# CLEARSY
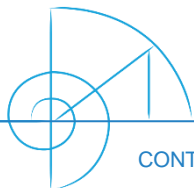
Safety Solutions Designer

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Safety railway
engineering and products
CLEARSY

CONTACT@CLEARSY.COM

# Independent French Company

▶ Created in 2001 by **the team authors of the ATELIER B**, famous formal method tool

▶ **Independent from any customer and owned by French ICE Group, founders and employees**

▶ 2023 turnover: **20 M€, 160 engineers & PhDs**

▶ **20% abroad**: Brazil, Chile, Luxembourg, Sweden, Norway, Switzerland, Belgium, Germany, Azerbaijan, Cameroon, Macao, Japan, USA, Canada, Italy …

▶ **Partnership with Paris metro** (RATP) to develop and deploy innovative custom safety solutions

▶ Partnership with factories to provide industrial equipment and local companies for exportation/distribution



Paris

Strasbourg

Lyon

Aix en Provence

# We are designer
## CLEARSY Offer

### Range of safety critical systems designed by CLEARSY - Products

▷ Supply of **safety systems already developed and in revenue service**

▷ Adaption of existing systems to specific requirements

### Safety critical systems design

▷ Design of **turn-key safety critical systems** (hardware and software) certified SIL2 to SIL4

▷ Prototype of safety critical system and proof of concept

### Safety critical software design

▷ Usage of **the B formal method to develop safety critical software** and to **prove system specifications**: formal specification and code verification

▷ Support for the software development toolkit: Atelier B, used by Alstom and Siemens to develop ATP safety critical systems

▷ Design of supervision and simulation systems

▷ Safety critical data validation

# ERTMS/ETCS CLEARSY Offer

## In-depth knowledge of ERTMS/ETCS:

▷ SUBSET 026, ERA DMI specification
▷ DMI development (SIL0, SIL2)
▷ Track plan editor
▷ EVC development

## In-depth expertise in Simulation and Testing:

▷ Training
▷ Testing (SUBSET 094, SUBSET 110/111/112)
▷ Train behavior simulation
▷ Trackside simulation (IXL, RBC, …)

Available tools developed by CLEARSY:

► **ETCS operational simulator**
► **ETCS traffic simulator – Track plan editor**
► **ETCS RBC test bench**
► **ETCS on-board unit test bench (EVC)**
► **Multi-platform DMI software**
► **Safety critical data validation software**

Available product developed with CENTRALP:

► **A SIL2 DMI**
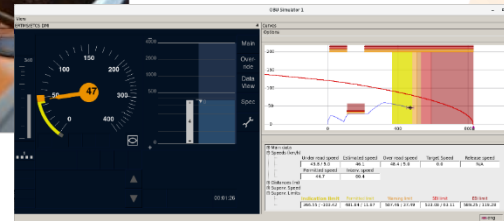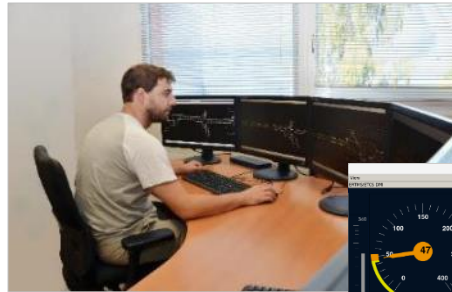
# ERTMS/ETCS
# 20 years of experience

## More than 20 years of Experience – since the very beginning of ERTMS

▷ Founded as part of the former **ERRI** (European Railway Research Institute – financed by the UIC – International Union of Railways) to develop the first ETCS simulator for the **project A200.**

▷ Our first mission: **translate complex details of Technical Specifications for interoperability (TSI) into a suit of tools for training and testing equipment**

## Reference in ERTMS

▷ Developed the **first ETCS simulator**

▷ **UNISIG** asked us to develop the first test bench for on-board systems

▷ The test bench was delivered to **CEDEX**, then **DLR** and **MULTITEL**, **3 well-known ERTMS laboratories in Europe that certify systems are compliant with TSIs**

▷ Helps the **ERA** (European Railway Agency) and the **ERTMS Users Group** in the consolidation of the specifications of Baseline 3

▷ Today, our set of tools is still helping companies **to develop and test their new ERTMS systems and train their collaborators**

UNISIG

EUROPEAN UNION AGENCY FOR RAILWAYS

ERTMS USERS GROUP

# Our Expertise

## Standards for railway safety critical systems

▷ **CENELEC** standards: EN 50126, EN 50128 and EN 50129
▷ **AREMA**

## Urban line – Metro and Light Rail

▷ **CBTC** (Communication Based Train Control): worked with the main suppliers on their Automatic Train Operation (ATO), Automatic Train Protection (ATP) and Automatic Train Supervision (ATS). Experienced with GoA2 to 4 operation
▷ **Signaling** - Realized several interlocking systems based on PLC and relays

## Main line – Regional trains and commuters

▷ **ERTMS** (European Rail Traffic Management System)
▷ **Signaling** - Realized several interlocking systems based on PLC and relays

# Railway clients and partners

# Design and implementation of certified safety critical systems and software

# Usage of B formal method

## Formal software development of ATP (CBTC)

▷ SIL4 sub-system Design, software Development, Verification & Validation

▷ ALSTOM (Urbalis), SIEMENS (Trainguard)

## Property-based formal system verification for authorities

▷ MTA (New York City) for CBTC

▷ SNCF for ERTMS level 2 and Hybrid Level 3

▷ RATP for CBTC

## Property-based formal software verification

▷ ALSTOM, SIEMENS, THALES, RATP

## Formal data validation

▷ ALSTOM, RATP, SNCF, THALES, ATOS, SIEMENS, SETEC

# Property-based formal system verification
## *Safety verification of the CBTC of NYCT*

NYCT entrusted us to demonstrate system properties are compliant with specifications and which assumptions need to be verified to ensure safety of daily operation

► **Save time**
  ▷ Address every design detail in the early phase

► **Enhance Safety**
  ▷ Define sufficient tests which need to be passed before daily operation
  ▷ Define tests for acceptance of subcomponents

► **Less dependent**
  ▷ Ease subcomponents integration thanks to a model of the system.
  ▷ Less dependent to one supplier
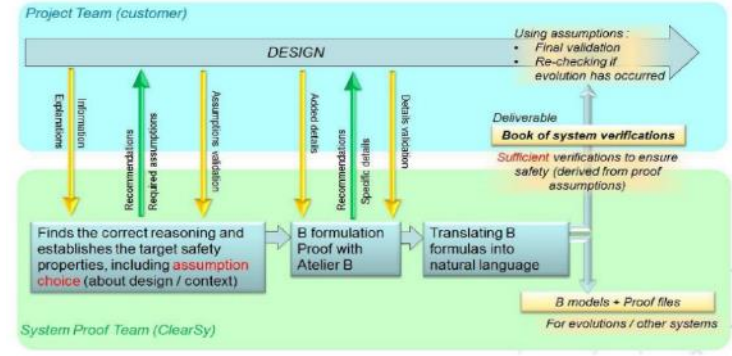


*This organisation was used for the NYCT project*

**System :** Method for **verifying the CBTC of the line 7 in New York**, for **CBTCs for Paris metro (RATP),** for **ERTMS** for **SNCF (Marseille Vintimille ETCS HL3**
**Software : ALSTOM, RATP**

# Formal data validation

## Ensure safety critical data/system parameters are correct

Safety critical software applications are developed and validated independently and each part must be safe at the same level: SIL4

CLEARSY proposes a **data validation tool** and its associated services.

