CLEARSY
Safety Solutions Designer

MARCH
2021

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

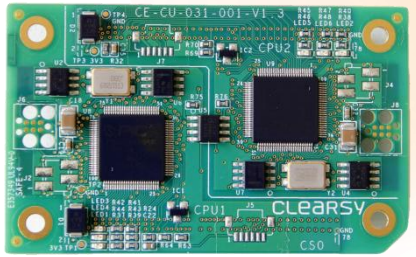
CLEARSY Safety Platform SIL4

Low-Cost safe execution platform for SIL4 applications

CONTACT@CLEARSY.COM

Aim of CLEARSY Safety Platform

- Development and deployment of safety-critical applications, up to SIL4
- A comprehensive and consistent framework that natively integrates safety principles and eases the design of safety critical system
- For designing cyclic or acyclic applications running directly on the hardware without any underlying operating system
- Drastically Reduce the time and effort required for certification (- 80%)

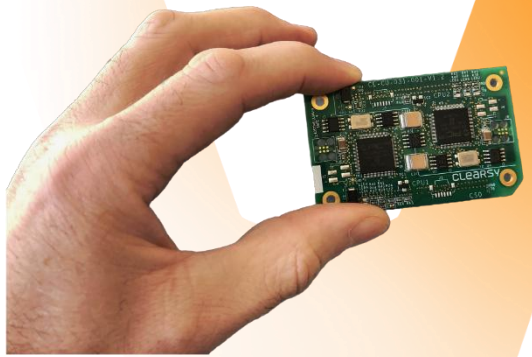


2oo2 microcontrollers

Main features

Ready for industry

Provided as a daughter board (8*5cm) with certification kit to be included in in-house designs



- The hardware peripheral blocks of this technology have already been **certified (SIL3 and SIL4)** in several railway projects worldwide
- Safety principles are out of reach of the developer who cannot alter them
- The vital computer board of the CLEARSY Safety Platform could be
  - adapted to another specific development process used by the customer
  - associated with other instances of the vital computer board to improve availability or computing performances

Platform composition

Safety on hardware

- Based on 2oo2 PIC32MX microcontrollers
- Offers up to 80 MIPS for lightweight applications
- All interfaces from PIC32MX are available in order to address customer's requirements (I/O, analog, communication bus, …)

Safety on software

- Based on 4oo4 software
- Correctness is ensured by mathematical proof
- Cross checks between software instances and between microcontrollers

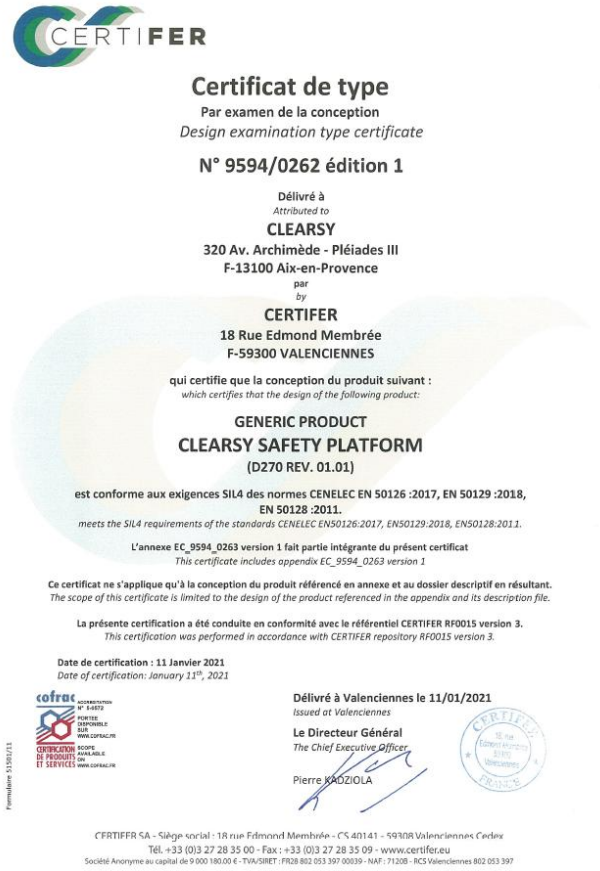
SIL4 certified Solution

- The CLEARSY Safety Platform has been certified SIL4 by CERTIFER
  - Certificate n°9594/0262

SIL4 certified by CERTIFER EN50126:2018

SIL4 certified by CERTIFER EN50128:2011

SIL4 certified by CERTIFER EN50129:2018



CERTIFER

Certificat de type

Par examen de la conception

Design examination type certificate

N° 9594/0262 édition 1

Délivré à
Attributed to

CLEARSY
320 Av. Archimède - Pléiades III
F-13100 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:

GENERIC PRODUCT
CLEARSY SAFETY PLATFORM
(D270 REV. 01.01)

est conforme aux exigences SIL4 des normes CENELEC EN 50126 :2017, EN 50129 :2018, EN 50128 :2011.
meets the SIL4 requirements of the standards CENELEC EN50126:2017, EN50129:2018, EN50128:2011.

