Made in Germany

Durable and cyber-secure IT hardware for airports

So far, it is mainly the 24/7 availability requirements, local support hotlines and fast maintenance services that have persuaded airport operators to use robust IT hardware made in Germany. When it comes to new investments, the trustworthiness of the manufacturers involved and the resilience of the systems are becoming much more important, giving hardware developed, produced, assembled and tested in Germany a further advantage.

kontron

Table of content

EXTRA Computer GmbH
Giengen-Sachsenhausen

Project:
Cybersecure IT and OT hardware

Kontron Platform:
SMARTCASE™ S711 incl.
D3713-V/R Mini-ITX motherboard

www.extracomputer.de
www.calmo-pc.de

Founded in 1989, EXTRA Computer GmbH near Giengen an der Brenz specializes in the development, manufacture and sale of high-quality IT solutions. Under its own brands exone® (business IT), Calmo® and Pokini (industrial IT), the company offers a wide range of PCs, servers, notebooks, industrial PCs, rugged tablets, panel PCs and much more. The BTO production in Germany enables high flexibility and very short delivery times.

Airports are not only major traffic hubs, but also agglomerations for IT systems. Several tens of thousands of systems are used at international hubs for passenger and cargo flows. They control numerous applications that every passenger is familiar with - from arrival and departure display boards distributed throughout the airports, to classic check-in terminals and newer self-service terminals for boarding passes and baggage check-in, to robust client systems with boarding pass readers at the gate.

In other infrastructure areas, they are also used for video surveillance, communications technology, baggage handling systems and parking guidance systems. The total market for smart information (IT) and operational (OT) technology for airports is estimated at over $3.5 billion worldwide. The market for passenger, baggage and cargo handling control systems accounts for a share of around 25 %, car parking systems 19.5 % and digital signage around 15 %.

High availability requirements

Since all these systems have to be operational 24/7 for years to come in order to ensure the smooth running of the airport, there are high demands on their reliability. After all, the failure of just one system can shut down an entire airport if it is in an exposed position. At Orly Airport in Paris, for example, thousands of passengers were unable to take off on time several years ago. This was due to a glitch on a computer responsible for transmitting weather data to the pilots.

But even less critical failures are a burden for airport staff and passengers: At peak times, downtimes of baggage handling systems, display panels or clients at the gate invariably lead to delays and the costs associated with them. This is why the hardware has to be absolutely reliable. Airports therefore stipulate system designs that have at least IP30, ideally even IP50 protection and are therefore dustproof. In areas of application with strong temperature fluctuations, protection against condensation is required.

Robust design for harsh environments

In the event of a power failure, the systems must also be able to withstand high voltage fluctuations and peaks that can be caused by emergency power generators starting up. Because airports are subject to high levels of radio wave pollution, a high level of protection against electromagnetic interference (EMI) is also required. Systems must also not interfere with radio traffic, so a high level of electromagnetic compatibility (EMC) is mandatory. HDMI connections, for example, interfere in both directions - which is why DisplayPort is generally preferred.

> With our solutions, we opt for Kontron motherboards as they are designed and produced in Germany with a focus on quality and long-term availability, just like our Calmo IPCs.
>
> Uwe Silberhorn, Product Manager Industrial IT at EXTRA Computer

Large IT broadliners that design systems for office use generally do not offer such systems. For them, airports are a niche market. That is the reason why airport operators prefer manufacturers that focus on robustly designed systems and offer them an all-round service that is ideally just as available 24/7 as their systems. However, due to the increasing threat level from cyberattacks on critical infrastructures (CRITIS), which of course include airports, other requirements have also been added recently.

Increased exposure to cyberattacks

The German government has imposed additional obligations on operators of critical infrastructures to ensure security of supply for society and the economy. For example, operators must report their critical infrastructures and designate responsible contact persons who must be available at all times. They should be able to respond immediately to emerging threats in order to contain escalations. For this reason, they are also required to report their own incidents immediately.

In addition, airport operators must take state-of-the-art measures to protect their IT, OT, infrastructure and operational organization. Solutions that enable attack detection must also be installed for this purpose. Facilities that airport operators need to pay particular attention to currently include passenger and cargo handling, infrastructure operations, airport management, air traffic control and airline traffic control centers.

As the most important first step, airport operators resort to security technology for network infrastructures and secure the respective network segments via state-of-the-art gateways. However, what is the use of protecting a network segment if sabotage can also be carried out from the inside?

Installations have to be state-of-the-art

From the point of view of critical infrastructure protection, all systems at an airport must therefore be checked for state-of-the-art security and - if necessary - upgraded to it. The system at Orly, for example, was a 23-year-old computer operating Windows 3.1. Moreover, the airport's system administrator then confirmed that the systems in his area of responsibility were between 10 and 20 years old on average. It can be assumed that this is not an exception but common practice at many airports. As a result, airport operators in Germany are faced with the challenge of renewing their outdated IT and OT systems completely, if only because of legal regulations.

The current state-of-the-art, for example, consists of much more secure chipsets than 5 to 10 years ago, when platform security processors were not yet part of the standard system design. Secure boot implementations are designed to protect against OS compromises and the installation of manipulated boot loaders and thus ultimately ensure image stable hardware. Trusted platform modules, which make systems clearly identifiable and offer protection against software manipulation by unauthorized third parties, are also standard. Password protection of the BIOS is also recommended, and access to storage media must be protected. This is crucial not only because of general security, but also because of the GDPR.

Less is more

To prevent IT and OT systems from being compromised, a high level of mechanical security is also necessary, because once a malicious code has been infiltrated into a system, the entire IT infrastructure of the affected network segment can be disrupted. For this reason, accessible interfaces on the enclosure must be reduced to what is necessary and protected from improper use.

Finally, it is mandatory that the latest security updates are continuously provided. For example, AMD recently published a new chipset driver for AMD Ryzen™. As a highlight, the driver team mentioned the prevention of a downgrade in the PSP driver (Platform Security Processor), which is a security-relevant issue. System providers should also proactively communicate such updates to their end users and support upgrade procedures in the long term.

Cybersecure IT and OT hardware

One provider of robust and state-of-the-art cyber-secure IT and OT hardware for airports is Extra Computer. Their systems have been listed with the central purchasing department of leading airports in Germany for many years and have been put into operation in substantialnumbers.Thecompanyhasbeendevelopingand producing these systems since 1989 and is one of the largest independent manufacturers of server, storage and industrial systems in Germany with more than 350 employees.

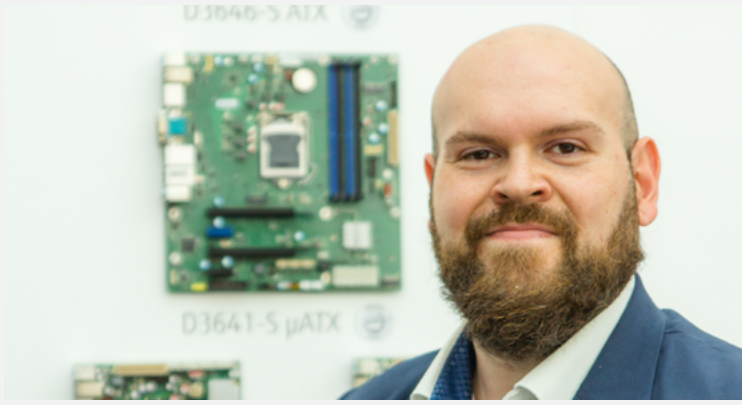
Customers are convinced by both the systems and the services of the company meeting the quality standard “Made in Germany”. They are developed, produced, assembled and tested in Germany. Moreover, only motherboards are used that are also made in Germany - namely by Kontron. This guarantees airport operators a high level of trustworthiness on the part of the manufacturers involved and, in times of uncertain supply chains, also short delivery times and low transport costs as well as competent technical support and repair services directly from Germany.

Systems with industrial motherboards

Systems that German airport operators use for durable and cyber-secure IT hardware are, for example, those of the Calmo brand, which are assembled and tested according to DIN 9001 and are already available in four generations and numerous performance variants with industrially hardened Mini-ITX motherboards from Kontron. Due to the high demands placed on processor-integrated graphics in the airport environment, these are usually equipped with processor technology from AMD.

In the Calmo S Ryzen design, these motherboards impress with up to four independently controllable DisplayPort connections and their IP 50-protected housing. Despite the limited ventilation options due to the high dust protection, the systems are designed for 24/7 operation. To ensure that the systems do not overheat, particularly robust, industrially hardened components are used, which are not even affected by strong temperature fluctuations and have been examined regarding their longevity through burn-in tests. Their energy-saving power management also reduces operating costs, as the systems hardly consume any power in idle mode.

The systems are available in identical configuration for up to seven years, which facilitates system administration and maintenance. Hundreds or even thousands of systems can thus be automatically updated with the same service patch. Since the manufacturer also has full system responsibility for the housing, which is developed and manufactured in Germany, system designs that are mechanically protected against sabotage can be adapted to the needs of the application at any time.



> With their Calmo systems, Extra Computer have proven over many years that they are a reliable and loyal partner to the industrial sector. I am all the more pleased to be able to continue to build on this success and cooperation with our new generations of platforms.
>
> Emanuele De Marinis, Business Development Manager Motherboards at Kontron Europe GmbH

Calmo S

Mini-ITX Board
D3713-V/R

Calmo UNI Ryzen

Up to four independent monitors

The latest system configuration, which recently went into series production, features Kontron's D3713-V/R mini-ITX board (170 x 170 mm) with AMD Ryzen™ Embedded R1000/V1000 processor configuration and integrated AMD Radeon™ Vega graphics for applications with particularly high graphic requirements. It is equipped with up to four DisplayPorts, one Embedded DisplayPort and a dual-channel LVDS (24-bit) and supplies up to four independent monitors with 4K resolution. Depending on how much performance is required, six motherboard versions with different AMD processors are available.
In addition to the Calmo S Ryzen system designs, the company also offers more cost-effective Calmo UNI Ryzen system designs with IP 20 protection, for which Kontron also provides the SMARTCASE™ chassis design. The systems are designed for DIN rail mounting and control cabinet installation, so that a higher level of dust protection of the systems can be ensured by the installation location. These systems are also available with the same Mini-ITX motherboards as used in the Calmo S systems. In addition, systems for particularly space-constrained installation situations will also be available soon. They will be equipped with a Kontron motherboard in the mini-STX form factor (147 x 140 mm) and will be launched as Calmo TINY Ryzen with IP 20 protection and as Calmo XS with IP 50 protection.

Uniform shopping basket for heterogeneous tasks

Airport operators receive a homogeneous product basket for the most diverse tasks, since all systems can be procured with different variants of a processor generation and thus, identical board support packages can be used across all system designs. A total of hundreds of variation options are available - coupled with a system integration service through which the most heterogeneous requirements of airport operators have already been successfully realized in numerous projects.

The board manufacturer also provides its product families with homogeneous BIOS designs and standardized APIs across processor sockets, so that OEMs, system integrators and end users can program and parameterise them homogeneously across the most diverse use cases. This also makes maintenance and servicing highly automatable for IT administrators. Ultimately, it is also a question of IT staff not having to look after their systems around the clock. Rather, only the systems should run 24/7.

Calmo XS mit
Mini-STX D3714-V/R

Weitere Informationen:
Calmo Systeme
Kontron Motherboards
SMARTCASE Kit für Kontron D3713 Motherboards

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT) and offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontronprovides secure and innovative applications for a wide variety of industries. As a result, customers benefit from aceerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

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

About the Intel® Partner Alliance

From modular components to market-ready systems, Intel and the over 1,000+ global member companies of the Intel® Partner Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest IoT technologies, helping developers deliver first-in-market solutions.

Intel and Atom are registered trademarks of Intel Corporation in the U.S. and other countries.

Global Headquarters

Kontron Europe GmbH

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

www.kontron.com