**Advantages:**

▶ It is **fast**: a couple of hours is enough for validating a complete railway project. This speed can never be matched by human verification.

▶ It is **automatic**, **exhaustive**, push-button and **repeatable at will** (it avoids fastidious non-regression phase, easy iteration phases).

▶ 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 and the generic rules database).

▶ It is **T2 certified** (including ProB engine) for SIL4 project regarding Cenelec EN 50128.

▶ Targets = CBTC, Mainline, Interlocking, …

# Formal data validation principles T2 for SIL4 tool
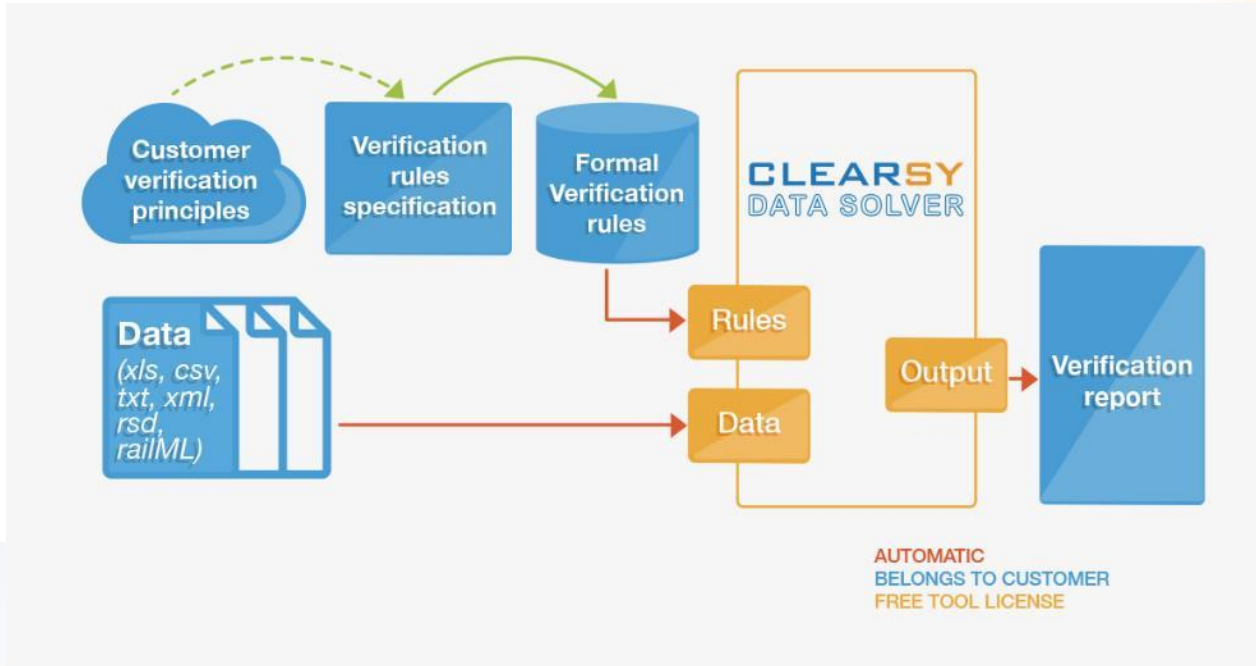
# CLEARSY has deployed its systems worlwide
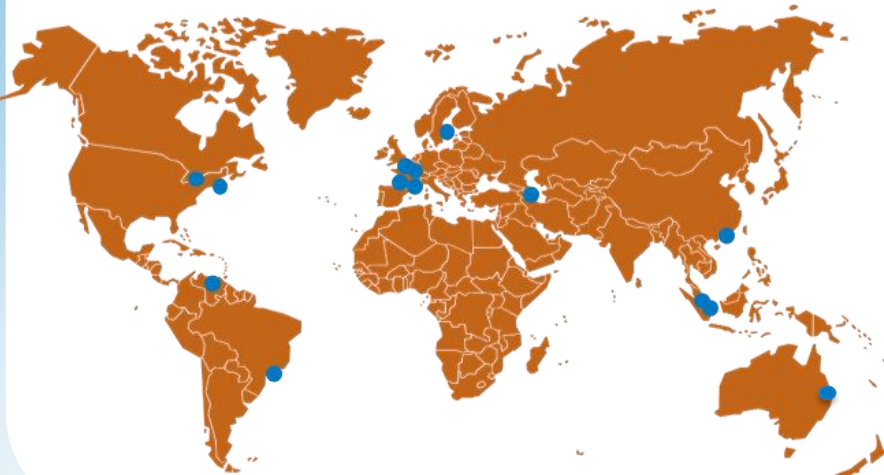
**Automatic train stop**

Deployed in Valenciennes, Nice, Lyon (France) and Baku in Azerbaijan, in deployment in Corsica France

**Overspeed control system**

Deployed in Paris (France) and Baku (Azerbaijan)

**PSD Control systems**

Deployed in Paris (France), Stockholm (Sweden), Sao Paulo (Brazil), Caracas (Venezuela), Kuala Lumpur (Malaysia), in deployment in Brisbane (Australia)

**Track intrusion detection system**

Deployed in New York (USA) and in Paris (FRANCE)

**Safety remote I/O network (SIL0, SIL2 and SIL4)**

In deployment in North America

**Supervision system**

Deployed in Paris, Grand Paris (France) and Honolulu (USA)

**RS4 safety critical relays (SIL4)**

Deployed in France, Luxembourg, Singapore, Greece, Turkey, Egypt, USA …

# Autonomous Platform Screen Door opening and closing systems

COPPILOT & DOF Systems

► **Independent** from any train control systems (ATC or only ATP) and signaling
► Can be installed on existing and new line, existing and new trains with existing or new train control system
► Connected to PSD controller

## SOLUTIONS FOR

**Metro authorities**

▷ Driverless turnback project

▷ PSD tests

▷ PSD operation before commissioning of a new ATC*

▷ Mixed operation during ATC deployment (new and old train mixed)

