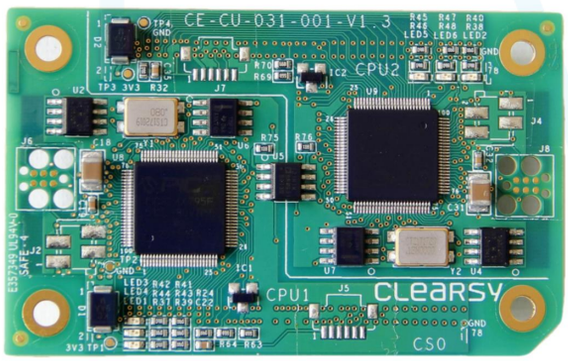
clearsy

Safety Solutions Designer

TECHNICAL DOCUMENT CLEARSY

CLEARSY SAFETY PLATFORM

Vital computer for SIL4 applications



SIL4 certified by CERTIFER EN50126:2017

SIL4 certified by CERTIFER EN50128:2011

SIL4 certified by CERTIFER EN50129:2018

FRANCE

CLEARSY Safety Platform: simplifying SIL4 systems design

Since its creation in 2001, CLEARSY is a major player in the industrial use of formal methods to improve the functional safety of systems and critical software.

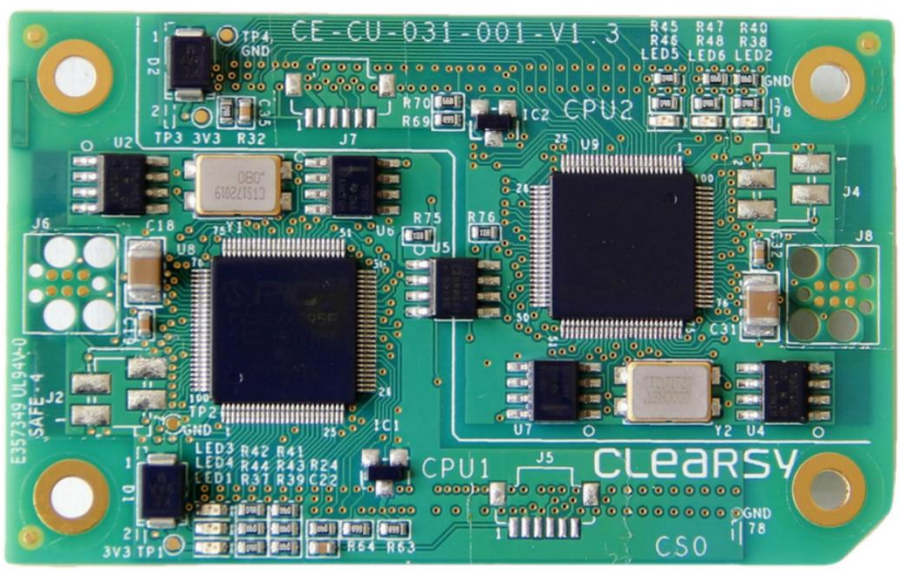
Based on its 25 years of experience, CLEARSY has designed the CLEARSY Safety Platform**: a certified single-board composite failsafe computer (per EN50129 definition)**. Thanks to this innovation, the end-user can now focus only on designing his custom business system/application, saving the complexity and costs associated with the design and certification of processor safety software layers. According to existing use-cases, the CLEARSY Safety Platform allows a reduction of up to 80% of the design cost and certification effort, leading to a shorter time to market for the solution based on the CLEARSY Safety Platform.

The CLEARSY Safety Platform **facilitates the development of SIL3 and SIL4 applications and is already certified against EN50126, EN50129, and EN50128 with a SIL4 level by CERTIFER (French Independent Safety Assessor).**

OVERVIEW

The CLEARSY Safety Platform is made of the following items:

- Dedicated hardware assembled printed circuit board called Safety Computer (CS0) slightly smaller than a credit card (72.5mm x 45mm)
- A software library that provides all the safety mechanisms required for ensuring the integrity of the platform and the proper execution of the customer application. In addition to this vital software, a board-specific package (BSP) is provided to the end-user for interacting with the hardware features of the board.
- A compilation suite that launches the generation of the target binary with a single command.
- Full documentation set for the development of end-user applications. The user manual covers both functional and critical design rules and also provides tips to the developer to ease the learning curve. This manual also provides the Safety Related Application Conditions (SRACs) that the final application has to meet to fulfill the certificate requirements.



