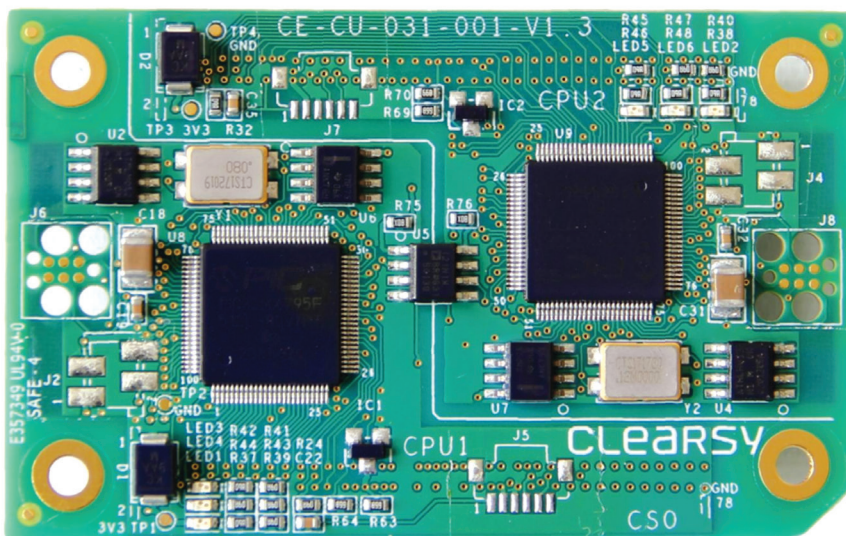


# THE CLEARSY SAFETY PLATFORM, A NEW SOLUTION FOR DESIGNING NEW SAFETY CRITICAL SYSTEMS

- BASED ON ITS 25 YEARS OF EXPERIENCE, CLEARSY HAS DESIGNED THE CLEARSY SAFETY PLATFORM: A CERTIFIED SINGLE-BOARD COMPOSITE FAILSAFE COMPUTER (PER EN50129 DEFINITION).



Certified single board CLEARSY Safety Platform.

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.

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).

## A solution for safety critical applications

The CLEARSY Safety Platform is a comprehensive and consistent set of hardware, software, and tools easing the development of SIL4 systems. As the vital computer board is already certified, the end-user

only needs to focus on the design of its own business application and system.

### CLEARSY Safety Platform is made of:

- A single board vital computer (SIL4) bundled on credit card sized printed circuit board. External interfaces and peripherals have to be designed on a dedicated motherboard accordingly to customer requirements. CLEARSY offers support and services to design this custom motherboard.
- A software library that includes all the safety principles required to reach a SIL4 execution level. This library is in charge of performing all the vital built-in health tests. This software library is formally proven with the B formal method.
- A fully integrated toolchain (running on a docker or within a virtual machine) allows building directly the final binary. Thanks to this setup, all the configuration and installation steps related to the tools' ecosystem are completely avoided.

### 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 vital and non-vital software



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

- check that your design meets the Safety Related Application Conditions (SRACs) of the CLEARSY Safety Platform (SCACs are conditions of use included in the certificate).

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 sensitive 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).

So the global safety case will integer all these points already supported by this certificate, which represents the major part of the global cost development.



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

