Security Partner Preferred

Partner Use Case

Embedded Secure Elements in Edge Computing Solutions for Industry 4.0

secunet

secunet edge box secures machines “at the edge” of the network and allows additional IoT Edge Computing.

Products

SLE 78CUFX5000PH

Security Partner Preferred

Use case

Application context and security requirement

Industry 4.0 connects Information Technology (IT) with Operational Technology (OT), thereby bringing together two worlds that were previously completely separate. Connected sensors, machines and plants in Industry 4.0 ecosystems increase the complexity and provide new opportunities for cyber criminals to launch attacks. This leads to a higher risk of system failures or even production outages.

Challenge

The industry is currently facing major challenges: A machine pool may well be up to 30 years old, but the control systems developed in the past no longer meet the requirements of today's IT networking. Secured solutions have to be provided that allow reliable operation and at the same time enable connections to modern networks. However, it would be too short-sighted to focus solely on the necessary protection of machines. There are other challenges as well: How, for example, can 5G be used? And how can the connection of machines to any internal or external services or platforms be implemented in the respective individual application cases? A holistic approach is required that combines the following aspects:

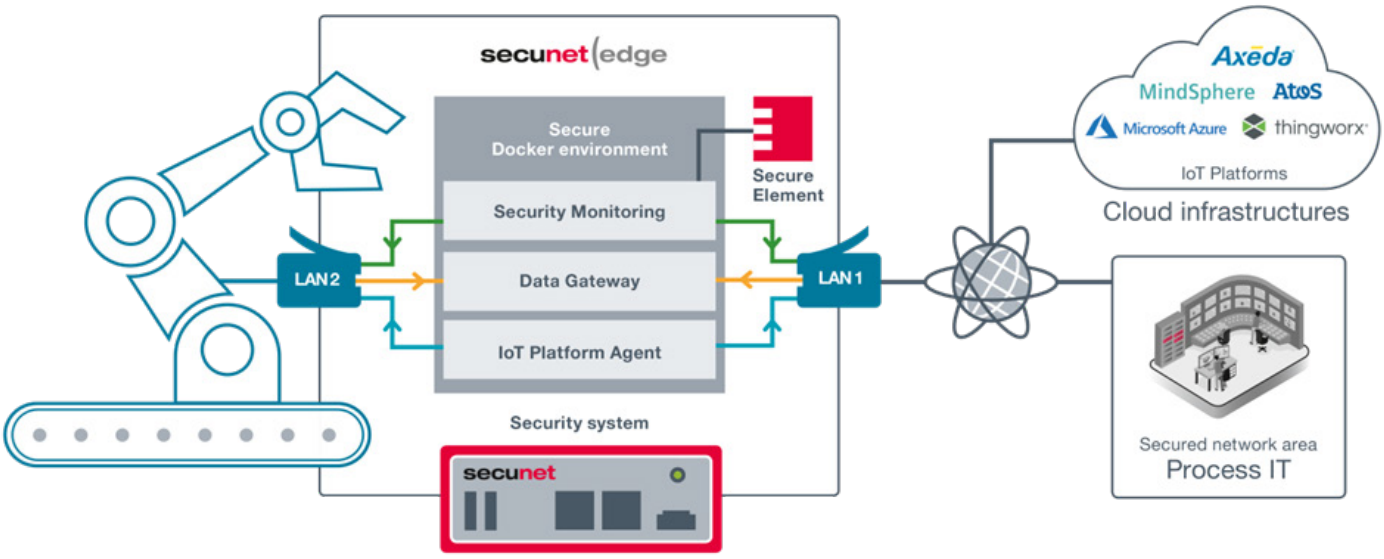
› Secured networking and regulated communication behaviour of machines
› Use of software for flexible integration of machines in Internet of Things applications
› Security monitoring of data communication to strengthen the defence against cyber attacks

Use case

Implementation

Secunet edge is a modular security appliance to bridge the IT and OT lifecycle. It allows connecting machines in a secured way to the IT world including cloud environments. The solution provides the flexibility by the feature secured Docker environment, which allows running applications for different use cases, created by customers, partners or secunet. In addition, the implemented security monitoring makes the data stream transparent and enables the analysis of the machine's communication behaviour. In secunet edge, an integrated sensor system continuously monitors incoming and outgoing data traffic at the interface between the machine and the external network and evaluates the data using a central analysis system.
The trust for secunet edge is based on the build-in embedded secure element, the hardened operating system, the security applications and the long-term security lifecycle service from secunet.

The Infineon SLE 78 security controller is installed on the secunet product CryptoCore SSD (Solid State Disk). It is a m.2 SSD disk with the SLE 78 on one printed circuit board (pcb), connected to the Industrial PC mainboard via m.2 USB (Universal Serial Bus) and in parallel to the SSD controller. It allows maximum flexibility, transparency, compatibility and performance.



User benefits

- Customer can concentrate on their current business and new digital business
- The FIPS (Federal Information Processing Standard) and Common Criteria (CC) certified and flexible SLE 78 allows projects also in critical infrastructures
- Secunet edge (Hardware + Software + Services) is made in Germany
- The solution is compatible with all important IoT platforms
- It allows to run own applications in a secured way with a secured Docker environment

Solution

Secunet edge was specially designed, developed and patented for industrial systems and environments. Thanks to its flexible architecture, secunet edge is also suitable for connecting devices in the medical IoT, production, finance, automotive production and energy sectors as well as in public transport, smart building and military applications. In the finance sector, for example, secunet edge can show its benefits quite well, because cash processing solutions represent a special type of industry 4.0 application with very high demands on security.

Cash processing solutions have become digitally connected on a huge scale. A development that has brought advantages in terms of speed, transparency, and cost, but also entails high security risks. Critical equipment for banknote processing, packaging and process automation has become vulnerable to threats of cyber-attack.

Used by many national central banks, secunet edge is a secured, efficient, and comprehensive solution for protecting cash processing machines against any kind of cyber-attack. The secunet edge box is placed between the network and the processing machines, concealing them out of reach from cyber threats such as viruses, trojans, malware, scareware, and ransomware. It acts as an industrial firewall, housed in a robust box, which decouples the system from the customer IT network, while still protecting communication to and from the cash processing solution.

- Comprehensive. Secunet edge secures all kind of industrial applications and systems (including third-party systems) so they can be safely connected to any networks up to the cloud.
- Up-to-date. The appliance is fully compliant with the latest security requirements, and has an up-to-date user interface that fulfills current IT security standard.
- State-of-the-art. Secunet edge runs on a hardened Linux operating system and transforms unencrypted legacy protocols to secure encrypted protocols.
- Future proven: With the secured Docker environment own apps can be installed on secunet edge as containers and allow covering todays and future use cases.
- The SLE 78 integration in an industrial edge device was driven by the requirements from system self-security, storing secrets, flexibility for all current and possible future use cases in IoT and trust in hardware security.

A bank note processing machine of a large European central bank.

Security Partner Preferred

Solution

secunet

Main benefits of the Infineon product

Infineon's embedded Secure Element provides the security and flexibility for todays and future use cases in IoT and cyber security. Especially for the use in cash processing scenarios, it is important that the solution meets the security requirements of international standards. To this end, secunet edge leverages the Infineon SLE 78CUFX5000PH security controller for state-of-the-art cryptographic functionality, which is provided by the security certified chip platform based on Integrity Guard and SOLID FLASH™. Integrity Guard offers comprehensive error detection, a self-checking dual central processing unit (CPU) and a fully encrypted data path including encrypted calculation in the CPU. Thereby it provides security certification according to FIPS 140-2 Level 3, CC Evaluation Assurance Level (EAL) 6+ (high) and EMVCo (Europay, Mastercard, and Visa consortium). In addition, this solution based on a tamper-resistant security controller provides a very high protection level against a wide range of current and future attacks, such as physical attacks to extract keys or side-channel attacks.

Security Partner Preferred

Partner

secunet

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

secunet Security Network AG

The secunet Security Network AG is a German based market leader for IT security with public sector clients. More than 500 experts concentrate on topics such as cryptography, digital identities, authentication, biometrics and the security of edge and cloud computing.

The company develops highly secure IT solutions for governments, ministries, authorities and administrations as well as innovative products for critical infrastructures, border control systems, the automotive industry and industry 4.0. The range of services extends from consulting to the development and integration of software and hardware to training, support and security analyses.

The secunet Security Network AG is the IT security partner of the Federal Republic of Germany and a partner of the Alliance for Cyber Security. The company was established in 1997 and achieved a turnover of around 163 million euros in 2018.

secunet Security Network AG's contribution to the Infineon Security Partner Network

The secunet Security Network AG is as well as Infineon Technology one of the main partner of Federal Republic of Germany in regards to security, security consulting and usage of IT security products. Infineon and secunet Security Network AG are present in several standard bodies and initiatives by the BSI.

Additionally secunet has a long history in cyber security consulting, penetration testing and public key infrastructure (PKI) implementation in the automotive industry.

secunet is using Infineon's security controllers in their industry firewall product family "secunet edge", which is of strong interest to connect all kind of "things" and machines to the internet and companies' IT-systems.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10/2019

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.