CLEARSY
SYSTEMS ENGINEERING

CLEARSY SYSTEMS ENGINEERING

Formal Data Validation

CLEARSY DATA SOLVER TOOL

Aix
Lyon
Paris
Strasbourg

WWW CLEARSY.COM

Key points

CLEARSY provides a data validation tool and associated services.

The benefits of this formal approach are diverse:

- It is fast: up to 10x 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, easy iteration if parameters are modified)
- It removes human errors
- It allows a strong reuse from one project to another (**capitalization of the knowledge**)
- Especially targets railway projects such as CBTC, ERTMS, IXL, RBC, ATS…

Formal data validation process

Safety critical software and application parameters are usually developed and validated independently. Each part must be safe at the same level: SIL4.

Formal data validation consists in ensuring that the system parameters (data) are safe and ensures SIL4.

Formal data validation follows the following step:

1. Properties that make parameters correct are captured into a formal model using a mathematical language
2. A formal proof tool exhaustively checks the correctness of parameters
3. Correctness is determined independently. No need to execute / run the software / system

What is a verification rule? ERTMS example

- In ERTMS, tracks are equipped with signals associated with an "information point“. Information of the point are transmitted to the trains via beacons
- When the train antenna approaches near the beacon, it causes cyclic transmission of the same message by the beacon
- The number of information to be transmitted can be large, but the speed of the train and the transmission limit the size of the message. So we need several beacons which each transmits part of the information (telegram) reconstituted by the on-board software in message

Examples of properties:

- The topology of the track and the trackside equipment:
  - Each signal must have an associated balise group (no more than 8)
  - The distance between two beacons must not be greater than 2 meters, because the train must perform an emergency break as soon as possible if it crosses a restrictive signal
  - The distance between the signal and the first balise must not be greater than 2 meters

- The parameters of the telegrams
  - The telegrams sent by the beacons are of variable size and delimited by an ID witch presence must be verified
  - Values of the parameters (distances, lengths, gradients, speed limits…) and structure of the telegrams (consistency) must all be checked

