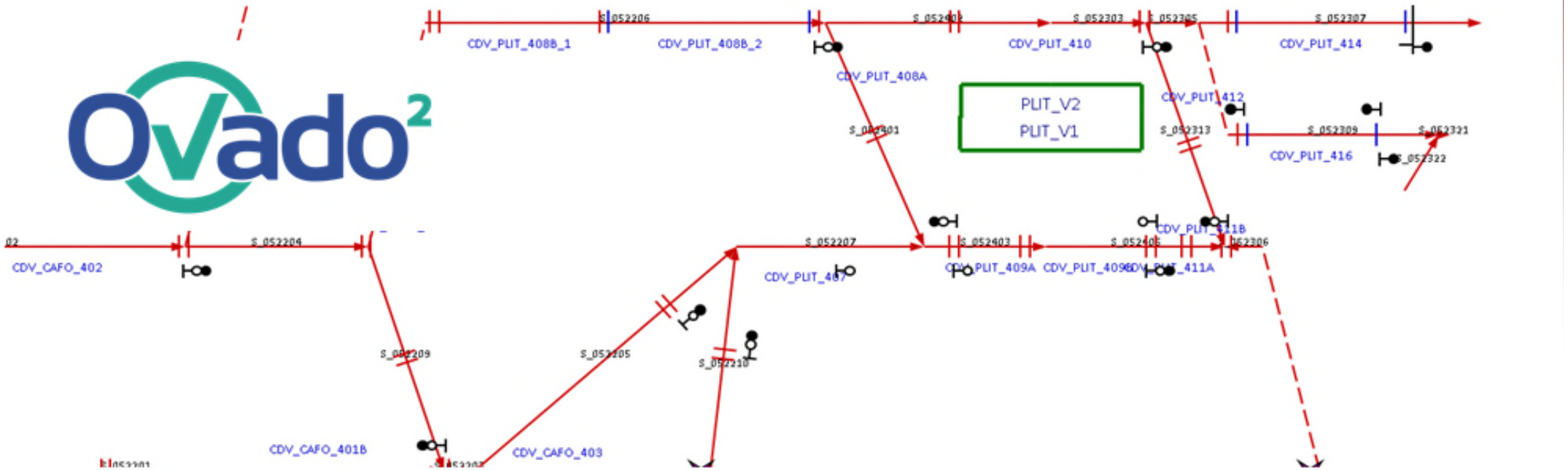
OVADO
Enhancing Data Validation for Safety-Critical Railway Systems

Pistoia, Italy

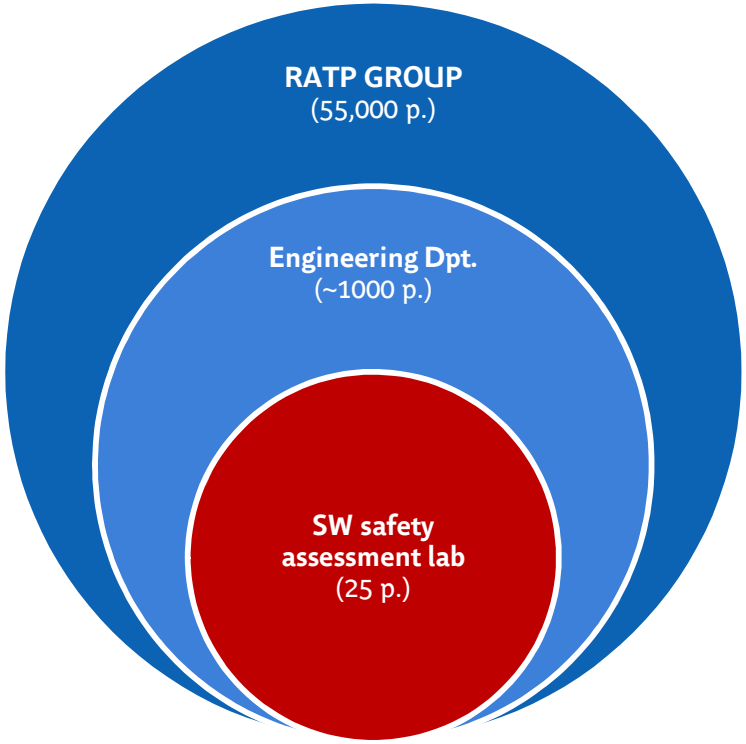
RATP – Software Assessment (RATP/ ING/STF/QS/AQL) **RSSRail 2017**

Manel FREDJ, Sven Leger, Abderrahmane Feliachi and Julien Ordioni **November 15th, 2017**



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



Agenda

What is OVADO?

- The tool
- Data validation process

Use cases

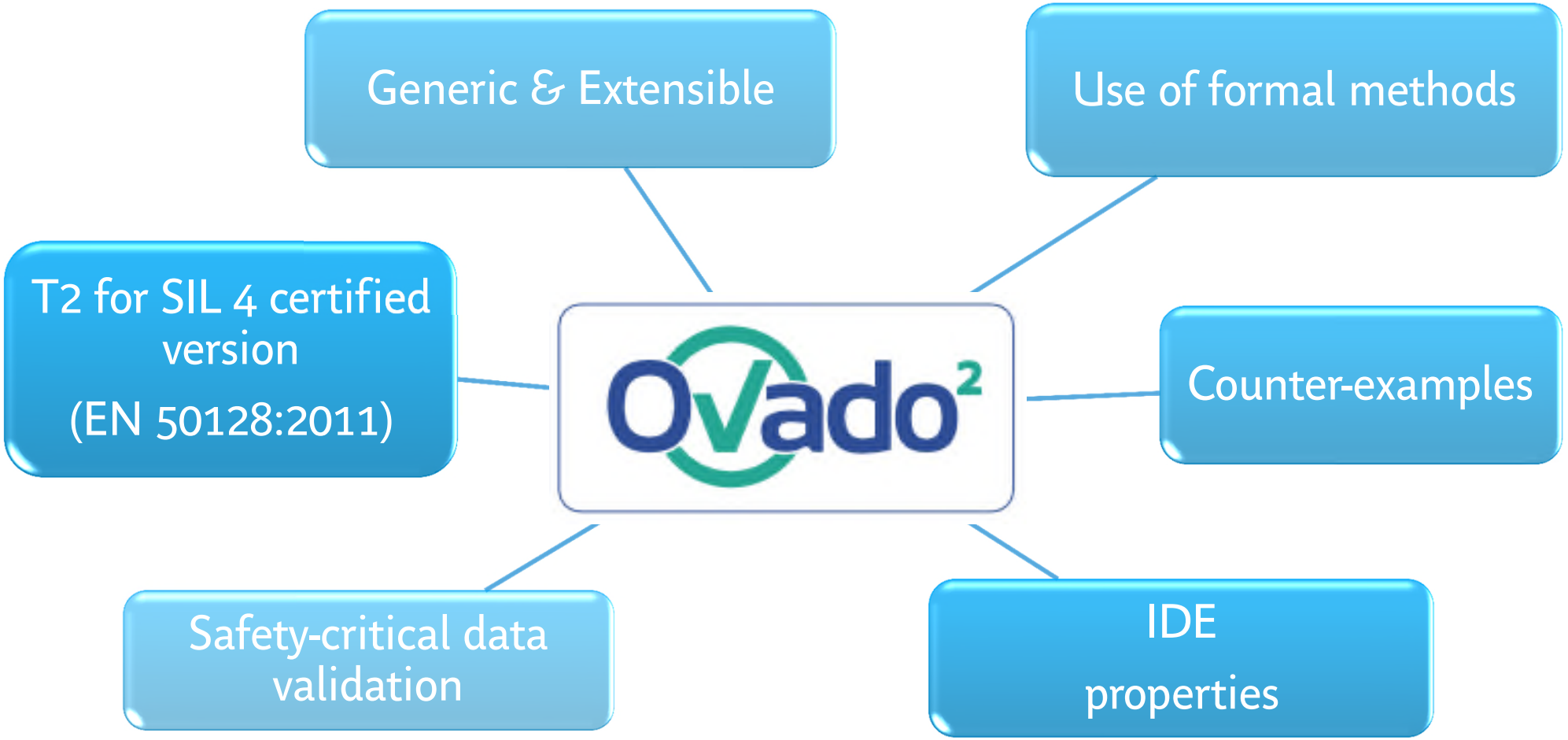
- Concrete cases : Metro line CBTC
- Emerging needs?

