MADE IN FRANCE

CLEARSY DATA SOLVER

CLEARSY Safety Solutions Designer

FORMAL DATA VALIDATION
CLEARSY DATA SOLVER

CONTACT@CLEARSY.COM

CLEARSY DATA SOLVER

CLEARSY DATA SOLVER

In the railways, safety critical software applications are usually developed and validated independently from the parameters or constant data that fine-tune their behavior. For example, the track topology, signal and point positions, kilometer points, etc. are constant data used by an automatic pilot to compute braking curves and to determine when to trigger the emergency brake.
So, each part must be safe at the same level: SIL4.

Data validation process consists in ensuring that the data set is correct. For example: in ERTMS standard, tracks are equipped with signals and beacons. Rules to verify are related to the topology: each signal should have an associated beacon group, distance between signal and its beacon group should be less than 2 meters, beacons should be less than 2 meters apart from each other's. Other rules to verify are related to the content of the messages sent by the beacons to the trains (distances, gradients, speeds…).

Manual data validation process used to be entirely human, leading to painful, error-prone, long-term activities (requiring several months to check manually up to 100,000 items of data against 1,000 rules). Formal data validation process is the natural evolution of this human-based process into a secure one. This approach has been invented by CLEARSY, thanks to its deep knowledge and skills on formal method technology and associated tools.

Screen shot of the CLEARSY tool

CLEARSY provides a data validation tool and associated services. The benefits of this formal approach are diverse:

- It is fast: up to 100x faster than a pure human verification, a couple of hours are enough for validating a complete railway project.
- It is automatic, exhaustive, push-button and repeatable at will (avoids fastidious non-regression phase).
- It removes human errors, as it makes use of certified formal techniques
- It allows a strong reuse from one project to another (capitalization of the knowledge).
- The solution is based on a tool certified T2.
- Especially targets railway projects such as CBTC, ERTMS, IXL, RBC, ATS…

Why is this approach better than scripts or Python/C++ algorithms?

- Scripts can be used to do quick small checks, but they are not efficient when dealing with complexity… and there are lots of tricky verification to do on CTBC projects.
- Scripts and algorithms are hard to maintain because the rely on architecture/design choices. So, if you change a part of the specification, part of the code can be obsolete.
- Biggest strength of B language is its expressivity: less code to produce, and closer to the specification.
- The only part described by the formal rule is the selection of the data and the property to fulfil. The rest is automatically generated by our Data Solver Core.
- Better robustness: ProB and the Data Solver tool are been used in lots of industrial projects and has a large return of experience.
- In formal Data Validation, rules are independent from one another. Each rule is produced using a mastered process. Rules are also independent from the data part. So, if you change the data format, rules are not affected.

PRODUCT DESCRIPTION

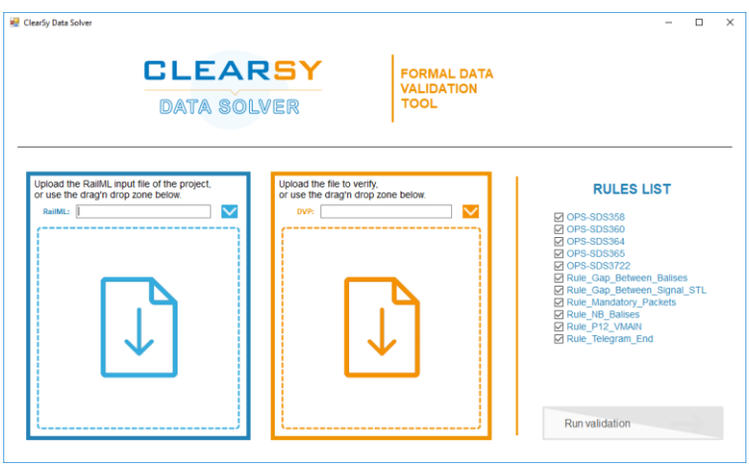
A customized tool

- Adapted to the customers data file format (xml, xls, parameter file, railML, csv, txt …).
- Adapted to the customers verification report documents and process.
- End users can also specify their own rules and use the tool by themselves.

A service of formal rules modelling

The tool is a solver: that means the data set is verified, rule by rule on all the data concerned. These project rules can be developed by the customer himself or by CLEARSY. We propose this service:

- Modelling the formal rules to be satisfied by the data concerned.
- These formal rules are easily readable after training.
- The rules belong to the customer and can be reused at will, all along the different projects or the different versions of a product.