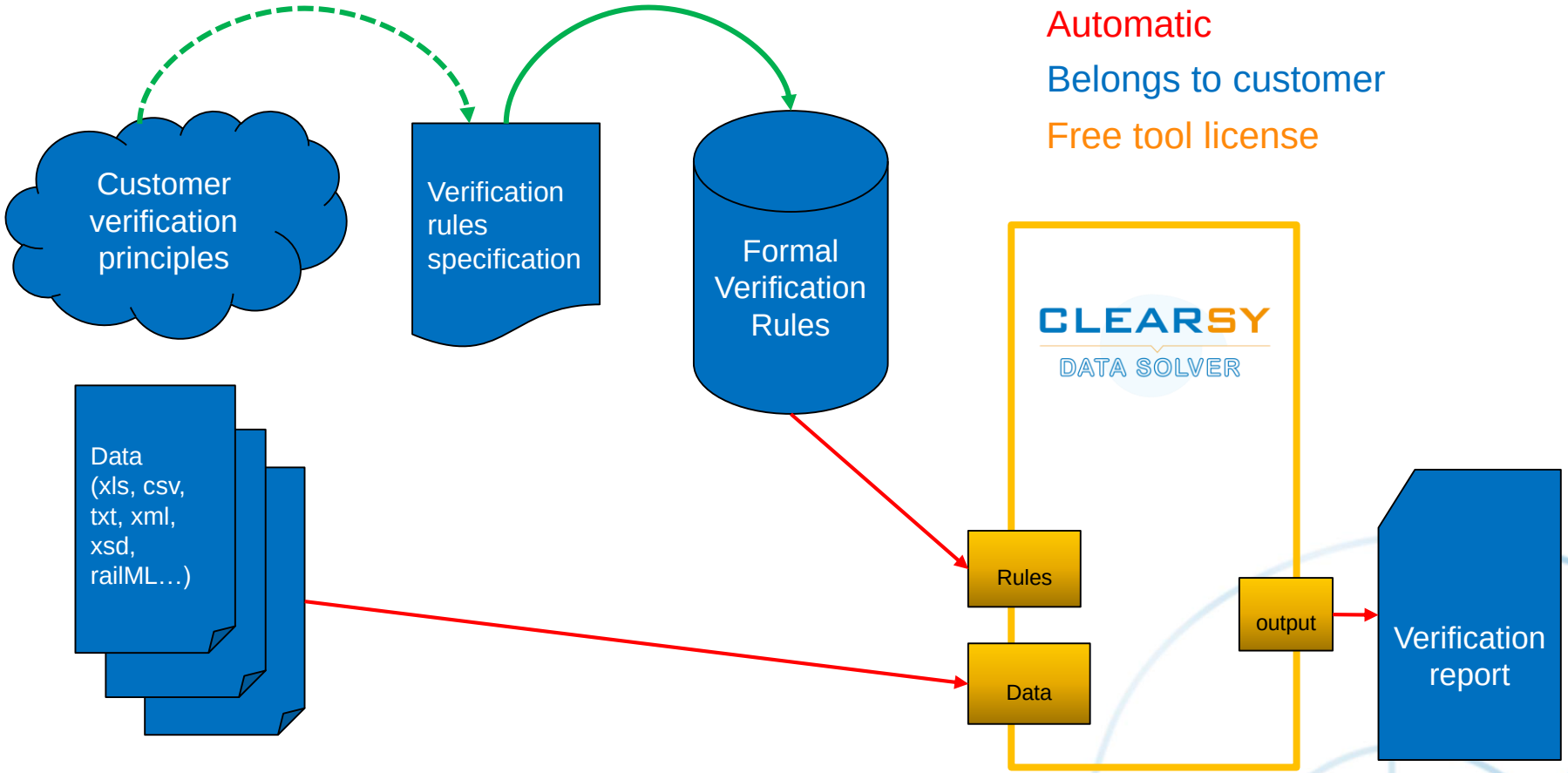
TOOL Principles

Manual activities by CLEARSY

Automatic

Belongs to customer

Free tool license



CLEARSY DATA SOLVER

- **A customized tool**
  - Will be adapted to the customers data file format (xml, xls, parameter file, railML, csv, txt …)
  - Will be adapted to the customers verification report documents and process: can be specified by the customers
- **The non-compliant outputs are expressed in natural language**
  - can be understood by the customer engineers
- **The list of non-compliant outputs are exhaustive**
  - When no error is reported, the correctness of the data set is guarantied
- **The End User can specify its own rules**
  - And use the same tool