Enhancing data validation process

- Genericity
- B-OVADO editor
- Guidelines

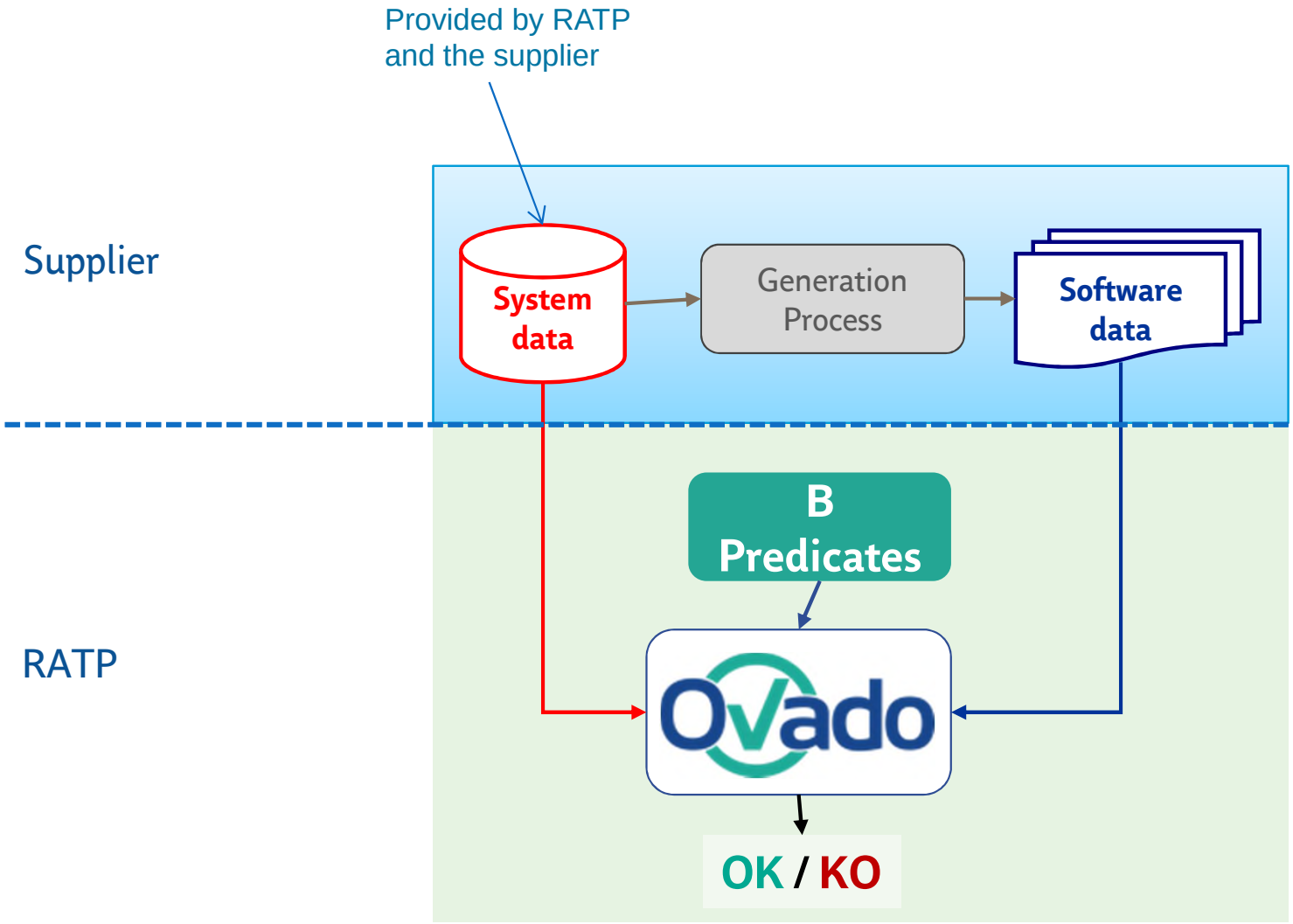
Conclusion & future work

What is OVADO?



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

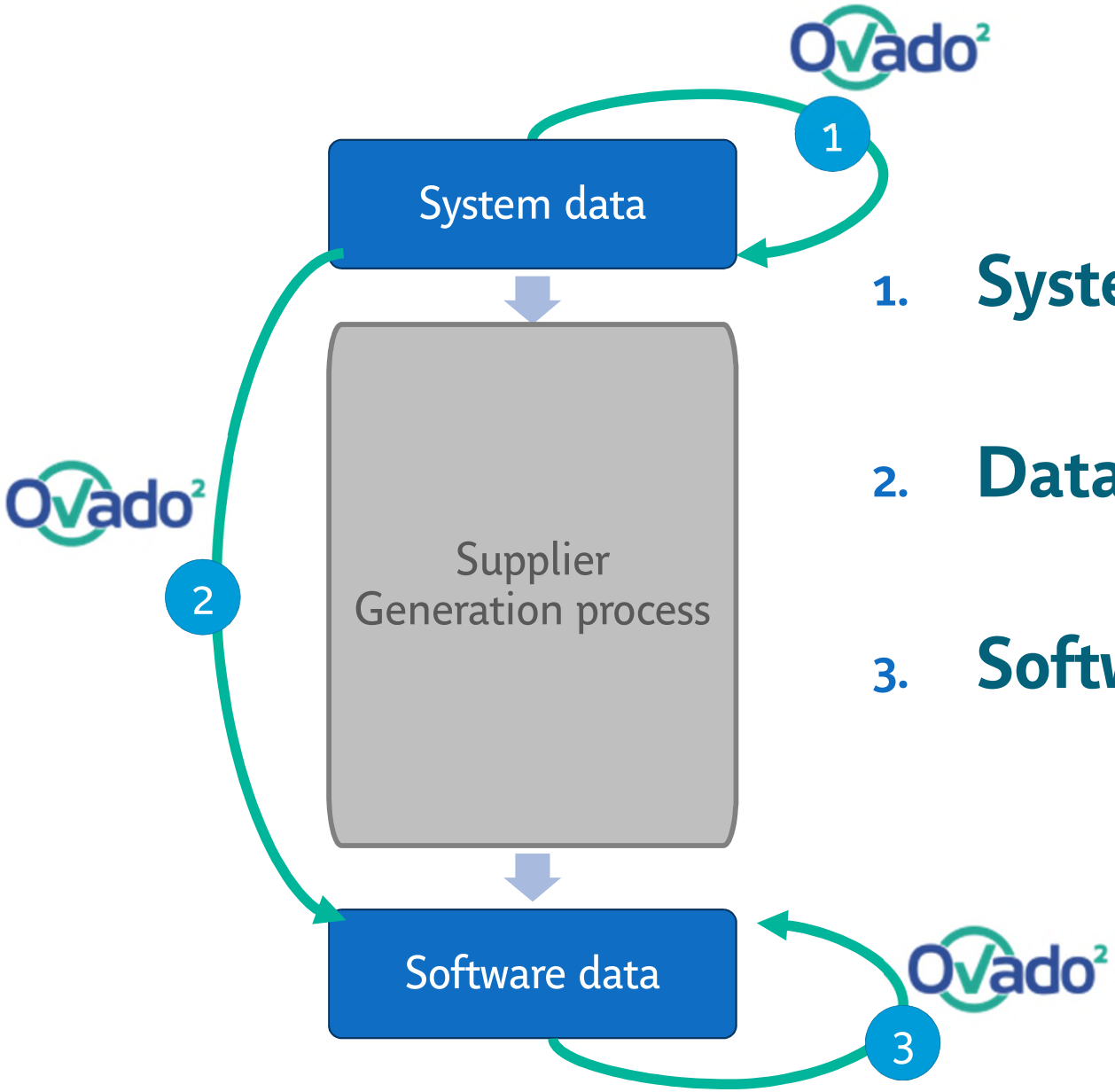
Which purpose?



