endian|os

Medical Technology: Retrofit for secure digitization

One of the world's largest manufacturers of diagnostic ultrasound and MRI scanners has relied on remote maintenance for many years. To ensure that digital access is not a target for cyber-attacks, the company protects its sensitive medical technology with Endian 4i Edge Software. This allowed the existing gateways with radio frequency protection to be upgraded to a powerful security appliance.

"For a long time, medical technology was designed for use in closed systems. Due to digitization and the associated connection to the Internet, these devices have become a potential target for cyber attacks," explains Raphael Vallazza, CEO of Endian. "The ENDIAN SECURE DIGITAL PLATFORM offers the opportunity to network and secure medical devices through a quick and easy retrofit without the need for subsequent approval procedures."

Medical technology: a special case of digitization

Installing an IoT security gateway in front of a medical device is generally a good solution for retrofitting existing medical technology with all the necessary connectivity and security components for secure digitization. However, deploying IoT security gateways for MRI scanners and ultrasound devices is challenging because these devices generate high-frequency radiation during use, which can interfere with the operation of IoT security gateways. To establish connectivity in the typical heterogeneous IT environment of a hospital, the medical device manufacturer used special gateways from SECO that are protected against radio frequencies and comply with all medical regulations.

IoT security gateway software for comprehensive IT security

In order to continue using these gateways, the manufacturer opted for a unique solution from Endian. The South Tyrolean manufacturer offers an integrated cybersecurity platform that connects the digital world (IT) and the physical world (OT). The Endian 4i Edge X Gateway is used to connect physical devices and there is also a software version, the Endian 4i Software.

The Endian 4i Edge Software transforms any industrial PC and IoT gateway (x86 or ARM technology) into Endian's powerful connectivity and cybersecurity solution to secure medical devices. Several finely tuned security functions then ensure comprehensive protection. Deep Packet Inspection (DPI) analyzes the data packets sent over the network. In contrast to normal analysis methods, which are limited purely to metadata, DPI goes right down to the user level and is able to detect over 300 IT and OT protocols, as well as 2,000 applications. A Virtual Private Network (VPN) ensures secure remote access by encrypting the data during transmission so that it cannot be read or manipulated. If an attacker gets past the firewall, the Intrusion Detection System (IDS) recognizes the attack and the Intrusion Prevention System (IPS) can stop it from continuing or spreading throughout the network.

## Granular rights management for greater security

Granular access rights management provides an additional level of security. The Endian Switchboard, the central management tool of the ENDIAN SECURE DIGITAL PLATFORM, offers the possibility to assign different rights to users or user groups. For example, it is possible to define who can access which devices, what actions can be performed there and what data can be viewed. Every access is documented so that it is always transparent who was on which device, when, and what actions were performed there.

Up-to-date protection despite outdated operating system

The Endian Switchboard also allows the latest security updates to be installed on all IoT gateways. This was particularly important for the medical device manufacturer because the ultrasound machines and MRI scanners that needed remote access were based on the Windows XP operating system. Since Microsoft stopped providing updates for this operating system in 2014, its use is now too risky from an IT security perspective. "In industry and also in medical technology, machines are often in operation for ten years or more," explains Raphael Vallazza. "It is therefore not uncommon for medical devices to still be in use with older operating systems. By updating the gateways through the switchboard, all devices are protected. This is a key aspect in view of the NIS2 directive, which will be transposed into national law by the end of 2024".

No danger from mobile storage devices

The ultrasound machines and MRI scanners were also exposed to another IT security risk - doctors and hospital staff regularly use USB sticks to store images from examinations. However, malware can also enter the machines via these external storage media and even spread via the network if the devices are connected to the IT system.
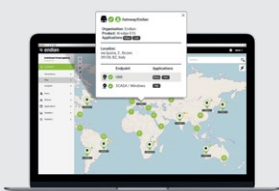
The **Endian Switchboard** is the heart of the Endian Secure Digital Platform that provides secure remote access to field equipment, data collection and visualization, edge computing and powerful user and device permission management.

Endian 4i Edge Software:
turn any IoT Gateway (x86) or industrial PC into an Endian 4i industrial cybersecurity appliance. The Endian 4i platform (powered by EndianOS) is tailored to the needs of the market to protect and connect industrial assets like PLCs, HMIs, RTUs and other SCADA systems.

To counter this, it was decided that the USB sticks should no longer be plugged directly into the ultrasound or MRI scanner, but into the IoT gateway, which also has the necessary USB port. Anti-virus software was installed on the IoT gateway to protect the devices from malware. Whenever a USB flash drive is used, it is first scanned for possible viruses or Trojans and any malicious programs are blocked.

The fact that all existing systems could be retrofitted so quickly and securely without having to purchase new hardware convinced the manufacturer of diagnostic ultrasound equipment and MRI scanners. In the future, all devices of the new generation will be delivered with the ENDIAN SECURE DIGITAL PLATFORM.