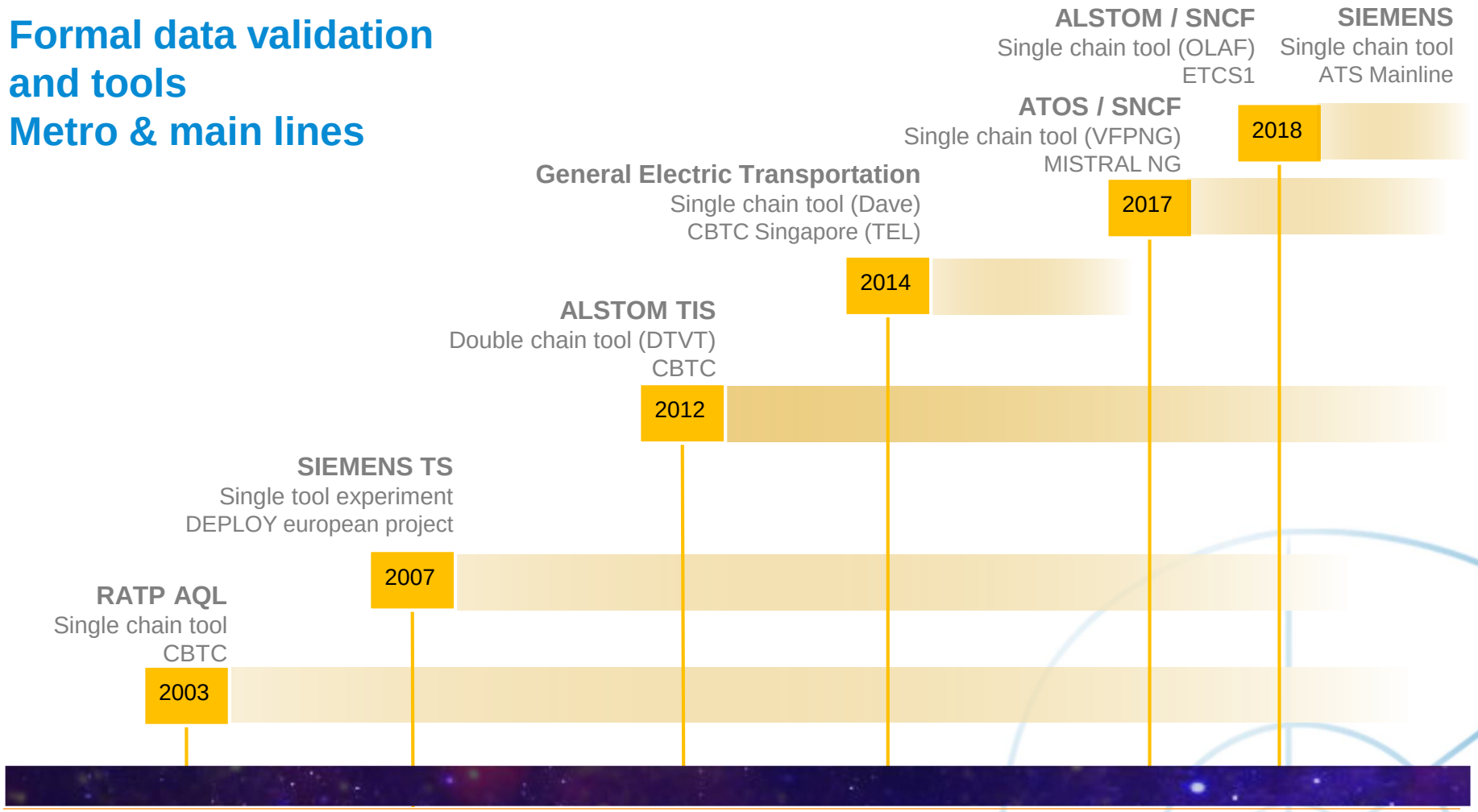
- **A service of formal rules modelling**
  - The tool is a solver: the data set is verified, rule by rule on all the data concerned
  - These project rules can be specified by the customer himself or by CLEARSY
  - This service is proposed by CLEARSY: Modelling the properties as a formal rule to be 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

Benefits

- **Why this approach is working well in the railways?**
  - Set theory is convenient to express graph-based properties, Boolean equations, etc
- **Formal (mathematical) model adds semantics**
  - **No ambiguity** : meaning fixed, to verify that the correct meaning has been chosen
  - No Implicit rules but Explicit: formal model may be (very) verbose
  - Better verification confidence
- **Mature tools**
  - More than 10 years of developing and optimizing the tools, based on internal research and development, and university research (ProB from University of Dusseldorf)
  - Can process industrial sized data
    - simple rules application takes seconds
    - complete verification within a couple of hours
  - Formal data validation is now required by SNCF for projects such as MISTRAL NG, ERTMS parameters and ATS+ parameters validation.

