SEC-Line PLATFORM

Using Embedded Computers in Edge Computing

Kontron Open Platform for Far Edge Micro Clouds

- Turnkey firewall / router with QEMU™ hypervisor for any OS support
- Security by design: hardware root of trust, secure boot and measured boot
- Small footprint (<200 MByte) distribution with cyber-attacks self protection
- Remote fleet management with OpCenter supports remote attestations
- Deploy and protect in a single computer unmodified software from multiple boxPC

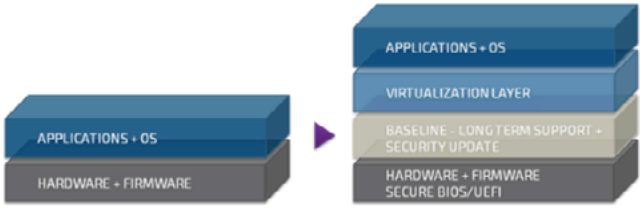
POSSIBILITIES START HERE kontron S&T Group

SEC-Line PLATFORM

Using Kontron computers with SEC-Line is the quickest route to deploy secure edge computer software stacks in todays' computing infrastructures, leveraging Kontron hardware platforms already qualified for the most demanding industry segments.

Embedded computing is rapidly morphing into Edge computing, with always connected systems deployed in the real world. Exposed to logical and physical attacks, they must be continuously monitored, secured and maintained, a challenge which requires specific tools to achieve security, operational efficiency and business agility at the same time in deployments that can involve hundreds of computers.
Kontron SEC-Line Open Platform is designed to tackle this challenge with a firmware based on an augmented version of OpenWRT™ and OpCenter, its remote management console.

SEC-Line FIRMWARE: A SECURE FIREWALL/ROUTER WITH HYPERVISOR BASED ON OPENWRT™



Kontron OpenWRT™-based firmware implements hardware root of trust security and offers hypervisor firewall router and cyberdefense features in a small footprint (<200 MByte).
This unique combination of leading edge technologies can deploy legacy applications side to side with modern OS stacks:

- Built from the reference in open source router/ firewall distribution: **OpenWRT™**
- Hardware root of trust: **TPM, AppProtect™**
- Enhanced security: **OSSEC, AppArmor, cgroups**
- Augmented with Virtual Machine support via **QEMU**

Kontron SEC-Line open platform enables a trusted computing environment, allowing embedded computer hardware to operate micro clouds in remote secured servers. Embedding firewall/router/cybersecurity functions, they can be managed remotely by IT personnel as easily as typical core network resources.

SEC-Line allows users to architect their solution around the **embedded micro clouds** concept where modern DevOps approaches to dynamic application and network management are applied to embedded computers by leveraging techniques developed for the cloud computing industry. In **embedded micro clouds** application code and OSes are managed as complete stacks and operate within virtual machines, instead of directly on the hardware. Application software is broken as independent containers (eg docker) and is dynamically distributed across computers by orchestrators (docker swarm, kubernetes). Communication channels are described as primitives and deployed from a single point (SDN, SDWAN)

OpCenter: SEC-Line MANAGEMENT CONSOLE

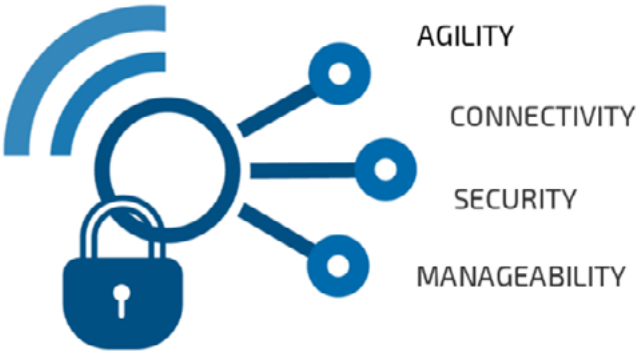
SEC-Line OpCenter is a remote management console for fleets of deployed computers.

- IT friendly: Embedded firewall, router and virtual machines in SEC-Line computers are managed like generic firewall/ routers/cloud Virtual Machines.
- Infrastructure : Opcenter virtual machine runs autonomously on any infrastructure server, there is no dependence to a public cloud or on-line service.
- Vulnerability management: system settings, and firmware updates can be deployed from a single point of control.
- Tampering detection: thank to measured boot, a regular **Remote Attestation** mechanism can detect software alterations.
- Data storage: Firmware images and settings profiles are managed in OpCenter in the computer fleet database.
- Communications: OpCenter systems management operations are designed for unreliable or intermittent connectivity. Remote systems operate as standalone embedded computers.

All data needed to manage and maintain the computers in the fleet is stored in OpCenter. From its GUI, remote computers firmware can be updated, and their multiple network and security settings captured and stored as settings archives. Such settings can later be applied after device replacement at a simple click of a button. OpCenter can also import information from higher level asset management platforms, avoiding manual data entry for device creation. It can also export all the fleet data to other corporate tools in various formats.
Users can monitor remote systems and trigger firmware updates. Network and cybersecurity settings are kept across firmware updates. Secure and reliable operation is enforced via encrypted channels with protocols designed to operate on very intermittent connections often found in mobile operations (road vehicles, trains, airplanes, etc.)