HARDWARE CHARACTERISTICS

From a hardware point of view, the CLEARSY platform is packaged as a small single-board computer that embeds two microcontrollers PIC32MX from Microchip providing 80 MIPS. This board has to be fitted inside the motherboard of the final design (motherboard to be designed in function of the specific application). The choice has been made to keep the bare minimum on the CLEARSY Safety Platform, as generic hardware interfaces are neither aligned nor optimized with respect to final product requirements. Therefore, end-users are free to implement any input/output channels, network interfaces whether vital or non-vital on the motherboard. CLEARSY offers to provide guidance or to take part in the design of the hardware interfaces required. This can be achieved by the adaptation of SIL3/SIL4 hardware blocks already designed by CLEARSY and already used in revenue services or by the design and qualification of a new custom interface tailored to end-users' needs.
The hardware safety principle of the CLEARSY Safety Platform relies on the two out of two (2oo2) hardware architecture to mitigate any random failure that could happen on the microcontrollers. Hardware diversification is also used to avoid common-mode failure (for the clock for example).
The safety computer (CS0) exposes most of the pins (74 pins) of each microcontroller. From a design point of view, using the CLEARSY Safety Platform is identical to using a regular MCU with the benefit of avoiding the design and the demonstration of the safety of the platform. Only the safety demonstration of the application and custom interfaces is remaining. For the hardware engineering team, the CLEARSY Safety Platform can be seen as a single component that can be directly included in the final design.
The minimum mandatory interface of the CLEARSY Safety Platform consists of two isolated voltage buses capable of delivering 2 watts under 3.3VDC. Except for this constraint, you can build your solution without any design constraints.

All the native interfaces of the microcontroller can be used for the final product (non-exhaustive list):

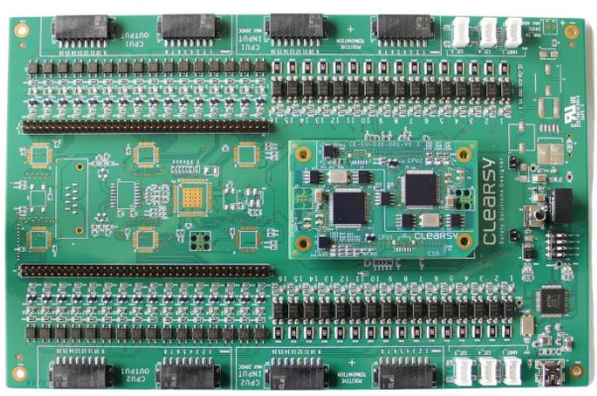
- 13x Analog inputs (10 bits 1Msps)
- 6x PWM hardware
- 63x GPIO
- 4x UART
- 2x SPI
- 4x I2C
- 2x CAN bus
- 1x Ethernet (RMII interface)

In addition to these native interfaces, the safety computer also includes:

- two thermal sensors (from -40°C to +125 °C)
- two isolated EEPROM of 1kbit for storing secret keys or application parameters
- 6x LEDs

A starter-kit motherboard is also available for the evaluation of the CLEARSY Safety Platform (see picture below). This starter-kit can be used for prototyping, proof of concepts, or training. The only interface required for using the starter-kit is a simple mini USB interface offering directly out of the box the following peripherals:

- 32x non-vital digital inputs
- 32x non-vital digital output connector for 4xI2C
- 2x debug interfaces with USB over UART
- 2x76 pins headers for wire interface with the CPU

