WHITE PAPER

VIRTUALIZATION IN SMART TRANSPORTATION SYSTEMS

POSSIBILITIES START HERE

kontron
S&T Group

CONTENTS

INTRODUCTION // 3

VIRTUALIZATION OFFERS MULTIPLE ADVANTAGES TO TRANSPORTATION SMART SOLUTIONS AND SYSTEMS // 4

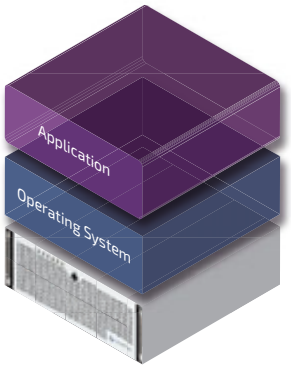
SMART TRANSPORTATION PLATFORMS EVOLUTION // 5

THE VIRTUALIZATION TECHNIQUES // 7

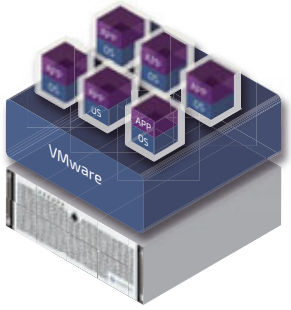
THE FUTURE OF VIRTUALIZATION IN SMART TRANSPORTATION SYSTEMS // 8

TRANSPORTATION COMPUTING PLATFORMS FROM KONTRON // 9

Virtualization has become a major software tool in embedded computing platforms thanks to the flexibility it provides. Combined with the availability of new multicore processors, it offers multiple advantages in rolling stock solutions that can benefit also to safety critical solutions. This whitepaper describes how the advantages of virtualization can be brought to embedded applications in mobility for smart transportation and safety systems.



// Traditional architecture



// Virtual architecture

INTRODUCTION

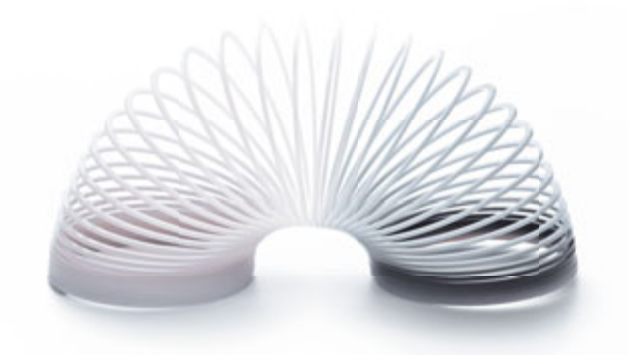
Virtualization encompasses a powerful set of technologies that has been used for decades in servers and mainframes for large IT data centers, or more recently on PCs for multiple use cases: personal, office or technical application. However, until recently, virtualization was not broadly used in embedded market segments, with few transportation computer systems or mobile equipment taking advantage of it. The environmental constraints request mobile embedded computers to endure restrictions that were impacting the processor performances and memory capacity, mainly due to real time requirements, small size and compactness combined with tough operating temperatures. Most of the time, virtualization was adding an extra-burden preventing the application to take advantage of the available performance from the embedded CPU. These advantages were reserved to server-class processors, with high thermal dissipation and low operational temperature (home/office/IT rooms).

// TRACe-B40x-TR, TRACe-V40x-TR

Fortunately, new processors dedicated to embedded applications are now featuring higher performances, while still limiting power budget and keeping a small footprint. This breakthrough is due to the availability of new multicore silicon dies implemented in a single chip. The larger number of available cores allow to offer a high-performance level in multi-tasks contexts, without increasing the processor frequency, hence the power consumption. Consequently, the advantages of virtualization can be brought to critical embedded application in mobility for smart transportation systems.

This white paper walks through the main benefits of virtualization for computing systems in Transportation, then describes some use cases performing virtualization in the field, to end up introducing computing platforms addressing this class of embedded solutions.

