systerel
Solutions temps réel sécurisées

RSSRail 22
Generating and verifying configuration data with OVADO

Frédéric Badeau, Systerel
Joris Lamare, RATP
Julien Chappelin, Alstom

02/06/2022

Summary

Project context

RATP: Paris metro Line 6, system OCTYS VTPA

ALSTOM: providing the railway system

Systerel

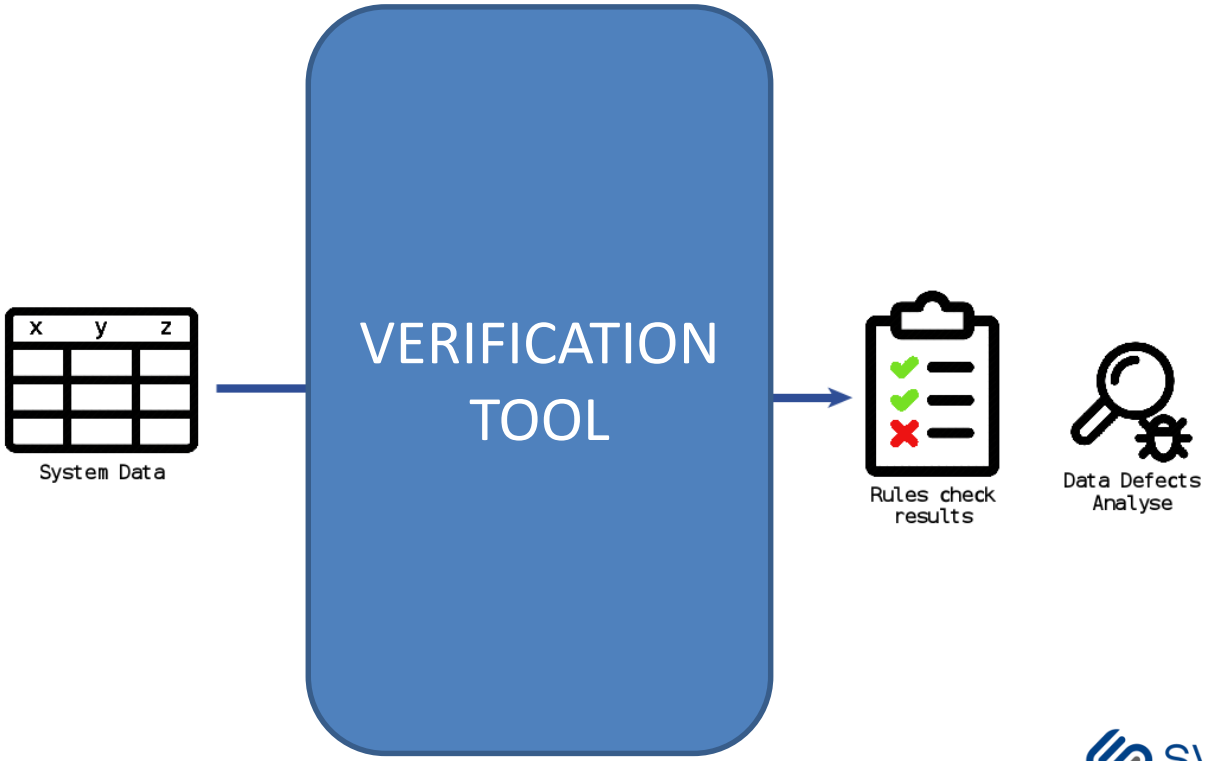
- Verification of configuration data with OVADO® (property of RATP) using a formal model of data rules (based on the B Language)
- For the first time generation of equipment configuration data with OVADO