Screen shot of the CLEARSY tool


CERTIFER

Certificat de type

par examen de la conception

design examination type certificate

N° 9322/0235 édition 1

délivré à

attributed to

CLEARSY Systems Engineering
320 av. Archimède
Les Pléiades III - Bat A
F-13090 AIX-EN-PROVENCE

par

by

CERTIFER
18 Rue Edmond Membrée
F-59300 VALENCIENNES

qui certifie que la conception du produit suivant :

which certifies that the design of the following product:

CLEARSY DATA SOLVER (CAVAL) version 2.1.1

CLEARSY DATA SOLVER (CAVAL) version 2.1.1

est conforme aux exigences de la norme EN 50128 :2011 §6.7 outil classe T2

meets the tools class T2 requirements of the standard EN 50128:2011 §6.7.

L'annexe EC_9322_0051 édition 1 fait partie intégrante du présent certificat.

This certificate includes appendix EC_9322_0051 edition 1.

Ce certificat ne s'applique qu'à la conception du produit référencé en annexe et au dossier descriptif en résultant.

The scope of this certificate is limited to the design of the product referenced in the appendix and its description file.

Date de délivrance: **25 Novembre 2019**
Date of certification: *November, 25th 2019*

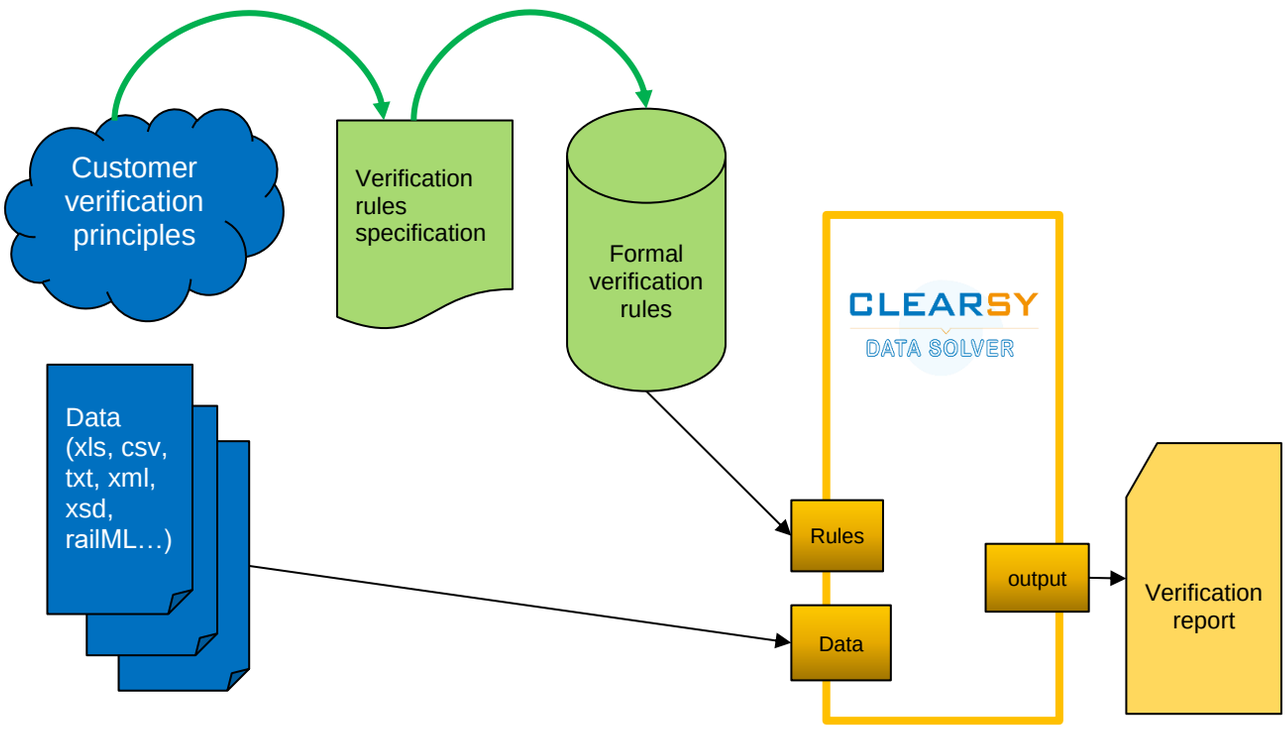
Le Directeur Général
The Chief Executive Officer

Pierre KADZIOLA

CERTIFER SA - Siège social : 18 rue Edmond Membrée - CS 40141 - 59308 Valenciennes Cedex
Tél. +33 (0)3 27 28 35 00 - Fax : +33 (0)3 27 28 35 09 - www.certifer.eu
Société Anonyme au capital de 9 060 180,00 € - TVA/SIRET : FR28 802 053 397 00019 - NAF : 7120B - RCS Valenciennes 802 053 397

The verification tool is certified T2 according to CENELEC EN50128.