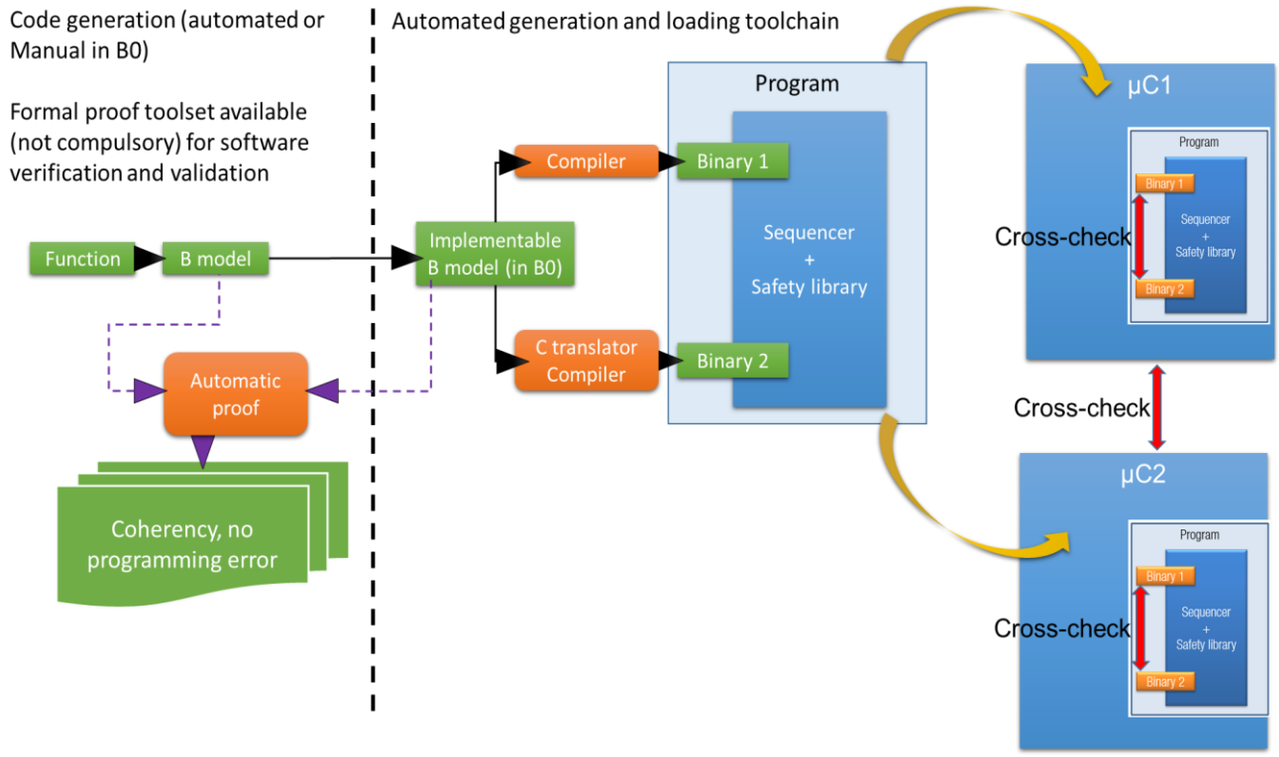


SOFTWARE CHARACTERISTICS

The software architecture of the CLEARSY Safety Platform is based on a replicated execution on each microcontroller. The vital software is compiled using two diversified compilation chains and the two resulting binaries are merged into the final binary that is executed by the hardware.

Both internal safety software library and customer application are double compiled. At runtime, both replicated instances of the vital software are executed in sequence with the same input dataset. The computed output datasets of each replicated instance are cross-compared to detect any diverging behavior or random error during execution. This process is performed on the two microcontrollers such that overall four instances of the applicative software are executed by the platform and cross-compared.

Thanks to this patented architecture, the CLEARSY Safety Platform can achieve a SIL4 integrity level for the vital software running on it.



Safety is based on a software library (covered by the SIL4 certificate) on top of which the final user can develop its custom application. The only constraint consists of calling periodically a set of primitives to perform vital health tests, otherwise, the system will fall back into safe state mode.
The software development on the CLEARSY Safety Platform can be split between vital software and non-vital software.

- The development of non-vital software is strictly identical to regular C language software that you would have written for any application on this microcontroller. Therefore, the development of a custom peripheral driver or non-vital business logic comes without any overhead or extra costs compared to regular development on an embedded target.
- The development of the vital software has to be done in B0 language. The B0 is an imperative language developed with the B formal method that is close to the ADA language. From a process point of view several options are possible:
  - The business application can be developed with the full process of the B formal method. This implies writing a formal model of the application and to establish that the formal model matches the expected safety properties of the product. Then the formal model can be refined several times until its level of detail is fine enough for its expression into B0 (either by manually writing implementation or by using automatic refinement tools). This strategy allows using formal proof to ensure the mathematical correctness of the application and thus save costs in terms of verification and validation.
  - The business application can be written directly in B0 manually by the software team. With this strategy, you do not need to use the B formal method to use the CLEARSY Safety Platform but you still have to establish that your software is correct (no bug) with a level of confidence that corresponds to your safety goal (SIL3 or SIL4).
  - The business application can be written with your regular tool and language and the output of your generation chain (C language, SCADE, …) can be translated directly in B0 using dedicated translation tools. As these kinds of use-cases are closely related to the output of existing toolchains, such strategies need to be jointly studied for each application. Note that this option allows re-using an existing code source which can be relevant in case of porting an existing system to the CLEARSY Safety Platform.