Safety context: SIL4 process regarding CENELEC EN50128

systerel
Solutions temps réel sécurisées

OVADO to verify system configuration data

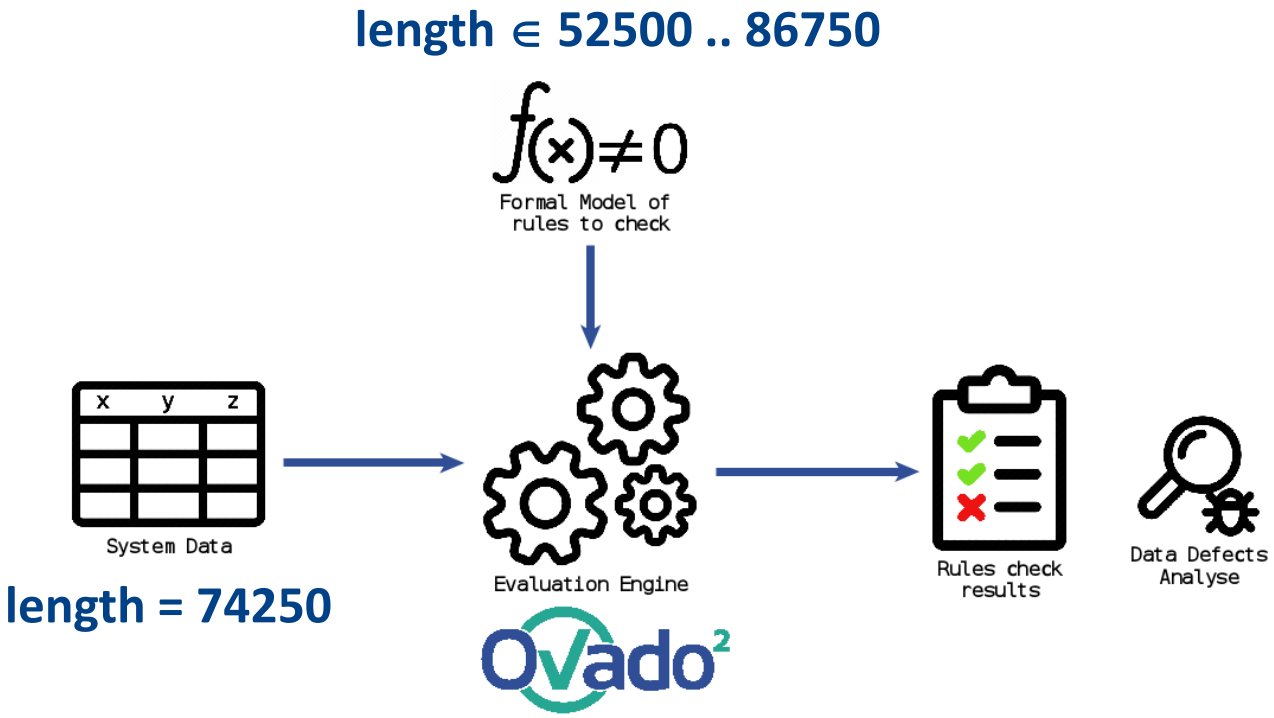
Verifying system rules on configuration data (system data)



systerel
Solutions temps réel sécurisées

OVADO to verify system configuration data

Verifying system rules on configuration data (system data)



