Empowering the Future.

Verification of Railway Network Models with EVEREST

J. Martins[1], J. Fonseca[1], R. Costa[2], J. Campos[23], A. Cunha[23], **N. Macedo[24]**, J. Oliveira[23]
[1]Efacec, [2]INESC TEC, [3]U. Minho, [4]U. Porto, Portugal

efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Efacec

- Portuguese Company
- Approximately 2000 Employees
- Founded in 1948

Transportation

Energy

Environment

efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Transportation – Signalling Products

AEGIS BY EFACEC

XSafe BY EFACEC

- Turn-key products
- Develops and integrates technology to deliver the best product
- Multidisciplinary engineering teams
- Long history in signalling systems
- References around the world

efacec Empowering the future

Cofinanciado por:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

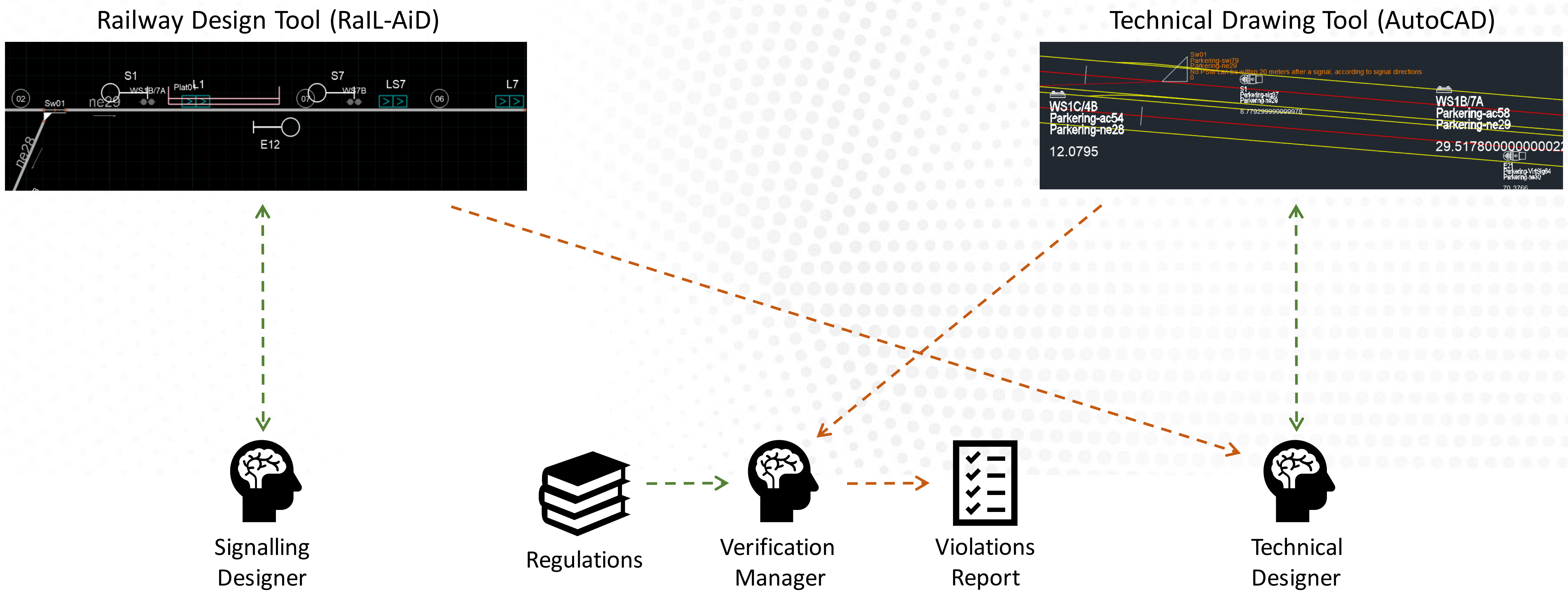
Railway Signalling System Design

- The **design** of railway signalling systems is performed by multi-disciplinary teams
  - Different expertise
  - Different views of the system
  - Accustomed to different tools
- Must be **verified** against regulations
  - Requires info from different views
  - Rules vary from project/market

(© omada Rail Systems)

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Railway Signalling System Design



efacec Empowering the future

Cofinanciado por:

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA

Fundo Europeu de Desenvolvimento Regional

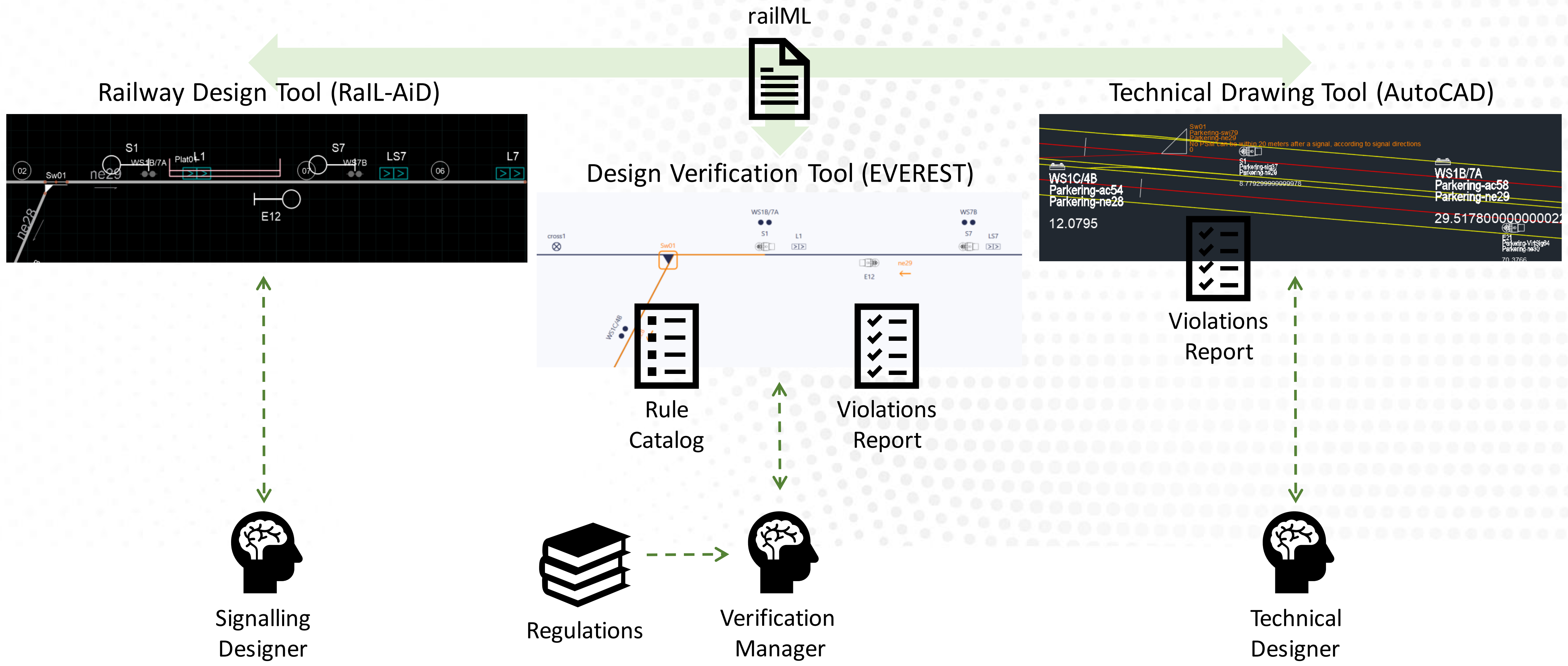
Railway Signalling System Design

- Phases of the process still manual and error prone
  - Where technical designers add the signalling information manually
  - Verification considers signalling and physical information
  - Verification manager validates infrastructure rules manually
- Main goals
  - How to automatically **synchronize information** in a consistent network model?
  - How to formalize and **automate the verification** of imposed regulation?

efacec Empowering the future

Cofinanciado por: COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Railway Signalling System Design

