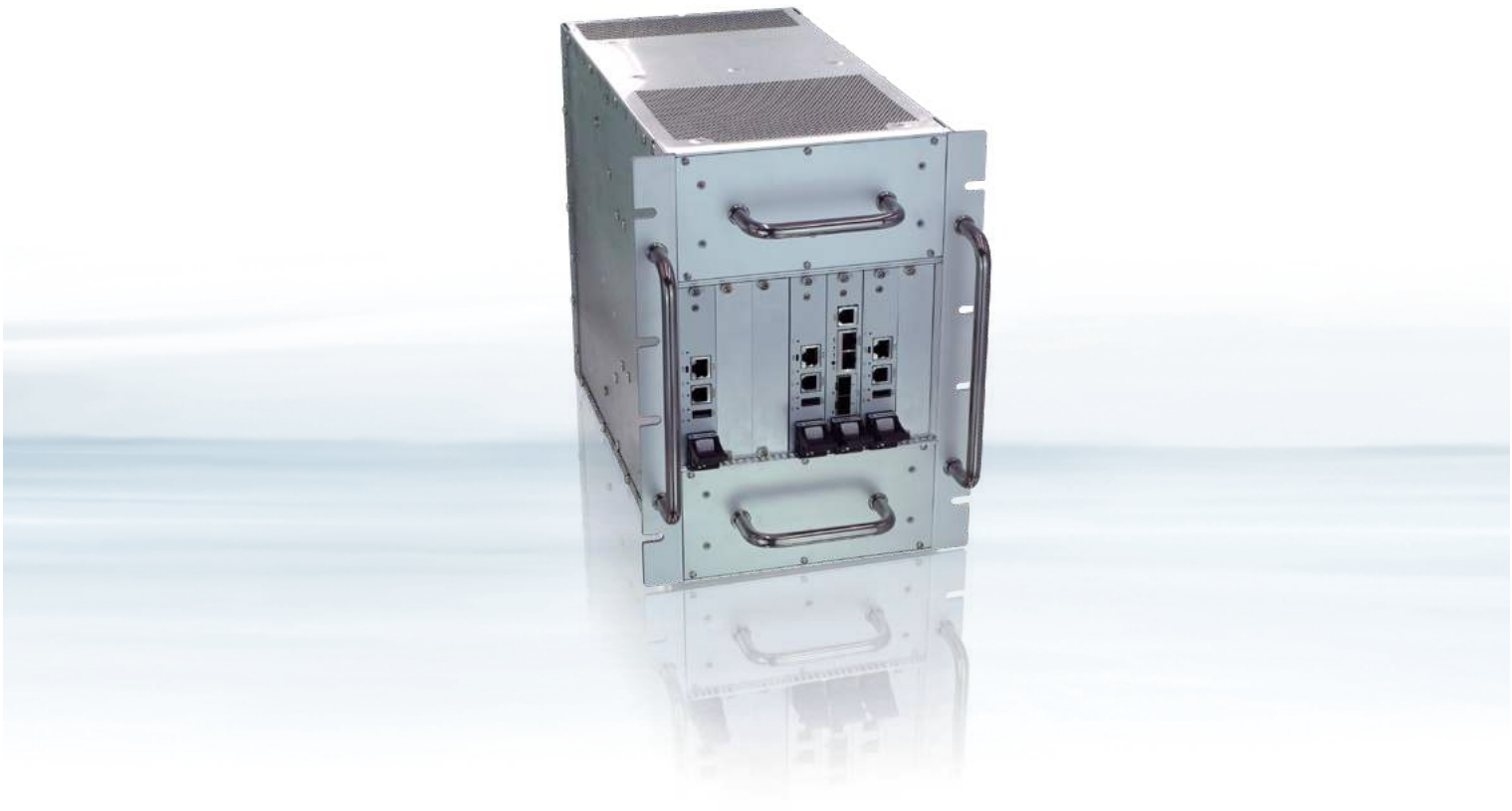
SAFe-VX-DEV

Safe Computing Development Platform by Kontron



Vital Computing Development Platform for Safety-critical Systems in Railway Applications

- Safety-critical computer based on qualified 3U VPX building blocks
- Certifiable architecture up to SIL4
- Compact half 19" modular platform
- For wayside or rolling stock applications