SUPPLIER PROCESS

INDEPENDENT ASSESSMENT OF SAFETY CRITICAL DATA

Usage scenarios



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

1 System data validation

- Safety requirements extracted from system specification

Input

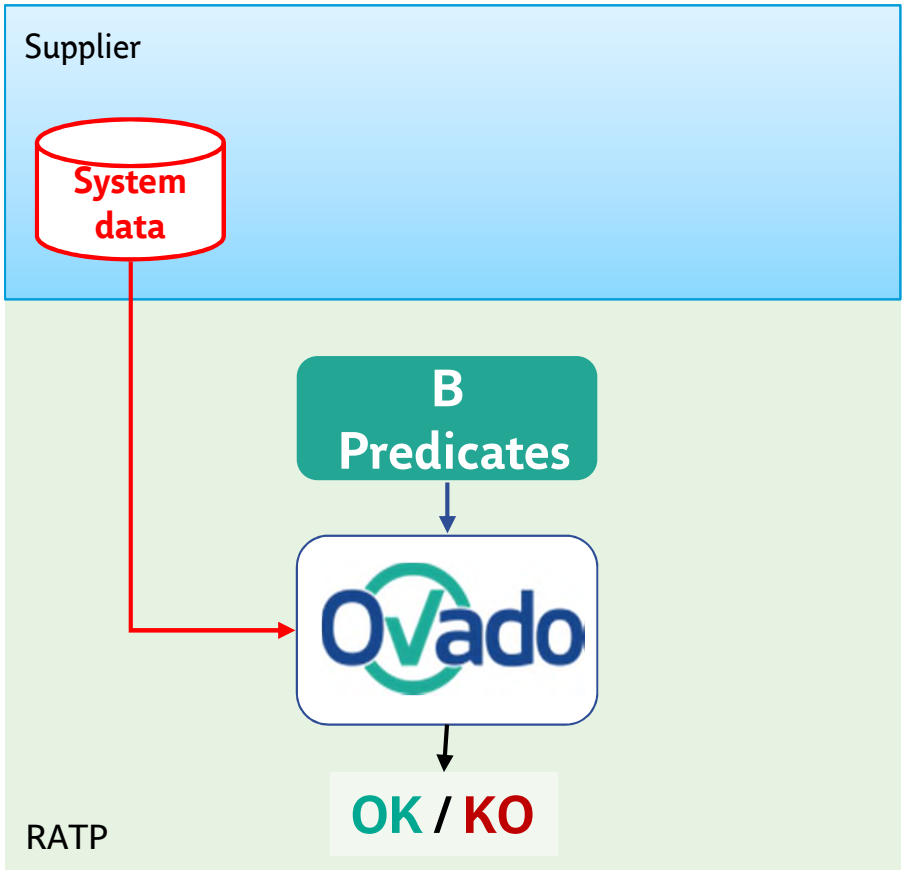
- System data specification
- Supplier system data (DB)

B Predicate

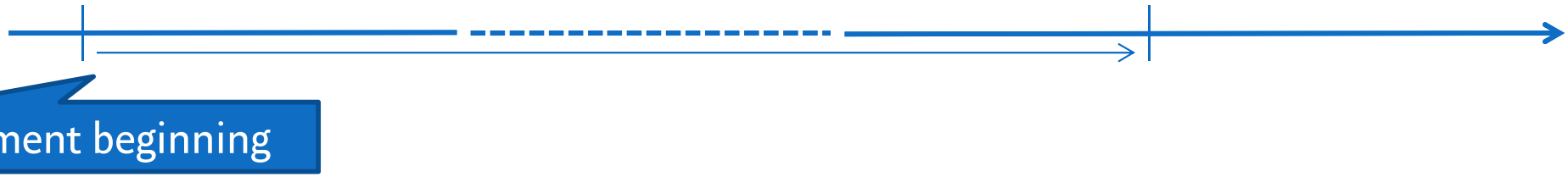
- Safety constraints related to system data