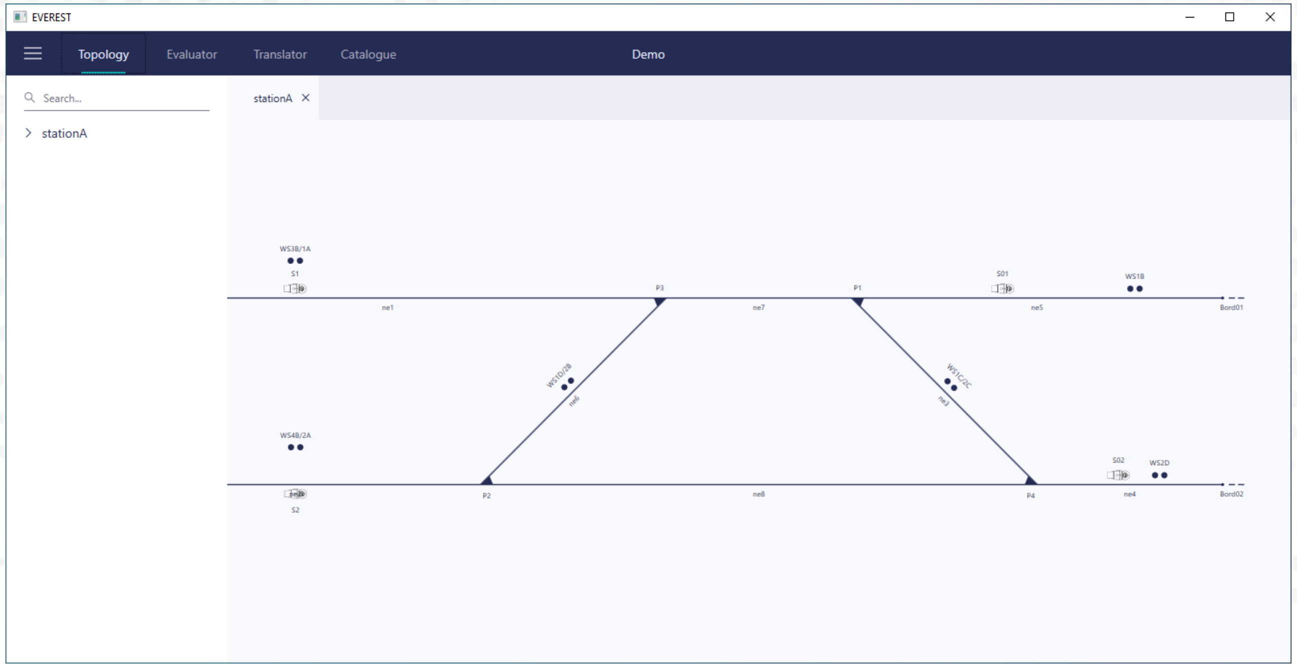


efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST - Efacec Verification of Railway Networks Tool

- EVEREST is a design verification tool for railway network models
- Preserves the loosely coupled nature of the workflow
- Coalesces the information in a common exchange format (railML)
- Provides a specification language for infrastructure rules
- Automates the verification of such rules



efacec Empowering the future

Cofinanciado por:

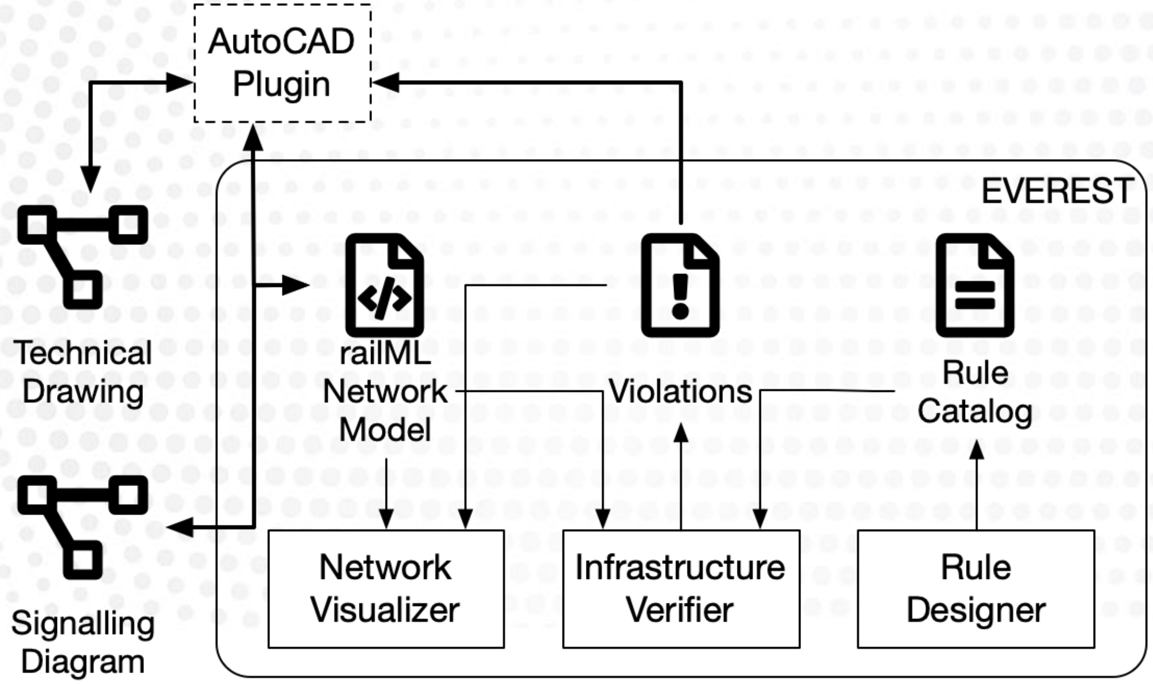
COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Overview

