Safety Driven Design with UML and STPA

Martin Rejzek, Sven Krauss, Christian Hilbes

Zurich University of Applied Sciences, Switzerland
A typical situation:

System Engineer / Developer

Safety Engineer

Safety Case

Product
System and Safety Engineering

The challenges with this situation:

- Product development and safety management separated
- Different teams, methods, terminology
- Different processes and mindset
The challenge is even more severe for complex systems involving sub-contractors:
Processes

V-Model Zoo:

Risk Management Processes:
System and Safety Engineering

System Engineer / Developer

- Model based development with UML
- UML Case Tools
- Automated Code Generation

Safety Engineer

- FTA, FMEA, HAZOP, …
- Dedicated Tools
A typical situation in smaller companies:

System Engineer = Developer = Safety Engineer

Developer wants to do a good job but has no chance to cope with “everything” …

Solution: Empower developer to incorporate the safety aspects right into system development
State of the Art in Systems Engineering: Model Based Development with UML

Structural:
- Class Diagram
- Object Diagram
- Package Diagram
- Component Diagram
- Composite Structure Diagram
- Deployment Diagram

Behavioral:
- UseCase Diagram
- Sequence Diagram
- Activity Diagram
- StateMachine Diagram
- Interaction (Overview) Diagram
- Communication Diagram
- Timing Diagram
Example

Fictitious example (examples from our industry partners are confidential):

Illustration adapted from Y.S. Weng, et al., *Design of Traffic Safety Control Systems for Railroads and Roadways Using Timed Petri Nets*
Model system requirements as UML UseCase diagram
Initial architecture concept as SysML Block diagram

- Suitable for a systematic safety analysis? … No
STPA Hierarchical Control Structure for System Concept Development

We propose to use a Hierarchical Control Structure for system concept development instead.
STPA Hierarchical Control Structure: Support for Multiple Levels of Detail

Diagram of a Railroad Crossing Control System showing levels of detail from the top level HCS to the gate controller.
Block Diagram vs. Hierarchical Control Structure (HCS)

• Block diagram
  – Focus on components emphasizes component failures
  – Was not designed as a basis for systematic safety analysis

• Hierarchical Control Structure:
  – Is designed as basis for safety analysis with STPA Step 1
  – Step 1 questions correspond to questions developer would naturally ask

• Critical challenge: do not force developer to change scope/mindset. Therefore…
  – Capture HCS, perform Step 1 in the same UML case tool
  – Invent new UML diagram types for HCS, Step 1
Proposal for STPA Step 1 diagram:

- **Control Action**: Close Gates
- **Keyword**: Expected but given too early
- **Logical operator**: and
- **Unwanted Process Reaction/State**: Gates are closed much earlier than expected.
- **Safety Constraint**: Time between closing of gates and train approaching shall not be too long.
- **Hazard**: Pedestrians could interpret closing of the gates as failure since they have to wait longer than usual.
- **Keyword**: Pedestrians are crossing the tracks although the gates are closed.
- **Hazard**: Pedestrians on crossing when train approaching.
System Development and Traceability

- New diagram types to model functional architecture and safety analysis
- Standard UML diagrams to progress system development and model detailed implementation
System Development and Traceability

Traceability between elements:
- From design model to STPA
- From Control Action to System Level Losses

Hierarchical Control Structure

Step 1

System Level Definitions
- System Loss
- System Hazard
- Unwanted Process State
- Unwanted Process Reaction

Traceability
- From design model to STPA
- From Control Action to System Level Losses
Graph Visualization

Visualizing elements and relationships as graph allows:

- Seeing the “big picture”
- Analyzing the relevance of controllers
- Doing a safety constraint impact analysis
Methods to identify accident scenarios:

- For simple actuators, sensors, data transmission: FTA, FMEA,
- For complex actuators, sensors: dedicated subsystem STPA
- For controller algorithm: Annotation of Behavioral diagrams
Organization of accident scenarios with generic fault tree:

- Structured documentation
- Interface to other tools

In principal: allows quantification of accident scenarios
Conclusion and Outlook (1/2)

We developed a practical approach to safety driven design: the integration of system and safety engineering

- Extended UML with profile for STPA diagrams
  - Hierarchical Control Structure
  - STPA Step 1 diagrams
- Augment behavioral and structural diagrams with annotations to capture accident scenarios
  - STPA Step 2
- Realize and maintain traceability between system design, system implementation and hazards, accidents
- Organize accident scenarios with generic fault tree
Conclusion and Outlook (2/2)

- Project in collaboration with Curtiss Wright Drive Technology, Schaffhausen, Switzerland and funded by Swiss Commission of Technology and Information
- Tool Development:
  - Plan to present the tool at the European STAMP Workshop 2015