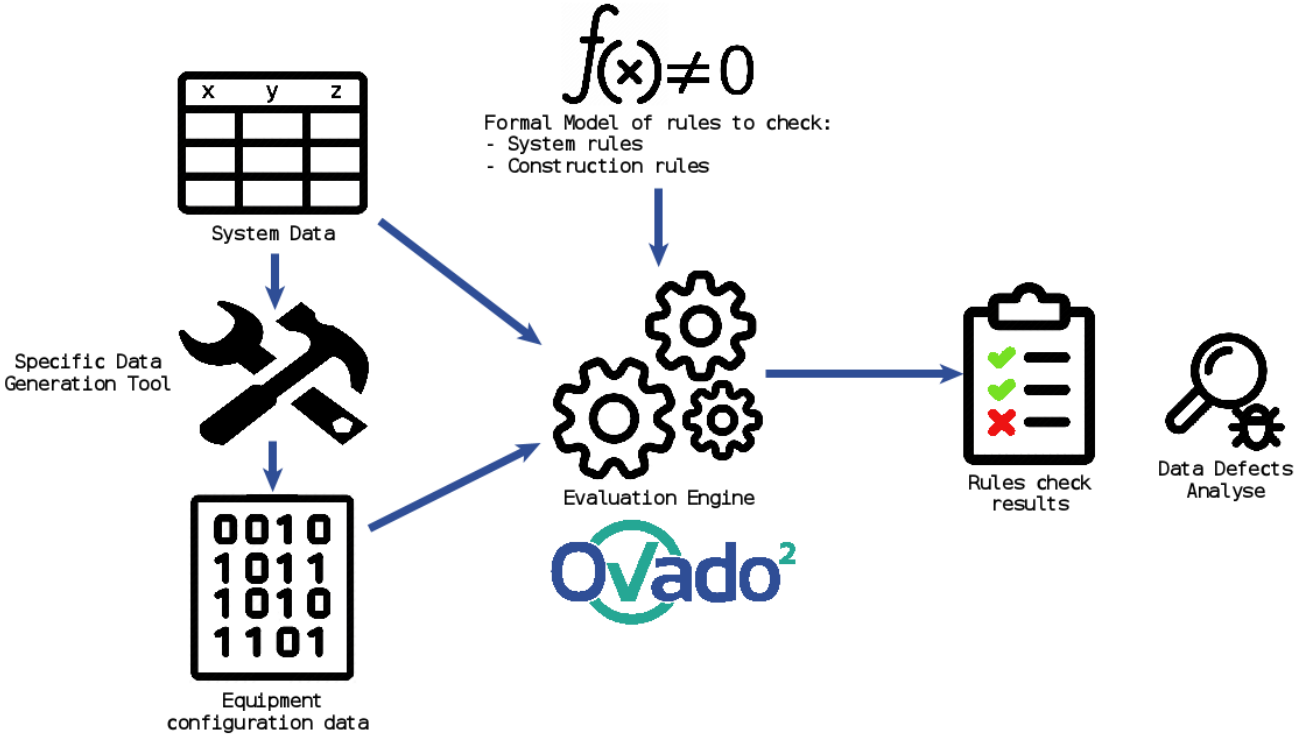
systerel
Solutions temps réel sécurisées

OVADO to verify equipment configuration data

Verifying construction rules on configuration data

(Final equipment configuration data / system data)

Eqpt_data1 = Eqpt_data1_computed_from_syst_data



systerel
Solutions temps réel sécurisées

OVADO to generate equipment configuration data

The idea

- Using also OVADO to generate equipment configuration data

The goals

- Rising quality: taking advantage of a formal model
- Decreasing budget: factorizing data generation/data verification

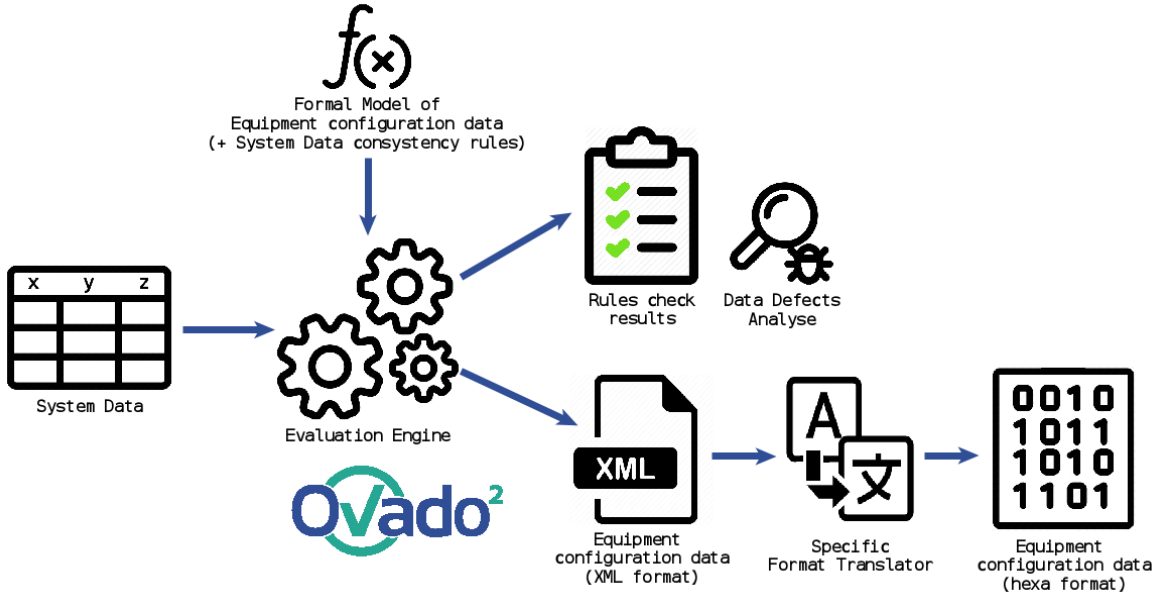
Let’s do it!