▷ Backup system to control PSD

**PSD supplier**

▷ Turnkey PSD project:

➜ Including safety critical control system on existing and new line

➜ Compatible with any types of PSD and interfaces (half, semi-full, full height)

**ATC supplier**

▷ PSD control managed independently of the ATC

*ATC: Automatic Train Control like CBTC, ETCS,…

# SIL3 platform screen doors control system
## with onboard equipment

*DOF System*

**PSD opening authorization when the train stops in the tolerance zone and train doors are opening**

**Onboard**
**1 Control Unit** + **1 Sensor,** per active cabin
**Wayside**
**1 Antenna** per stopping point
**1 Control Unit** per platform
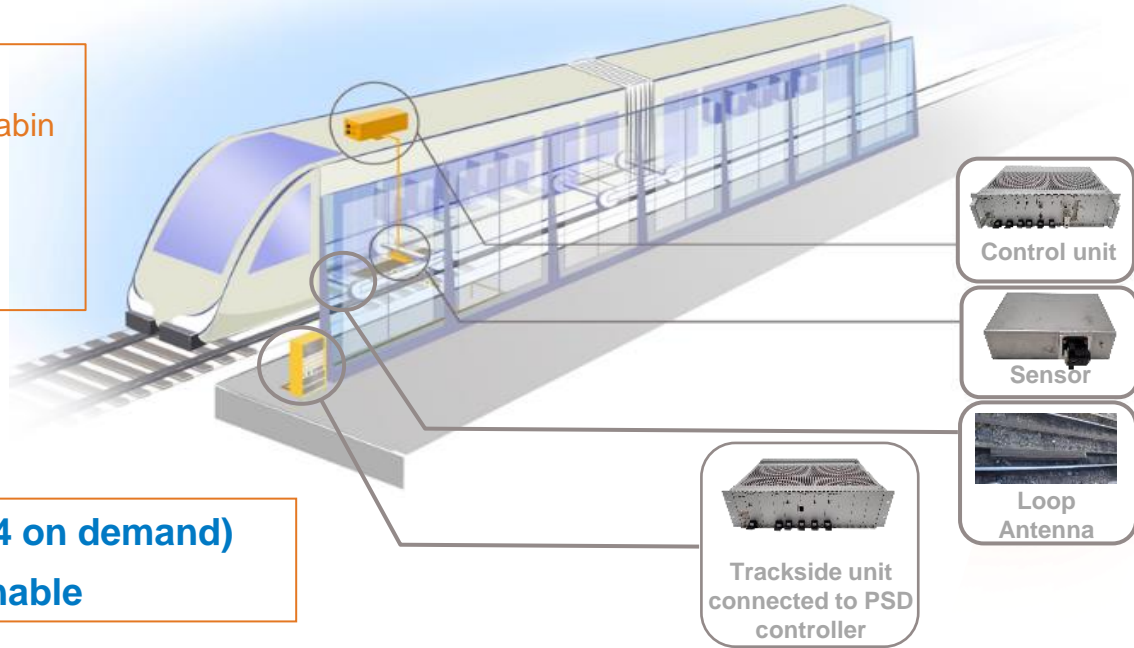
**SIL3:** **Door opening control (SIL4 on demand)**

**SIL4:** **Correct train side doors enable**

Control unit

Sensor

Loop Antenna

Trackside unit connected to PSD controller

# Proven product already in use

**Paris Metro Line 1** (four years of operation), in operation on Line 13 and 4

- DOF is independent from the CBTC system
- CBTC doesn't manage the PSD

**Upgraded version of DOF for Brisbane Metro**

- Doors selectivity: each opposite PSD and train doors are synchronized
- Opening adapted to different train lengths
- LAN connectivity and relays interface : Interfaced with PSD controller and train network

# SIL3 PSD control system
## with only wayside equipment

**PSD opening authorization as: the train stops in the tolerance zone and the train doors are opening**
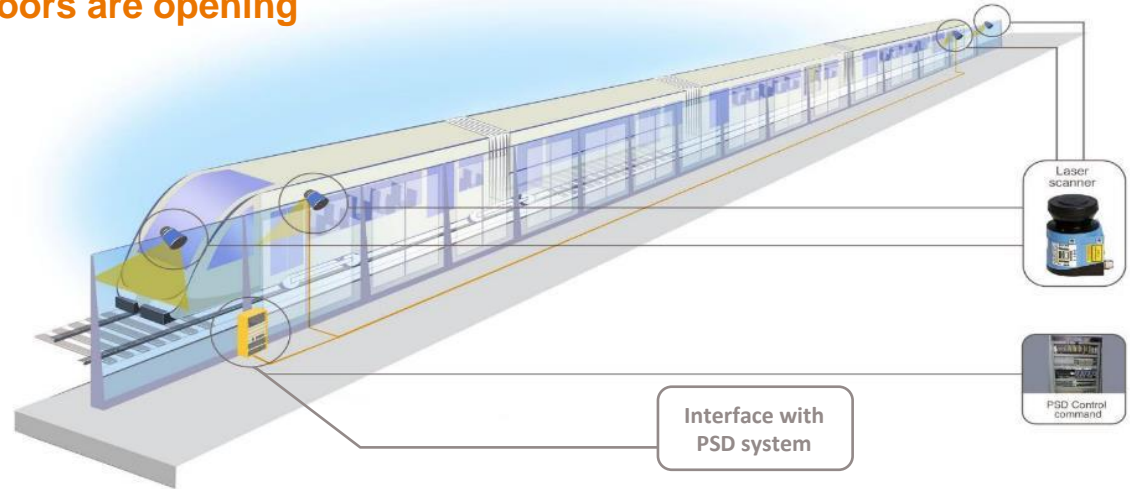


Laser scanner

Interface with PSD system

PSD Control command

SIL4 certified by CERTIFER EN50128:2011

SIL4 certified by CERTIFER EN50129:2003

SIL4 certified by CERTIFER EN50126:2000

▷ **No equipment on-board** only on the wayside

▷ 2 doors lasers detect: opening and closing of train doors managed by train operator

▷ Head and tail lasers ensure: correct train positioning and zero train speed

▷ **Based on SIL4 control unit**

# Easy-to-install on new and existing stations

▶ **In service in Sao Paulo Metro : Tamanduatei, Vila matilde, Sacoma, Vila prudente** (1st project in South America), deployment on line 1, 2, 3

- 2024: 7 stations in service and 2 more under deployment
- 143 trains shared on 3 lines, 7 train types : impossible to install equipment on-board
- Metro wanted an auxiliary SIL3 system to control PSD. COPPILOT was selected and became the main system to compensate late CBTC delivery…
- Driverless turnback project

▶ A monorail version in test for **Sao Paulo Monorail** line 15. It was upgraded for monorail application (SIL4). 13 stations will be equipped