Examples

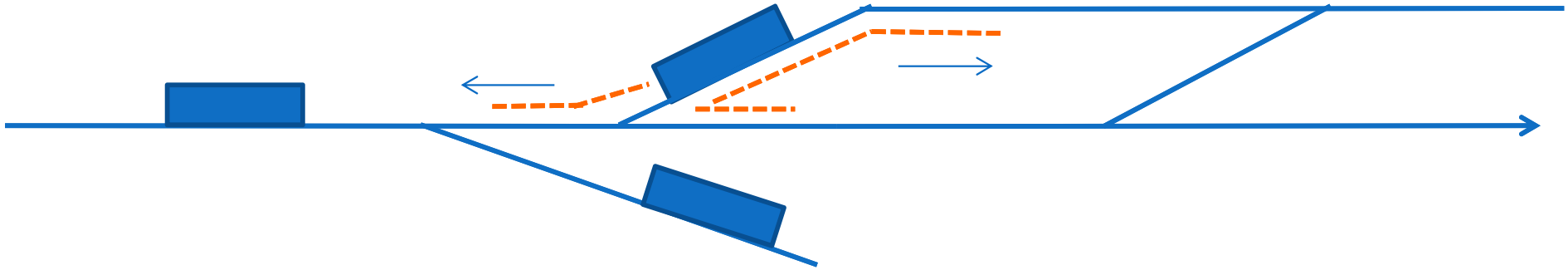
- Segment length
- Beacon spacing



1 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

2 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

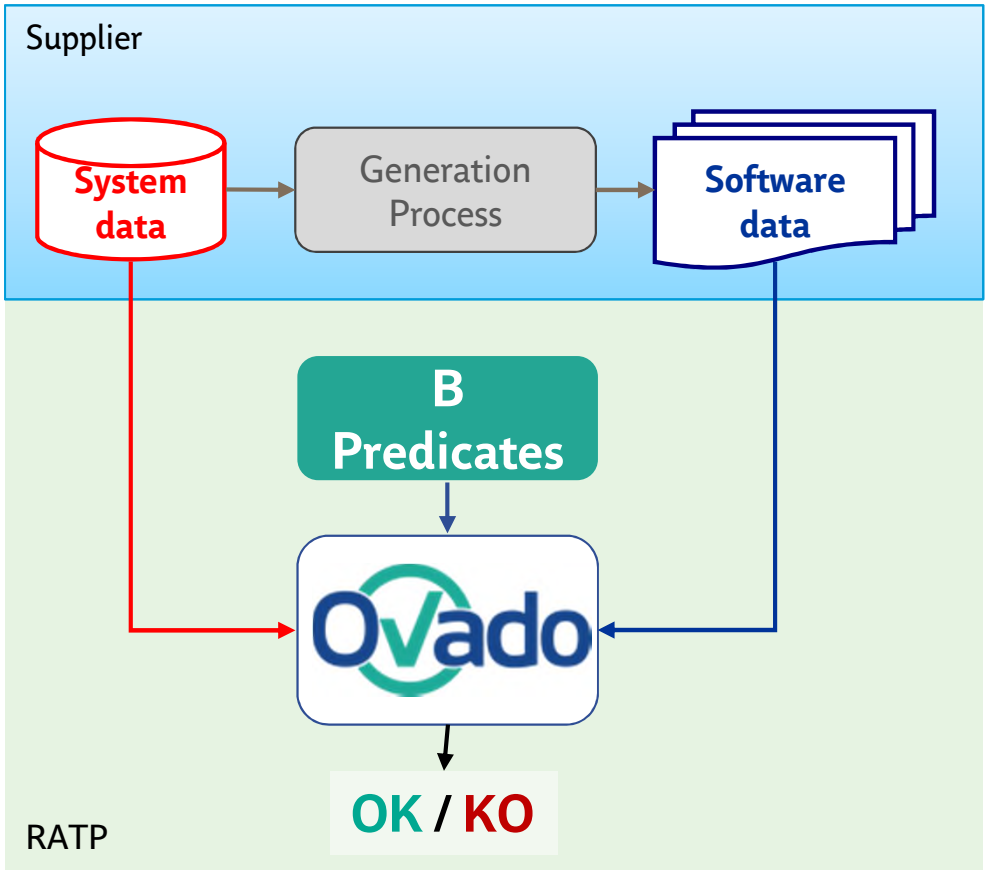
- Transformation of software data with respect to system data
- Matching between Supplier and RATP results of transformation

Example

For a specific equipment

For a virtual sub-block of the track

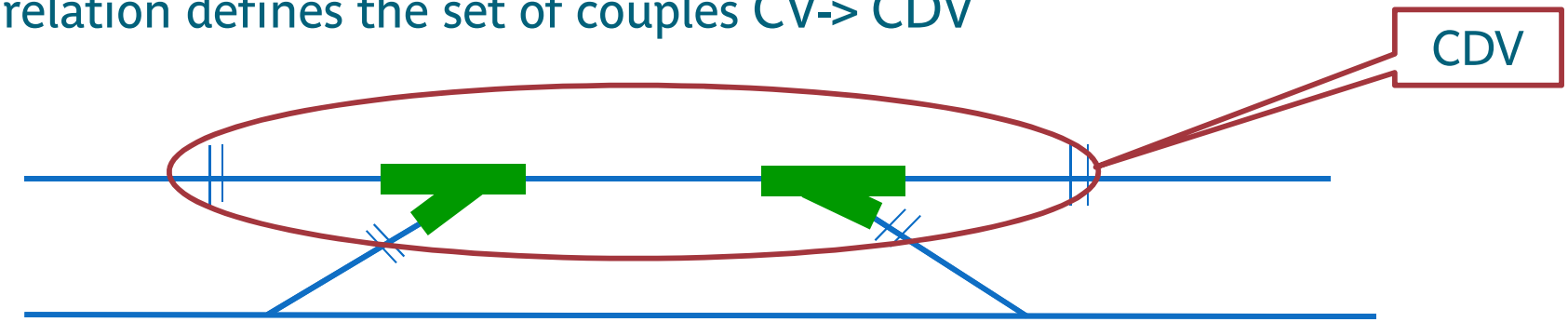
→ Compute all the track circuits associated



2 Data transformation validation - Example

- 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

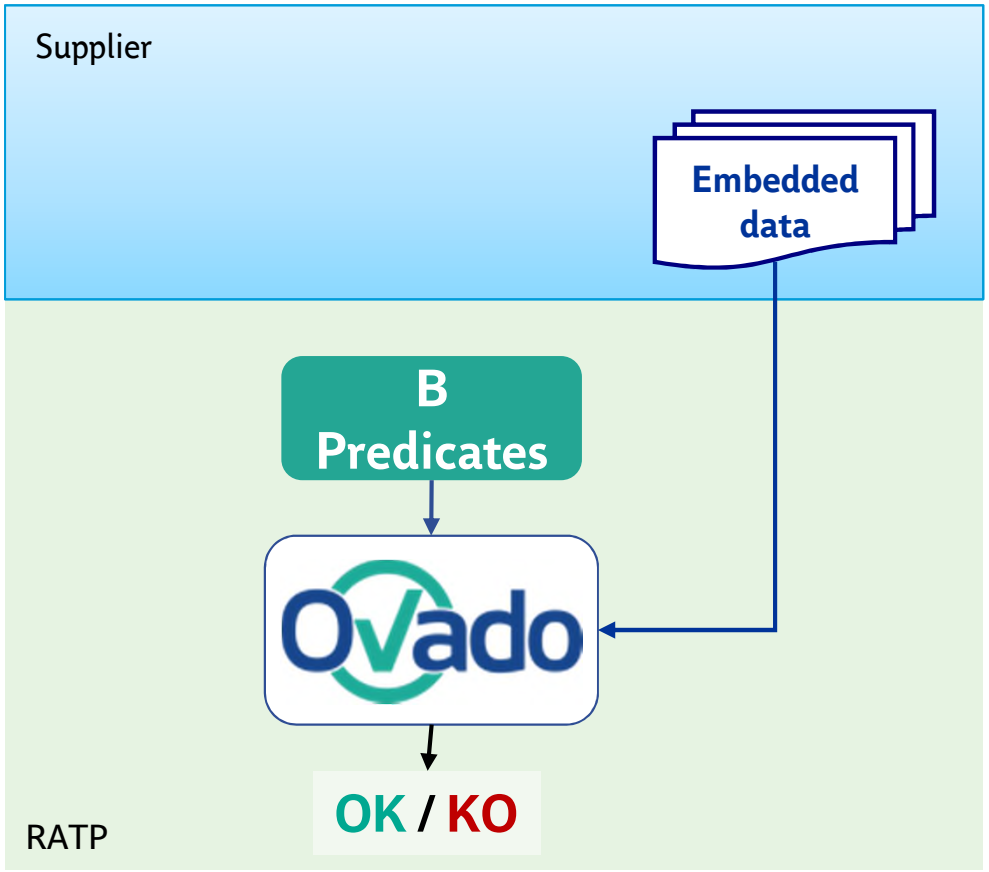
3 Software data validation

- 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

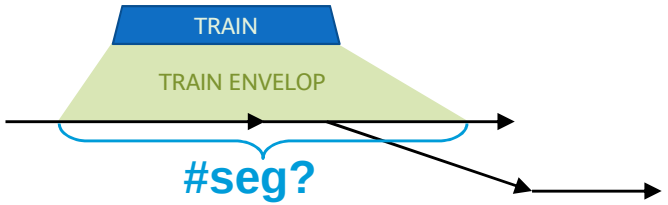
- **Example**
  - Number of segments under the train