History: CLEARSY's experience

Formal data validation and tools
Metro & main lines



ALSTOM and GE references

CBTC

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

CBTC + Interlocking

- 2014-2016
- New tool created, faster and easier to use
- 1000 validation rules designed in 18 month
- Coverage of verified data

ATOS et SNCF references

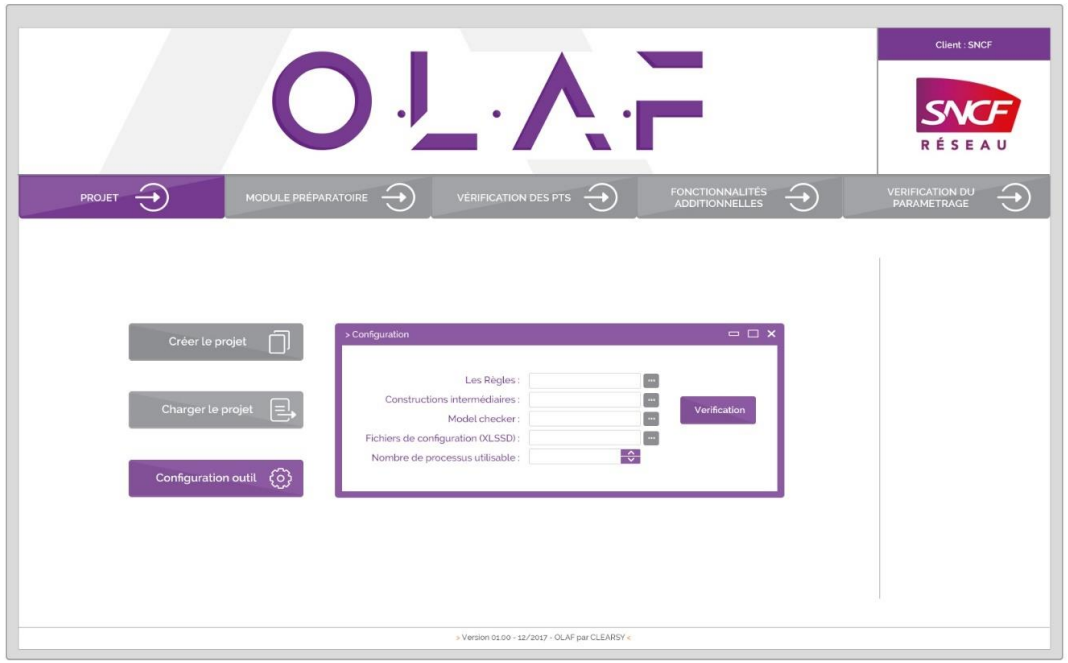
- **MISTRAL NG (new centralized command/control rail management system):**
  - Since 2017
  - New specific tool, customized by CLEARSY for ATOS and SNCF
  - New features: client-server architecture connected to a database of parameters to validation.
  - Additional rules designed specifically for SNCF (final customer)
  - Formal validation of:
    - Functional parameters
    - Technical parameters
    - Parameters consistency (example : XML vs XSD)

ALSTOM – SNCF reference

Formal data validation of ERTMS parameters

ALSTOM

- Since 2017
- New tool, customized for **Alstom and SNCF**.
- ETCS Baseline 2 level 1 with KVB fallback
- Compatibility for B3 braking curves



SIEMENS references

ATS and ATS+ Parameters (Mainline)