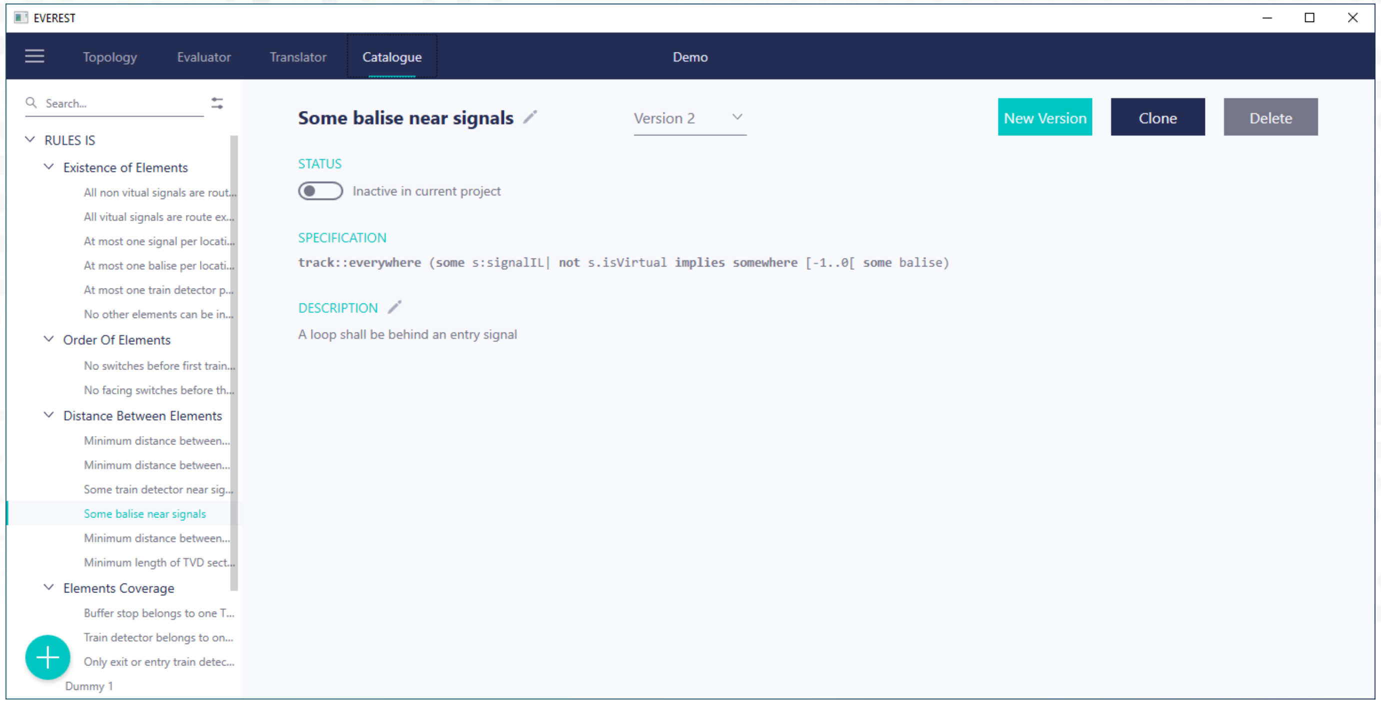
- An EVEREST project is a set of railML models
- The **Rule Designer** supports writing and maintaining a catalog of rules
- The **Infrastructure Verifier** automatically verifies rules selected for the project
- Violations can be seen in the **Network Visualizer**
- The **AutoCAD Plug-in** imports signalling data and exports physical data



Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Rule Designer

- Supports writing of rules (syntax checker, type checker)
- Collects and organizes rules in a catalog shared by all projects
- Provides basic versioning functionalities
- Supports expression macros to tame verbosity of railML



RULES IS

- Existence of Elements
  - All non vitual signals are rout...
  - All vitual signals are route ex...
  - At most one signal per locati...
  - At most one balise per locati...
  - At most one train detector p...
  - No other elements can be in...
- Order Of Elements
  - No switches before first train...
  - No facing switches before th...
- Distance Between Elements
  - Minimum distance between...
  - Minimum distance between...
  - Some train detector near sig...
  - Some balise near signals
  - Minimum distance between...
  - Minimum length of TVD sect...
- Elements Coverage
  - Buffer stop belongs to one T...
  - Train detector belongs to on...
  - Only exit or entry train detec...
- Dummy 1

Some balise near signals — Version 2

STATUS

Inactive in current project

SPECIFICATION

```
track::everywhere (some s:signalIL| not s.isVirtual implies somewhere [-1..0[ some balise)
```

DESCRIPTION

A loop shall be behind an entry signal

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

efacec Empowering the future

EVEREST Rule Language

- Provides a formal specification language for infrastructure rules over network models
- Language based on relational logic of Alloy
  - Eases navigation over railML elements
- Semantics based on metric interval linear temporal logic
  - Temporal modalities adapted to spatial context

Along a route, there's a minimum distance of 20 meters between every signal and a switch.

```
route ::
  everywhere (some signalIS implies
    everywhere [0..20] no switchIS)
```

