Medical Device Developments

Media partner:
Eucomed Medical Technology
www.eucomed.org

MEDICAL IVAM
COMPAMED
14th-17th November, 2016
Dusseldorf, DE

electronica
8th-11th November, 2016
Messe Müchen

2016 Vol. 2

www.medicaldevice-developments.com

£29.99 €46.49 $61.99

Reach out to the future

Robotic grippers with more touch sensitivity could mean a revolution in medical manufacturing

IoT and M2M

We examine how the internet of things can be best used in the medical industry

Body-rocking treatment

Advances in bioelectronic devices mean manufacturing partnerships are now crucial to success

Protecting endpoint security of medical systems

Protecting networks when accessed by remote devices such as laptops, or other wireless and mobile devices, is now a priority for medical device operators and manufacturers. **Oliver Winzenried**, CEO and co-founder of Wibu-Systems, explains the risk and rewards of endpoint security.

It is an undisputed fact that the internet is becoming increasingly pervasive in every aspect of our lives, resulting in an explosion of the numbers of machines, devices, and sensors connected to it.

By the same token, software is taking over hardware and reshaping business models by retrofitting existing systems, providing new functions, updates, upgrades, and bug fixing. Similarly, medical devices are no longer isolated boxes; instead, they are controlled remotely, equipped with new features, and engaged in a constant dialogue with other pieces of hardware and software, just like a smart phone, or any high-tech device.

There is no gain without pain, however. Cybersecurity, which encompasses policies, technologies and implementation methods, needs to become an integral part of any connected system – and the medical field is no exception.

Earlier this year, a German hospital was the target of ransomware, a type of malware that makes data inaccessible to its rightful owner. Hackers demanded ransom payments in exchange for a key that unlocked all the files they had encrypted. Just a few days later, another

hospital was attacked by a virus: 200 servers and all connected systems had to be shut down. There was no risk to patients or hospital operations because IT administrators had a safety plan in place, and all significant medical devices work without internet access.

However, the blackmailing of hospitals around the world is becoming more frequent, and we should expect further serious attacks as technology advances. Just as driverless cars seem to promise convenience, but currently also suggest accidents, attacks intended to tamper with diagnostic systems and surgical robots can have extreme consequences.

While smart and connected systems boost performance and herald an economic renaissance, piracy adds another layer of instability. Despite tougher legislation and a broader spectrum of educational resources, the threat of illegally sourced products has far from disappeared.

In a 2016 study, the German Engineering Federation showed that nine out of ten manufacturers were victims of piracy, and that in 70% of all cases reported, reverse-engineering was the main trigger.

Components, industrial designs, and even entire systems are being counterfeited across all sectors of industry. The intellectual property of today's X-ray machines, MRI scanners, dental devices, infusion pumps, nanotechnologies and mobile patient monitoring, to name just a few common cases, is encapsulated in embedded software.

There are different schools of thought about how best to combat piracy, but international frameworks are being set up to secure technology as it progresses.

The reference architecture RAMI 4.0 and the Plattform Industrie 4.0 Management Shell are cross-industry reference models designed to lay sophisticated foundations for the new concept of Industrie 4.0, in which the requirements of the IT industry, automation technology and mechanical and plant engineering are merged into one shared design.

The discussion is moving beyond definitions, standards, and norms. The Industrial Internet Security Framework (IISF), for instance, offers a common framework that helps define "trustworthiness" in IT systems and operational technology (OT) systems. The IISF redefines risk assessments, threat metrics, and performance indicators by focusing on five characteristics: security, privacy, resilience, reliability and safety.

In particular, endpoint security concerns multiple levels:

- physical security prevents uncontrolled changes to or the removal of the endpoint
- root of trust provides confidence on the endpoint identity
- integrity protection ensures that the endpoint is in the configuration that enables it to perform its functions predictably
- access control ensures that proper identification, authentication and authorisation protocols are performed
- secure configuration and management control updates of security policies and configurations
- monitoring and analysis includes integrity checking, detecting malicious usage patterns or denial of service activities, and enforcing security policies and analytics

- data protection controls data integrity, confidentiality and availability
- security model and policy governs the implementation of security functions.

Oliver Winzenried
Oliver Winzenried is CEO and co-founder of Wibu-Systems. He is also head of the board of product and know-how protection at the Association of German Engineering Federation and a member of the board of directors of the Medical Technology working group of the Mechanical Engineering Industry Association.

Protect technical know-how

Dentsply-Sirona is a case in point. Sirona, a spin-off of Siemens' medical business unit, is a leading maker of dental products. In order to comply with directives from the Medical Practice Group (MPG), the regulatory body for medical appliances, and protect the intellectual property of its software against reverse engineering and tampering, Sirona reinforced its built-in security by applying a special encryption recipe to its software and using a hardware secure element on the appliance. While a secure communication channel remains paramount, that in itself cannot safeguard the endpoint.

Secure key storage at the endpoint offers the most effective approach to security, especially when the secure element is designed with industry-grade components, relies on smart card technology and is fully certified.

Rethink the business model

Agfa HealthCare is a leading provider of diagnostic imaging and healthcare IT solutions. Its complete set-up for digital computed radiography encompasses the most cutting-edge technology in CR, but small laboratories, orthopaedic doctors, and other facilities cannot afford the upfront investment for hard and software. To reach the vast low-end market, the company introduced its easy payment scheme: software assets are simultaneously encrypted to protect them against illegal and fraudulent use, and distributed with time-based licences. The return on the investment was guaranteed in just a few months, and Agfa can now count on a larger customer reservoir.

Remote management and control

Custo med is a well-established brand for a diagnostic cardio-respiratory acquisition and reporting system. Special additions were injected into its embedded software ensuring that its medical systems are protected against technological manipulation and can be monitored in accordance with legal requirements. Full modularity and scalability in terms of performance and usability in all kinds of clinical IT networks is also guaranteed.

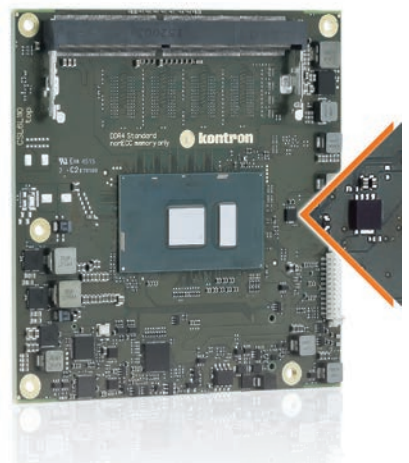
Should technical problems occur, the specific release and licence status of the user can be identified, allowing quick and safe after-sales support. ››

Reducing bottom-line costs and planning for the future

The success stories described have a common denominator: the fact that it is imperative for medical device manufacturers to protect their code, machine configuration and patient data throughout.

Implementing security is not meant to be an investment forced by circumstance; instead, it can be used to generate new and recurring sources of income.

Technologies such as CodeMeter from Wibu-Systems can support a wide array of platforms, from computers, embedded systems and PLCs, down to the most advanced microcontrollers. They couple intellectual property protection and licence life-cycle management, allowing for an extremely versatile redesign of the complete workflow.



A Kontron-made CPU module with integrated key storage.

> “Implementing security is not meant to be an investment forced by circumstance; instead, it can be used to generate new and recurring sources of income.”

Software and know-how protection by encryption

Digital know-how is protected by encrypting any executable material. During this process, the software publisher can opt for the automatic encryption of whole applications, encryption of specific tagged functions, or a combination of both.

Rather than creating separate applications for the different variants, every customer receives the exact same piece of software – it is the licensing system that defines the entitlement rights.

Secure key storage

As per Kerckhoffs' Principle, encryption methods are typically publicly documented – the only secret element is the key itself. It is therefore essential that the key is stored in a special repository. Containers can embed a smart card chip and rely on its additional encryption and certification properties. They can then withstand side channel or differential power analysis (DPA) attacks.

The key never leaves the secure area and all major cryptographic operations take place inside the secure hardware. External secure elements provide mobility and licence transferability, internal secure elements can be mounted directly on the printed circuit board, offering physical anti-tampering characteristics, and software secure elements can be bound exclusively to the properties of a specific machine.

Tailored services for each customer

The shift from hardware to software sophistication has enabled customers' demands and expectations to be met more accurately than ever. Manufacturers can remotely enable and disable functions, update and upgrade machines, turn demo licences into fully featured products and subsequently control their use, adjust their offerings and billing criteria, and predict demand for consumables or spare parts.

Temporary assignment of rights for maintenance

Even maintenance is a delicate matter that may involve security breaches. To mitigate these risks, technicians should be authorised to access machines and any related documents only temporarily. This restriction can be set up with the use of licence entitlement on a case-by-case basis.

Protecting confidential patient data from misuse

Regardless of specific national arrangements, all countries prescribe the privacy and confidentiality of patients' data. Medical device manufacturers can comply with these directives by relying on encrypted and digitally signed data, which cannot be accessed by unauthorised personnel, tampered with, or transferred to other devices other than those identified and assigned to the job.

Centralised licence management

Licence management systems facilitate creating, delivering and managing users' rights in the form of software licences associated with product stock keeping units (SKUs). The more flexible the product design modelling, the more avenues for business are created.

This stage fits in well with the concept of app stores, where sales are driven by on-demand features, pay-per-use and upgrades. Integration with mainstream ERP, CRM and ecommerce systems optimises and automates back-office processes, with additional savings in time and performance.

Same difference

When it comes to the use of medical devices, there are always at least two relevant groups with different, but complementary, demands concerning security. Device manufacturers want to capitalise on their investment by protecting it against counterfeiting and fraudulent manipulation, and by enabling new business models and streamlining their logistic processes.

Device operators, meanwhile, have the integrity of their devices and patient data at heart, and want to ensure the correct behaviour and performance of the medical device as it was originally tested and approved. ■