▶ In service for 9 months in **Paris** during the **PSD test period**

- COPPILOT was chosen to manage 3 PSD from 3 different manufacturers of mechanical PSD on 3 platforms. RATP did not want any installation on the 65 trains during the test

▶ In service in **Stockholm**: 6 platforms in operation (2 stations)

- Additional functions: PSD individual opening, 2 trains lengths, platform berthing guidance, two way trains, and can handle 2 berthing positions
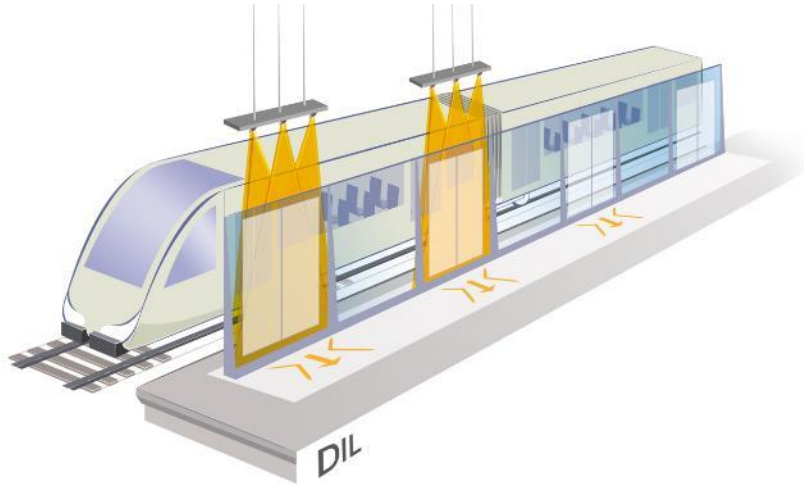- Adaption of PSD opening widths to where the train stopped for optimal train access

# SIL3 platform gap safety monitoring system

## GAP SAFETY MONITORING

▶ In operation in PARIS line 1, deployment in PARIS on Line 4, safety critical system

▶ System to detect a person in the gap zone between platform door and train door



Laser sensors monitoring gaps

# Monitoring these spaces
## *(DIL system)*
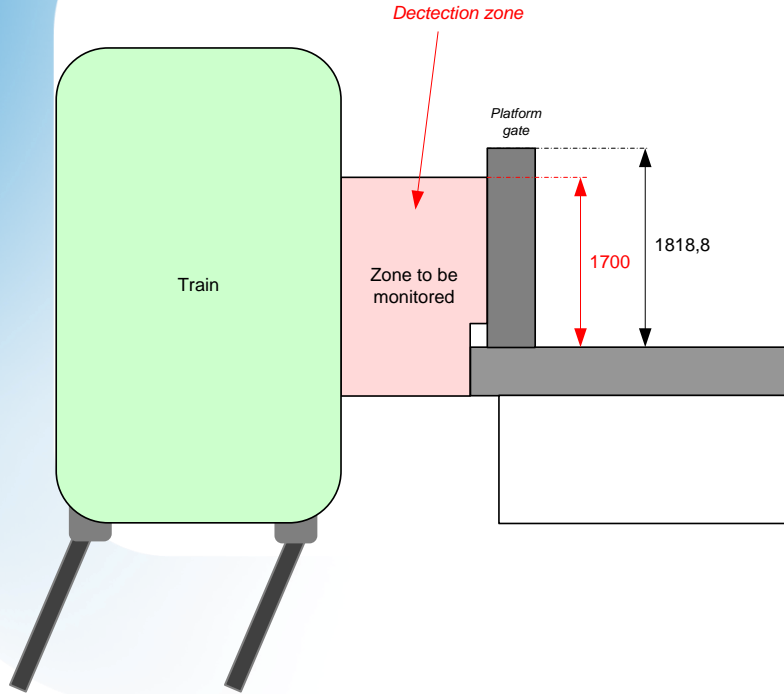


Bastille station in Paris

- ▶ Lasers are also used to detect people who try to escape into the tunnel
- ▶ In revenue service in 3 stations in Parisian network: Charles de Gaulle Etoile, Nation and Bastille
- ▶ In revenue service on Paris line 4

# Flexible gap filler
## *between platform and door edge on Paris&Lyon metro lines*

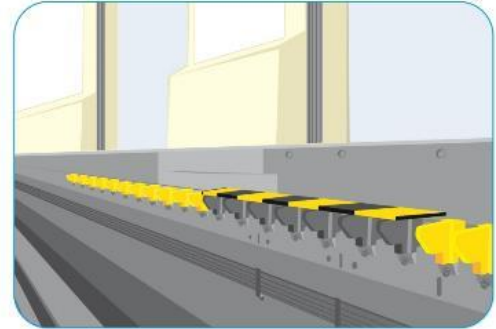► Gap filler prevents accidental fall if a person steps between platform and train

▷ Fixed on the platform

▷ Rubber material - Flexible

**Already in Service**

► Paris metro lines 1&4

► Lyon lines A&B

# Track intrusion detection system,
*Tested in New York City (MTA)*

## Detects falling passenger onto the tracks

► **Laser**

Pictures are analysed to discern an object as a rodent or a human

> **Accuracy is crucial:**
> To avoid false positive alarms

► **Alarm and Stroboscope**

They are activated to warn the train officer in the case of a person falling onto the tracks

Similar systems already in service in:

▷ **Lyon**: based on Infrared
▷ **Nuremberg**: based on radar
▷ **Budapest**: based on radar

# To detect platform and measure gap between train and platform (SIL2)

**All system components are mounted on board**

**ALSTOM**
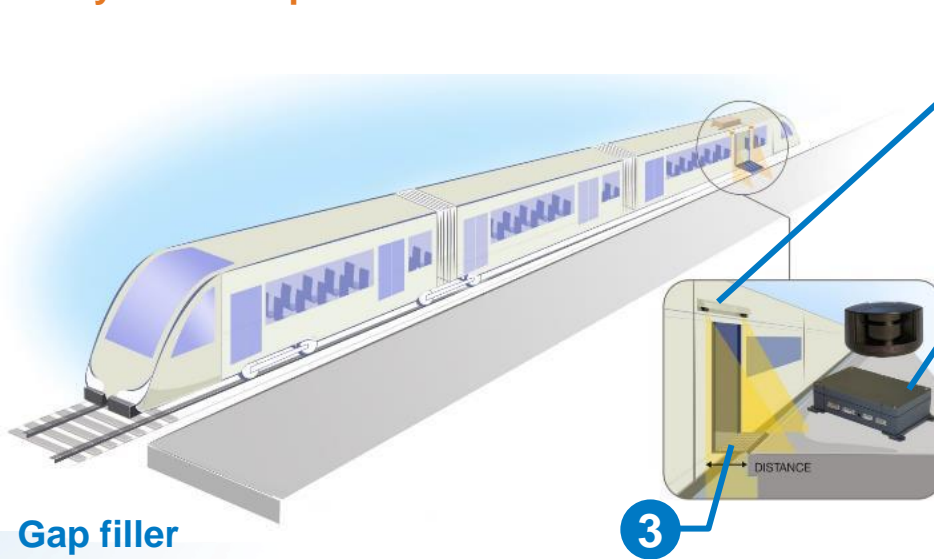
**1 Laser scanners**
*Measure gap between train and platform*

**2 Controller**
*Will authorise the car doors to open or/and the gap filler to move if platform is present in front of doors*