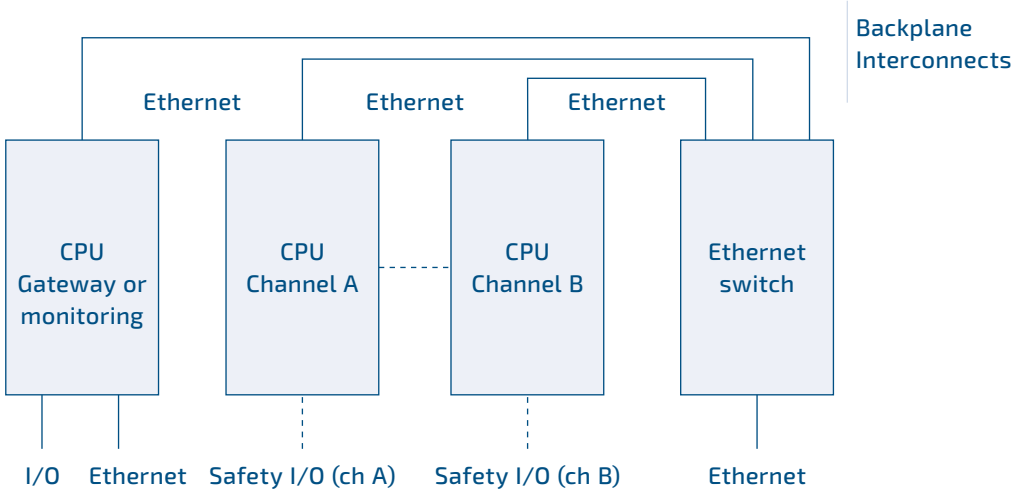
POSSIBILITIES START HERE kontron S&T Group

INTRODUCTION

The SAFe-VX-DEV development platform for safety computing is a half 19" platform based on VPX 3U building blocks. It is certifiable up to SIL 4 and specifically designed for safety-critical rolling stock or wayside applications. It is well suited for the control of all safety-related functions in wayside applications as well as in new trains and also for the refurbishment of trains. Thanks to its modularity and VPX standard openness, it is easy to tailor the SAFe-VX to the required I/O subset and environ-mental conditions. It is also possible to build an all-in-one safe control system plus non-vital processing safely separated through strict partitioning when running PikeOS RTOS from SYSGO acting as an hypervisor. Interfacing to existing train communication is achieved through Ethernet links or optional fieldbuses. The versatility and the segregation of the tasks and the application allow critical and non-critical partitions to cohabit without jeopardizing the safety, enabling train operators to run several applications on a single platform needed for example in Data Analytics, Artificial Intelligence or Autonomous Trains. The total cost of ownership is dramatically decreased through an easy maintenance of standard compo-nents. Longer operating life is achieved by the modularity and the longevity of the VPX architecture, designed for long term programs, and for partial technology refresh with a minimum impact on appli-cations.

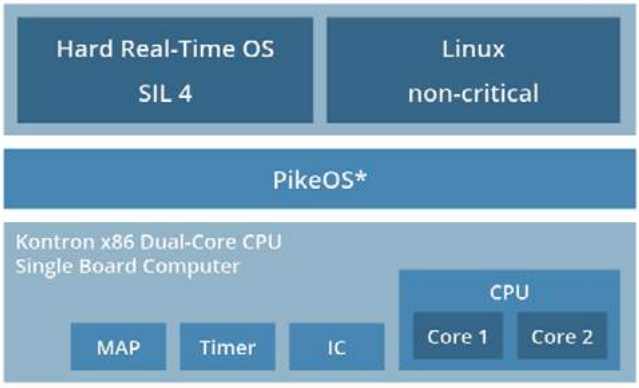
PLATFORM ARCHITECTURE

The base configuration (SAFe-VX-DEV) is a redundant one, including three identical VPX processor modules, interconnected by a Gigabit Ethernet switch module through a backplane. SAFe-VX does not present any single point of failure. Due to its modular architecture, SAFe-VX offers a high level of flexibility in terms of CPU, storage and I/Os. The other major building blocks like the PSU and the fan trays can be offered with redundancy. In the simplest implementation , all boards are sharing the same Power Supply Unit. The boards are electrically isolated from each other by the backplane design in order to guarantee the absence of common root cause of failure. When needed, two SAFe-VX can be used in parallel to reach the expected availability at SIL4 level.



SOFTWARE ARCHITECTURE

Several options are possible for software architecture. Since SAFe-VX is an open modular platform, customer can chose the final software implementation depending on its application or preferences. For example it can based on standard Linux distributions, or real time OS such as QNX , PikeOS or other…
One recommended RTOS is PikeOS, a well-established embedded SIL 4 RTOS from Kontron's software partner SYSGO. PikeOS acts as a hypervisor partitioning the critical and non-critical application code in independent time and memory spaces. The critical part of the application runs under the PikeOS hard real time partition whereas all complex non-safety related code can run in a Linux parti-tion, as depicted in the figure below.