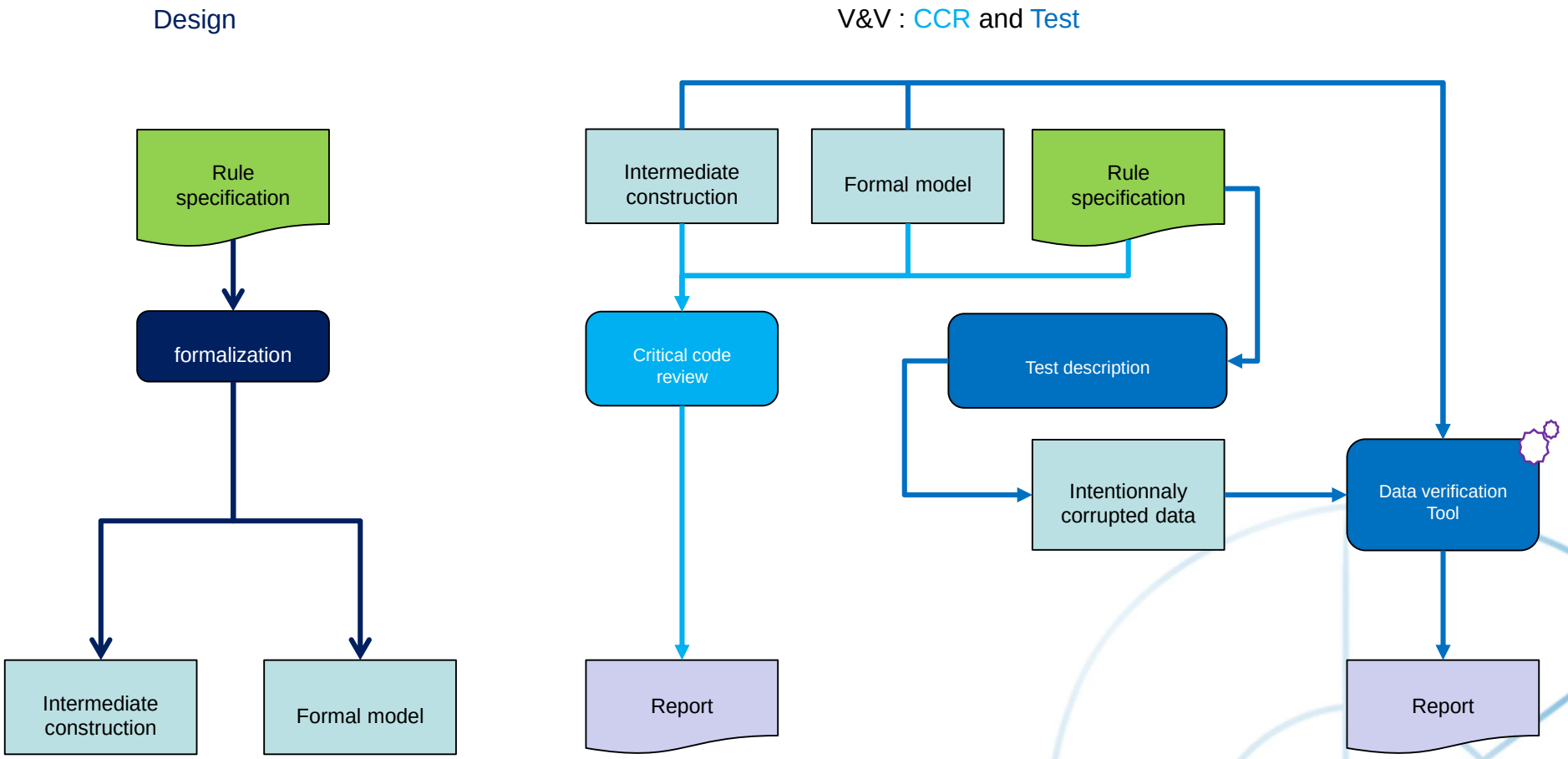
SIEMENS

- Since 2018
- New tool designed by CLEARSY, customized for Siemens
- Workshops to capture verification process
- Formal validation of graphical objects (.ilv files)

T2 certification

- The verification tool can be certified T2 according to CENELEC EN50128:
  - EN 50128 compliance matrix
  - All the documentation is provided
  - Redmine for issue tracking tool
  - Proof of independence between design and validation
  - Md5 of inputs and tools used for a verification campaign
  - Nightly non-regression tests

Design, validation & verification process mastered



Figures

- CLEARSY means:
  - 8 projects, as much tools designed
  - 5000+ rules created
  - 20+ trained engineers
  - Dedicated trainings
- New CBTC project: first iteration (1.000 rules)
  - Easy (70%): 1 day (design + validation, auditable process)
  - Medium (20%): 2/3 days
  - Complex (10%): 5/6 days
- Next Updated CBTC projects
  - Reuse 85%
  - New rules: 5%
  - Adaptations: 10%

Field-to-field comparison
simple property on data

Intermediate computations
more complex properties

Traversal algorithm
many fields requiring
optimization,
complex computation