**3**

**DISTANCE**

**Gap filler**
*Is deployed to just fill the gap which is measured by the laser scanners*

SSIL2 certified by **CERTIFER** EN50128:2001

SIL2 certified by **CERTIFER** EN50129:2001

**operating on ALSTOM Train STI PMR**

# Automatic Train Stop (ATS) – *SIL2*
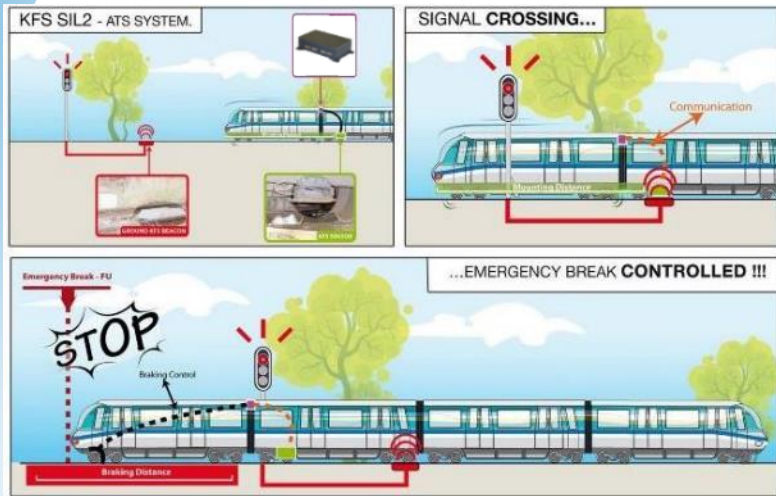
**1** Train operator is in charge of stopping the train when there is a restrictive signal and is responsible of the speed of the train.

**2** Emergency brake is applied if train overruns a restrictive signal

KFS musts be **HIGHLY AVAILABLE** and that's why SIL2 is enough.

*Ex: ATS system of Paris commuter trains is SIL0*

KPVA measures **instantaneous speed of trains** at defined point of the line and apply **emergency break in case of overspeed**.

# Automatic Train Stop (ATS) – SIL2

Railway - CENELEC
EN 50128 - EN 50129
**BUREAU VERITAS**
Certification

SIL2 certified by
CERTIFER
EN50128:2011

SIL2 certified by
CERTIFER
EN50129:2003

**KFS Beacon**

**KPVA Beacon**

**Sensor**

**Controler Unit**
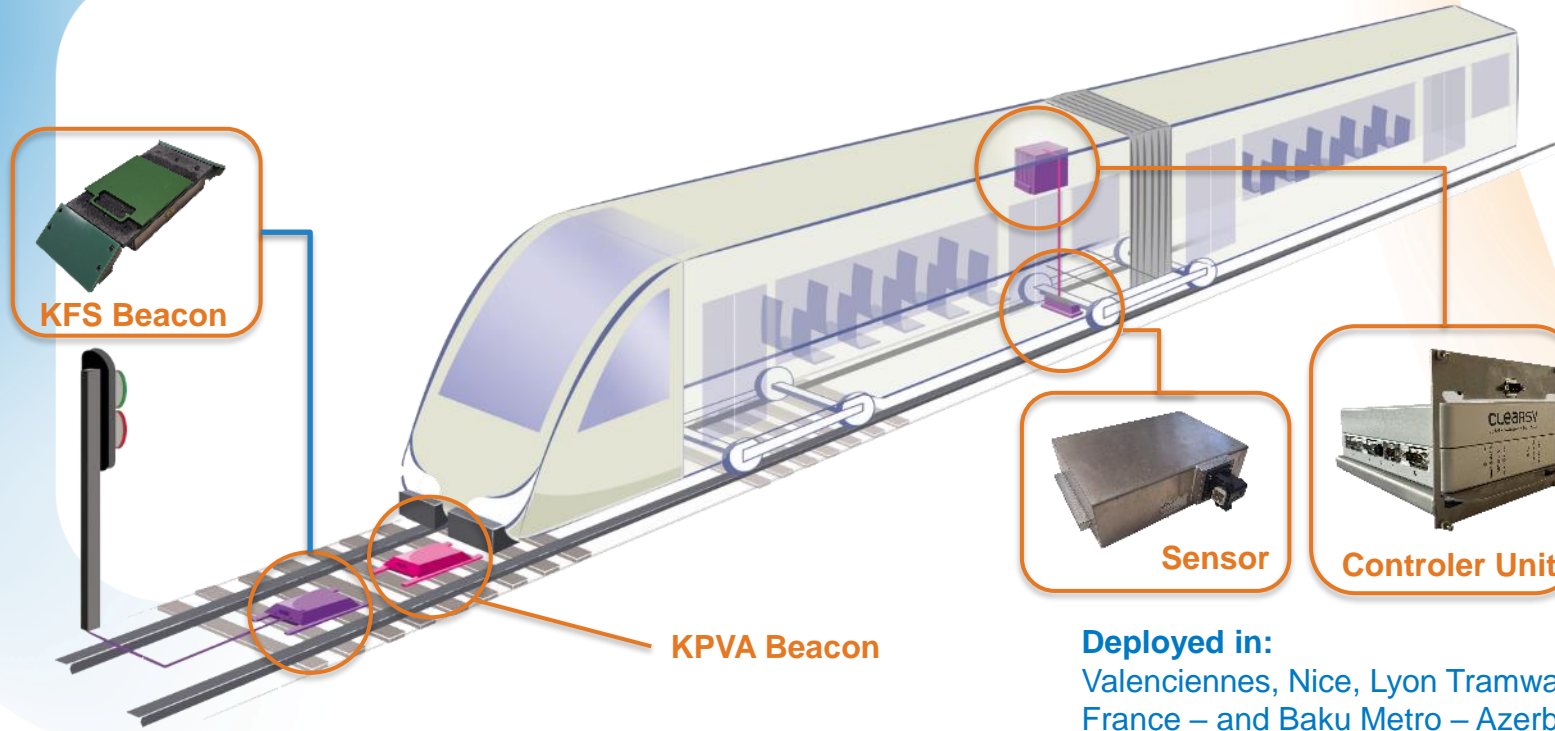
**Deployed in:**
Valenciennes, Nice, Lyon Tramway –
France – and Baku Metro – Azerbaijan
**In deployment in Corsica**

# Speed control by section
## *KFSV*

► Beacons installed on the track communicate the speed limits to the controller on board.