Whatever the development strategy selected, the resulting application will be bare-metal software (no underlying operating system) allowing to unleash the full real-time capability of the hardware target. Moreover, there are no software design constraints. The developer is completely free to architecture its software in the way he/she desires, especially the scheduling function, the use of interruption service routine, … are selected at his/her own discretion.

INTEGRATION

The CLEARSY Safety Platform is ready to use industrial solution for anyone who wants to build a custom SIL3/4 device at a limited cost and with managed risks. To effectively use the CLEARSY Safety Platform you simply need to:

- design a motherboard with all the required hardware interface with your custom application environment
- write and validate your custom business vital and non-vital software
- check that your design meets the Safety Related Application Conditions (SRACs) of the CLEARSY Safety Platform

Then you are done: the CLEARSY Safety Platform ensures the SIL4 processing.
CLEARSY can provide support for all or part of each of these design and validation activities.
Especially you do not need to address all the complex questions of safety-critical computational architecture like (non-exhaustive list)

- Does my program memory is healthy or corrupted?
- Does my RAM is corrupted?
- Does my compilation is correct or not?
- Does my time counter is accurate or not?
- …

All these sensitives items are already addressed and compliant with the CENELEC standard as established by the SIL4 certificate of the CLEARSY SAFETY Platform (type certificate n°9954/0262 from CERTIFER).

ENVIRONMENTAL / RELIABILITY

From an environmental point of view, the CLEARSY Safety Platform is not qualified right out of the box, because the environmental stress will depend on the final package of the application that embeds the CLEARSY Safety Platform. Nevertheless, according to already deployed and qualified systems based on the platform, the CLEARSY Safety Platform should comply with the following standard granted that the usual precautions are implemented:

- **Thermal:** -40°C/+85°C per
- **EMC/EMI:** EN50121-4 ; EN55016-2-3 ; EN61000-4-x
- **Vib and shocks**: EN60068-2-27 ; EN60068-2-64 ; AREMA Class B

The predicted reliability of the CLEARSY Safety Platform is equal to a Mean Time Between Failure (MTBF) 12 285 000 hours (performed with FIDES methodology in 40°C environments). The redundancy of the CLEARSY Safety Platform (2oo2) is for functional safety purposes. Especially it does not increase the overall availability of the platform. The most straightforward way to increase the availability of the vital computer (if needed) will consist on duplicating the computer board itself to have two redundant computing units.

TOOLS

The CLEARSY Safety Platform is distributed with a full set of qualified tools (T3 and T2 according to EN50128) that enable the end-user to generate the final binary image of her/his project. Especially, two compilers developed by CLEARSY and Microchip allows building the two replicated instances of the vital software. Also, the correctness of the software may be established through formal proof by using the integrated development framework called Atelier B (used by major railway manufacturers to develop SIL4 software).
The provided tools also provide methods and associated tools for checking the proper upload of the firmware on the final hardware target.
The configuration of these tools is straight forward as they come packaged in a virtual machine or a container (docker image). Therefore, the developer simply has to launch a single command to get the final result of its work. No complex setup of the various tools is required.

REFERENCES

The architecture of the CLEARSY Safety Platform has already been successfully used within several projects running in revenue services:

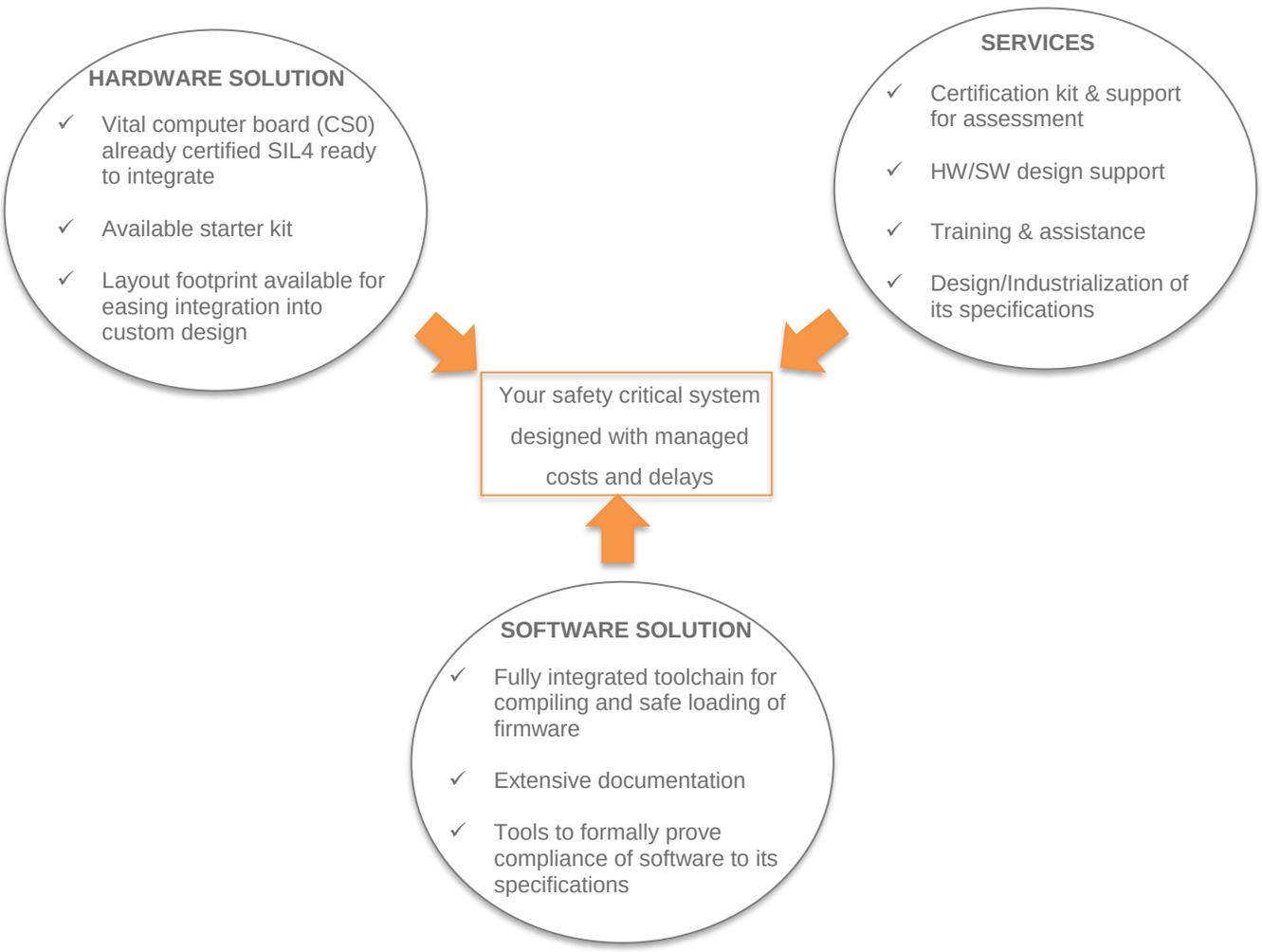
- 1st design for platform screen door operation in monorail Sao Paulo line 15
  - **Generic product** certificate CERTIFER #8891/200-1 27th February 2017 **SIL4**

- Product fitted for Stockholm City Line platform screen door operation
  - **System certificate** BUREAU VERITAS #63937413 3rd March 2017 **SIL3**

- CBTC Remote Input/output module (confidential customer)
  - **Generic product** certificate BUREAU VERITAS #7092509 23rd July 2019 **SIL4**
  - **AREMA** compliant (asserted by TÜV)

CLEARSY Safety Solutions Designer
contact@clearsy.com
www.clearsy.com

PLATFORM ECOSYSTEM



PUBLICATIONS

More details on the CLEARSY Safety Platform can be found in the dedicated section of CLEARSY's website.

If you have any questions related to the CLEARSY Safety Platform, do not hesitate to contact us. Our expert team will be please to support you.

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

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

Phone.+33 (0)4 42 37 12 70 - Fax: +33 (0)4 42 37 12 71

contact@clearsy.com I www.clearsy.com