PRINCIPLES



The non-compliance outputs are expressed in natural language, so they can be understood by the data preparation or data validation teams.
List of counter-example is exhaustive; when no error is reported, the correctness of the data set is guaranteed.
Reports are filled with all the information related to its verification campaign, **including coverage of data set verified**, missing verifications, checksums of inputs.

COMMERCIAL REFERENCES

The customers are railway or subway operators, or industrial companies.
.

ALSTOM · SNCF RÉSEAU · RATP · Atos · THALES · SIEMENS · GE · ATKINS Member of the SNC-Lavalin Group

To ALSTOM (CBTC): Tool and rules

- Since 2012
- Specific tool designed by CLEARSY
- Several CBTC projects verified (more than 15 lines)
- 2000+ validation rules designed
- Training

To GE transportation (CBTC + IXL): Tool and rules

- 2014-2016
- New specific tool designed by CLEARSY, faster and easier to use
- 1000 validation rules designed in 18 months
- Coverage of validated data

To ATOS and SNCF (ATS Mainline) parameters of MISTRAL NG (new centralized command/control rail management system): Tool and rules

- Since 2017
- New specific tool, customized by CLEARSY for ATOS and SNCF
- Improved performances, new features: client-server architecture connected to a database of parameters to validation
- Rules designed, Additional rules designed specifically for SNCF (final customer)

To SIEMENS: ATS and ATS+ Parameters (Mainline): Tool and rules

- Since 2018
- New tool designed by CLEARSY, customized for Siemens
- Formal validation of graphical objects (.ilv files)
- Workshops on rules specification definition

To THALES: SelTrac CBTC: Tool and rules

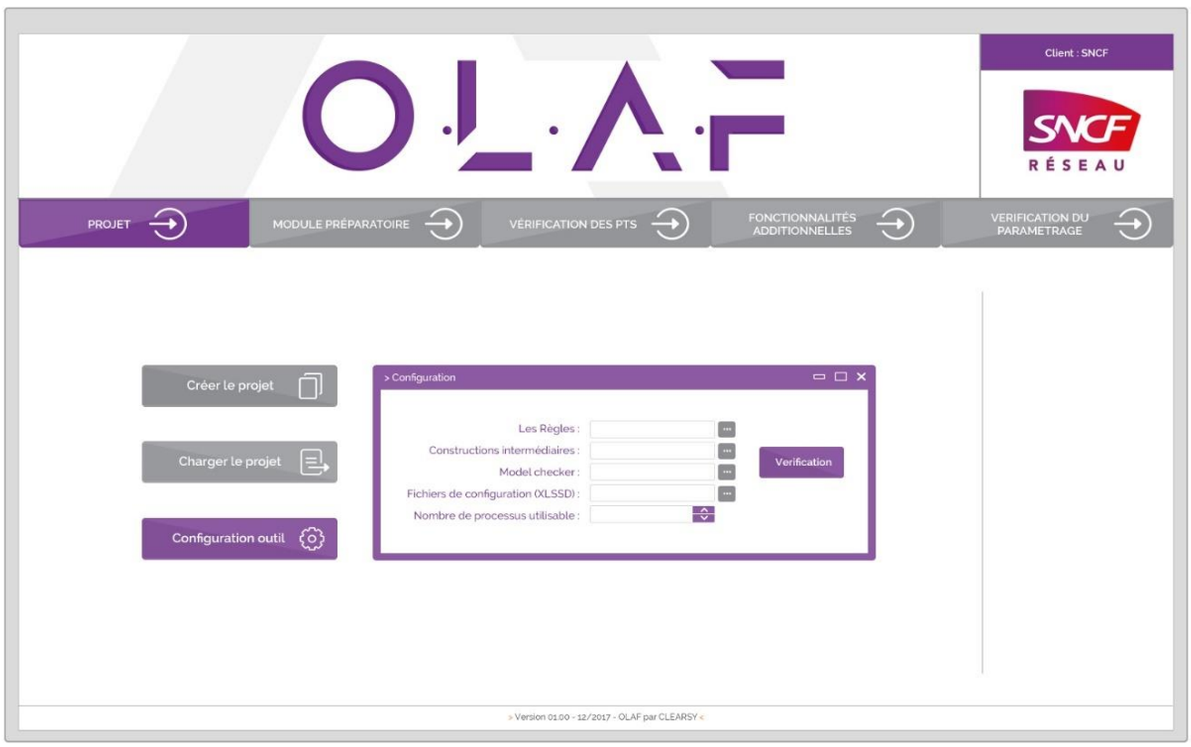
- Since 2019
- Specific tool designed by CLEARSY
- Rules designed
- Dedicated T2 certification of the new tool
- Integration to a track plan editor