► Controller compares the speed limit to the train speed. In case of overspeed: **it applies emergency brake**

Direction of the vehicle

KFS-V beacon n°2

50 Track

KFS-V or KV beacon n°1

Section 2 | 30 meters | Section 0

Speed of the vehicle

Speed limit given by the beacon n° 2

Speed limit given by the beacon n° 1

Speed of the vehicle

Default speed limit

Position of the vehicle
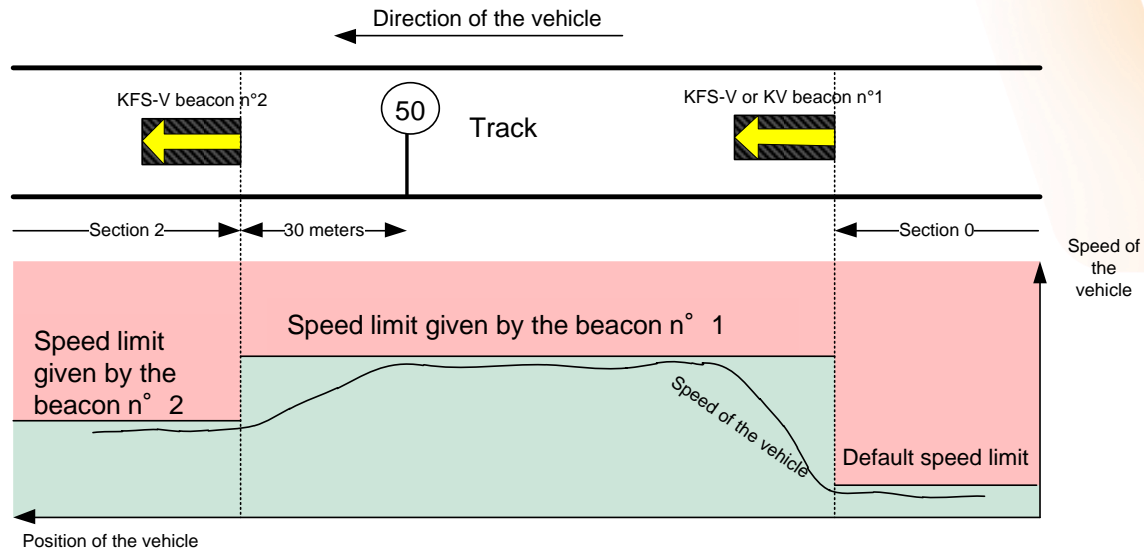
# Track vacancy detection - hyper frequency barrier
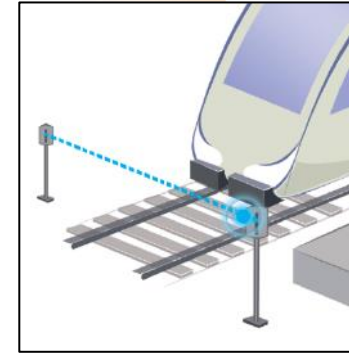## *In Research & Development*

Alternative to steel wheel sensor: when a train crosses the barrier, it is detected.

► SIL4 system

► Hyper frequency technology

► Less maintenance than infrared sensor:
**better availability**

► Fit for outdoor and indoor applications

► Plug and play system: system is very compact



tested in Lyon

# SIL4 certified vital relays
## *RS4*


SIL4 certified by CERTIFER EN50129:2018


SIL4 certified by CERTIFER EN50129:2003

**RS4 vital relay features:**

▷ Normally Open contacts guaranteed to open with a **Safety Integrity Level 4**\*

▷ **Weld no transfer contacts**

▷ Fit **onboard and trackside application** (vibration, shock, environment,…)

▷ Sealed contacts to assure **making contact at low current** (4mA at 1 VAC and 1VDC)

▷ **DIN mounted or 3U**

▷ **Small size** and **light weight**

| REFERENCES | SIL4 NO CONTACTS | NC CONTACTS |
|---|---|---|
| RS4.DIN.202.24V | 2 | 2 |
| RS4.3U.202.24V | 2*2 (2 relays 202) | 2*2 |
| RS4.DIN.304.24V | 3 | 4 |
| RS4.DIN.402.24V | 4 | 2 |
| RS4.DIN.406.24V | 4 | 6 |
| RS4.DIN.202.110V | 2 | 2 |
| RS4.B.24.0.24 | 24 contacts right and left | |

DIN packaging, Relays ▶



◀ Relay 3U card packaging



◀ Latching interface system
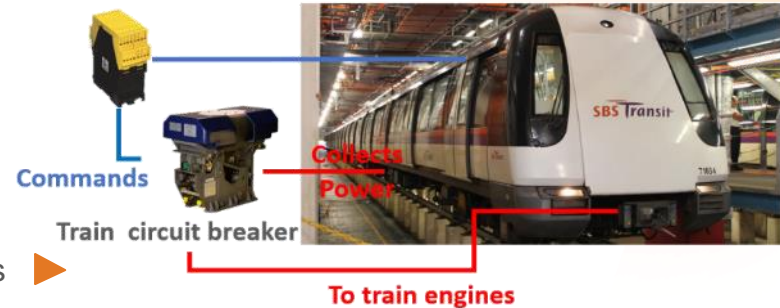24 NC and 24 NO contacts
6U card packaging

\*SIL4: Probability of the NO contacts not opening is of 10-8 per hour

# RS4 vital relay applications

▶ Safety interface relay for SIL4 PLC
  ▷ Inputs and outputs
  ▷ Galvanic isolation of 2kV (AC)
▶ Closed and locked signal contacts commanded by door control unit of platform screen doors
▶ Safety relay for onboard applications
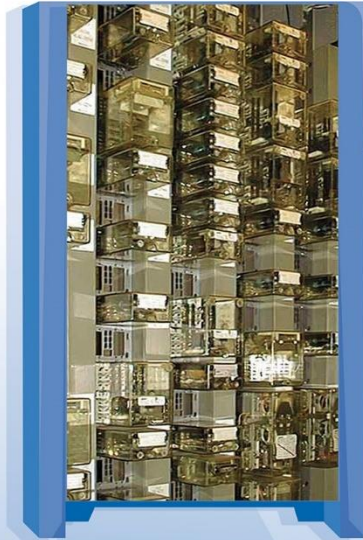  ▷ Control train traction circuit breaker



