A Tool-Based STPA Process

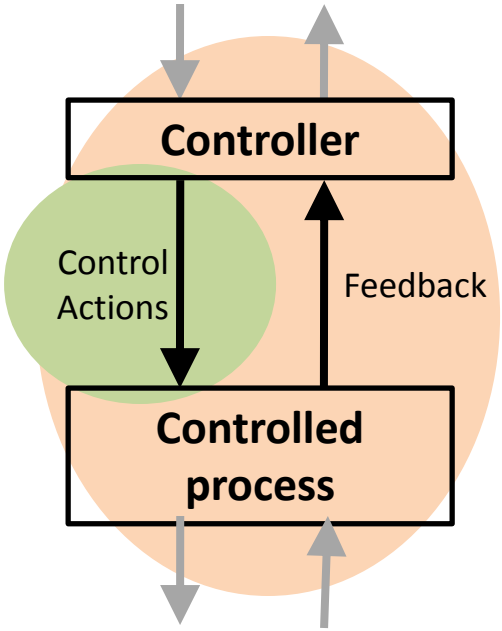
John Thomas and Dajiang Suo

Outline

- Formal approach to STPA
- Current tool-based STPA process
- New tool-based STPA process

STPA
(System-Theoretic Process Analysis)

- System engineering foundation
  - Define accidents, hazards
  - Create control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios

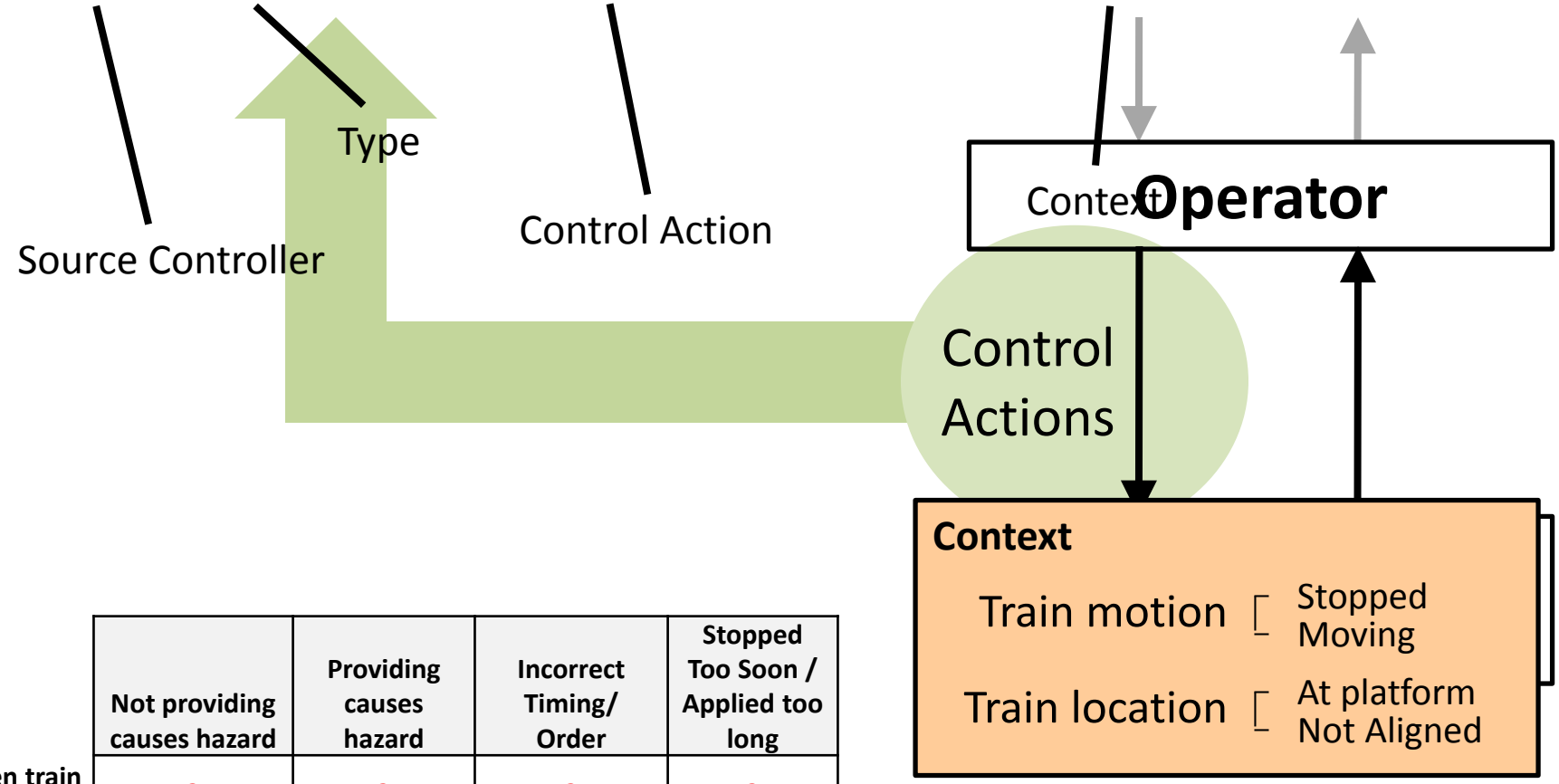


(Leveson, 2012)

Structure of an Unsafe Control Action

Example UCA:

"Operator provides open train door command when train is moving"



	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Open train door	?	?	?	?

Formalizing Unsafe Control Actions

Example UCA:
"Operator provides open train door command when train is moving"

Controller	Action Type	Control Action	Train Motion	Emergency	Train Position	Hazardous?
Operator	**Provides**	**Door open command**	Moving	No	(doesn't matter)	**Yes**
Operator	**Provides**	**Door open command**	Moving	Yes	(doesn't matter)	**Yes***
Operator	**Provides**	**Door open command**	Stopped	Yes	(doesn't matter)	**No**
Operator	**Provides**	**Door open command**	Stopped	No	Not at platform	**Yes**
Operator	**Provides**	**Door open command**	Stopped	No	At platform	**No**

*Design decision: In this situation, evacuate passengers to other cars. Meanwhile, stop the train and then open doors.

Controller	Action Type	Control Action	Train Motion	Emergency	Train Position	Hazardous?
Operator	**Provides**	**Door open cmd**	Moving	No	(doesn't matter)	**Yes**
Operator	**Provides**	**Door open cmd**	Moving	Yes	(doesn't matter)	**Yes***
Operator	**Provides**	**Door open cmd**	Stopped	Yes	(doesn't matter)	No
Operator	**Provides**	**Door open cmd**	Stopped	No	Not at platform	**Yes**
Operator	**Provides**	**Door open cmd**	Stopped	No	At platform	No

Much of this can be automated!

Unsafe Control Actions
Door open command provided while train is moving and there is no emergency
Door open command provided too late while train is stopped and emergency exists
Door open command provided while train is stopped, no emergency, and not at platform
Door open command provided while train is moving and emergency exists
Door open command <u>not</u> provided while train is stopped and emergency exists
Door open command <u>not</u> provided while doors are closing on someone and train is stopped

Automating STPA

Automatically generated
(from control structure and PMVs)

Generated from
simple rules
(from engineers)

Controller	Action Type	Control Action	Train Motion	Emergency	Train Position	Hazardous?
Operator	**Provides**	**Door open command**	Moving	No	(doesn't matter)	**Yes**
Operator	**Provides**	**Door open command**	Moving	Yes	(doesn't matter)	**Yes***
Operator	**Provides**	**Door open command**	Stopped	Yes	(doesn't matter)	**No**
Operator	**Provides**	**Door open command**	Stopped	No	Not at platform	**Yes**
Operator	**Provides**	**Door open command**	Stopped	No	At platform	**No**