To ATKINS: IXL: Tool and rules

- Since 2019
- Specific tool designed by CLEARSY
- Rules designed

To SNCF: ERTMS track data for freight corridor (ETCS): Tool and rules

- Since 2018
- New tool designed by CLEARSY
- ETCS Baseline 2 level 1 with KVB fallback
- Compatibility for B3 braking curves



Screenshot of the SNCF tool designed by CLEARSY

Pour SIEMENS : CBTC : Tool and rules

- Since 2021
- Tool based on CLEARSY Data Solver
- Automatic validation of railway invariants
- System analysis of setting errors

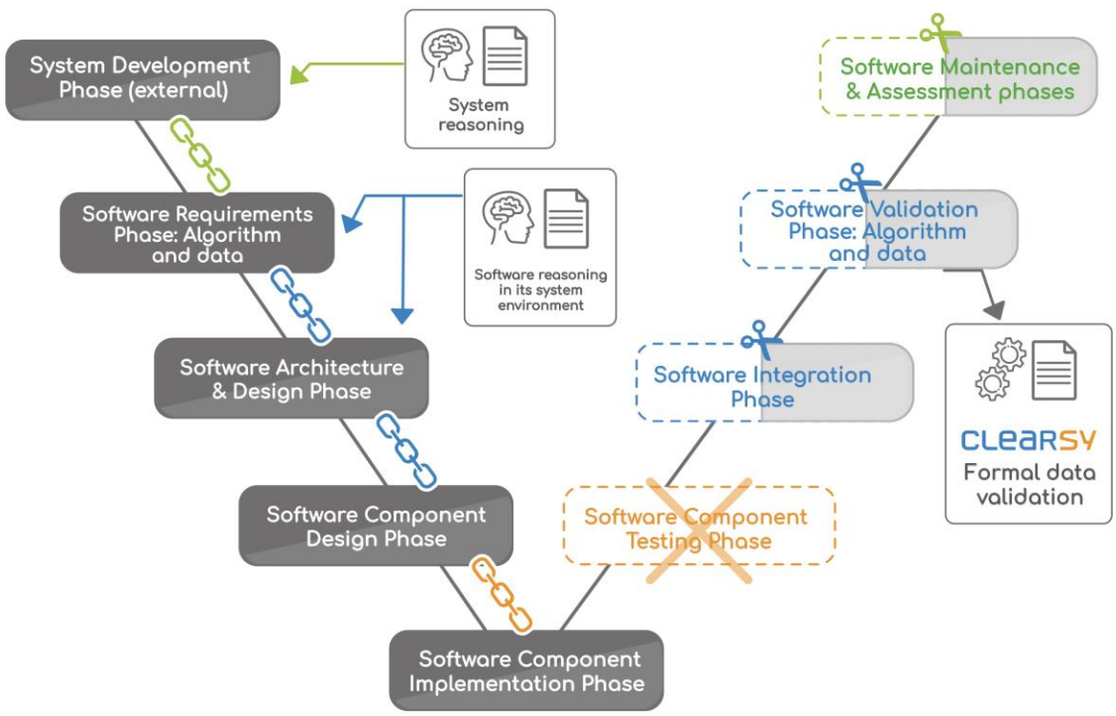
Pour RATP : CBTC OTCYS : Tool and rules

- Since 2021
- Use of CLEARSY Data Solver
  Second look at OTCYS data verification

BENEFITS AND ROI

- Better level of confidence on the verification, when using a formal method.
- Capitalization of knowledge by formal modelling of verification principles.
- Faster data verification: fully automatic once the rules are created.
- Formal verification tool: required by SNCF for projects such as MISTRAL NG, ERTMS parameters and ATS+ parameters validation.

Formal activities through the V cycle



Activity reduction

Formal Proof

Formal Proof at system level

Formal Proof at equipment level

Formal Proof at software level

320 AVENUE ARCHIMEDE
LES PLEIADES III BAT A
13100 AIX-EN-PROVENCE - FRANCE

TEL. +33 (0)4 42 37 12 70 FAX. +33 (0)4 42 37 12 71

WEB. contact@clearsy.com / www.clearsy.com

CLEARSY DATA SOLVER

OFFER 2023