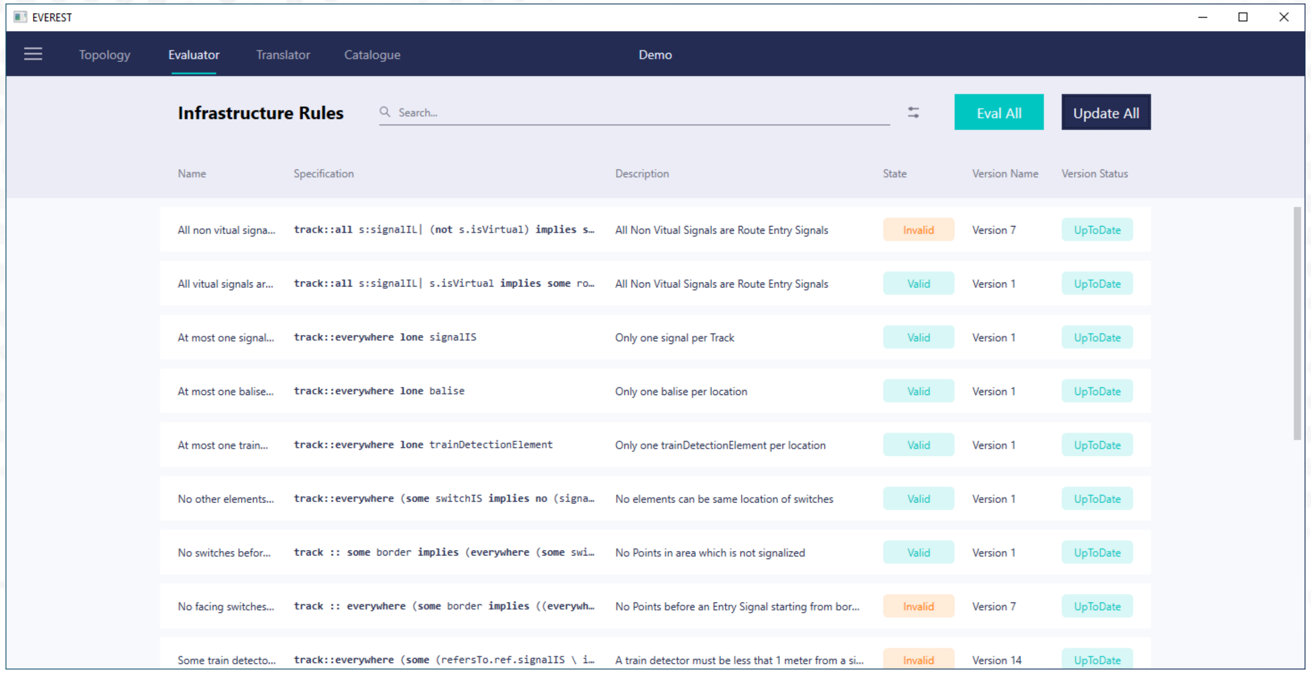
efacec Empowering the future

Cofinanciado por:

COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

EVEREST Infrastructure Verifier

- Automates the verification of rules
- Rules relevant for each project selected from the catalog
- Found violations reported in the EVEREST Visualizer and the AutoCAD drawing



Infrastructure Rules

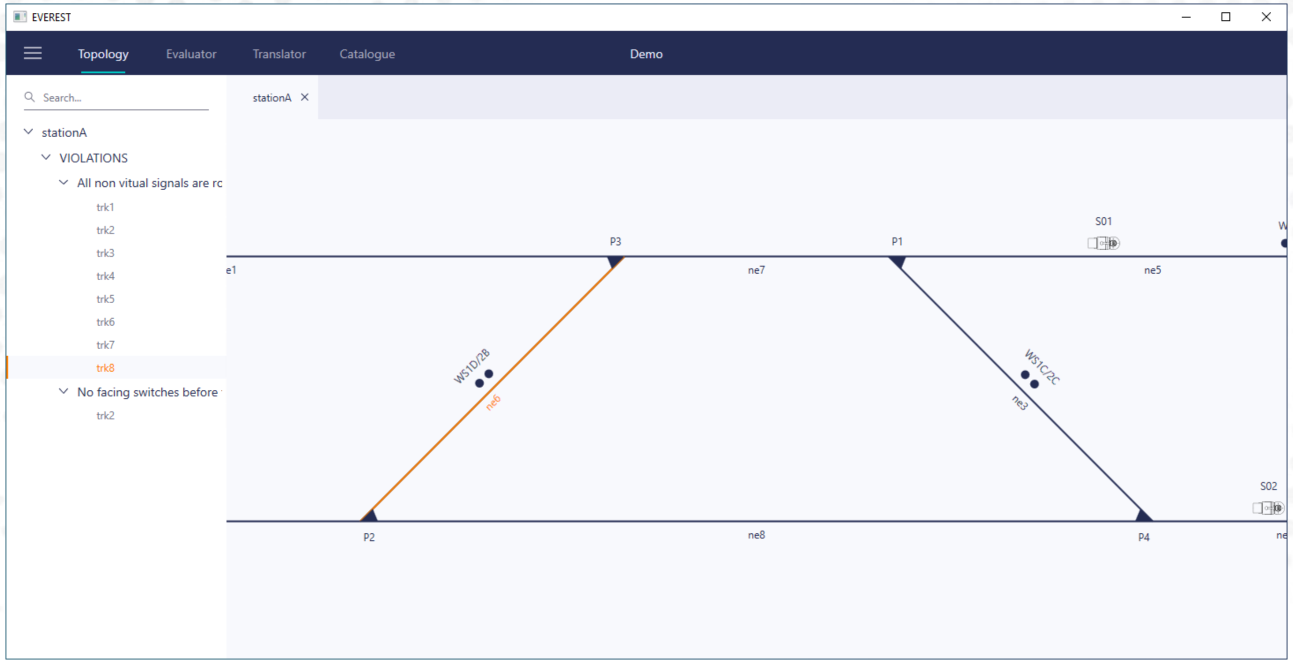
Name	Specification	Description	State	Version Name	Version Status
All non vitual signa...	`track::all s:signalIL| (not s.isVirtual) implies s...`	All Non Vitual Signals are Route Entry Signals	Invalid	Version 7	UpToDate
All vitual signals ar...	`track::all s:signalIL| s.isVirtual implies some ro...`	All Non Vitual Signals are Route Entry Signals	Valid	Version 1	UpToDate
At most one signal...	`track::everywhere lone signalIS`	Only one signal per Track	Valid	Version 1	UpToDate
At most one balise...	`track::everywhere lone balise`	Only one balise per location	Valid	Version 1	UpToDate
At most one train...	`track::everywhere lone trainDetectionElement`	Only one trainDetectionElement per location	Valid	Version 1	UpToDate
No other elements...	`track::everywhere (some switchIS implies no (signa...`	No elements can be same location of switches	Valid	Version 1	UpToDate
No switches befor...	`track :: some border implies (everywhere (some swi...`	No Points in area which is not signalized	Valid	Version 1	UpToDate
No facing switches...	`track :: everywhere (some border implies ((everywh...`	No Points before an Entry Signal starting from bor...	Invalid	Version 7	UpToDate
Some train detecto...	`track::everywhere (some (refersTo.ref.signalIS \ i...`	A train detector must be less that 1 meter from a si...	Invalid	Version 14	UpToDate

efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Network Visualizer

- Provides a visualization of the network model
- Allows the visualization of the found violations
- Network elements involved in violations are highlighted

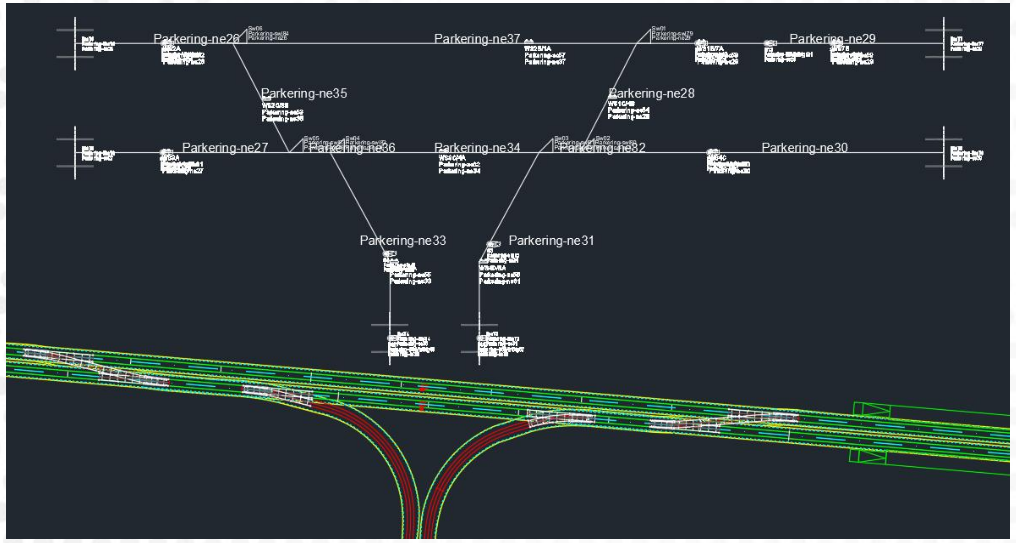


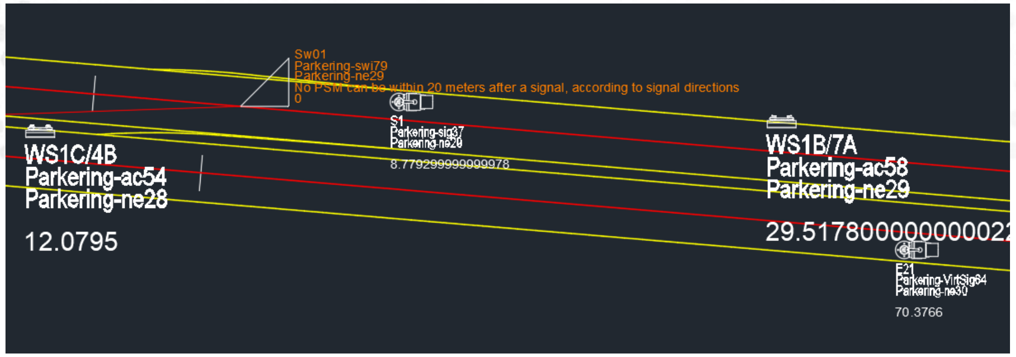
efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST AutoCAD Plug-in

- Imports signalling diagram to kickstart positioning process
- Supports the automatic partitioning of physical track into network elements
- Exports physical information about elements
- Imports back found rule violations for inspection





No PSM can be within 20 meters after a signal, according to signal directions

efacec Empowering the future

Cofinanciado por:

COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

EVEREST Evaluation

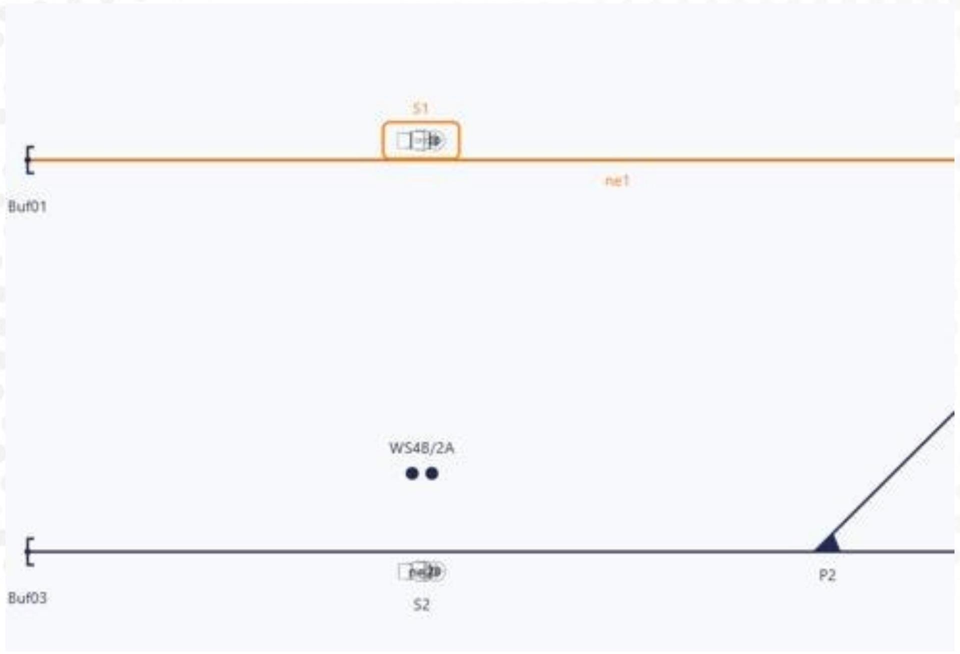
- **Performance**:
  - Time spent evaluating the rules is negligible for real projects
- **Expressiveness**:
  - Able to support most classes of properties encountered so far
- **Usability**:
  - Needs further studies (initial feedback from designers positive)
  - Engineers welcome the formalization and documentation of rules

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Expressiveness: Existence of Elements

All virtual signals must be the exit signal of some route.

```
track :: everywhere (all s : signalIS |
  isVirtual.refersTo.ref.s implies
    some exitSignal.refersTo.ref.s)
```



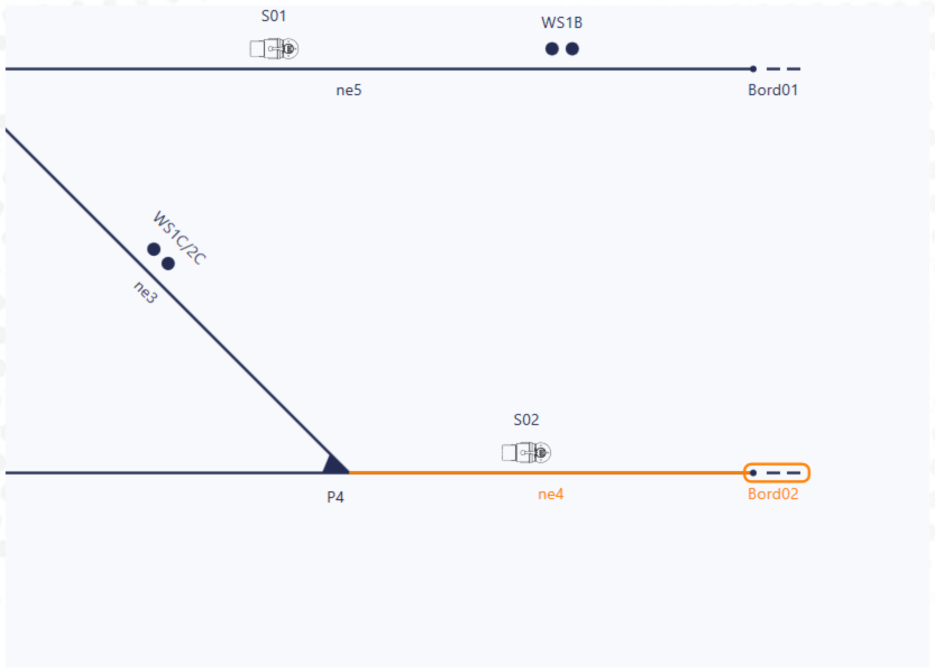
efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Expressiveness: Order of Elements

The first switch after entering an area must be preceded by a train detection element.

```
track :: some border implies
  everywhere (some switchIS implies
    somewhere ]..0[ some trainDetectionElement)
```