OVADO to generate equipment configuration data

Formal model of equipment data computed from system data

- + XML export plugin
- + specific translator

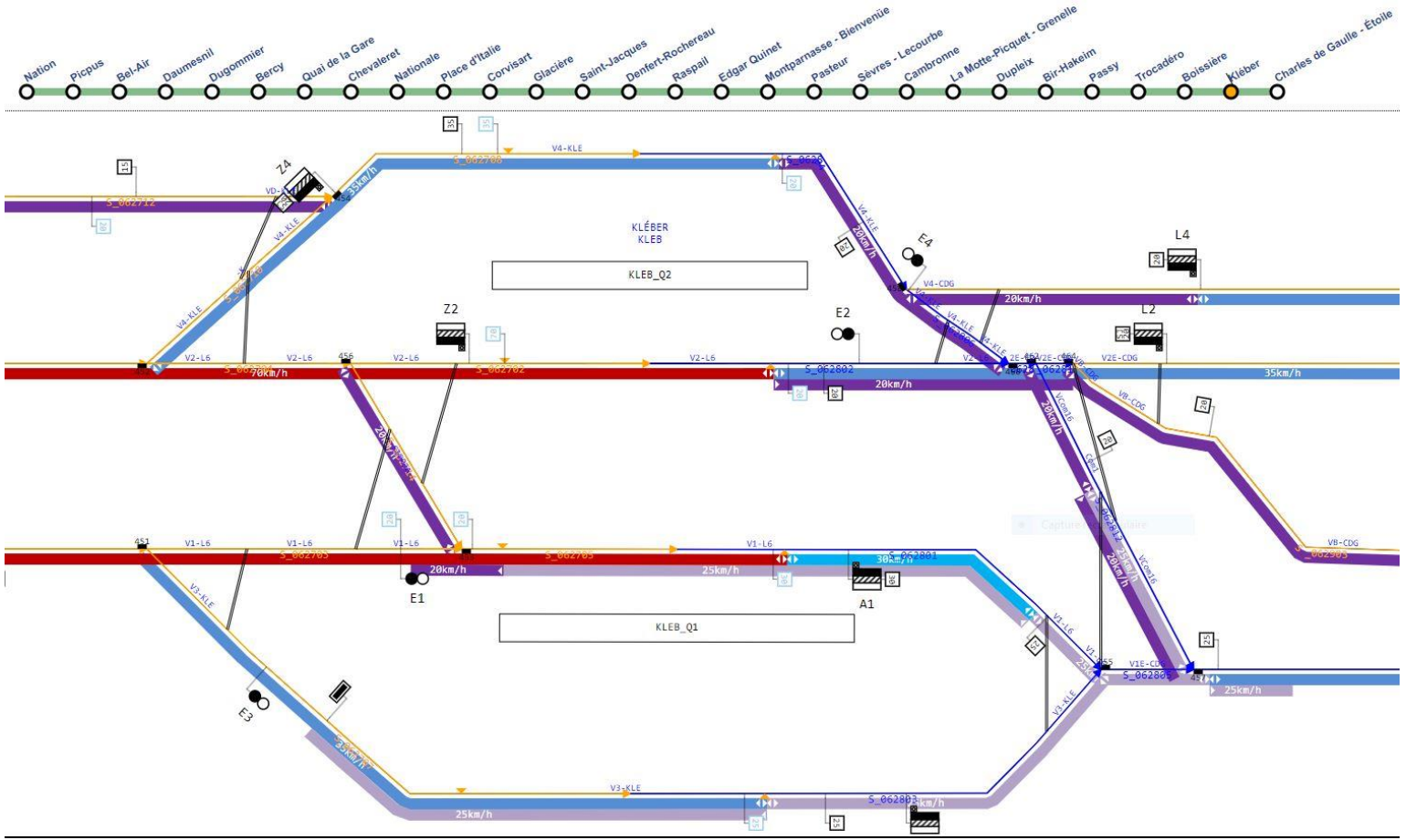
Verification of system data consistency by rules verified by OVADO