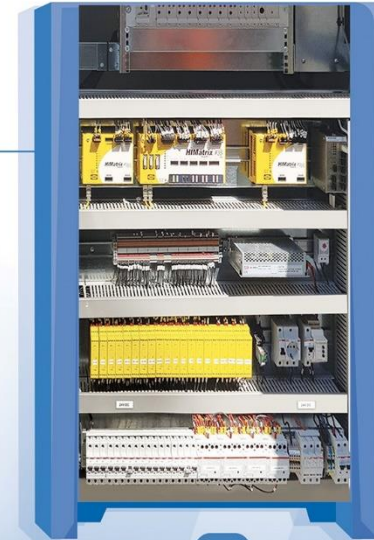**LUXTRAM** - Luxembourg tramway ▲

RS4 controls circuit breakers ▶



Commands

Collects Power

Train circuit breaker

To train engines

# Safety remote I/O network (SIL0, SIL2, SIL4)
## *SATURN*

## Reducing wiring for onboard or trackside application

▶ Replace wiring by a safety network

▶ Non standard open source communication protocol

   Protocole compatible EN50159

▶ Different safety level modules on the same network

▶ Industrial network response time: 10 to 15 ms

▶ Data rates: 12 Mbits/s over 100 m

▶ 3U packaging

▶ Up to 512 Inputs/Outputs

▶ Partnership with: Leroy Automation



SIL2 certified by CERTIFER EN50129:2003

MIXED SIL0, SIL2, SIL4 I/O NETWORK
CONTROL, MONITORING AND DIAGNOSTIC

SATURN

# CLEARSY Safety Platform

## Low-Cost safety execution platform for SIL4 application

▶ A **complete software development environment** based on **formal language** (B mathematical language) and using a double compilation chain (certified T3)

▶ A **computing platform** that **natively integrates safety principles** (5cm x 8cm)

▶ A **safety controller : 3U rack including 4 Inputs / 3 Outputs and 1 ETHERNET base 10/100 TX**

▶ **Starter kit : non safety mother board 32 I/O**

**+**

**Ease development of SIL4 certified systems and software**

**Drastically reduce the time and effort to certify (80%),** SIL4 generic certificate supplied

**Drastically reduce costs** associated with their development



SIL4 certified by CERTIFER EN50129:2018

SIL4 certified by CERTIFER EN50128:2011

SIL4 certified by CERTIFER EN50126:2017

# DAME
## *Railway custom SCADA*



► **Custom SCADA for small and large applications or systems:** **flexible architecture**

► **Extend on demand the range of supported devices and protocols**

► **Interface with SCADA available on the market:** *data preparation, component status*

► **Real-time supervision of large complex systems (PLC, digital I/O devices, …)**

► Real-time calculation and alarms triggering

► Collecting and archiving of input data

► Archiving of **alarms**

► Provides data and alarms in HMI, Modbus, OPC
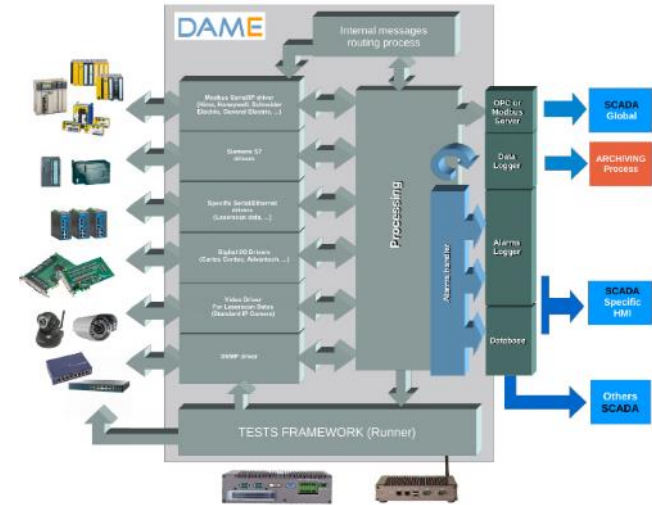
**RATP** line 1 on 3 stations (DIL): PLC and laserscan data

**Sao Paulo Monorail** line 15 (COPPILOT): Modbus IP, Laser sensors data, video (13 stations)

**Caracas Los Teques line** (6 stations) (COPPILOT): PLC, Modbus IP server (export to SCADA)

**Honolulu Line** (21 stations): I/O board, RS485 (ATC), Modbus RTU (Doors Control Unit)

# SIL2 centralized supervision system of fire safety systems



Screen 1

Screen 2

► Forwards fire safety data (alarms and equipment statuses) **from stations to the command centre**

► Examines fire safety equipment and its own system status

► Informs officers in charge of fire safety, on a real-time basis about any events occurring on the supervised network.

► Supplies the operating system with all the **data necessary for the first inspection prior emergency procedure**

► **Remotely controls in SIL2 (IEC 61508 (edition 2) – Parts 1 to 4), the safety devices on site**

► Continuously controls data validity (alarms, command execution)



BUREAU VERITAS
Certification

# Supervision system certified, approved and interoperable

► Suitable to supervise fire systems of **public-access buildings**

► Approved by **the CNPP**, the French association for risk prevention and control (article GA44.2) and Certified **SIL2**

► **Interoperable:** work on hardware from any manufacturer

► **Flexible:** can be interfaced with many different fire safety systems

In deployment in **Paris Metro (RATP):** it centralizes supervision of all fire safety systems of the Paris metro network, and **in "Grand Paris",** the extended commuter and metro network of Paris area