L'annexe EC_9594_0263 version 1 fait partie intégrante du présent certificat
This certificate includes appendix EC_9594_0263 version 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.

La présente certification a été conduite en conformité avec le référentiel CERTIFER RF0015 version 3.
This certification was performed in accordance with CERTIFER repository RF0015 version 3.

Date de certification : 11 Janvier 2021
Date of certification: January 11th, 2021

Délivré à Valenciennes le 11/01/2021
Issued at Valenciennes

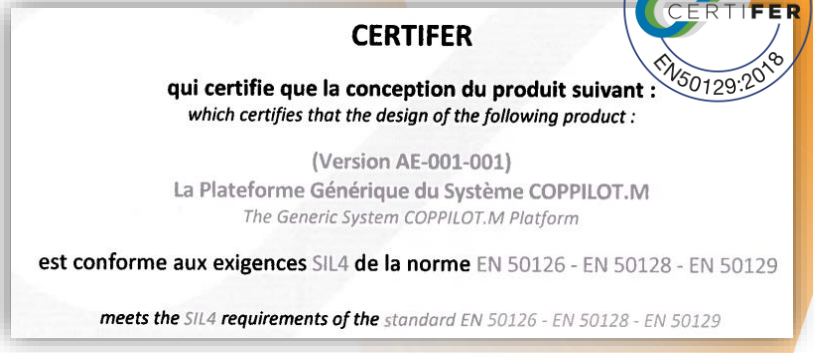
Le Directeur Général
The Chief Executive Officer

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 9 000 180,00 € - TVA/SIRET : FR28 802 053 397 00039 - NAF : 7120B - RCS Valenciennes 802 053 397

Background & references

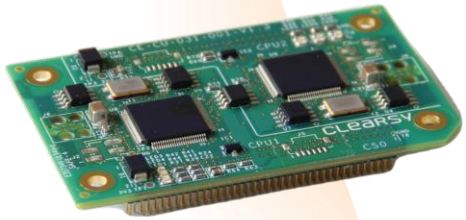
- 1st design of CLEARSY SIL4 processing architecture: for platform screen door operation, **monorail Sao Paulo line 15**
  - Generic product certificate, CERTIFER #8891/200-1 27th Feb 2017 **SIL4**
- Product fitted for **Stockholm City Line** platform screen door operation
  - System certificate BUREAU VERITAS #6393741 3rd March 2017 **SIL3**
- Supported by the *LCHIP project consortium since 2015*
- New design for **CBTC** input / output module (*customer confidential*)
  - Generic product certificate BUREAU VERITAS #7092509 23rd July 2019 **SIL4**
  - Also **AREMA** compliant (asserted by TÜV)