VIRTUALIZATION OFFERS MULTIPLE ADVANTAGES TO TRANSPORTATION SMART SOLUTIONS AND SYSTEMS



Flexibility

The main advantage of virtualization lies in the solution flexibility. As a matter of fact, a transportation solution will be in exploitation for a number of decades; however the requirements will evolve along the years to adapt and provide better or new services and functions. This will apply to all types of application like Passenger Information Systems, On-board Infotainment, TCMS, Asset/Fleet management, etc. Since it is impossible to foresee which new features will be required in the far future, it is very important to design a solution which is flexible at software level. Virtualization is the perfect tool to answer this question. When a solution is based on an hypervisor, it will be easy to add new functions, such as new middleware or new software to upgrade the solution with a minimum effort for the global re-qualification. Since the hypervisor usually provides segregation between applications, the impact of new software on the existing environment is hierarchized by the hypervisor, and reduces dramatically software trouble-shooting and verification when qualifying the new functions. It is also easier to merge various functions that used to run on different computers onto a more powerful processing platform, thus saving space, time and cost.

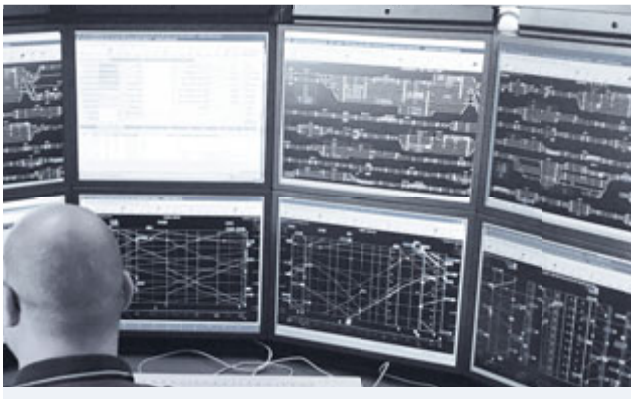
Program Lifetime

Transportation programs require long lifetime from commissioning until final end of exploitation of the embedded computing solution, whether onboard in rolling stocks, in stations or in wayside equipment. It generally means 20 to 30 years of operations, sometimes more. Over such long period, hardware obsolescence will happen in any case, and will require technology refresh, upward compatible, and as backward compatible as possible. This long term management requires specialized support capabilities from the computer platform provider. When possible, hardware technology refreshes are offered every 10 to 15 years, as far as embedded computer technology is concerned. However software happens to be a tougher issue to handle: after decades, it may be difficult migrating application & middleware to adapt to the hardware evolutions fixing obsolescence, to protect against new security threats, not to mention the cost of such migration, including testing and re-certification. Virtualization will help neutralize such issue by allowing the legacy software and even its legacy operating system to continue running under the hypervisor environment, provided that few provisions were taken at the initial design stage of the software based on a standard hypervisor. This is especially useful for proprietary software, or old middleware still necessary to run the application. Finally,

virtualization reduces the total cost of ownership of a program by facilitating the long term maintenance and extending the solution lifetime.

Virtualization and Safety requirements

Even if it looks unexpected at first glance, Virtualization can bring major advantages to these safety critical systems, thanks to its software architecture that segregates the tasks. This guaranties by design that the different tasks run fully independently from each other. When such partitions have to communicate, their communication channels are also thoroughly structured and controlled to avoid unexpected interactions, especially when it is concerning safety communication channels. Consequently, critical and non-critical tasks may run on the same processing platform without compromising the global safety-critical solution. Non-safe tasks only handle non-safe I/Os and non-safe signals. Virtualization running with a safe critical hypervisor gives new possibilities in system architecture. Each program can only access its partition



and its own set of resources. The programs running in partitions cannot interfere with each other, even in the case of software code errors. Therefore, they do not need to trust each other and individual criticality levels can be assigned to each of them independently. For example, it is possible to associate a safety critical ETCS system with non-critical data analytics linked to the traffic management, dealing with noncritical I/Os. Such systems allow building rich analytics and improving the final safety of the overall solution. The future smart autonomous trains will require artificial intelligence computing associated to safe rail control solution: virtualization will be a new answer to deal with both worlds.

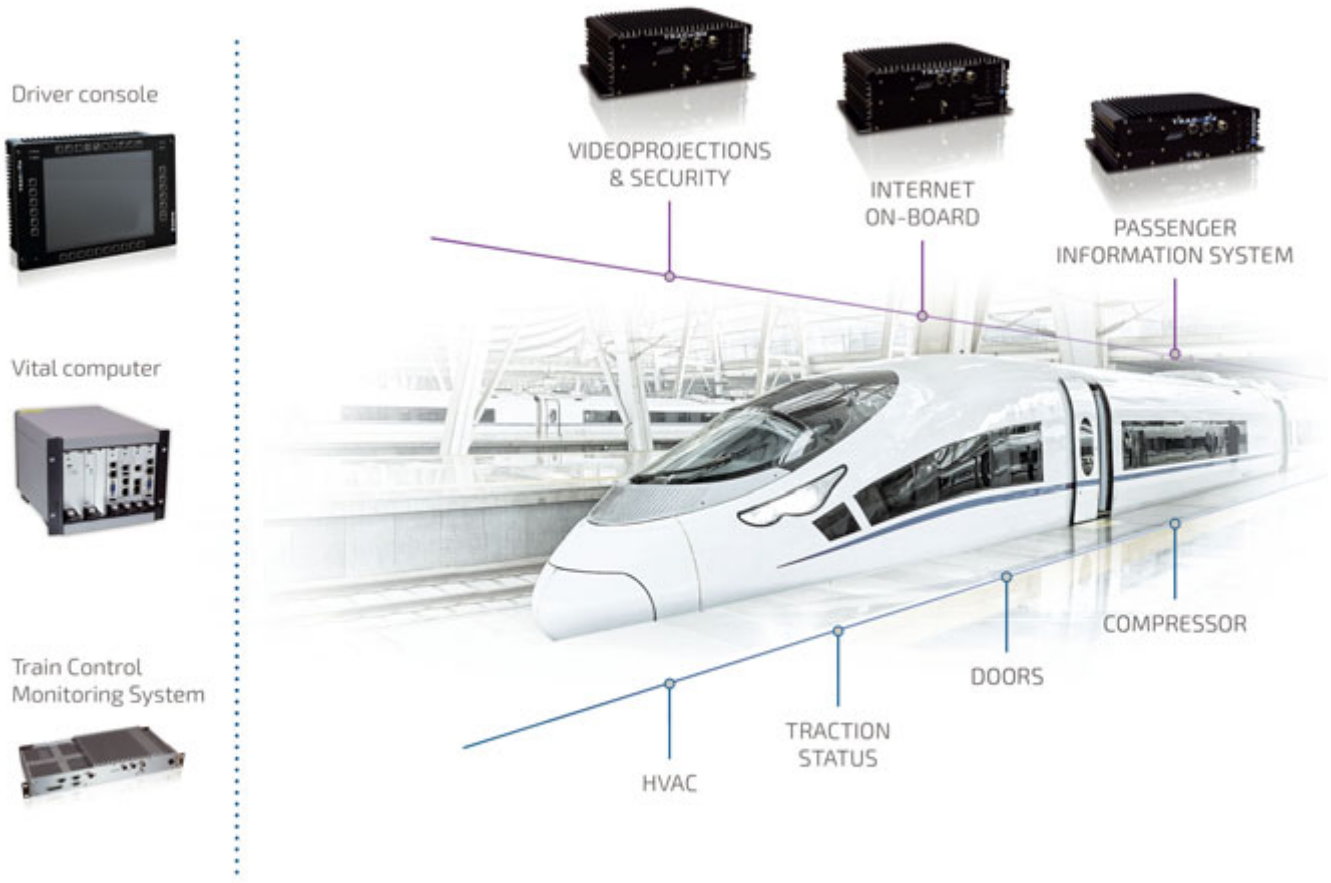
Performances and Virtualization

Smart transportation systems require more performance in each domain. This is driven by a need of new services and associated processing capacities rather than by a requirement of faster execution. Until recently, transportation compute platforms were connected just to their local sub-system, or their onboard field buses,

dedicated to local tasks. Safety critical systems were most of the time strictly isolated from Internet for obvious reasons of integrity and security.
However the need of new services for operational systems and for passengers demands connectivity and interaction. Such software architecture (client-server, data-analytics) require more capacity from the computer platforms, without compromising the real-time constraints of operational systems. To this respect, the use of virtualization and hypervisor was perceived as a possible issue. Recent hypervisors do not add overhead in terms of latency; they do not overweight the Operating Software stack. Actually, this virtualization architecture allows bringing new application software and services without degrading the performances behavior of the critical tasks. Real Time characteristics will be preserved: time partitioning is a deterministic way to insure that the critical tasks will get the necessary processor bandwidth.

SMART TRANSPORTATION PLATFORMS EVOLUTION

Since computers started pervading transportation platforms, on-board systems have performed mostly as stand-alone units using dedicated electronics with private subsystems, private local networks, and sometimes specific protocols. Actually every onboard function was implemented on a specific dedicated compute platform.
Coming from the information technology world, transportation Box-PCs and COTS have progressively introduced more and more standardization in terms of Operating Systems and networking. With Ethernet everywhere and Internet industry standard stacks, running on open Linux, the services and solutions began to change dramatically: PIS (Passenger Information System) and Infotainment solutions took advantage of such Ethernet centered architecture to facilitate interoperability and connection to remote servers. With video surveillance/CCTV, the increasing data throughput created a major technology breakthrough: a few years ago when cameras switched from analog to digital (over IP), the need for scalable and flexible compute platforms grew quickly over a short period. More recently, the advent of Bring-Your-Own-Device onboard (BYOD), added the domestic passenger digital traffic over the onboard local networks.
Consequently, multiple independent systems and networks still coexist in trains, creating multiple interoperability challenges in operation, maintenance and support.



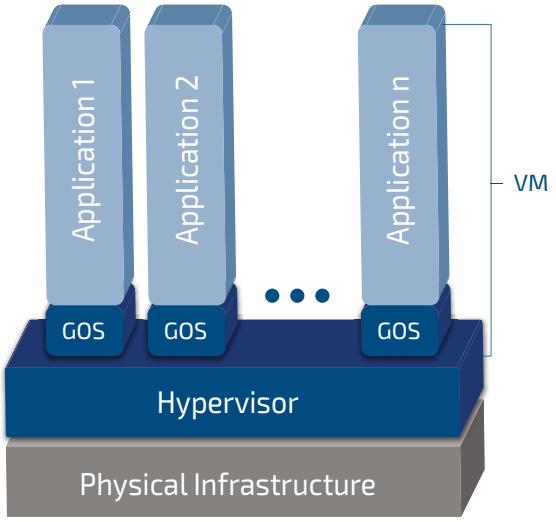
To minimize complexity and cost of ownership, these heterogeneous systems can now be merged in a single standardized common platform, delivering higher capacity, performances, and connectivity thanks to its modularity and flexibility. Such common platform can accommodate various solutions. This multifunction rolling stock embedded server can support PIS, Infotainment, CCTV, TCMS and Asset management solutions. Separate middleware and applications are dedicated to each function: the hypervisor will help to keep the management of each function simple and efficient.

In the case of safety critical applications, each platform has generally to be certified at a required SIL level; hence the hardware and software must follow precise design and development rules to be certified. The hardware platform cannot be certified without its safety application, and vice-versa. For such safety solutions, using a safety certified hypervisor is a great advantage in terms of software configuration management.

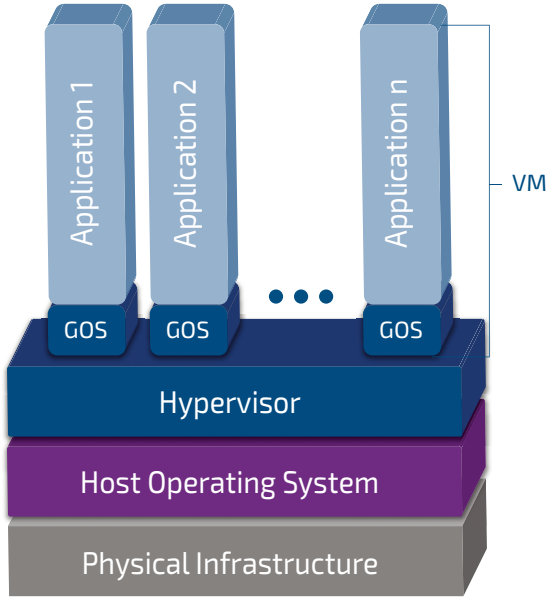
THE VIRTUALIZATION TECHNIQUES

In IT computing, an hypervisor is a virtualization platform that allows multiple operating systems to work on the same physical machine at the same time. They are classified into two categories: the Type 1 (bare metal) and the type 2 (hosted).

- A Type 1 (*Bare metal*) hypervisor runs directly on the hardware platform and is considered as an operating system control tool which is light and optimized for modern processors that supports hardware virtualization instructions (e.g. AMD-V and Intel VT).



- A type 2 (*Hosted*) hypervisor is a software that runs on top of the host's operating system. The user operating system runs at the upper level on top of the hypervisor.



Compared to IT infrastructure where virtualization is being used commonly, embedded systems have architecture constraints that will require specific performances from the virtualization software system.

Most of the embedded computing platforms face critical requirements:

- Large number of Inputs/Outputs: embedded systems have to interact with multiple I/Os, generally with short response time constraints. These systems sometimes run Real Time Operating Systems. Such deterministic performance must remain untouched with a lightweight hypervisor.

Compactness:

- embedded systems are often built in small form factor to fit into the embedded environment, running in large operative temperature range while being required to support longer lifetime than IT systems. Consequently, these systems use low power dissipation processors and limited memory capacities to deal with a reduced thermal dissipation budget. The hypervisor will have to accommodate such restrictions without degrading any operational performances.

Security and safety:

- virtualization used in smart transportation systems has the same level of Security and Safety as required by the application. Most of the time, virtualization will allow with a better software management to improve Security and Safety.

Legacy software:

- the virtualization for the embedded systems gives the capability to host multiple operating systems and software entities in a total independency thanks to software segregation, offering the backward compatibility with older legacy software.

The association of a single computer platform acting as a central server with virtualized computing can easily host multiple functions reducing the number of computer platforms, hence facilitating the final certification of the transportation solution.

When implementing safety-critical functions for transportation, advantage can be taken of the use of hypervisor thanks to the strict segregation of modules organized in different partitions, so as to facilitate the certification of each application according to its individual SIL safety level, according to EN 50128. The resulting effort to get the final safety certification will be significantly reduced. In addition, the hypervisor will

structure and hierarchize interactions between safety critical levels, since they are comprehensively controlled and isolated, preventing unpredicted behavior of software. This is even more applicable to systems combining safety critical and non-critical tasks.
For example, new autonomous trains need computing systems able to combine non-safety critical data analytics with the control of the train, which is safety critical: sensors and cameras watching the external environment of the train can detect on line anomalies on the railway or in the close surrounding of the train: obstacles, people, anomalies. Such video detection or sensors are not safety critical: they bring important information to the rail control solution that may require potentially emergency action towards the signaling or the controlling of the train. Real time constraints are mandatory and often require the computing system to host both critical and non-critical tasks in the same system, with related safety critical I/Os and non-safety critical I/OS. In such application, virtualization is the best technology to perform and support all these requirements.

THE FUTURE OF VIRTUALIZATION IN SMART TRANSPORTATION SYSTEMS

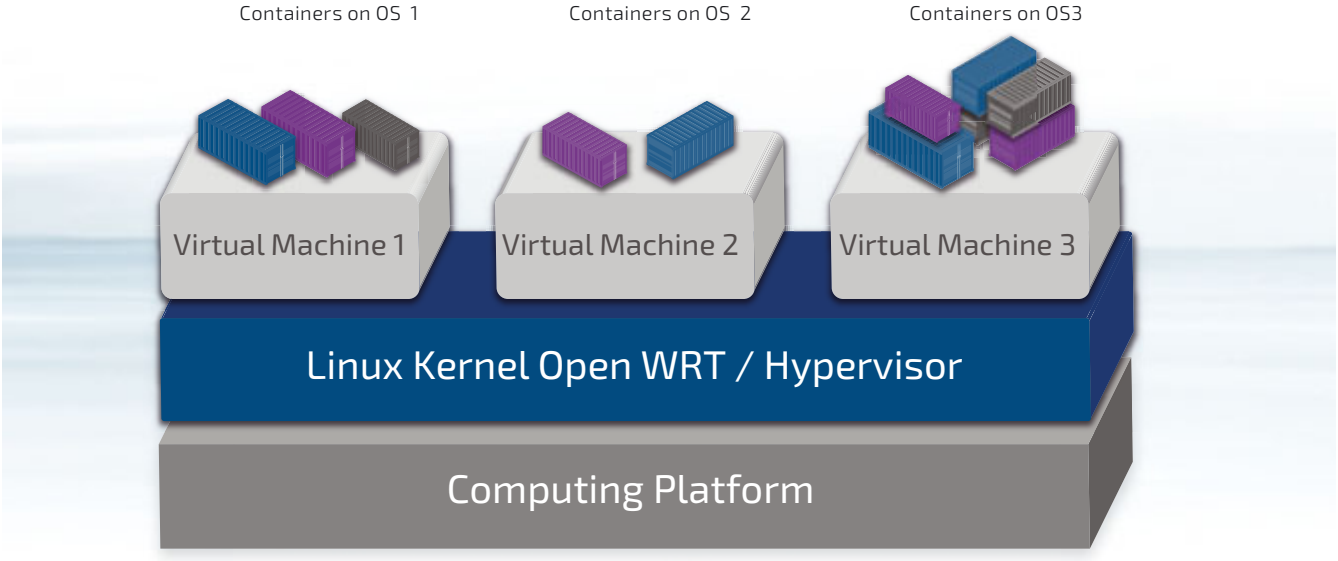
A recent refinement of virtual machines has given birth to a complementary approach to computing running Linux Operating System; it's the *Operating-system-level* virtualization, called *containerization*.

When the Hypervisor architecture supports diversity by hosting different Operating Systems, containers running on a single Operating System in which the Linux kernel allows the operation of multiple isolated user space instances.

In this example, OS1 could be a Linux, OS2 could be a Windows, and OS3 could be an RTOS

With such containerization, it is possible to execute programs to which only parts of the system resources are allocated. A program running inside a container will only see the allocated allowed resources. Several containers can be created, each of them being allocated with only a subset of the computer resources. Each container may include several computer programs. Such programs may run concurrently or separately, whether interacting with each other or not.

Containers are isolated and bundled with their own tools, libraries and configuration files; they can communicate with each other through well-defined channels. All containers are run by a single operating system kernel which allows keeping their real-time behavior, their direct I/O control access and management.



TRANSPORTATION COMPUTING PLATFORMS FROM KONTRON

// TRACe Family

Kontron is offering a family of computers for transportation in rolling stock, the TRACe line of products. TRACe is a standard generic embedded serverfamily, EN50155 certified, supporting Linux, Windows and RTOS.

Various TRACe versions are available with different flavors to address the solutions for transportation: video surveillance, passenger information system, train management control systems, multimedia infotainment, gateways for connectivity to IoT, multiple networks and field buses, asset management, etc.

By design, the Hypervisor technology is available on these TRACe servers under our EDGE-Line firmware so as to host any types of OS and applications, while reducing total cost of ownership over the whole duration of exploitation and operations.
The whole family is coming with a firmware stack called EDGE-Line, based on OpenWRT Linux, which provides KVM/QEMU virtualization technology and container support tools. EDGE-Line comes as well with a full set of management tools:

- To remotely administrate and configure the computing platforms fleet, even when being used in mobile rolling stock configuration: OS updates, patches or application can be updated.
- To guaranty integrity, availability and confidentiality of the platform: protecting the application (Approtect), detecting system software alteration (Trusted Boot), securing network protocols (Authentication with TPM), and restricting boot to signed images(Secure Boot). This security is based on hardware secure elements included in the TRACe computing platforms, making violation of security impossible. Only the host hypervisor is directly connected to the external network. It improves the security of its virtualized applications thanks to its firewall and intrusion detection tools.
- To monitor and control the platform in terms of vital computing parameters, checking that vital signals are nominal at power-on and during continuous operations. (Availability, Temperature of key components, Power Supply, System software sensors, ...)

CONCLUSION

Virtualization has become a major tool in embedded platforms, and offers multiple advantages especially for transportation. New computing platforms take advantage of the virtualization techniques in rolling stock solutions as well as for safety critical solutions, for example to watch on line the environment (tracks, obstacles) and detect potential danger or threats. Security and fleet supervision are also greatly facilitated. Virtualization opens up the transportation solutions to new unexplored capacities and Kontron TRACe edge computing solutions with EDGE-Line technology are ready for this new era.

About Kontron – Member of the S&T Group

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). As a part of technology group S&T, Kontron, together with its sister company S&T Technologies, offers a combined portfolio of secure hardware, middleware and services for Internet of Things (IoT) and Industry 4.0 applications. With its standard products and tailor-made solutions based on highly reliable state-of-the-art embedded technologies, Kontron provides secure and innovative applications for a variety of industries. As a result, customers benefit from accelerated time-to-market, reduced total cost of ownership, product longevity and the best fully integrated applications overall.

For more information, please visit: **www.kontron.com**

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