hhu.

Validation Obligations in Practice

Fabian Vu

ABZ 2024, IVOIRE Workshop, Bergamo

2023-06-25

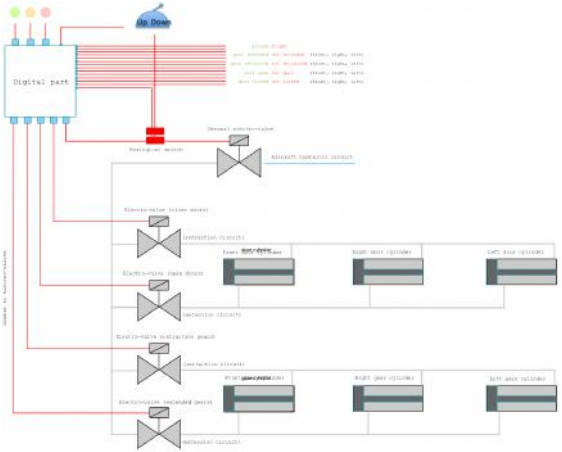
Introduction

- VOs - shall be applicable to multiple domains with different kind of systems
- VOs - should help validation process; should complement POs for verification
- How does the validation process with VOs look like?

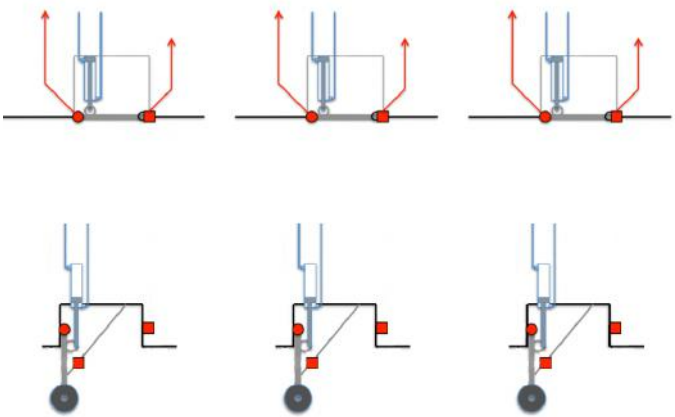
Overview: Case Studies

- Landing Gear: Aviation
- Exterior Light System: Automotive
- Arrival Manager: Aviation, GUI
- Shunting: Railway, AI
- Highway Environment: Automotive, AI

Landing Gear



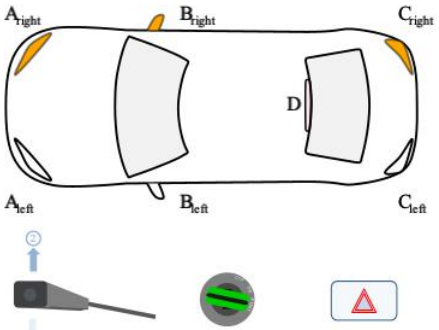
Landing Gear



Landing Gear

- Developed before VOs; VOs applied afterward
- Outgoing/Retraction Sequence: Validation by Trace Replay
- Safety Requirements (with Timing Property): Validation by (LTL) Model Checking, Simulation + Hypothesis Testing, Interactive Simulation
- Tracking Requirements, Validation Tasks, VOs, Formal Model

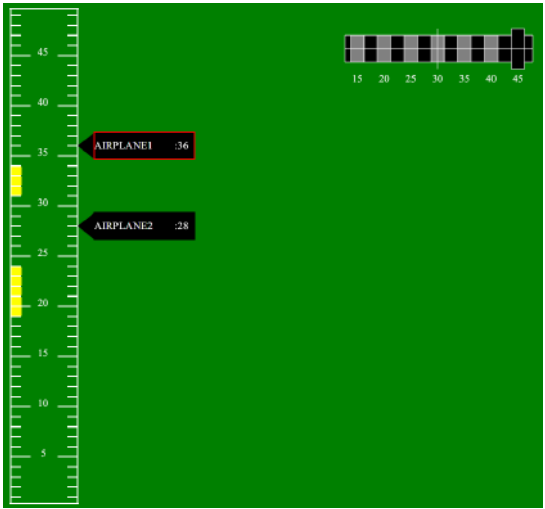
Exterior Light System



Exterior Light System

- Developed before VOs; VOs applied afterward
- Validation Sequences from Requirements Documents - Validation by Trace Replay
- Safety Properties and Deadlock-freedom - Validation by (LTL) Model Checking
- Timing Properties - Validation by (Interactive) Simulation

Arrival Manager (AMAN)