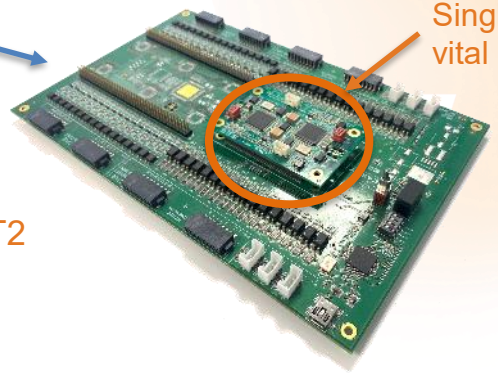


Generic industrial product

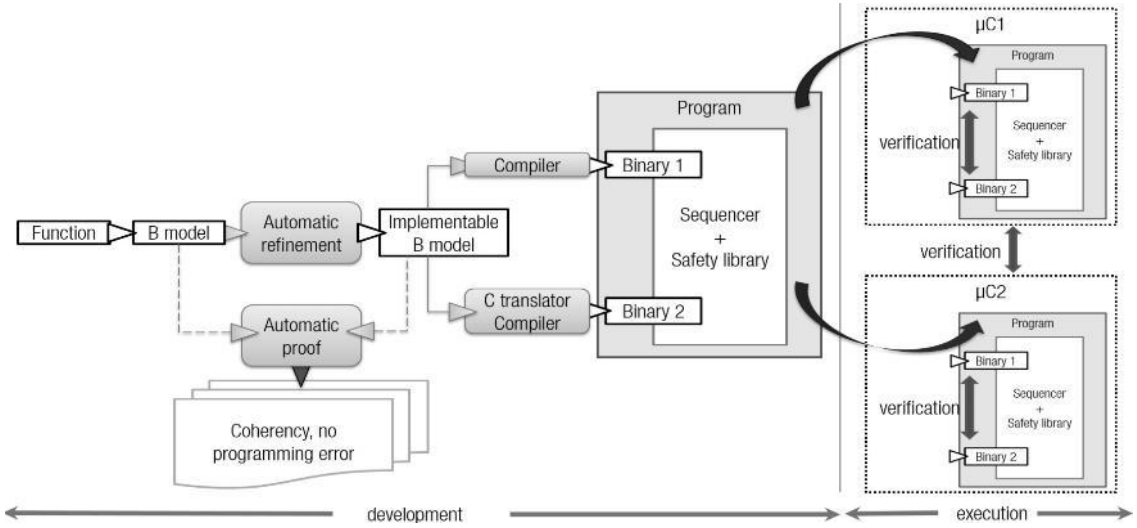
CLEARSY Safety Platform is made of:

- Vital single board computer
  - 5 cm X 8 cm, pluggable or solderable
- Starter kit
  - Motherboard connected to this board
    - Learning resource
    - Prototyping
    - Proof of concepts
- SIL4 generic certificate
- Development suite
  - Double compilation chain T3 (EN50128:2011)
  - Configuration tools T3 (EN50128:2011)
  - Possibility of developing formal application, based on Atelier B T2 (EN50128:2011)
- User manuals & application certification guide





Double compilation chain



- Code generation from a formal model (mathematical proof against its specification) and guarantee of no programming error.
  - *But the implementable B model can also be obtained using other methods / languages*
- Detection of divergent behavior (by this design)
- Based on a hardware/software dual processor architecture **patented** by CLEARSY
- Toolchain and generation process included in the SIL4 certificate

CLEARSY offer

CLEARSY Safety platform offers

Hardware solution:

Starter kit

Board ready for prototyping

Safety board ready to integrate on system

Layout &/or schematic ready to integrate in a design

Software solution:

IDE to develop safety systems

Tools to prove the software compliance

Tools to load and debug software

Services:

Certification Kit &

Support for certification

Support for hardware and / or software design

Design / industrialize specific safety products based on CSP

Training and assistance to engineer

Interfaces

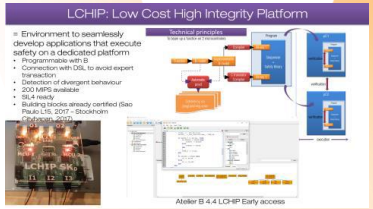
- The vital computer board offers at board level the following HW interfaces:
  - 13x Analog to digital converter (10 bits 1Msps)
  - 19x Change notification Inputs
  - 5x Capture inputs
  - 6x Outputs Compare (PWM HW)
  - 5x External Interrupt pins
  - 63x General purpose Input Output
  - 4x UART
  - 2x SPI
  - 4x I^2C
  - 2x Comparators
  - 1x Parallel Master Port (16 bits)
  - 5x PWM output
  - 1x USB
  - 2x CAN (Controller Area Network)

Interfaces

- Thanks to this panel of HW interfaces CLEARSY has already developped on system operated in revenue service the following interfaces
  - SIL4 double cut interface (with safety electromechanical relays)
    COPPILOT.M product (max current 8A voltage up to 220VAC)
  - SIL4 double cut interface (with safety electromechanical relays ans solid state relay with ultra high reliability and flashing capability)
    Remote IO product max current 200mA from 5VDC to 220VAC with SIL4 guaranteed flashing – for signals)
  - SIL4 frequency input
    Saturn product (72-110VDC hardwired train lines)
  - SIL4 digital input based on optocoupler
    Remote IO product (5VDC-64VDC digital input)
  - Interface with computing unit of LIDAR and other laser based sensors
    COPPILOT.M product
  - Train/wayside wireless SIL4 communication (near field magnetic communication)
    DOF1-L product
  - SIL4 custom proprietary communication based on Ethernet over fiber
    Remote IO product (100Base FX UDP custom protocol 125kB/s over 20km)
- Each of this interfaces can be included and/or adapted for your custom project.
- Possible to develop new custom interfaces

