OVADO
Enhancing Data Validation for Safety-Critical Railway Systems

RATP – Software Assessment (RATP/ING/STF/QS/AQL)

Manel FREDJ, Sven Leger, Abderrahmane Feliachi and Julien Ordioni

November 15th, 2017

Pistoia, Italy
RATP – Software Safety Assessment

- **AQL: RATP SW safety assessment lab**
  - Internal assessment of safety critical software
  - Data validation

- **CBTC configuration data**
  - Line configuration and all objects on this line

---

Nov. 15th, RSSRail 2017, Pistoia, Italy
Agenda

What is OVADO?
- The tool
- Data validation process

Use cases
- Concrete cases: Metro line CBTC
- Emerging needs?

Enhancing data validation process
- Genericity
- B-OVADO editor
- Guidelines

Conclusion & future work

Nov. 15th, RSSRail 2017, Pistoia, Italy
What is OVADO?

http://www.ovado.net/fr/index.html

T2 for SIL 4 certified version (EN 50128:2011)

Generic & Extensible

Use of formal methods

Counter-examples

Safety-critical data validation

IDE properties

Nov. 15th, RSSRail 2017, Pistoia, Italy
Which purpose?

- Supplier
  - System data
  - Generation Process
  - Software data
  - B Predicates
  - Ovado
  - OK / KO

Provided by RATP and the supplier

RATP

INDEPENDENT ASSESSMENT OF SAFETY CRITICAL DATA

SUPPLIER PROCESS

Nov. 15th, RSSRail 2017, Pistoia, Italy
Usage scenarios

1. System data validation
2. Data transformation validation
3. Software data validation
System data validation

- Safety requirements extracted from system specification

- **Input**
  - System data specification
  - Supplier system data (DB)

- **B Predicate**
  - Safety constraints related to system data

- **Examples**
  - Segment length
  - Beacon spacing
System data validation - Examples

- Segment = virtual part of the track
- The length of a track segment must be less than 2047 m,
- Number of bits allocated in the exchange message is 12

- The distance between two beacons must be more than 3 m
Data transformation validation

Conformity of software data with regard to system data

- **Input**
  - Specification of system data
  - Specification of software data
  - System data
  - Software data

- **B Predicate**
  - Transformation of software data with respect to system data
  - Matching between Supplier and RATP results of transformation

- **Example**
  For a specific equipment
  For a virtual sub-block of the track
  → Compute all the track circuits associated
From the specification of invariants

- We compute the attribute of the invariant CV (virtual canton) – sub-block of the track circuit CDV

- The relation defines the set of couples CV-> CDV

- Matching
  - OVADO computed invariants may have not the same order as the supplier
Software data validation

Safety requirements extracted from software

- **Input**
  - Specification of software data
  - Software data

- **B Predicate**
  - Constraints resulting from safety analysis or emerging from the software assessment activity

- **Example**
  - Number of segments under the train
CHECK THE CORRECT DIMENSIONING OF A SW CONSTANT

Is the “maximum number of segments under a train” constant big enough for my line CBTC?
Constant = 2 for instance.

1. Write a relation $R$ which associates all 2 possible neighbouring segments and their additional length
   $R = \{$
   $\{S1, S2\} \mapsto 123456,$
   $\{S2, S3\} \mapsto 326548,$
   etc.
   $\}$

2. Write a property to check if longest train length is always lower than the combination of all 2 neighbouring segments length

3. Evaluate property
   **OK**: Property verified for all combinations of the CBTC data.
   **NOK**: all improper combinations of the CBTC data will be shown

\[
R = \text{UNION} \ (S1,S2, L1,L2).(
S1 : E\_Segments
&
S1 \mapsto S2 : K\_segment\_K_neighbour\_downstream
&
S1 \mapsto L1 : K\_segment\_U\_longueur
&
S2 \mapsto L2 : K\_segment\_U\_longueur
| \n\{ \{ S1,S2 \} \mapsto L1 + L2 \}
)
\]

\[
\text{PROPERTY} = ! ( S, L ).( S \mapsto L : R \Rightarrow L\_max\_train\_length < L )
\]
Gain in data validation process

Data preparation for providing OVADO inputs

Definitions and properties in B-OVADO - constraints

Properties assessment via OVADO

Result processing

Counter-examples

- Example: 3 Types of change in the specification of system data
  - Constraints 
  - Data base structure
  - Values in Data base (instance)
USE CASES
OVADO use cases

- Data validation for CBTC
  - SAET L1
  - OCTYS L3, L5 & L9
  - OURAGAN L13

- Tools migration:
  - SAET L14 (in progress)
  - SACEM RER A (in progress)
System data validation in L5

Place d’Italie – L5

From track layout to usable data (Supplier+ RATP)
Example of system data

- **System data format**
  - Tables & lists can be easily converted into mathematical objects

- **Functions & relations can be created with all data columns**

<table>
<thead>
<tr>
<th>switch_name</th>
<th>seg_toe</th>
<th>seg_l_point</th>
<th>seg_r_point</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWITCH_PLIT_1</td>
<td>S2234</td>
<td>S2236</td>
<td>S2235</td>
</tr>
<tr>
<td>SWITCH_EGPA_2</td>
<td>S0202</td>
<td>S0204</td>
<td>S0206</td>
</tr>
<tr>
<td>SWITCH_EGPA_1</td>
<td>S0204</td>
<td>S0205</td>
<td>S0203</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Function:**
```plaintext
I_switch_name = {
    1 ↦ SWITCH_PLIT_1
    2 ↦ SWITCH_EGPA_2
    3 ↦ SWITCH_EGPA_3
    ...
}
```

**Relations:**
```plaintext
K_switch_name__K_seg = {
    SWITCH_PLIT_1 ↦ S2234
    SWITCH_PLIT_1 ↦ S2235
    SWITCH_EGPA_2 ↦ S0202
    ...
    SWITCH_EGPA_2 ↦ S0202
    ...
}
```
Example of data transformation

- Compute the attribute of the invariant CV
- The relation defines the set of couple CV-> CDV
Example of software data

- Software data accepted format
  - Ada
  - Text
  - Binaries
  - XML
  - Excel
  - Etc.

- Example
  - The invariant CV has a list of CDV (at most 2)

INV.CV.LISTE_CDV : constant T_INV.CV.LISTE_CDV := T_INV.CV.LISTE_CDV
  5=> -- ident CV
    ( 1=> 1,  -- ident CDV
      OTHERS => 0),
  6=>
    ( 1=> 2,
      2=> 3,
      OTHERS=> 0),
  7=>
    ( 1=> 4,
      OTHERS=> 0),
  ...
  OTHERS=>
    (OTHERS=> 0)
Emerging new needs

ENHANCING DATA VALIDATION PROCESS

Genericity  Editor  Guidelines
In railways (CBTC), project-related data are similar

- Sharing elementary primitives
- Definition of RATP Model

Primitives data base + configuration management

- Migration is performed for existing projects
- Easy to use, well-documented and more safe for new projects
Common concepts - abstraction
- Oriented segment
- Canonical oriented abscissa
- Zone = area ...

Definitions: Reusable *basic definitions* of data generic concepts
- Area computing
- Object abscissa on segments
- Paths computing
- Neighborly object relations, Etc.

Gain
- Properties optimization
- Change management duration

New data table: 8 hours for L 13 before common library
New data table: 2 min for L 5, L9
Common library - use example

\[
\text{UNION} ( \text{k_bal} , \text{k_seg} , \text{u_abs} , \text{e_dir} , \text{bals} ). \\
\qquad \text{k_bal} \mapsto ( \text{k_seg} \mapsto \text{u_abs}) : \text{K_bal\_\_K_seg\_\_U_abs} \\
\quad \& \\
\quad \text{e_dir} : \text{E_dir} \\
\quad \& \\
\quad \text{bals} = \\
\quad \text{UNION} ( \sigma , x , y , k , z ). \\
\qquad \sigma \mapsto ( x \mapsto y ) : \text{zone_depuis_limite} ( \text{k_seg} \mapsto \text{e_dir} \mapsto \text{u_abs} \mapsto 3000 ) \\
\quad \& \\
\quad \text{k} \mapsto ( \sigma \mapsto z ) : \text{K_bal\_\_K_seg\_\_U_abs} \\
\quad \& \\
\quad \text{z} : x .. y \\
\quad | \\
\quad \{ k \} \\
\quad ) \\
\quad \& \\
\quad \text{not(} \\
\quad \text{bals} \leftarrow \{ \text{k_bal} \} \\
\quad ) \\
\quad | \\
\quad \{ \text{bals} \leftarrow K_bal\_\_K_seg\_\_U_abs \} \\
\quad )
\]
Genericity - Benefits

Lifecycle of OVADO Projects & effort sharing

1. L1 wayside, software data validation

2. L3 & L5 wayside, definitions and properties export

3. L5 on-board, adaptation of definitions and properties

4. Completing all projects on-board and wayside for L1, L3, L5 & L9 with the same initial definition set
- Syntactic check (key words)
- Semantic check (typing, scoping)
- Documentation
- Auto-completion
- Navigation
- Seamless integration to OVADO
B-OVADO - Rich integrated editor 2/2

File Edit Navigate Search Project Run Window Help

Package Explorer test.bovado test001.bovado *test.bovado

/**
 * @author: aukeki
 * @fr: Description Français
 * @en: Description English
 */

Definition def13 U(x,y) { (x, y) }

Open Generated File
- Quick Outline
- Open With
- Show In
- Cut
- Copy
- Copy Qualified Name
- Paste
- Rename Element
- Validate
- Quick Fix
- Source
- Find References
- Add to Snippets...
- Problems
- Errors (20 errors, 0 warnings)

Toggle Word Wrap

Source Location Type

master branch

def13:
	<unnamed>
	<unnamed>

Nov. 15th, RSSRail 2017, Pistoia, Italy
Guidelines

- Formatting rules
  - Naming conventions
  - Indentation
  - Structure, etc.

- Example

  - Easy: communication, sharing, reuse
  - Applied on common library
Metrics

- **Properties number (#P)**
  
  \#P = from 150 to 200

- **Sanity check properties are generated automatically**
  
  - Ex: Data base consistency
  - Ex: the object provided as a facing point of a switch is a segment

- **Number of data uploaded**
  
  - Between 30 000 and **100 000**
  - Ex: Around 30 Mo for system data

- **Execution time**
  
  From **few seconds or minutes** to 2-3 hours (max)

- **Assessment non-regression of a new version**
  
  - **Approximatively 1 month for a complete project** (system data, data transformation, and software data for the whole line equipments)

→ **OVADO**, used for all assessments of AQL
CONCLUSION
Conclusion

- OVADO for safety-critical data validation
  - System data
  - Software data

- OVADO is generic and mature industrial solution
  - usable for almost all RATP CBTC data assessment projects
  - and more…

- Enhancing data validation process
  - Genericity with the common library: easy reuse, reduce time to market
  - B-OVADO rich integrated editor
  - Guidelines: improve readability, sharing, cross reading, etc.
Looking Forward

- Extend OVADO usage to
  - Interlocking systems assessment
  - Ex: Internal validation of PHPI (Poste Hybride à Procédé Informatique)

- Extend the tool with
  - New project-specific plugins
  - Ex: integrate new data format as railML

- Enhance the functionalities provided by B-OVADO editor
  - Richer typing: semantic type control
  - Ex: Type « CDV » instead of « String »
Manel FREDJ

RATP

56, rue Roger Salengro
94 724 Fontenay-Sous-Bois

Phone: +33 1 587 79132
Email: manel.fredj@ratp.fr