CNPP

RATP

Société du Grand Paris

EN SERVICE
EN COURS
A VENIR
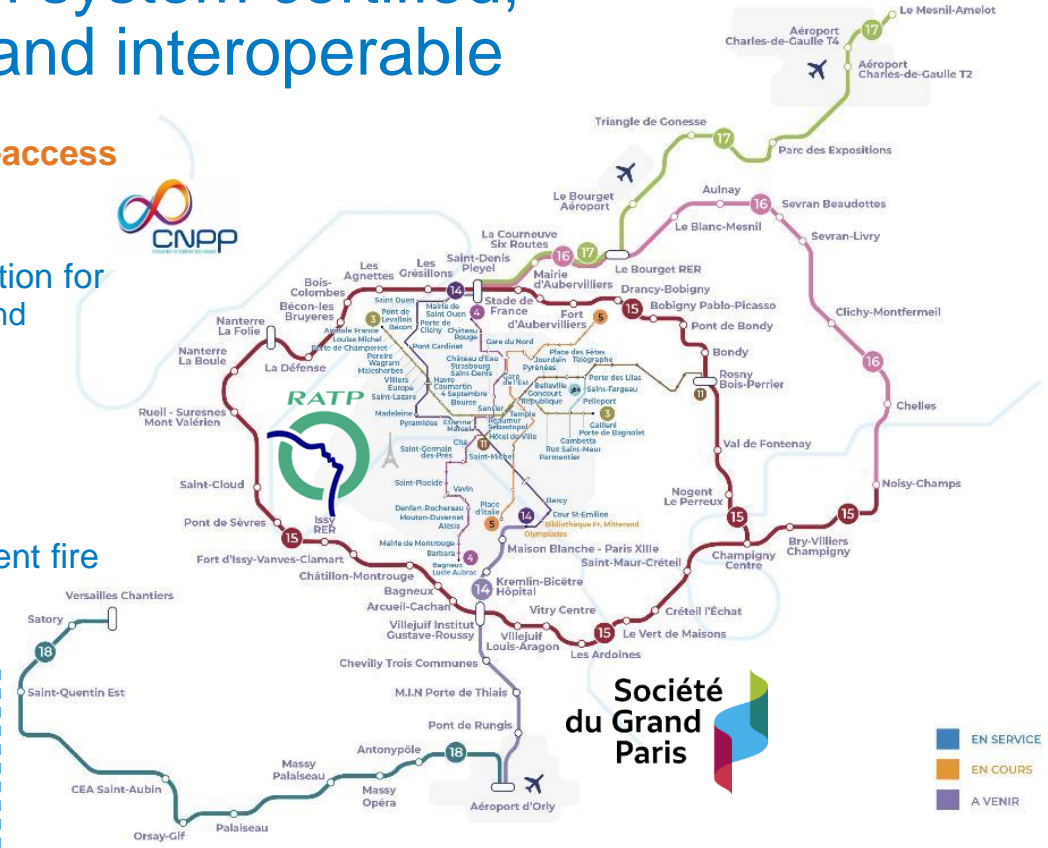
# Complete SIL2 DMI and SIL2 associated generic platform

▶ ETCS baseline 3 DMI Based on a **generic SIL2 platform**
▶ The specific customer HMI application can be added and doesn't change the certificate
▶ DMI manages safety features according CENELEC SIL2
▶ EN 50126 (RAMS), EN 50128 (Software), EN 50129 (Hardware)
▶ SUBSET 026 v 3.6.0 chapter 4.7 / ERA specification v 3.6.0 / SUBSET 091 v 3.6.0

| Certification | SIL2 certified by CERTIFER EN50126:2000 | SIL2 certified by CERTIFER EN50129:2003 | SIL2 certified by CERTIFER EN50128:2011 |
|---|---|---|---|
| **Software developed by CLEARSY** | | **Hardware developed by CENTRALP** | |
| | | **CENTRALP** Embedded electronic systems | |

# ETCS operational and traffic simulator

## Operational simulator

Build a real-time visualization of a train running under ERTMS supervision

- ► Predefined track side messages
- ► Simulated RBC messages
- ► Standalone
- ► Baseline 2 or Baseline 3
- ► First version in 2005
- ► Running on Linux

## Traffic simulator

Build a detailed engineering model of a complete railway running under ERTMS

- ► First version released in 2002
- ► Simulators for all parts of ERTMS:
  - ▷ IXL
  - ▷ RBC
  - ▷ Automatic route setting
  - ▷ Trains
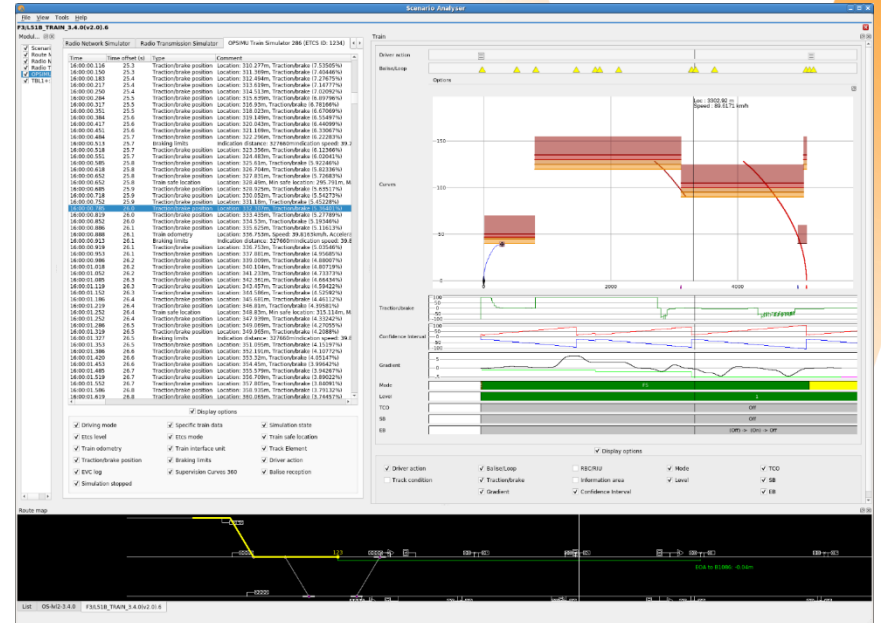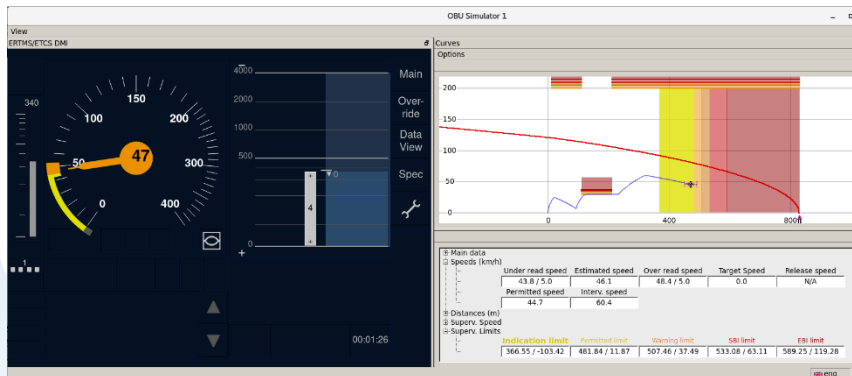- ► Can include multiple OPSIMUs w/o 3D



*Traffic Simulator*

# ETCS On-board unit test bench

## Testing of industrial on-board units

► First version in 2001 (EMSET EU project)

► Interfacing via SUBSET-094

# ETCS RBC* test bench

## Testing of Radio Bloc Centre (RBC)

► First version in 2009

► Based on Traffic Simulator

► Trackside simulators replaced by industrial equipment

► Simulated trains

► Enables connection with OBU Test Bench

► Enables integration of SUBSET-111-2 to perform IOP tests (TVS)



*RBC Test Bench hardware installed in a cabinet together with tested equipment*

# Contact

► www.clearsy.com

► contact@clearsy.com

► 320 Av. Archimède – Les Pléïades III
13100 Aix-en-Provence
FRANCE