3 Software data validation - Example

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} ↦ 123456,
{S2, S3} ↦ 326548,
etc.
}

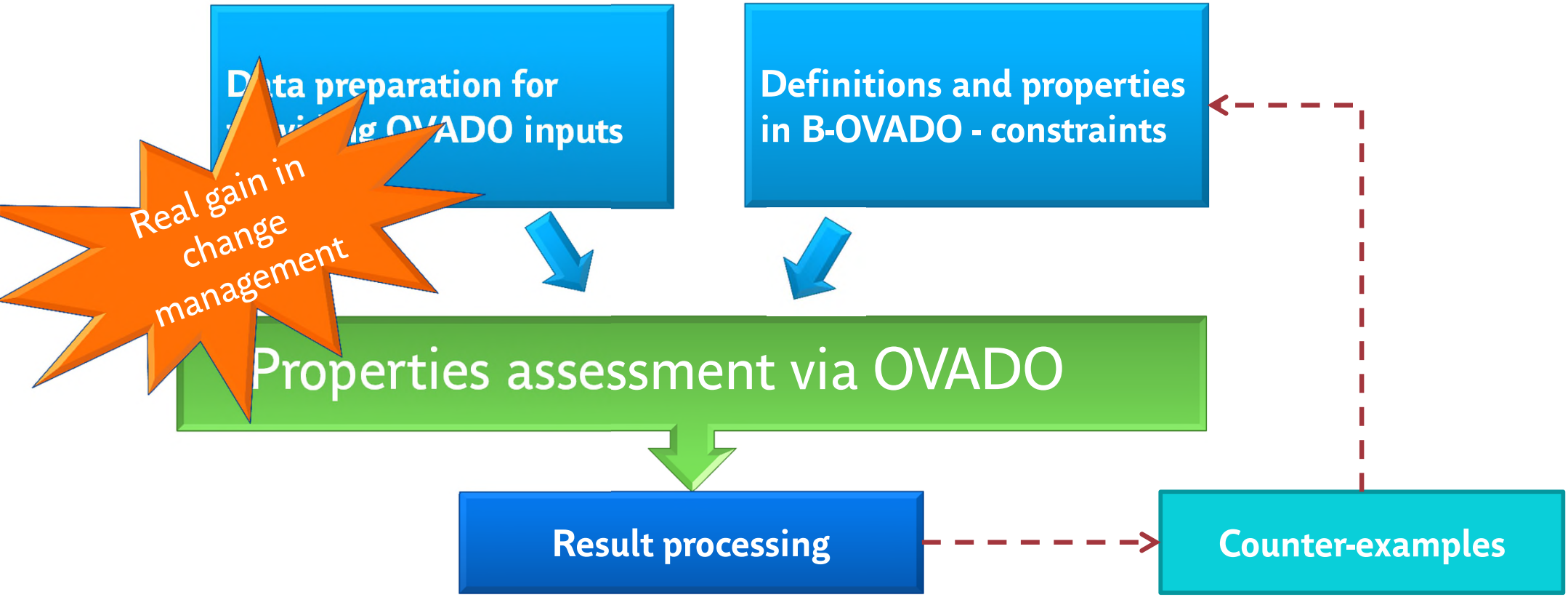
2. Write a property to check if *longest train length is always lower than the combination of all 2 neighbouring segments length*

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 = UNION  (S1,S2, L1,L2).(
                S1 : E_Segments
                &
                S1 ↦ S2 : K_segment__K_neighbour_downstream
                &
                S1↦ L1 : K_segment__U_longueur
                &
                S2 ↦ L2 : K_segment__U_longueur
                |
                { { S1,S2 } ↦ L1 + L2 }
)