Dissemination and references

- Conferences
  - **Conference FM** 2018 (Formal Methods) – Oxford **UK**
  - **Conference RSSR 2017** (*Reliability, Safety and Security of Railway Systems: Modelling, Analysis, Verification and Certification*) - Pistoia **Italia**
  - ***Ecole Doctorale ETMF 2017*** (Escola de Informática Teórica e Métodos Formais) - Recife **Brasil**
  - **Conference SBMF 2017** (Brazilian Symposium on Formal Methods) – Recife **Brasil**
  - **Conference GRTMS** (Global Conference on Signalling : the Evolution of ERTMS) - Milan **Italia**
- Training
  - Newcastle (**UK** - NewRail Centre for Railways Research) 02/2018
  - Montreal and Sherbrooke (**Canada**) - 04/2018
  - Niteroi / Pirnamirim / Natal (**Brasil**) - 05/2018



Summary

Already SIL4 certified industrial platform for easing safety critical system design

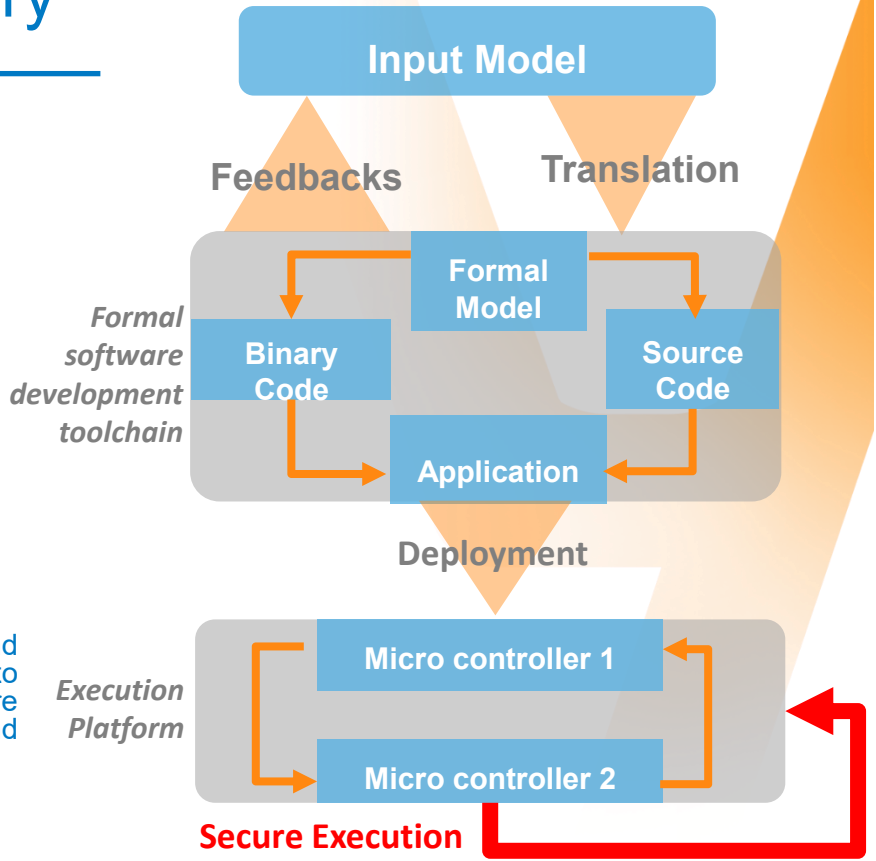
CLEARSY Safety platform combines:

- **A complete development environment** in formal language (B mathematical language)
- **A safety processing platform** to safely execute programs

Purposes of the platform are:

- **Ease development** of SIL4 certified systems and software
- **Drastically reduce costs** associated with their development and certification

The end user only needs to design his/her own hardware interfaces and to perform the safety analysis of his/her business application. Thanks to the SIL4 certificate of the CLEARSY Safety Platform, all the usual failure modes of a computer board do not need to be addressed by the end user.



Contact

- contact.csp@clearsy.com
- https://www.clearsy.com/en/our-tools/clearsy-safety-platform/

Parc de la Duranne
320 Av. Archimède – Les Pléïades III
13100 Aix-en-Provence
FRANCE