SEC-Watch included: maintaining cyber security in the field
Recent regional initiatives such as the EU-Cyber Security Act aim at protecting our digital world, which is under constant attacks. Critical infrastructure operators are being legally bound to maintain their deployments secure.

For deployed computers, this means monitoring certified sources about critical vulnerability events (CVE) impacting all the software embedded in the computer. Kontron SEC-Line platforms comes with a quarterly bulletin compiling all relevant CVE and their severity. Customers can thus assess their security exposure, and depending on their use case and configuration, act accordingly with configuration workaround, hotfixes or full firmware updates.



SEC-Line FEATURES AND BENEFITS

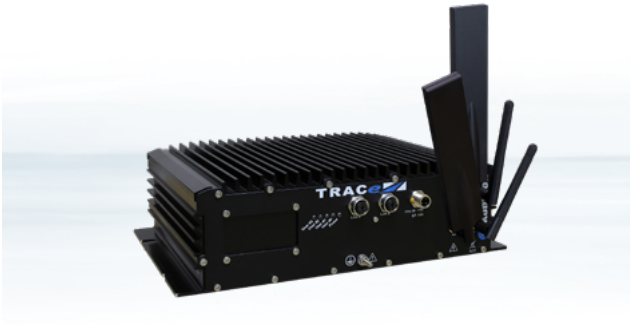
Agility: OS and Cloud agnostic, Legacy and DevOps friendly
Connectivity: Leading egde router/firewall, central management
Security: Hardware root of trust, Encrypted updates, Remote Attestation, Cyber defense
Manageability: Unique control point, Central database Store. OS updates, OS Settings, VM Images, System information.

KONTRON PLATFORMS POWERED BY SEC-Line

Railways

The TRACe family is a product range of fanless EN50155 railway computers offering easy customization to meet application-specific requirements. Designed to ensure stable operation in harsh environments and is ideal for any rolling stock system from Passenger Information Systems to Video Streaming & Storage Servers, Network Video Surveillance and Train Management Systems.

They now come as **SR-TRACe** (Server Router) variants, which can run complete software stacks inside virtual machines, secured through SEC-Line embedded secure firewall / router layers. These models can also be managed as fleets via OpCenter.



// **SR-TRACe-G40x**
EN50155 multi-network (LTE, Wi-Fi, GNSS, Wired ETH) Server/Router

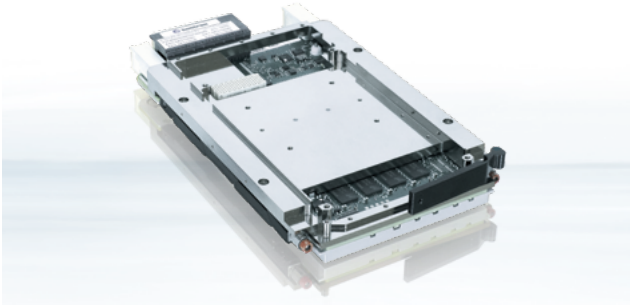
Avionics

The Kontron ACE Flight™ family is a line of products designed to support the digital transformation of commercial avionics. Some models are now powered by SEC-Line firmware offering leading edge secure firewall/router features and optional virtual machines on the more powerful server units.

// **AF1600**
Small Form Factor Avionics Gateway Router

Defense

Complex defense systems include in the same carrier (UAV, Navy vessel) multiple systems contributing to a global situational awareness. Embedded Micro Clouds techniques are becoming a valid and efficient alternative to proprietary middleware.
A Kontron high end SBC with SEC-Line can operate as a cloud connector for an existing HPEC systems (Radars, Sonars, etc).



// **VX305H-40G**
3U VPX Intel® Xeon® Single Board Computer with 40Gb ETHERNET

POWERED BY SEC-Line MEANS

HARDWARE ROOT OF TRUST

- TPM-based Secure Boot prevents device refactoring
- Secrets protection : all passwords, encryption keys and certificates are protected by the TPM
- Measured boot using TPM hashing mechanism enables Remote attestation
- Approtect™ protects application software also in Virtual Machines

COMPLETE ROUTER/FIREWALL BASED ON OPENWRT

- Control of device networking (wired, wireless, LTE, VPN)
- Settings management: local via a GUI, remote via OpCenter
- Health monitoring engine, a single view of the system in the CBIT dashboard

CYBER DEFENSE TECHNIQUES

- File Access Control: AppArmor restricts software to known usage patterns, seriously limiting the lateral impact of exploits
- Host Intrusion Detection Service: OSSEC, intrusions detection, Blocking Brute Force Attacks

COMPLETE CODE INDEPENDANCE

- Hypervisor allows any choice of modern stacks, application orchestration. No vendor lock in.
- Running legacy OS & apps with modern DevSecOps deployments in one computer saves space

... AND MUCH MORE

View and try SEC-Line in our E-Showroom:
https://kfrlabs.kontron.com/

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