SAFe-VX

Safe Computing by Kontron & SYSGO

PikeOS®

SYSGO
EMBEDDING INNOVATIONS

Vital Computing Platform for Safety-critical Systems in Rolling-stock and Wayside Applications

- Safety-critical computer based on qualified VPX building blocks
- Safety-critical RTOS: SYSGO PikeOS
- Compact 40HP platform, 4U height typical
- SIL-ready certifiable architecture (SIL2/SIL3/SIL4)
- Safety certification kit

POSSIBILITIES START HERE kontron S&T Group

INTRODUCTION

The SAFe-VX safety computing platform is a half 19" 4U 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.

SAFe-VX 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, it is easy to tailor the SAFe-VX to the required I/O subset and environmental conditions.

Due to its VPX standard openness, it is possible to build an all-in-one safe control system plus non-vital processing safely separated through strict partitioning with PikeOS RTOS from SYSGO acting as an hypervisor. Interfacing to existing train communication is achieved through Ethernet links or 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.

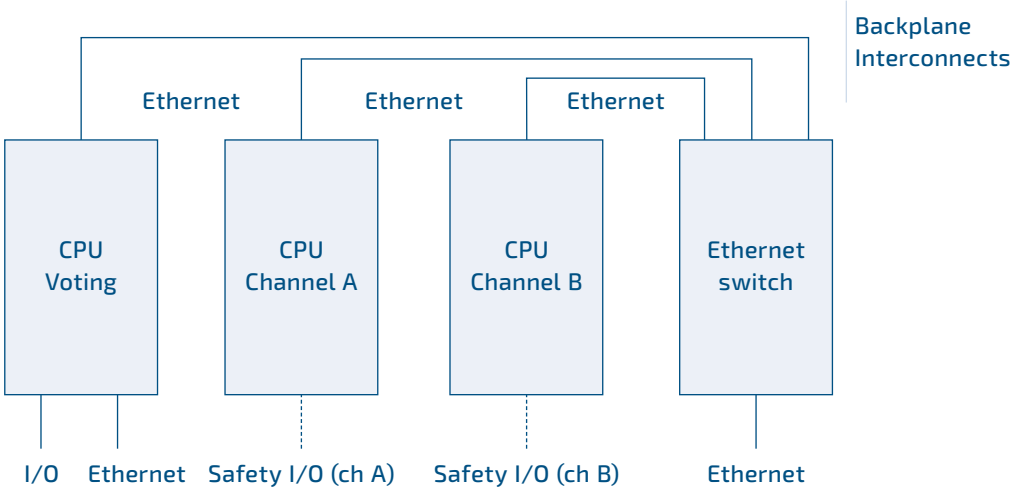
The total cost of ownership is dramatically decreased through an easy maintenance of standard components. Longer operating life is achieved by the modularity and the longevity of the VPX architecture, designed for long term programs, and for partial technology refresh with a minimum impact on applications.

PLATFORM ARCHITECTURE

The base configuration is a redundant one, including three VPX processor modules, interconnected by a Gigabit Ethernet switch module through a backplane. SAFe-VX does not present any single point of failure.

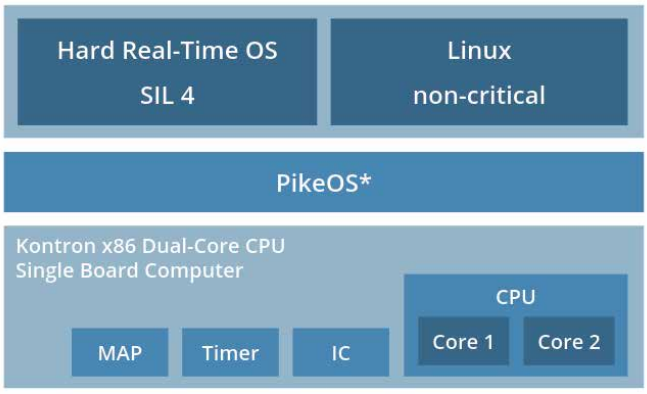
Due to its modular architecture, SAFe-VX offers a high level of flexibility in terms of CPU, storage and I/Os. CPU boards integrated in SAFe-VX have already been certified with safety critical real time hypervisor and RTOS such as PikeOS from SYSGO. The other major building blocks like the PSU and the 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

PikeOS, a well-established embedded RTOS from Kontron's software partner SYSGO, acts as an 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 partition, as depicted in the figure below.