PROPERTY = ! ( S, L ).( S ↦  L : R => L_max_train_lenght < L )
```

Gain in data validation process

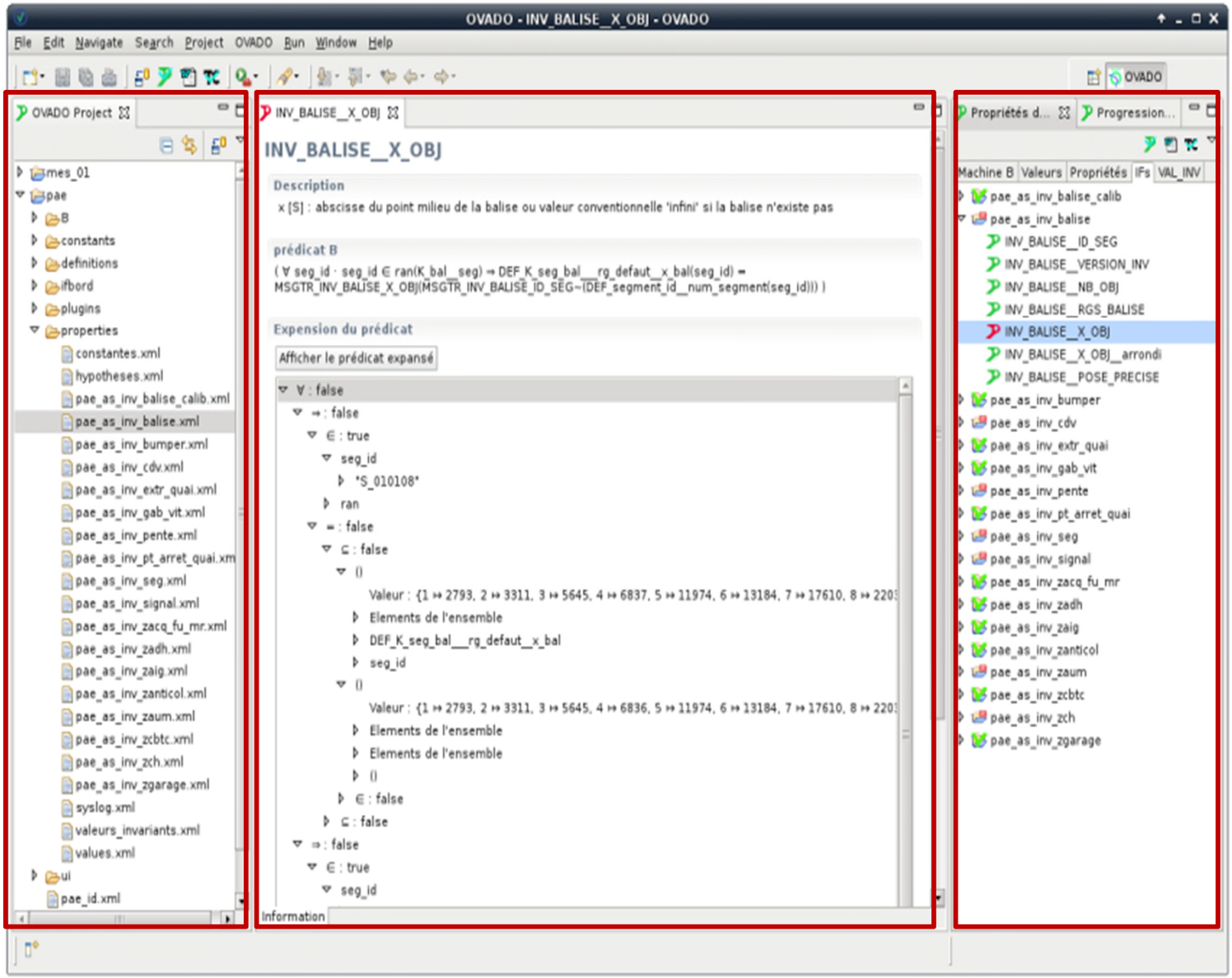


- Example : 3 Types of change in the specification of system data
  - Constraints - -
  - Data base structure + -
  - Values in Data base (instance) + +

OVADO screenshot

Property details + counter-examples

Project tree



List of properties

USE CASES

M 1 3 5 9 13 14

RER A

OVADO use cases

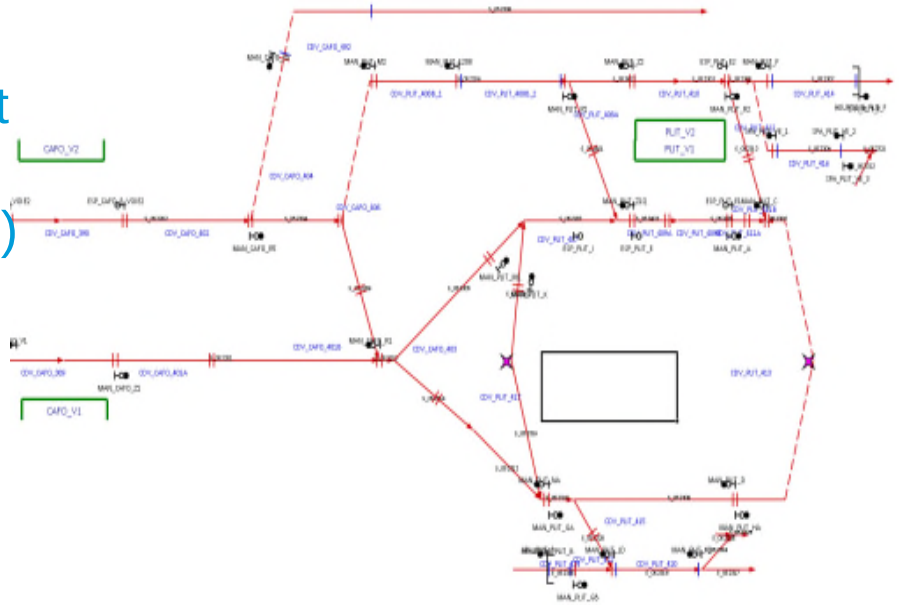
- Data validation for CBTC
  - SAET L1
  - OCTYS L3, L5 & L9
  - OURAGAN L13

➢ 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

switch_name	seg_toe	seg_l_point	seg_r_point
SWITCH_PLIT_1	S2234	S2236	S2235
SWITCH_EGPA_2	S0202	S0204	S0206
SWITCH_EGPA_1	S0204	S0205	S0203
…			

Function:
l_switch_name =
{
  1 ↦ SWITCH_PLIT_1
  2 ↦ SWITCH_EGPA_2
  3 ↦ SWITCH_EGPA_3
  …
}

Relations:
K_switch_name__K_seg =
{
  SWITCH_PLIT_1 ↦ S2234
  SWITCH_PLIT_1 ↦ S2235
  SWITCH_PLIT_1 ↦ S2236
  SWITCH_EGPA_2 ↦ S0202
  …
}

- Functions & relations can be created with all data columns

Example of data transformation

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

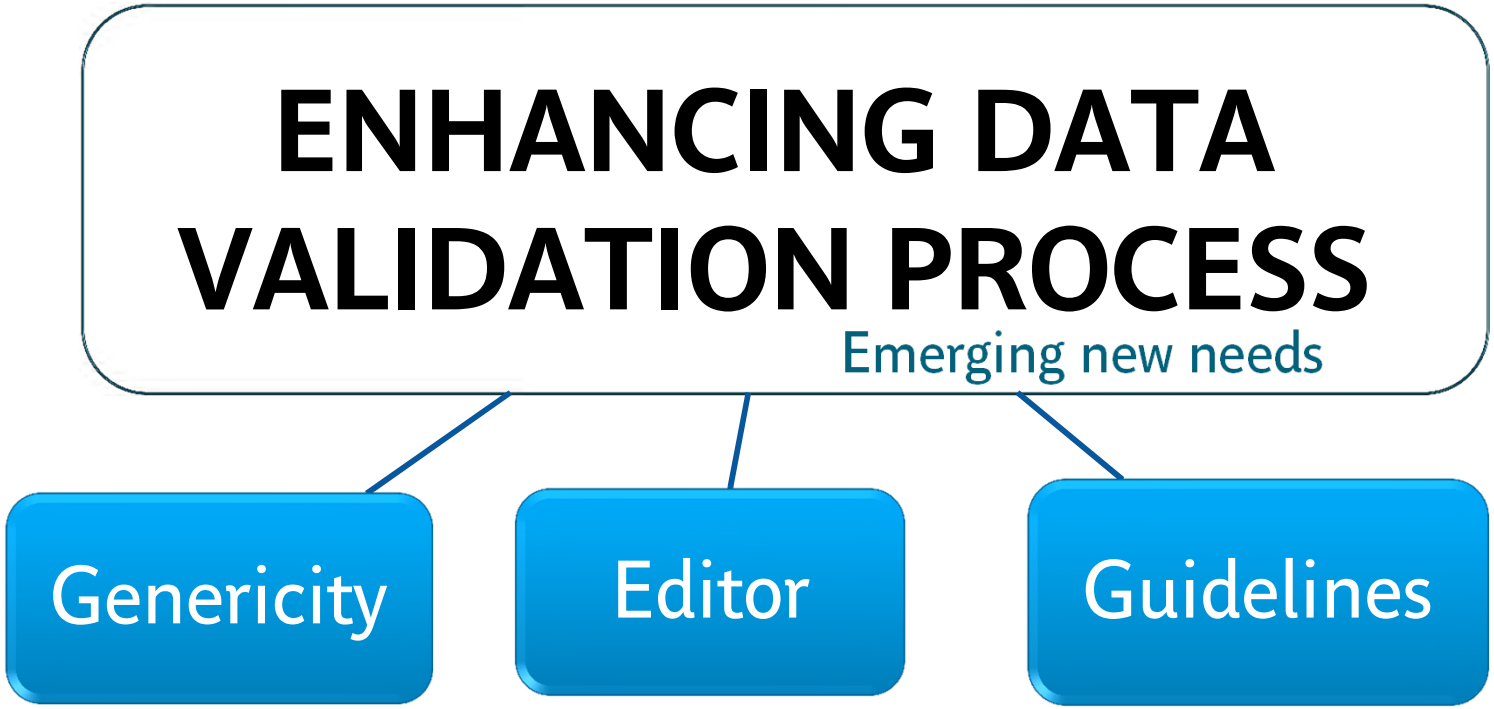
```
/**
 *@Auteur: RATP
 *@English: INV_CV.CDV : ( cv |-> cdv ) couples in intersection.
 */
Definition INV_CV__CDV {
    {
        cv |-> cdv
    |
        cv : K_cv
    &
        cdv : K_cdv
    &
        #(zone).(
                zone = intersection( K_cv__zone[{cv}] |-> K_cdv__zone[{cdv}] )
            &
                not( zone = {} )
        )
    }
}
```

Example of software data

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