Detecting conflicts

- Can automatically check consistency, search for conflicts

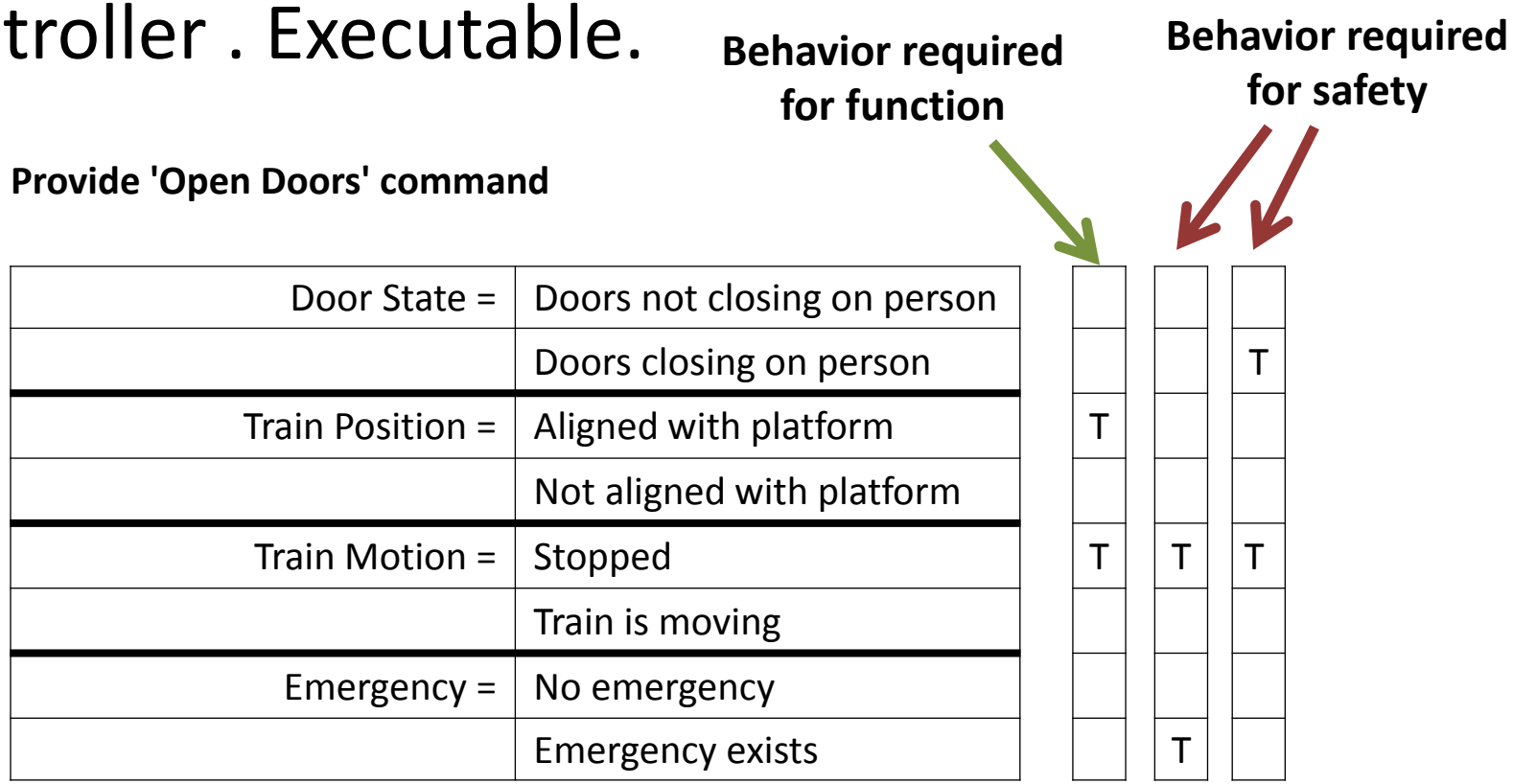
Control Action	Train Motion	Emergency	Hazardous?
Door open command	Moving	Yes	**Yes***

Control Action	Train Motion	Emergency	Hazardous?
Door open command not provided	Moving	Yes	**Yes***

- Example: Conflict between opening the door vs. not opening the door

Generating safety requirements

- Example: Generated black-box model for door controller . Executable.



Open Doors =
(Train Position in-state Aligned) ∧ (Train Motion in-state Stopped) ∨ (Train Motion in-state Stopped) ∧ (Emergency in-state exists) ∨ (Door State in-state closing on person) ∧ (Train Motion in-state Stopped)

