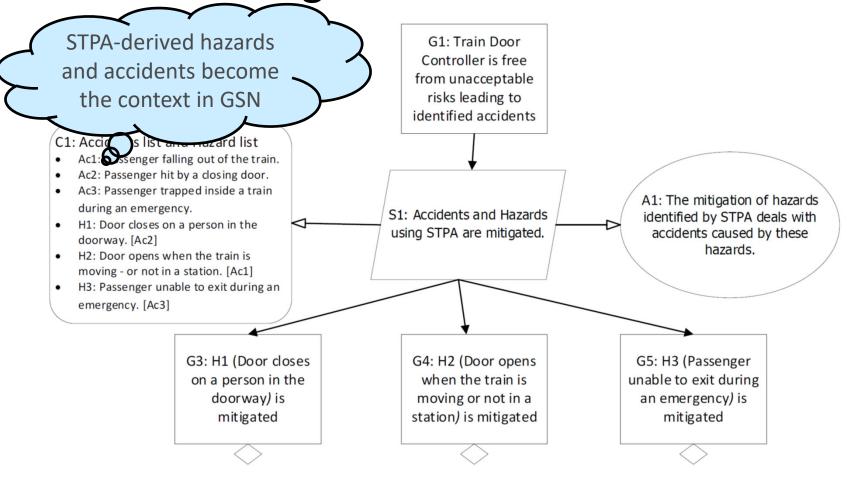


Example: Train door controller system



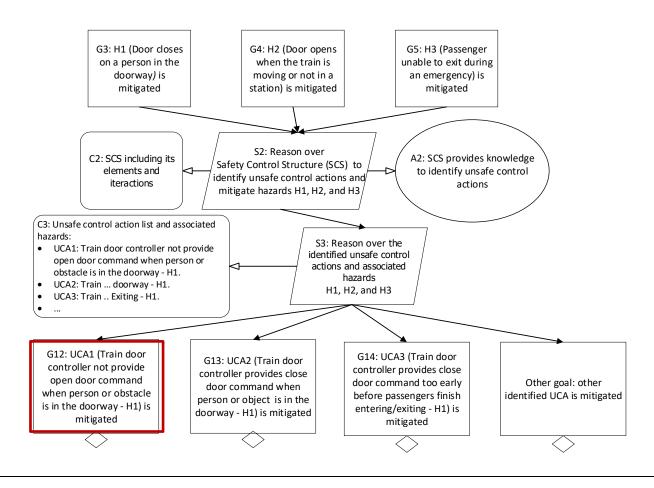


Documenting reliance on STPA





Mitigation of hazards





Using STPA for argument construction STPA-derived For each unsafe G12: UCA1 (Train door controller not scenarios & causal control action, here provide open door command when factors are potential UCA1 person or obstacle is in the doorway) is contexts ... mitigated CF1: Process model inconsistent: the process model does not consider that the S5: Arguments over scenarios A5: Identifying and controller must open the door and causal factors to identify elaborating scenarios and when person or obstacle is in mitigation of the unsafe causal factors mitigate the the doorway. control actions unsafe control action CF2: Sensor with inadequate operation: the sensor is not operating reliably; it does not sense that a person or obstacle is in the doorway. G16: CF1 (Process G17: CF2 (Sensor CF3: ... model inconsistent: with inadequate the process model operation: the sensor does not consider is not operating that the controller reliably; it does not must open the door sense that a person when person or or obstacle is in the obstacle is in the doorway) is doorway) is addressed addressed



From causes of accidents to Reqs

For each scenario and 16: CF1 (Process model inconsistent: causal factor at least ne process model does not consider at the controller must open the door one Req is generated when person or obstacle is in the doorway) is addressed Requirements list: Reg1: When Door state is "person in doorway" and Door position is "Partially open" then "Open door" A6: Verification of the S6: Argument over requirements control action shall be issued formulated requirements for Req2: Probability of sensor failure to achieve that the causal factors are each scenario addresses all per year shall be less than 0.01 addressed causal factors. • Req3: Sensor continuous correct operation shall be monitored G20: Req 1 (When Door state is Eventually we get to "person in doorway" and Door position is "Partially open" then "Open the point where door" control action shall be issued) is verification comes into correctly and completely implemented and verified play!



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/