*** PikeOS Separation Kernel & System Software**

The main software characteristics of the SAFe-VX which ensure the safety of the platform are:

- Verification of proper BIOS initialization by PikeOS
- The firmware allowing 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 the monitoring of temperature
- 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

CERTIFICATION KIT

The certification kit is made available for the customer at the very start of the SAFe-VX customer project. It includes the following artifacts:

Hardware documentation

- 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

- Certificate from TÜV for PikeOS, independent of the 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 the 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 voting) 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.

The SAFe-VX CPU module is based on a dual or quad core Xeon-D 3U VPX single board computer.

The main characteristics of this processing node are the following:

- CPU: Quad or dual Core Xeon® D Processor, 1.5 or 2.2 GHz
- DRAM memory: 4 GByte up to 16 GByte DDR4 with ECC
- Ethernet: 2x backplane Ethernet 1000BaseKX on the rear (or 10GBaseKR), 2x 1000BaseT on front
- Extended Life Cycle and 10-year Silicon Reliability

The CPU board 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 ms granularity precision watchdogs, cause of reset register
- Software verifiable master clock frequency
- Clean unexpected power interruption mechanism, dedicated memory for permanent history logs
- One on board SSD per CPU board
- CPU configuration optimized for deterministic behavior

The Ethernet switching board has the following features:

- Ethernet 10 ports L2 switch
- Backplane 1000BaseKX and cable RJ45 1000BaseT ports (10GBaseKR also available)
- 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 minimizes the cost of re-qualification: the blade's VPX modular architecture allows fit/form/function upgrades of the building blocks, providing the same electrical, mechanical and thermal specifications, with state-of-the-art silicon technology
- Long life-time program is supported for 25+ years

WHY CHOOSING KONTRON AND SYSGO

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 customers 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 field, 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.

SYSGO is the leading European provider of real-time operating systems for critical embedded systems. Our software products have been designed to meet the highest requirements when it comes to safety and security since 2005 when PikeOS was launched. PikeOS is the only RTOS that includes a hypervisor and enables customers to use the same code base in several development phases.

SYSGO's customers are leading players in aerospace, railway, automotive, medical and industrial automation industries. PikeOS is used as a platform for critical systems that need to be certified against industry specific safety and security standards, such as DO-178, ISO 26262, EN 50128, ISO 15408, or IEC 61508 with in-house certification know-how. It was the first operating system certified according to SIL4 for a multi-core processor.

SYSGO has strict in-house quality requirements in product development. We were one of the first companies to have all processes certified according to ISO 9001:2015, and in October 2016 we achieved certification against ISO/IEC 27001:2013.

As an operationally independent entity within the Thales Group since 2012, SYSGO has employees in Germany, France and the Czech Republic. Our international partner network includes leading technology providers as well as distribution and support partners worldwide. We support our products during the entire lifecycle of our customer's solutions, even when exceeding 20 years. As a European company, our products are ITAR free, and there are no export restrictions.

ORDERING INFORMATION

ARTICLE	PART NO.	DESCRIPTION
SAFE-VX-DEV		½ 19'' 4U Vital Computing Platform for Lab Development based on 3U VPX building blocks: 2x Vital Processing Units, 1 Voting Unit and 1 Gigabit Ethernet Switch. CPU boards configuration: Xeon D1508 Dual Core@2.2 GHz processor, 8 GByte DDR4 with ECC, 32 GByte SSD, 2x GbE, 1x Serial ,1x USB Pre-installed PikeOS from SYSGO: Floating development seats are provided for a 2-years period with technical support: one Integrator Suite to configure the system, to manage the multi-partitioning and the scheduling capabilities of PikeOS; and 5 Application Suite to develop customer applications. All licences are delivered with our CODEO Eclipse based integrated development environment and its tool chain. A 2 ays on-site workshop is included.

Global Headquarters

Kontron S&T AG

Lise-Meitner-Str. 3-5
86156 Augsburg, Germany
Tel.: + 49 821 4086 0
Fax: + 49 821 4086 111
info@kontron.com
www.kontron.com