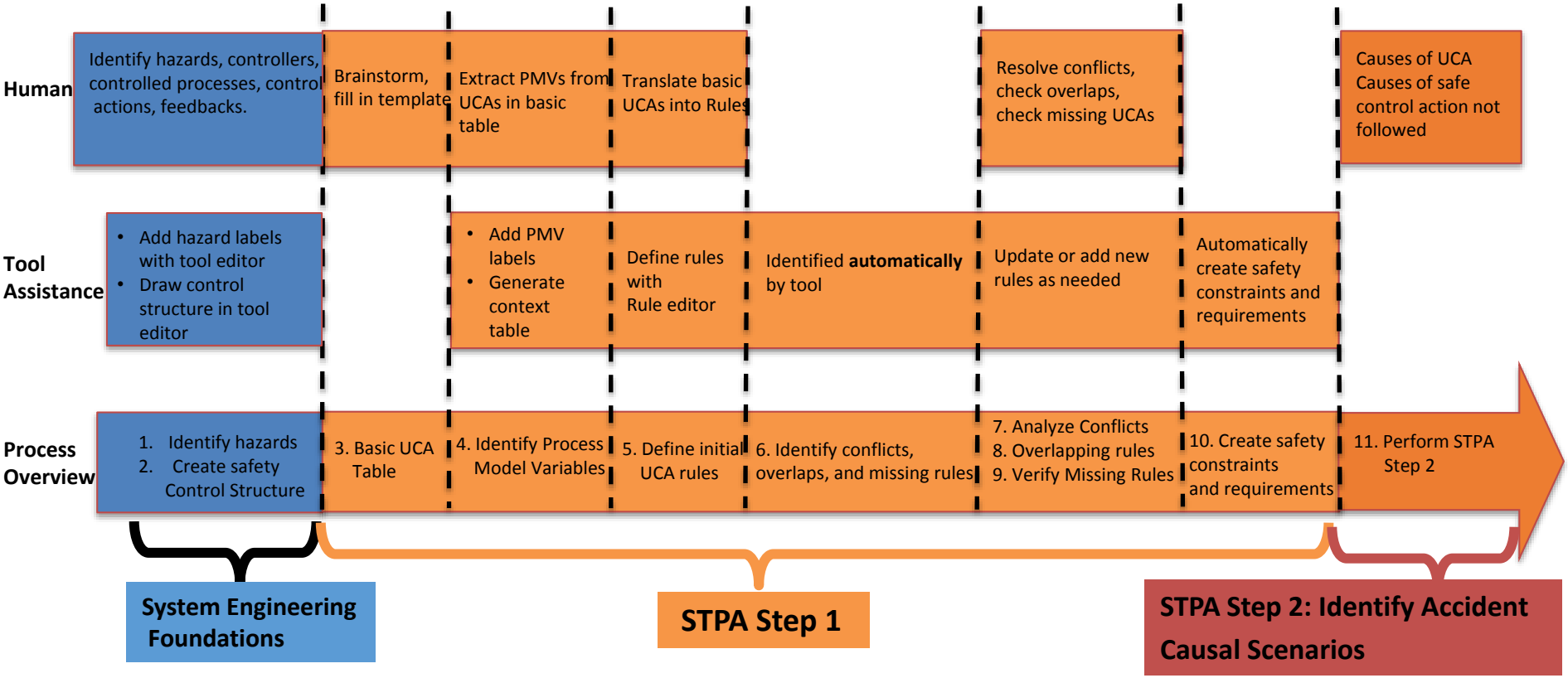
Tool-assisted Process

Tool-assisted process

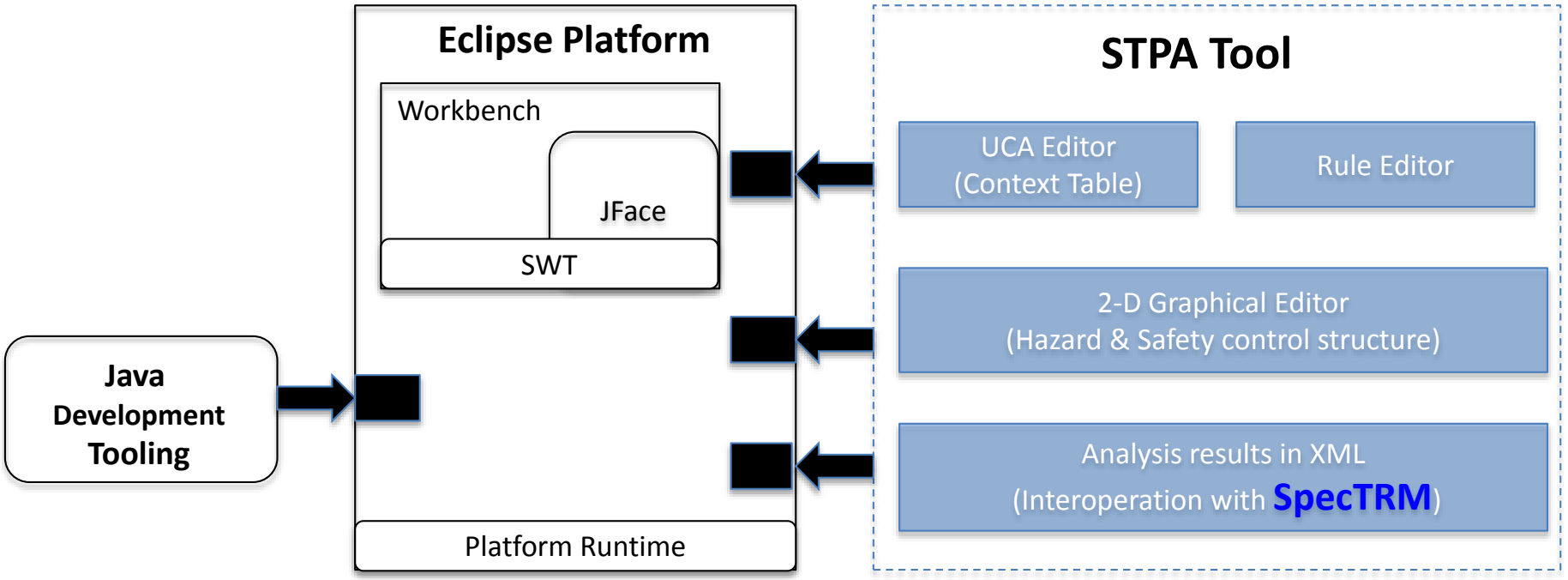
- System engineering foundation
  - Define hazards
  - Create control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios

Process Overview
1. Identify hazards
2. Create basic control structure
3. Basic UCA table
4. Identify process model variables
5. Define initial UCA rules
6. Identify conflicts, overlaps, and missing rules
7. Analyze conflicts
8. Analyze overlapping rules
9. Verify missing rules
10. Create safety constraints and requirements
11. Perform STPA Step 2

Tool-assisted process

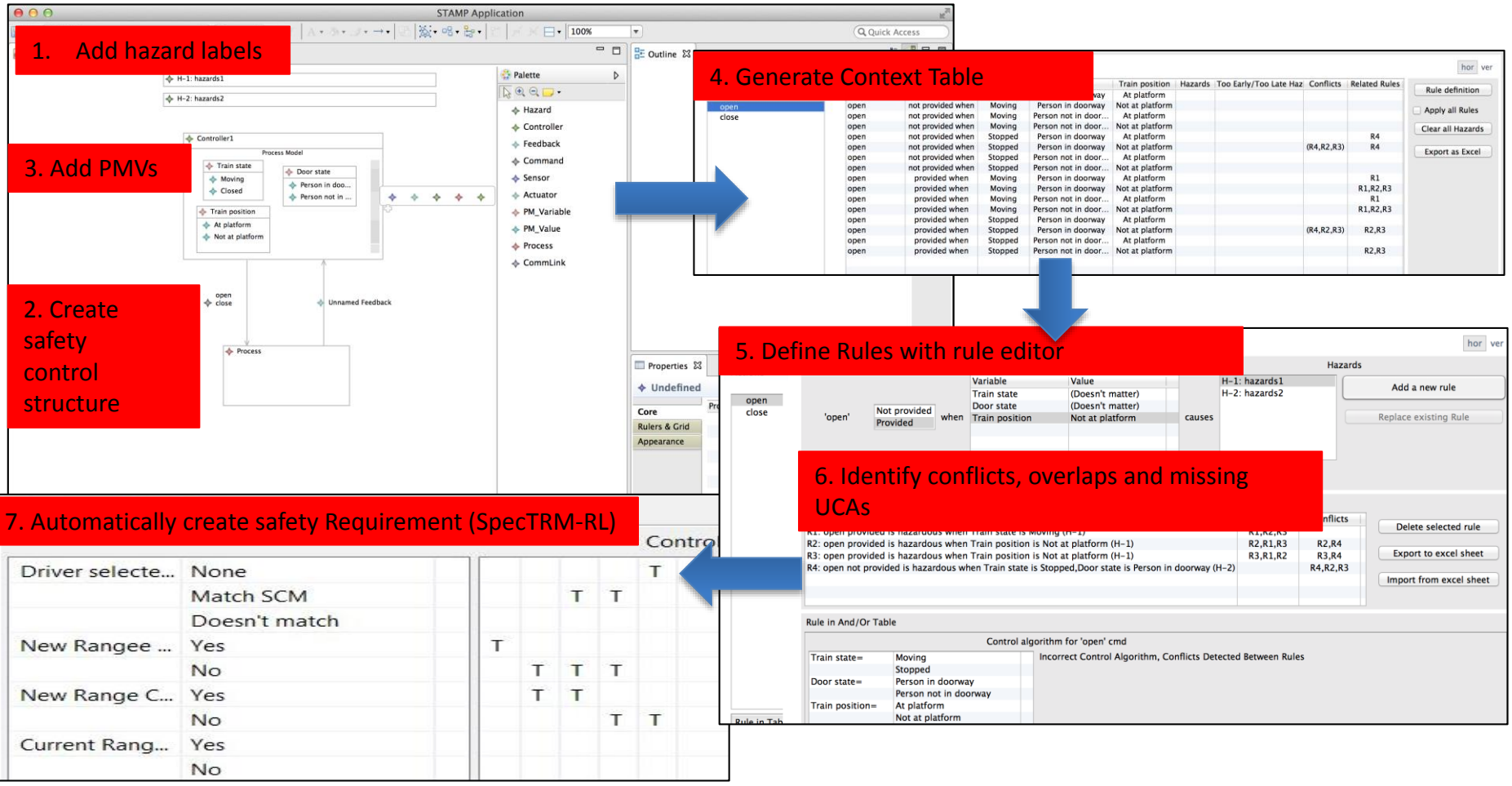