systerel
Solutions temps réel sécurisées

Example: bidirectionnal speed limit zones

- Verifying data
- Generating data
- Safety
- Conclusion



systerel
Solutions temps réel sécurisées

Example: bidirectionnal speed limit zones

System data

- Start position (track/abscissa, direction), end position (track/abscissa)
- Speed limit, anticipation distance at start/end

Semantics

- Zone = from start, in the given direction, follow the direct track, to the end
- An anticipation distance is significant at the border of 2 zones, entering a decreasing speed zone. 0 means no anticipation distance

System rules

- R2: bidirectionnal speed limit zones should cover all the tracks
- R3: there should not be 2 anticipation distances at some position

Equipment data: for each block [$segment_{(fr)}$]

- block_id, nb_obj, speed0, anticip_dist0, anticip_dir0
- Array of 6 objects: abs, speed, anticip_dist, anticip_dir

Safety issues: context + previous approach

Global context

- SIL4 process according to CENELEC EN50128 (2011)

Previous approach: OVADO only for data verification

- OVADO was used only for verification: tool class = **T2**
- Ovado²® = a double tool + double input plugins (diversified techno + tools called one after another)
- A complete process (planification, description, justification against the norm, verification, traceability, auditable)
- **Not much is required on the data generation tool: safety is based on output verification**
- The OVADO model of rules is a common mode for both tools:
  - Independent verification of rules (tracing only comments)
  - A few tests (ability to detect erroneous data)

Safety issues: current approach

Current approach: OVADO for data generation and verification

- OVADO is now used to produce (and verify) data: tool class = **T3**
- Ovado² = a double tool + double input plugins (diversified techno + tools called one after another)
- A complete process (planification, description, justification against the norm, verification, traceability, auditable)
- **Around 80% of the OVADO model is common to generation/verification!**
  - 20% to model rules
- **How to mitigate this common mode?**

Detailed verification of (all) the OVADO model

Activity of detailed verification of the OVADO model

Principle

- OVADO model is structured with: interface with data, definitions, rules
- Foreach structuring element: a detailed verification form based on 13 items
- Independent verification
- Auditable forms
- Precised references (elements, commits, dates, autors, reviewers)

Verification form items

- Element naming rule, typing, physical units
- Consistency of abscissae comparison on tracks, on blocks, on switch points
- Cases completeness
- Well-definedness: f(x), …
- Inner comments
- **Consistency/Completeness of description and model**
- Major enhancements
- Address of interface data, consistency/completeness with rule specification

Conclusion

Results

- This new approch using OVADO to factorize generation+verification of configuration data was a success
- We raised the formal model quality level (detailed verification activity)
- The overcost of the detailed verification activity is ≈10% of model dev
- This new use of OVADO still complies with a SIL4 process

systerel
Solutions temps réel sécurisées

Thank you. Any question?