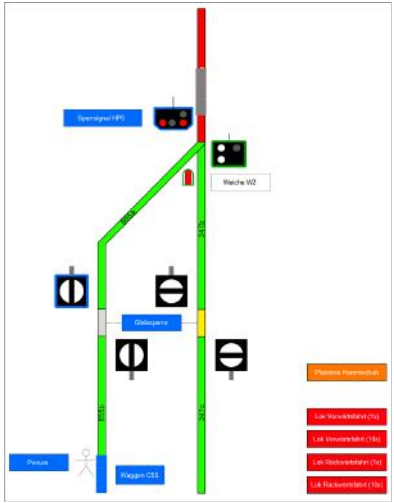
Arrival Manager (AMAN)

- Developed driven by VOs
- Developed in Event-B using Rodin
- Functional Requirements - Validation by LTL, CTL, and POs
- GUI Requirements - Validation by Inspection of Visualization, and POs
- Scenarios - Validation by Trace Replay
- Instantiation and Abstraction (+ Validation by State Space Projection) - to focus on specific properties

Arrival Manager (AMAN)

- A Priori Approach - Requirement Document $\rightarrow$ Requirement Extraction $\rightarrow$ Requirement Structure $\rightarrow$ VOs $\rightarrow$ Formal Model
- A Posteriori Approach - Requirement Document $\rightarrow$ Requirement Extraction $\rightarrow$ Requirement Structure $\rightarrow$ Formal Model $\rightarrow$ VOs

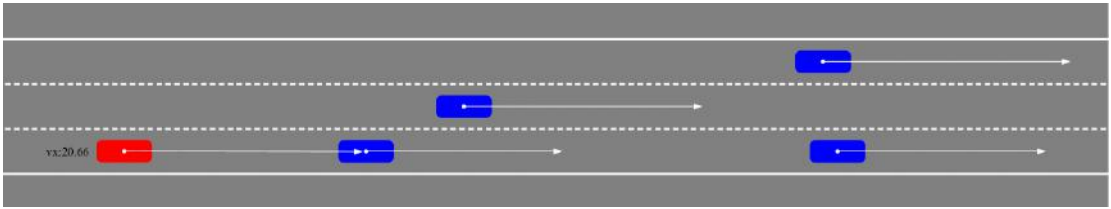
Shunting


Sperrsignal HP0
Weiche W2
Gleissperre
Gleis
Gleis
Gleis
Gleis
Prellbock
Rangier CSS

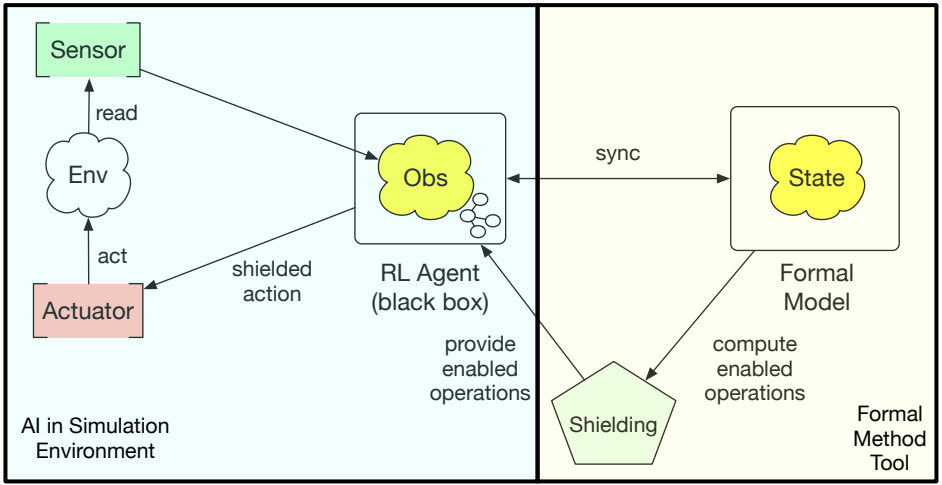
Shunting

- Developed before VOs; VOs applied afterward
- Trace Replay - evaluating different scenarios of Mission Order - including misrecognition
- LTL Model Checking
  - Assumption: AI acts perfectly
  - Train system will never reach a dangerous situation
- Simulation + Hypothesis Testing - computing likelihood of dangerous situation