The Architecture of an STPA tool



*The architecture of Eclipse platform is taken from eclipse.org

A Toolset for Supporting STPA and Requirement Generation

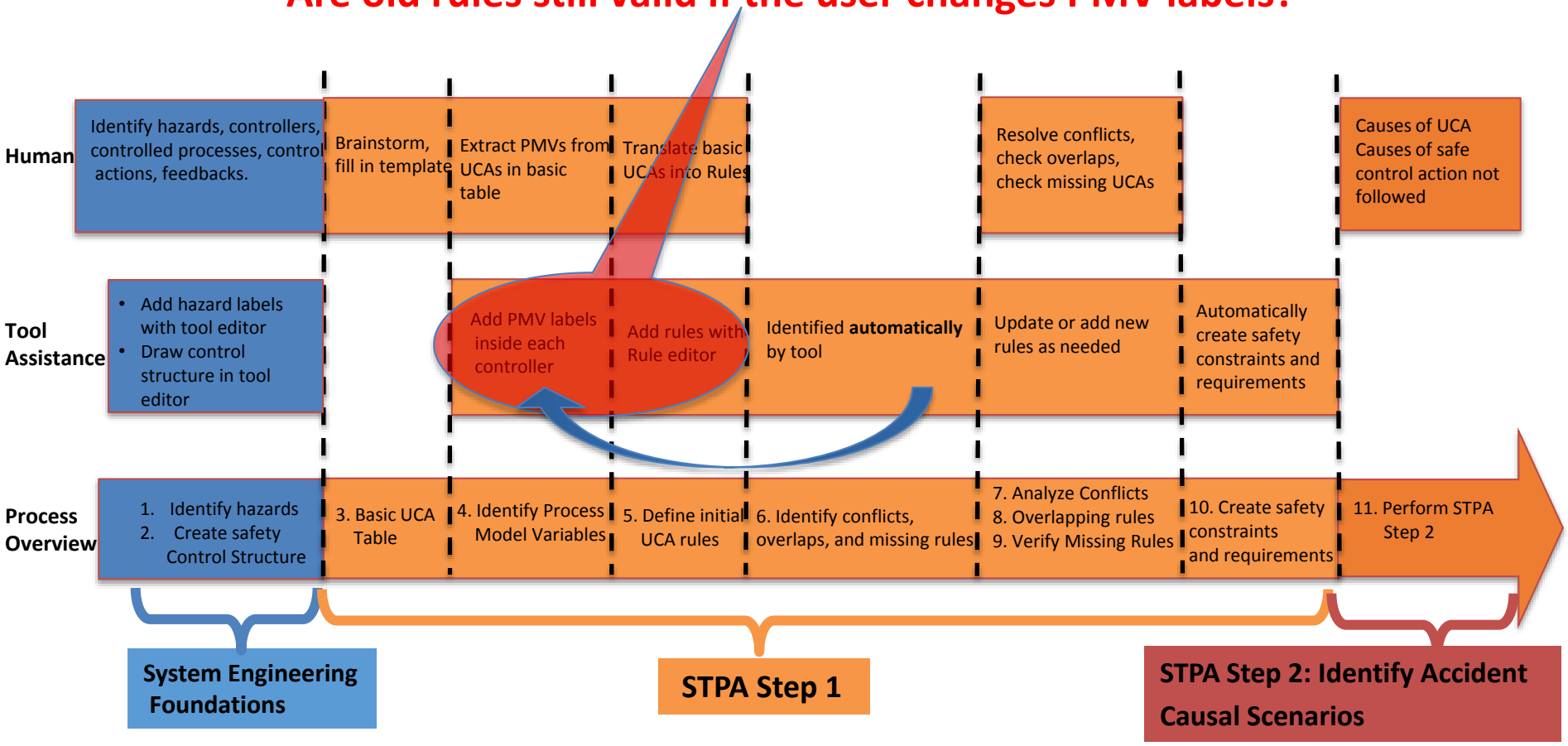


Feedback from “beta” testing

- I want to **change** the control structure in the middle of the analysis
  - Add new controller responsibility
  - Change a control action
  - Change feedback / process model variable
  - Etc.

Challenge(1):

Are old rules still valid if the user changes PMV labels?

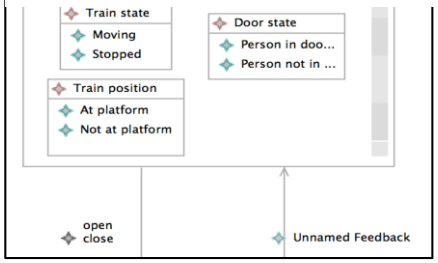


Tool Support for Modifying PMVs
Example: Add PMVs

Before Adding PMVs

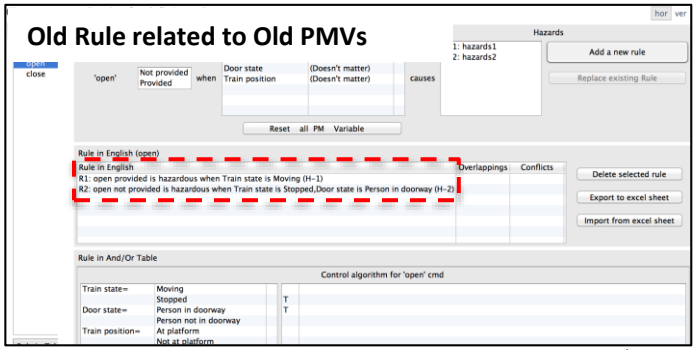
Safety Control Structure

Old PMVs and values in controller



Rule definition

Old Rule related to Old PMVs

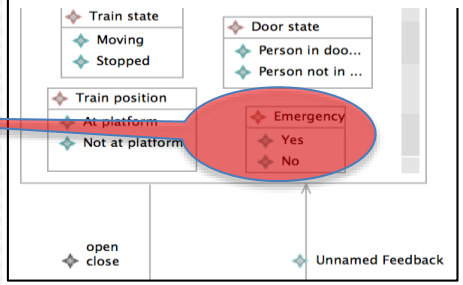


Add/delete PMVs

After Adding PMVs

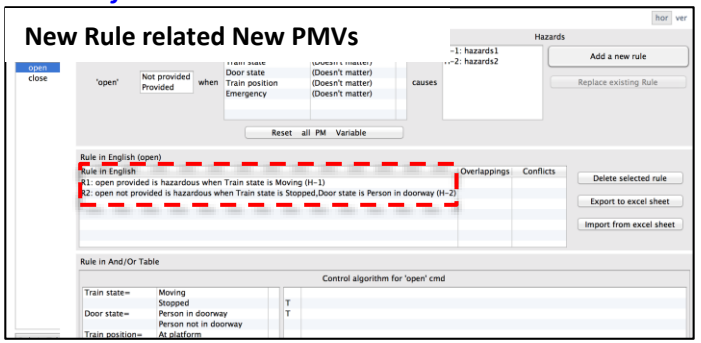
Safety Control Structure

New PMVs and values in controller

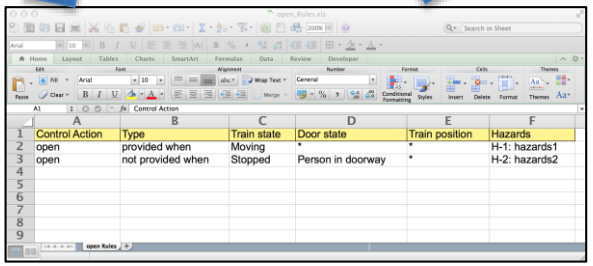


Rule definition

New Rule related New PMVs



Export Rules to external files



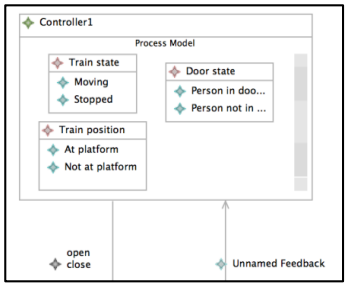
	A	B	C	D	E	F
1	Control Action	Type	Train state	Door state	Train position	Hazards
2	open	provided when	Moving	*	*	H-1: hazards1
3	open	not provided when	Stopped	Person in doorway	*	H-2: hazards2

Import Rules from external files

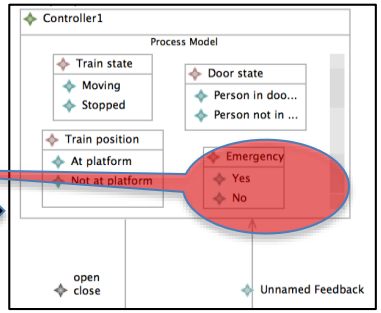
Are old rules still valid if the user changes PMV labels?
Example: Add PMVs

Before adding PMVs | ***After adding PMVs***

Safety Control Structure



Add/delete PMVs



Context Table

Control Actior	Type	Train state	Door state	Train positic	Hazards	Too Early/Too Late Hazar	Conflicts	Related Rules
open	not provided...	Moving	Person i...	At platform				
open	not provided...	Moving	Person i...	Not at pl...				
open	not provided...	Moving	Person n...	At platform				
open	not provided...	Moving	Person n...	Not at pl...				
open	not provided...	Stopped	Person i...	At platform				R2
open	not provided...	Stopped	Person i...	Not at pl...				R2
open	not provided...	Stopped	Person n...	At platform				
open	not provided...	Stopped	Person n...	Not at pl...				
open	provided when	Moving	Person i...	At platform				R1
open	provided when	Moving	Person i...	Not at pl...				R1
open	provided when	Moving	Person n...	At platform				R1
open	provided when	Moving	Person n...	Not at pl...				R1
open	provided when	Stopped	Person i...	At platform				
open	provided when	Stopped	Person i...	Not at pl...				
open	provided when	Stopped	Person n...	At platform				
open	provided when	Stopped	Person n...	Not at pl...				

Activating Table by choosing a Control Action below

Control Action List: open, close

Control Actio	Type	Train state	Door state	Train posit	Emergency	Hazards	Too Early/Too Late Haz	Conflicts	Related Rules
open	not provided...	Moving	Person i...	At platf...	Yes				
open	not provided...	Moving	Person i...	At platf...	No				
open	not provided...	Moving	Person i...	Not at...	Yes				
open	not provided...	Moving	Person i...	Not at...	No				
open	not provided...	Moving	Person...	At platf...	Yes				
open	not provided...	Moving	Person...	At platf...	No				
open	not provided...	Moving	Person...	Not at...	Yes				
open	not provided...	Moving	Person...	Not at...	No				
open	not provided...	Stopped	Person i...	At platf...	Yes				R2
open	not provided...	Stopped	Person i...	At platf...	No				R2
open	not provided...	Stopped	Person i...	Not at...	Yes				R2
open	not provided...	Stopped	Person i...	Not at...	No				R2
open	not provided...	Stopped	Person...	At platf...	Yes				
open	not provided...	Stopped	Person...	At platf...	No				
open	not provided...	Stopped	Person...	Not at...	Yes				
open	not provided...	Stopped	Person...	Not at...	No				
open	provided when	Moving	Person i...	At platf...	Yes				R1
open	provided when	Moving	Person i...	At platf...	No				R1
open	provided when	Moving	Person i...	Not at...	Yes				R1
open	provided when	Moving	Person i...	Not at...	No				R1
open	provided when	Moving	Person...	At platf...	Yes				R1
open	provided when	Moving	Person...	At platf...	No				R1
open	provided when	Moving	Person...	Not at...	Yes				R1
open	provided when	Moving	Person...	Not at...	No				R1
open	provided when	Stopped	Person i...	At platf...	Yes				
open	provided when	Stopped	Person i...	At platf...	No				
open	provided when	Stopped	Person i...	Not at...	Yes				
open	provided when	Stopped	Person i...	Not at...	No				
open	provided when	Stopped	Person...	At platf...	Yes				

Rule definition

Rule in English	Overlappings	Conflicts
R1: open provided is hazardous when Train state is Moving (H-1)		
R2: open not provided is hazardous when Train state is Stopped,Door state is Person in doorway (H-2)		

Rule in English	Overlappings	Conflicts
R1: open provided is hazardous when Train state is Moving (H-1)		R1,R2
R2: open not provided is hazardous when Door state is Person in doorway (H-1)		R2,R1

Observations:

- Contexts have been changed
- **More Rules** may become relevant
- **New Conflicts** are identified