```
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)
    )
```

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


ENHANCING DATA VALIDATION PROCESS
Emerging new needs
Genericity
Editor
Guidelines

Genericity - Common library 1/2

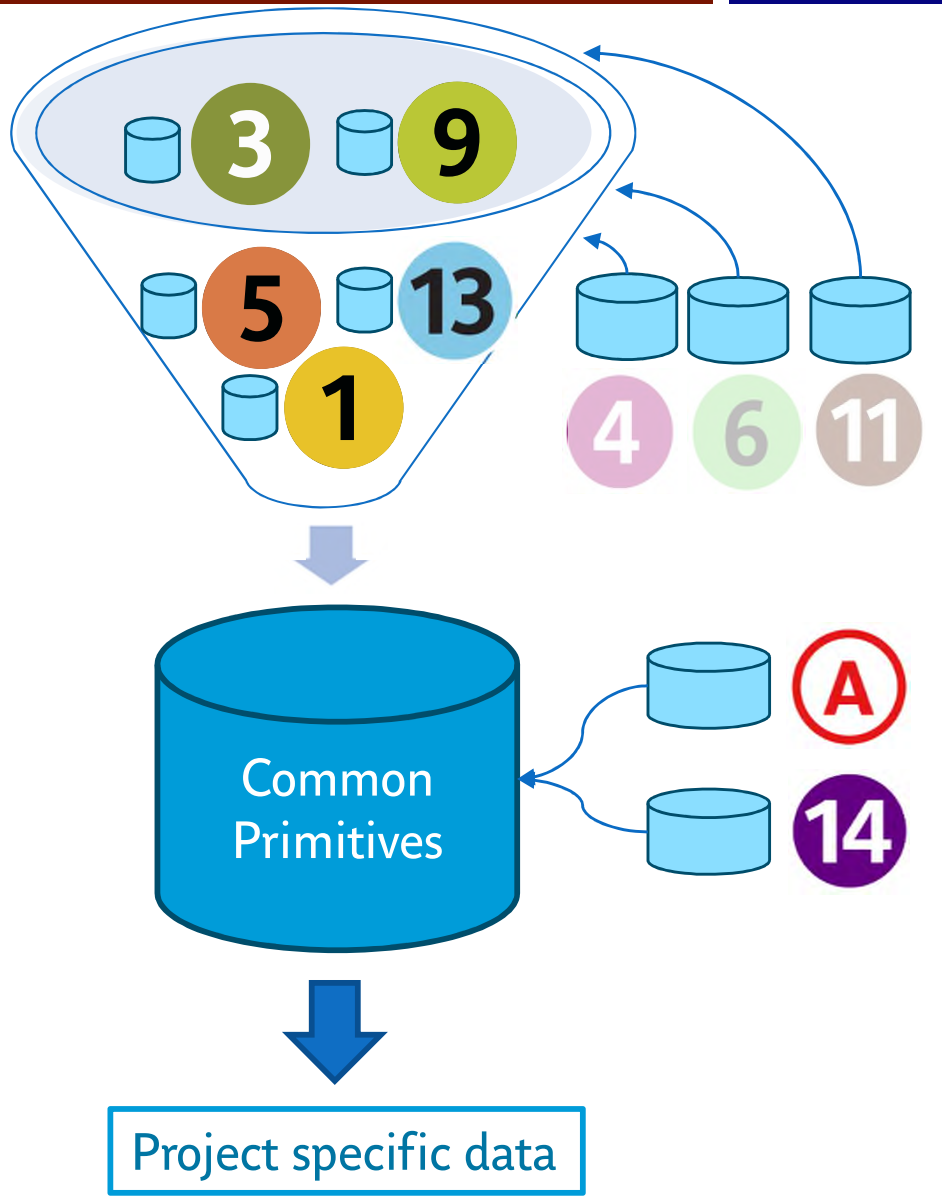
- In railways (CBTC), project-related data are similar

→ 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



Genericity - Common library 2/2

- 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

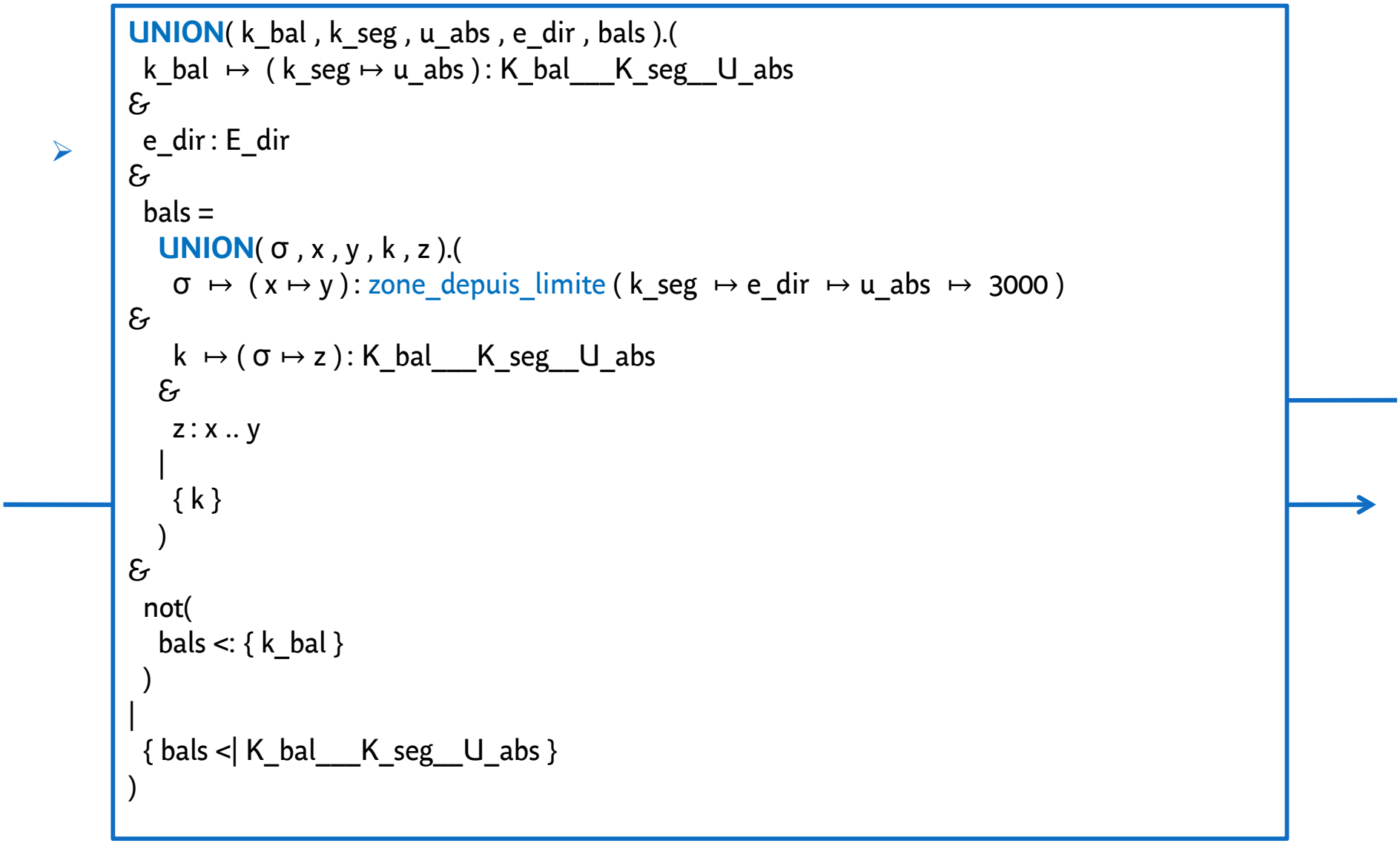
→ Properties optimization

→ Change management duration

New data table : 8 hours for L 13 before common library

New data table : 2 min for L 5, L9

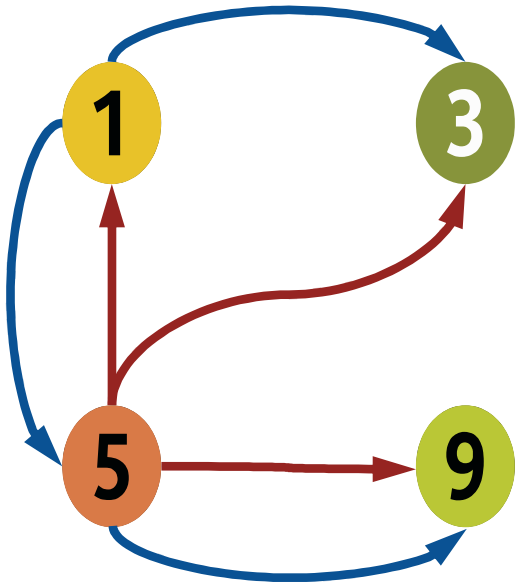
Common library - use example



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**

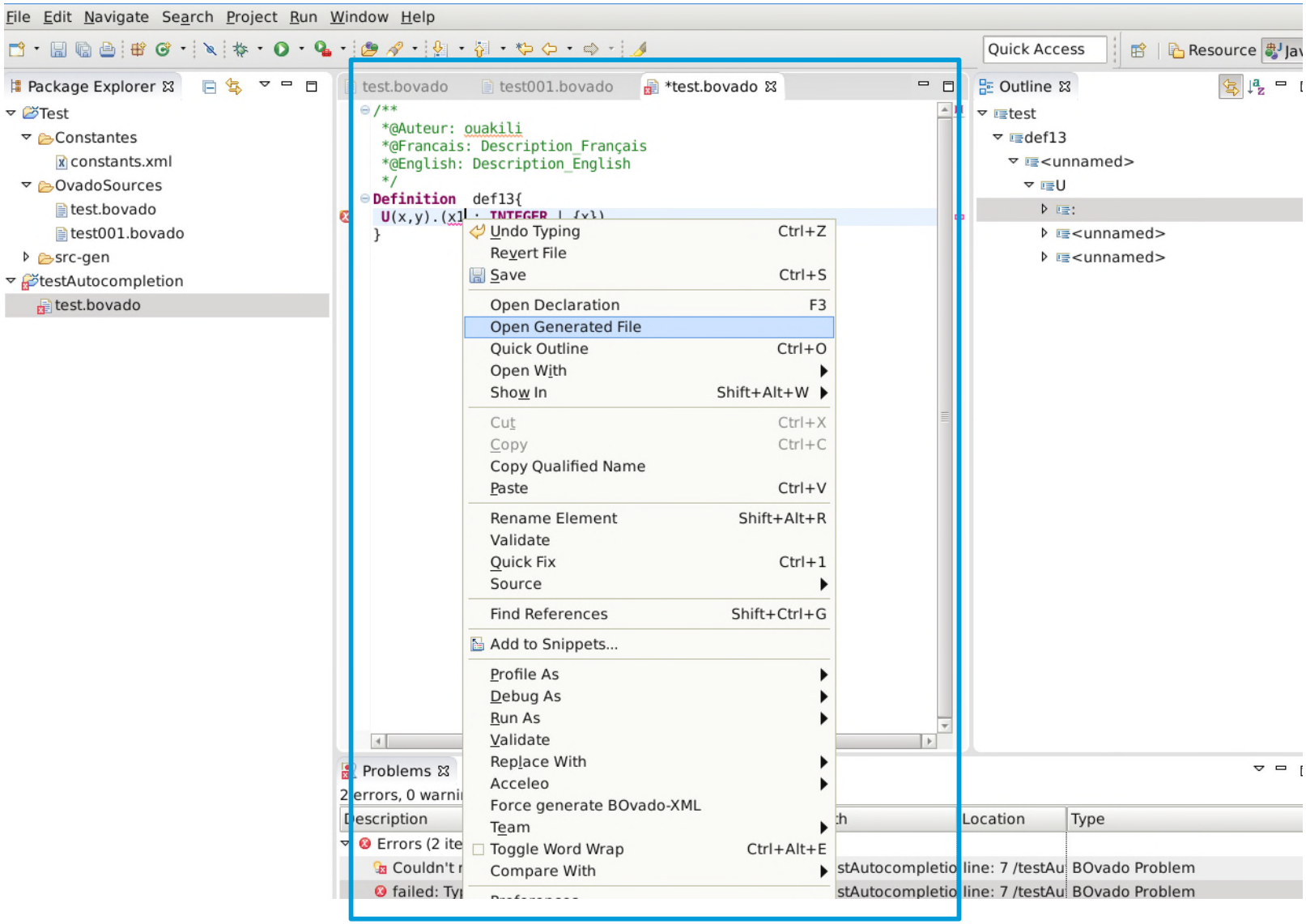


Wayside equipment
On-board equipment

B-OVADO - Rich integrated editor 1/2

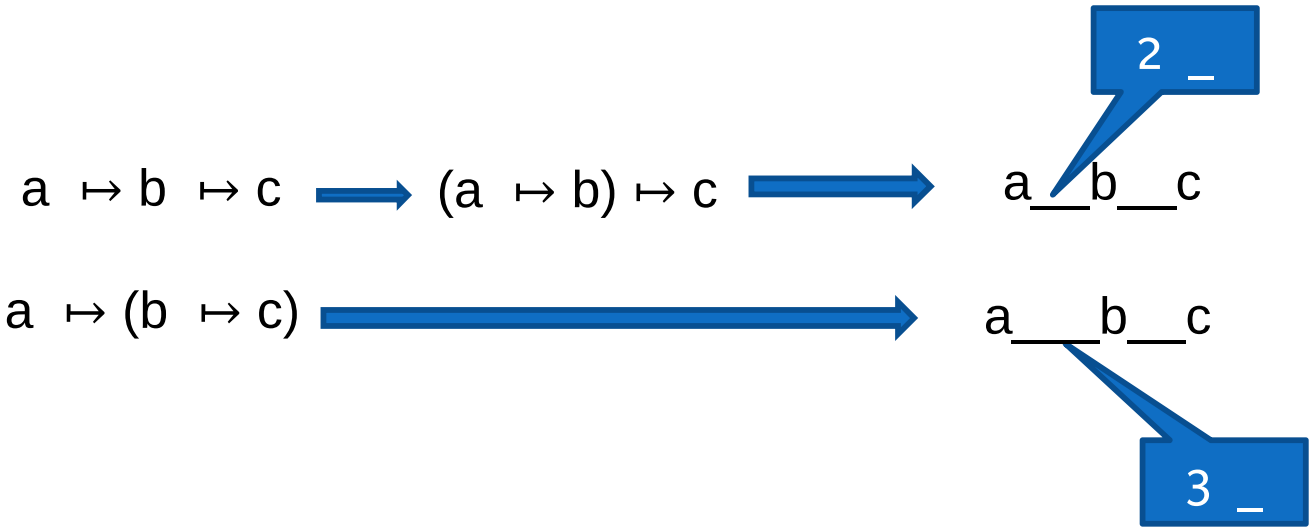
- Syntactic check (key words)
- Semantic check (typing, scoping)
- Documentation
- Auto-completion
- Navigation
- Seamless integration to OVADO

B-OVADO - Rich integrated editor 2/2



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