Highway Environment



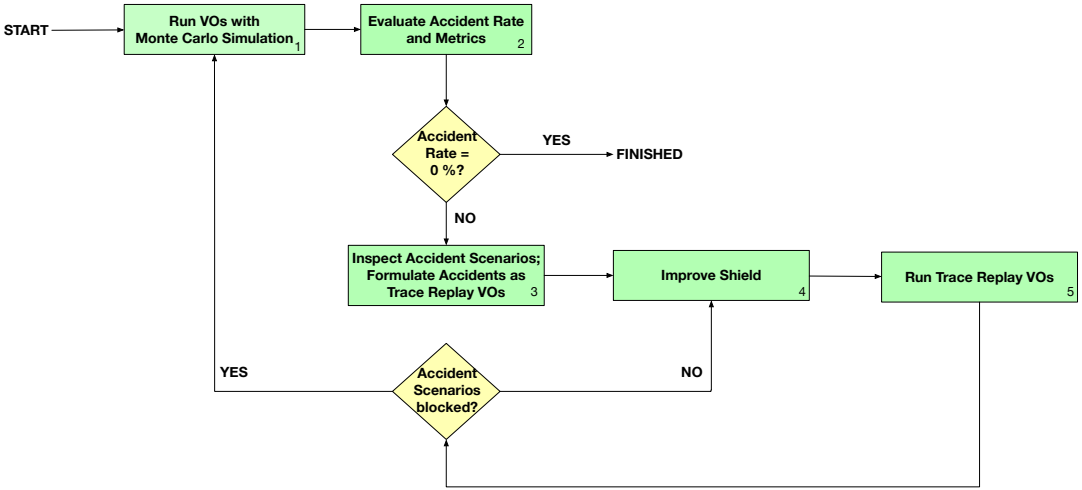
Highway Environment



Highway Environment

- Developed driven by VOs
- Simulation + Hypothesis Testing - for statistical validation of safety properties
- Trace Replay - evaluate whether improved safety shield avoids crashes

Highway Environment



Conclusion

- Successful Application of VOs to multiple domains
- Successful of VOs to GUI case study
- Successful of VOs to AI Systems
- Different Workflows with VOs
- Future Work: Runtime Verification/Validation/Monitoring

APPENDIX

Landing Gear

- *Outgoing Sequence*: The outgoing of gears is decomposed into a sequence of elementary actions. When the gears are locked in retracted position, and the doors are locked in closed position, if the pilot sets the handle to “Down”, then the software should have the following sequence of actions:
  1. stimulate the general electro-valve isolating the command unit in order to send hydraulic pressure to the maneuvering electro-valves,
  2. stimulate the door opening electro-valve,
  3. once the three doors are in the open position, stimulate the gear outgoing electro-valve,
  4. once the three gears are locked down, stop the stimulation of the gear outgoing electro-valve,
  5. ...
- Validation by 8 traces - covering different variations
  - Outgoing Sequence/LandingGear_R6: $TR_1 \wedge \ldots \wedge TR_8$

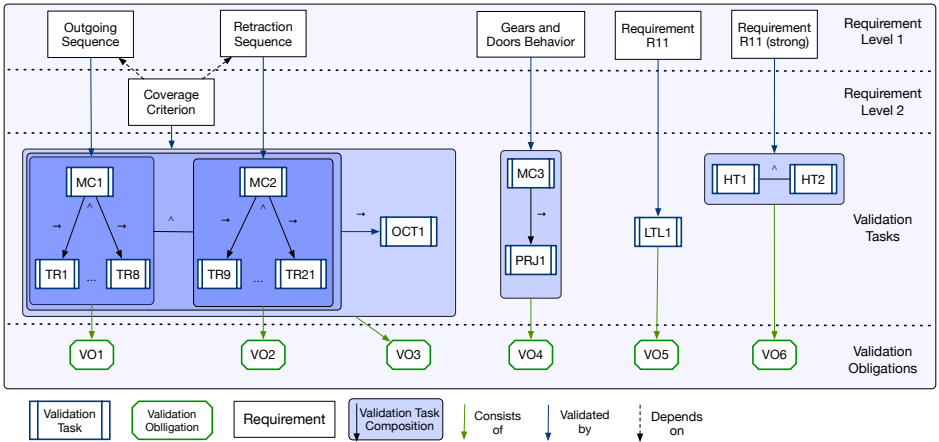
Landing Gear

- *R11*: When the command line is working (normal mode), if the landing gear command handle has been pushed DOWN and stays DOWN, then eventually the gears will be locked down and the doors will be seen closed.
- Validation by LTL Model Checking
  - R11/LandingGear_R2: G {handle=down} $\implies$ ((F {door = closed $\wedge$ gear = extended}) U {handle $\neq$ down})

Landing Gear

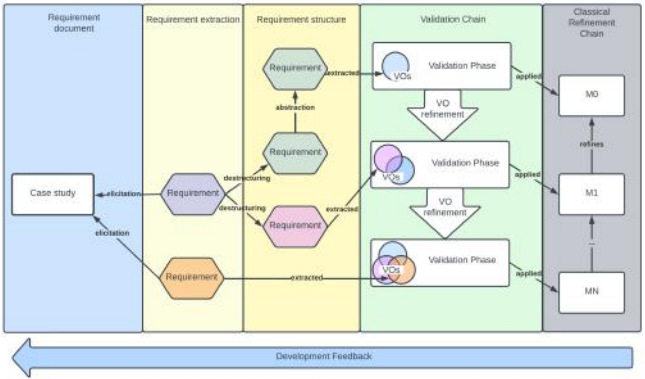
- *R11 (strong)*: When the command line is working (normal mode), if the landing gear command handle has been pushed DOWN and stays DOWN, then the gears will be locked down and the doors will be seen closed less than 15 seconds after the handle has been pushed.
- Validation by (Interactive) Simulation and Hypothesis Testing

Landing Gear



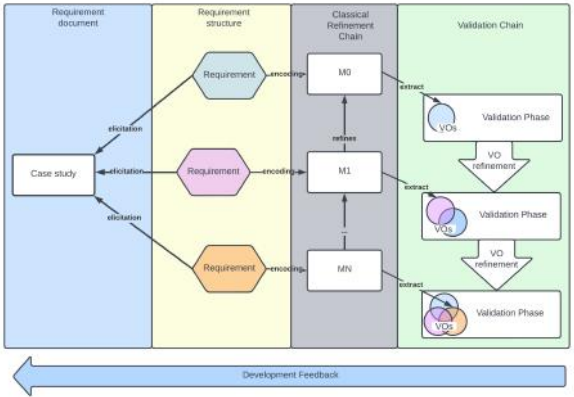
Arrival Manager (AMAN)

A Priori Validation Approach



Arrival Manager (AMAN)

A Posteriori Validation Approach



Shunting

- **Mission Order (Scenario):**
  1. Drive from the current position on track 347a to the stop signal and point
  2. Recognise stop signal and point position
  3. Enter 855a and drive to the derailer
  4. Recognise derailer
  5. Enter 855b and approach the wagon to the clutch position
  6. Recognise the person and the waggon

  Steps (2), (4) and (6) must recognise field elements or people correctly, otherwise, the Mission Order might not be achieved.
- Validation by 23 traces - covering all variations including accidents
  - Mission Order/Rangierfahrt: $TR_1 \wedge \ldots \wedge TR_{23}$

Shunting

- **SAF1-5:** When point positions, stop signals, derailers, and obstacles are recognised correctly, the train must not enter a safety-critical state (train derailing, train entering a blocked session, or collision with an obstacle).
- Validation by LTL
- Assumption: If the AI acts perfectly, the system will never reach a dangerous situation

Shunting

- **PROP1:** When driving along the route from 347a to 855b, safety-critical situations (train derailing, train entering a blocked section, collision with wagon or person) must occur less frequently with KI-LOK than with humans
- Artificial probabilities for image recognition
- Computing likelihood of accident - with those probabilities
- Validation by Simulation with Hypothesis Testing

Shunting

- **SAF1-5:** When point positions, stop signals, derailers, and obstacles are recognised correctly, the train must not enter a safety-critical state (train derailing, train entering a blocked session, or collision with an obstacle).
- Validation by LTL
- Assumption: If the AI acts perfectly, the system will never reach a dangerous situation
- SAF1-5/Rangierfahrt: LTL(

  G({“train moves forwards” ⇒

  Y (“control unit updates decision to move train forwards” ∧

  “train detected all signals correctly” ∧

  “train detected points correctly” ∧

  “train detected obstacles correctly” ∧

  “train detected track correctly”})

  ⇒ G({“train does not reach safety-critical situation”})

Shunting

- **PROP1:** When driving along the route from 347a to 855b, safety-critical situations (train derailing, train entering a blocked section, collision with wagon or person) must occur less frequently with KI-LOK than with humans
- Validation by Simulation: SIM(

SIM(ending: “train reaches the end of 855b” $\vee$
“train reaches the end of 347c” $\vee$
“train reaches a safety-critical situation”
prop: “train never reaches a safety-critical situation”
check: HYPOTHESIS
procedure: LEFT_TAILED
probability: 0.999
α: 0.001)