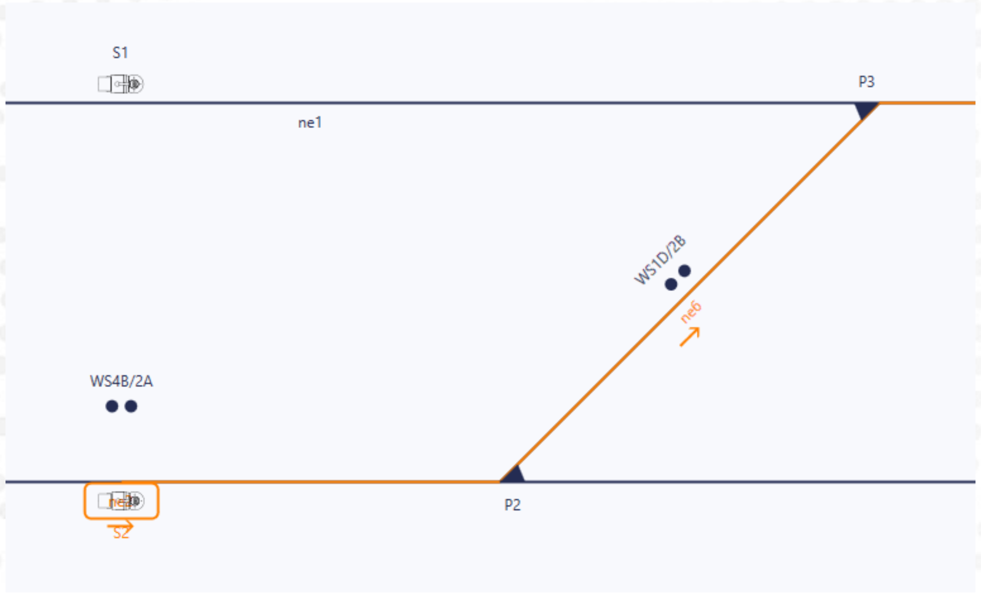
efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Expressiveness: Distance between Elements

There's a minimum distance of 50 meters between every signal and a facing switch.

```
route :: everywhere (some signalIS implies
   everywhere [0..50]
      no switchIS & facingSwitches.refersTo.ref)
```



efacec Empowering the future

Cofinanciado por:

COMPETE 2020

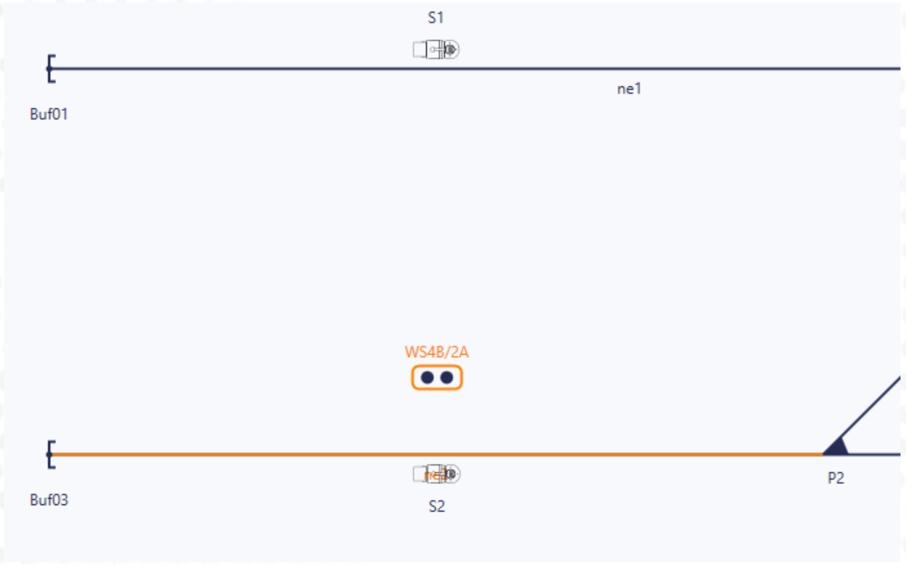
PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

EVEREST Expressiveness: Element Coverage

Only the last and first train detection devices in an area demarcate exactly one TVD section.
(Part of forcing every track to be correctly covered by TVD sections.)

```
track :: everywhere (all t : trainDetectionElement |
   #(hasDemarcatingTraindetector.ref.t) = 1 implies
    ((somewhere [0..[ some border) and
        (everywhere ]0..[ no trainDetectionElement) or
     (somewhere ]..0] some border) and
        (everywhere ]..0[ no trainDetectionElement)))
```



Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

efacec Empowering the future

Conclusion

- We propose a workflow backed by a toolset for the verification of railway networks
  - Automates the flow of information between teams
  - Supports the formalization of infrastructure regulation
  - Automates the verification of such properties
- Future work
  - Further **empirical studies** at EFACEC regarding usability and expressiveness
  - Verify **interlocking properties**, model checking needed
  - Use automatic **model repair** to suggest fixes to violations

efacec Empowering the future

Cofinanciado por: COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Thank You!

efacec Empowering the future

Cofinanciado por:
COMPETE 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional