Medical Device Developments

Media partner: Eucomed Medical Technology
www.eucomed.org

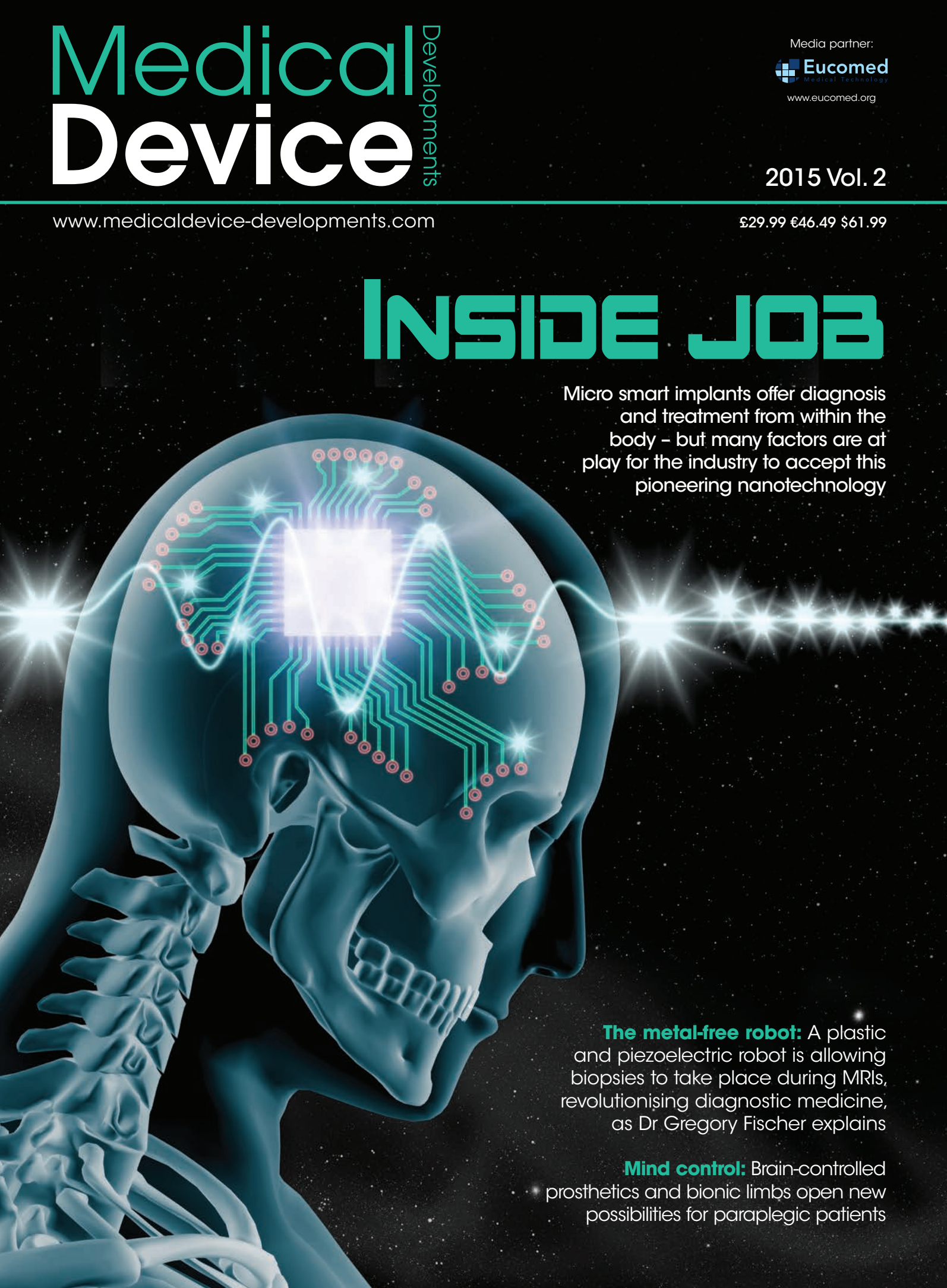
2015 Vol. 2

www.medicaldevice-developments.com

£29.99 €46.49 $61.99

Inside job

Micro smart implants offer diagnosis and treatment from within the body – but many factors are at play for the industry to accept this pioneering nanotechnology



The metal-free robot: A plastic and piezoelectric robot is allowing biopsies to take place during MRIs, revolutionising diagnostic medicine, as Dr Gregory Fischer explains

Mind control: Brain-controlled prosthetics and bionic limbs open new possibilities for paraplegic patients

Stay secure

Medical device manufacturers are moving into the internet-of-things space, producing devices with increased connectivity and upgradability. Such approaches, however, render these products more susceptible to security threats and counterfeiting. **Oliver Winzenried**, CEO of Wibu-Systems, advises OEMs how to most effectively meet these challenges.

The internet of things (IoT) is one of today's most debated topics. What makes an IoT product, and what separates it from the embedded devices of the past? It is an evolutionary leap: while embedded devices have often been stand-alone pieces using custom hardware, IoT products employ standard hardware and software platforms, and are connected to networks. They enable increased functionality and upgradability, but also face security threats and increased susceptibility to counterfeiting.

The types of medical devices that already are – or can become – IoT devices span a broad range. They include:

- stand-alone devices like infusion pumps, blood pressure meters, ECGs, lung monitors and various trackers
- large medical machines, like MRTs, X-rays and heart-lung machines, used in hospitals and intensive care
- home applications for ambient assisted living, on smartphones, smart watches or connected smart sensors
- support for mobile care services
- blister packaging for drugs.

But in enabling increased connectivity and software-driven features in these devices, several challenges are posed for manufacturers.

For instance, protecting the know-how and intellectual property invested in such devices is essential for the survival of the developers and manufacturers. According to a VDMA study on product piracy, nine out of ten manufacturers face this hurdle, while 51% grapple with the counterfeiting of complete devices. The main source of piracy is reverse engineering, by simply copying the original device or by understanding its algorithms and USPs with minimum effort then using this information in counterfeit products, which takes much less effort than the original research and development.

Network connectivity and the ability to upgrade features via the firmware of an IoT device also increases the risk of manipulation from the outside. Additionally, there is concern about tampering with the parameters of medical devices used for vital medical purposes in a hospital: German magazine *Der Spiegel*, for instance, has recently reported issues with infusion pumps and anaesthesia devices. Product certification for device manufacturers, according to US FDA or Germany's Medical Products Act, requires manufacturers to use state-of-the-art measures to guarantee that the device is operated as certified. The new connectivity and functionality of IoT devices requires security by design, with additional cryptographic mechanisms.

Additionally, with multiple devices connected to one system, OEMs must ensure their products receive non-compromised data from the correct sensors, and set-up or control commands from authorised devices or users. This requires device and user authentication, and data integrity.

Security on all scales

Personal security is also a worry. Medical IoT devices acquire personal patients' data, which needs exacting privacy standards. Data confidentiality has to be guaranteed within devices and in all communication between users, relatives and doctors, in the hospital networks or the internet. ››

Oliver Winzenried
Oliver Winzenried is the founder and CEO of Wibu-Systems. His passion for software protection has resulted in numerous patents and awards, covering areas from secure licence management and anti-tampering solutions to dongle feature innovations.

In the past, stand-alone devices had a fixed set of features defined during production, which, in some cases, were upgradeable during maintenance. Revenue comes from the selling of the product, updates or upgrades, maintenance or consumable sales, followed many years later by the sale of replacement devices. IoT products enable remote feature activation and updates; pay-per-use pre and post-paid options; and app-store-style features. These concepts enable new elements not thought of during initial product development. Recurring revenue streams can be established and manufacturers benefit from the shorter time to market, as devices can be introduced sooner with basic features due to upgradability in the field. A secure upgrade path is required to use this flexibility in compliance with regulations, but all is not lost: several technical solutions have been described as responses to these kinds of challenges.

The embedded software of the IoT device must be prevented from being used on another device. The solution for this is symmetric encryption. The software in the device's non-volatile memory, such as a flash drive or disk, is stored in encrypted form; at runtime, required parts of the software are decrypted in RAM. The required cryptographic keys need to be stored in secure key storage to prevent their duplication. This is done in trusted platform module chips or smart card chips in industrial dongles.

> "Manufacturers of IoT devices in the medical space must implement security mechanisms by design to safeguard patients' safety and privacy, and device availability and robustness against cyberattacks and product piracy."

Algorithms are often the results of intensive and expensive research and development, and they represent the USPs of a device. If competitors can analyse and understand these codes without major effort, they can quickly implement them in their own products. Copyright laws do not help in such cases; patents might provide legal protection, but enforcing them is time-consuming and expensive. In this case, the solution is to store the program code in encrypted form, as with the previous example. This will make using decompilers and disassemblers impossible. Additional measures are necessary to avoid dumping decrypted code from the RAM, such as disabling debugging interfaces.

Secure boot, digitally signed code and data, and configuration parameters are a basis for trust. An IoT device loads its embedded software in a specific sequence during booting, and to achieve integrity protection, this sequence needs to include the following steps:

- The bootloader verifies the integrity of the operating system and loads it after validation.
- The operating system only starts once the bootloader has been validated as trustworthy in a reverse check.
- The operating system verifies the integrity of the application and loads it only if it has been validated.
- The application only starts if the operating system has been validated to be trustworthy in a reverse check. The application verifies the integrity of the configuration data and only uses it after validation.

First, the unprotected original software has to be signed and encrypted, by:

- calculating the hash values of the original software
- signing the hash value with the private key of the vendor
- encrypting the original software with a key generated from a seed value within the original software, a secret key of the vendor and certain other parameters selected by the publisher
- attaching the public portion of the signature certificate to the encrypted software.

The verification consists of the following steps, which are executed while the application is being loaded:

- If a valid licence is present, the encrypted software is decrypted.
- The certificate attached to the credentials or the certificate chain is verified against the public root key.
- The hash value of the decrypted original software is calculated.
- The signature of the hash is verified using the public key.

In addition to these necessary steps, further measures can be implemented to attain a higher level of security, such as the sophisticated handling of certificates, checks against a preset expiration date for certificates, or the existence of a certificate revocation list (CRL). Such verifications can be executed periodically at runtime in the system memory.

Encryption, certification and licensing lead the way

OPC UA (Unified Architecture) is growing more established in the industry. It offers interoperable security functions according to IEC 62541, for:

- **confidentiality:** communication encryption
- **integrity:** data integrity against manipulation
- **application authentication:** software applications authenticating each other via certificates
- **user authentication:** a user needing to be authenticated to be able to use an application
- **user authorisation:** a user being granted access to data according to the role associated to them
- **auditing:** server logs having all relevant security access
- **availability:** redundancy mechanisms increasing availability. ››

It is a major challenge for IoT applications to distribute certificates to numerous networked OPC UA servers and clients, and store them securely. All efforts to implement standardised mechanisms are nevertheless a good investment. The benefit is interoperability between devices of different makes.

One hardware product can enable a large ecosystem with software-realised features. The number of physical products to be produced, certified and kept on stock – and the numbers of SKUs – can be reduced. Different product features can be activated using licences with different cryptographic keys, to decrypt the corresponding code in the IoT device. Completely new features can be downloaded and activated in the manner used by common consumer app stores. Users and vendors benefit from pay-per-use concepts, reducing the initial purchase price and adding recurring revenue streams.

The creation and deployment of keys, certificates and licences that define the IoT device features and track its usage need to be integrated in the manufacturer's business process. This includes customer portals on the internet or offline, and interfaces with existing ERP, BI or CRM systems. Flexible cloud-based or physical-premise solutions are available on the market.

Many developers already understand the principle of asymmetric and symmetric encryption, but lack experience implementing it. As there are many pitfalls, it eases developers' lives and saves implementation costs if tools are there to support these mechanisms. There are some sophisticated commercial tools available for microcontrollers, as well as embedded and PC-based platforms. They support IP protection by encryption, modular feature-based encryption, digital signing of data and code, verification and operating system integration, secure key storage with different secure elements and software-only variants, including time-based, usage-based and many more licence models.

Security by design is a must. Manufacturers of IoT devices in the medical space must implement security mechanisms by design to safeguard patients' safety and privacy, and device availability and robustness against cyberattacks and product piracy.

Connected IoT devices with flexible licensing herald new business models: rethinking device monetisation strategies enables recurring revenues and customer experience advantages.

There are solutions on the market for storing cryptographic keys securely, with IP protection, flexible licensing and tamper-proofing, achieved with sophisticated tools integrated in many development environments in embedded and PC-based systems. They offer a fast return on investment as well as ease of use, and guarantee not only fast and easy first integration and state-of-the-art security, but also continuous innovation and improvements to meet the requirements of today and the future. ■