* PikeOS Separation Kernel & System Software

The main software characteristics ensuring the safety of the SAFe-VX platform for the case of PikeOS are the following:

- Verification of proper BIOS initialization
- The firmware allows the OS to inject ECC errors for testing purpose
- Power-on built-in tests (PBIT) during the OS initialization including ECC error injection test
- Continuous built-in tests (CBIT) including temperature monitoring
- Memory regions protection against unexpected access from I/O controllers
- Modular update capability: OS, application
- Application safety library including heartbeat, voting, watchdog
- Eclipse Development tools: C compiler, debugger, performance monitor

More information on Sysgo webpage:
https://www.sysgo.com/pikeos

SAFETY ARTIFACTS

The following artifacts usually required for safety can be made available at the beginning of customer project:

Hardware documentation

- Boards MTBF reports based on IEC62380 with Railway mission profile
- Boards Failure mode analysis FMECA
- CPU board Hardware API detailed documentation
- Known errata for CPU, Ethernet switch and other boards
- Boards hardware verification reports
- Boards firmware verification reports
- Environmental test reports
- EMI and other electrical tests reports

Software documentation depends on chosen OS. For PikeOS, following packages can be made available:

- Certificate from TUV for PikeOS, independent of Platform Support package
- Certification artifacts for PikeOS generic part including requirements, test cases and test re-sults
- Certification artifacts for SAFe VX Board Support Package (CPU specific part and drivers)
- Certification artifacts for application safety library
- Safety manual
- Tool qualification reports
- Documentation for tools under Eclipse: C compiler, Debugger, monitor

PHYSICAL IMPLEMENTATION

The three CPU boards (channel A, channel B and gateway or monitoring) are Kontron x86 3U VPX modules. When CPU architecture dissimilarity is required, one of the two Channel A/Channel B boards could be also ARM-based.

SAFe-VX-DEV platform configuration:

- CPU: Xeon® D Processor quad-core @1.5 GHz or Intel® Core™ i7-1185GRE, quad-core @1,8 GHz
- DRAM memory: 8 GByte DDR4 with ECC or 32 GByte DDR4 with ECC
- Ethernet: 2x Ethernet 1000Base-KX or 10GBase-KR on the rear backplane, 2x 1000Base-T on front
- Extended Life Cycle and up to 15-year Silicon Reliability
- Reliability

Whatever the chosen version, the CPU boards design includes safety-oriented attributes including:

- Monitoring of temperatures and internal/external power supplies
- ECC protected memory with capability to inject error for testing
- 2 µs granularity precision watchdogs, cause of reset register
- Software verifiable master clock frequency
- Clean unexpected power interruption mechanism
- Dedicated memory for permanent history logs
- One onboard SSD (SATA / PCIe) per CPU board
- CPU configuration optimized for deterministic behavior
- Thermal Throttling Disable option

The Ethernet switching board is also a 3U VPX module with the following features:

- 1G or 10G Ethernet switch
- Backplane 1000Base-KX or 10GBase-KR and 2x front 1000Base-T RJ45 ports (optional 2x 10G SFP+)
- Port mirroring and port redirection capability

LONG TERM SUPPORT

Program life time management is supported over long periods thanks to Kontron solid background in obsolescence management.

- EoL management with early notice warranty
- Last time buy packages are offered
- Tech refresh minimizing requalification cost: Blade VPX modular architecture allows fit/form/function upgrades of building blocks, providing the same electrical, mechanical and thermal specifications, with state-of-the-art silicon technology
- Long lifetime program is supported for 25+ years

WHY CHOOSING KONTRON

Kontron is a preferred partner of major computer suppliers with early access to new technology and silicon. Kontron offers the best technology in terms of performance and low dissipation computers to provide the best trade-off and the longest lifetime. Kontron provides its technology to several cus-tomers in Transportation, all driven by similar requirements in terms of performance/consumption, rugged environment, lifecycle, reliability, and competitiveness. Kontron platforms are designed to make customization faster, system integration easier and reduce time to market while shrinking maintenance and support costs over the entire lifetime of the program.

Kontron is already the key supplier of Vital Computer Platforms for Rail Control solutions. With several thousands of VPX platforms deployed in the flied, in Safety Critical operation, excellent on-time delivery records and high-quality level, recognized by key customers, Kontron provides the best solution allowing customers to drastically cut down the Total Cost of Ownership.

ORDERING INFORMATION

ARTICLE	PART NO.	DESCRIPTION
SAFE-VX-DEV	1068-5081	Half 19'' Vital Computing Platform for Lab Development based on 3U VPX building blocks: 3x Processing Units (one can be used as Gateway or monitoring unit) and 1x Gigabit Ethernet Switch. CPU boards configuration: Intel® Xeon® D1519 processor, 8 GByte DDR4 with ECC, 32 GByte SSD, 2x GbE, 1x Serial ,1x USB on front Pre-installed Linux Fedora 64bits distribution on each CPU board.

GLOBAL HEADQUARTERS

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com

www.kontron.com