Ablation tools should be designed with security in mind

Patient safety comes first

Hacking of pacemakers and insulin pumps has raised concerns about lax medical device security, say **Nathan Sharp** and **Scott Jones**

Undergoing a medical procedure such as surgery is already an unnerving experience. The last thing that a patient should have to worry about is whether the surgical tools have been compromised in some way.

What if a breach causes a single-use tool to be reused, or the tool has been used beyond its expiry date? Or suppose a counterfeit version of an instrument is inadvertently put into use. The worst-case scenarios of such breaches could have fatal consequences.

A *Forbes* article, ‘The lack of medical device security – accidents waiting to happen’, cites a survey conducted by the privacy research body the Ponemon Institute, which found that 67% of hospital network security specialists questioned answered “no” or “unsure” when asked if medical device security was on their shortlist of concerns. About one third of the respondents indicated that they had not considered the issue during their budgeting processes.

The reasons for not implementing security are common across many industries and are, unfortunately, grounded in three pervasive myths: it’s too complicated; it takes too much time; and it’s expensive.

Device makers either pledge to address security later, or they go for a less robust route. While software encryption is seen as cost effective and easy to implement, it is not as effective as its hardware-based counterpart.

Security provided by the encryption code can be compromised if there is a security vulnerability in the operating system (OS). It is also difficult, if not impossible, to exhaustively determine all of the potential interactions that could trigger a security breach, which leaves a system with many potentially vulnerable points.

Hardware-based security, on the other hand, has proven to deliver a stronger level of protection for embedded devices.

Ablation tools, which enable

cardiac electrophysiologists to map the pathways of complex arrhythmias, are the kind of medical devices that should be designed with built-in protection against hacking and cloning.

Hardware protection

There are many advantages to implementing a hardware-based security approach using ICs such as secure microcontrollers and secure authenticators.

Secure microcontrollers use advanced cryptography and physical security to protect embedded devices from side-channel attacks, physical tampering, and reverse engineering. Using a secure microcontroller's internal, immutable memory to store startup code, for example, provides a root of trust that cannot be modified. This trusted software can then be used to verify and authenticate the application software's signature.

Secure authenticators provide crypto-strong authentication to protect the medical tool and sensor supply chain from unauthorised sources, to securely manage tool usage life, and to provide the ability to securely set tool or system features in a design.

Common cryptographic algorithms found on security ICs include the secure hash algorithm (SHA-x), which plays a role in symmetric (secret) key authentication. SHA-x cryptographic hash functions are computationally complex mathematical operations run on digital data.

Comparing the computed hash to a known, expected hash value provides an assessment of data integrity. Since cryptographic hash characteristics are non-reversible, it is computationally infeasible to determine the input corresponding to a message authentication code (MAC).

They are also collision-resistant, so it will be hard to find more than one input message that produces a given MAC. With their high avalanche effect, any change in input produces a significant change in the MAC result, so SHA-x has demonstrated the ability to be very effective for secure authentication and small digest encryption.

The elliptic curve digital signature algorithm (ECDSA) is another example of a cryptographic algorithm commonly supported by security ICs. ECDSA, which is used in asymmetric (public) key authentication, uses elliptic curve cryptography in which the keys should be roughly twice the length of equivalent-strength symmetric key algorithms.

With the ability to openly exchange a key from the sensor or device to the host system without security risk, public key cryptography is suitable for applications that are network connected or use the internet of things. Additionally, a public key-ECDSA enables strong security for systems where it is difficult or impossible to secure keys on a host system processor. Using a security IC offloads the main processor in a design from performing these compute-intensive cryptographic operations.

> “Some 67% of hospital network security specialists questioned answered ‘no’ or ‘unsure’ when asked if medical device security was on their shortlist of concerns

Cryptography protection

In addition to the cryptographic algorithm support, secure authenticators offer many other features to protect medical tools from unauthorised use or cloning.

For example, device memory can be configured with protection settings so that only a host with knowledge of device key/secret can make modifications. This is used to track and manage the number of times a limited-life tool is used.

Similarly, a decrement-only counter is commonly provided and can be used for the use-management function. A secure general purpose input/output (GPIO) pin supports secure switching with on/off control and sensing that is either ECDSA- or SHA-256-controlled.

Memory resources are integral in a secure authenticator where sensitive information, such as keys, certificates, and application data are stored. In addition to sensor life, non-volatile memory also typically stores calibration and manufacturing data. Another consideration for medical tools is the fact that many of these devices are exposed to high levels of radiation via gamma and e-beam medical sterilisation. These radiation levels can disrupt and damage certain types of non-volatile memory. An effective secure authenticator for these types of devices must provide radiation-resistant, bi-directional authentication.

Preventing harm perpetrated through unprotected medical tools and instruments can be as straightforward as integrating a security IC into the design. Secure microcontrollers and authenticators mean that developers do not have to be cryptography experts to protect medical designs. ❏

Secure authenticator is radiation resistant

Maxim recently introduced the DS28E83, a secure authenticator that provides security capabilities specifically for sterilised medical tools.

The radiation-resistant, secure authenticator allows user-programmable manufacturing or calibration data before medical sterilisation. It is claimed to be the industry's first radiation-resistant, one-wire secure authenticator for medical surgical tools or sensors that undergo gamma or e-beam sterilisation.

The authenticator resists up to 75kGY of radiation. It features ECDSA P256 asymmetric secure authentication, SHA-256 hash-based message authentication code (HMAC) symmetric key secure authentication, elliptic-curve Diffie-Hellman (ECDH) key exchange for optional secure session keys between host and slave authenticator communication, 10kbit of gamma-resistant memory to store keys and application data, and a GPIO pin with optional authentication control for a secure switch.

Applications that previously could not use secure authenticators because of the need to sterilise instruments now have an option, the company believes.

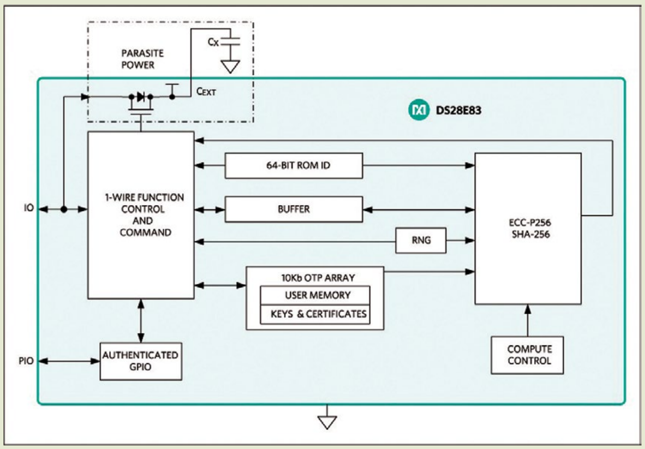

Figure 1: Maxim Integrated's DS28E83 provides security for sterilised medical tools

About the author

Nathan Sharp is senior business manager and **Scott Jones** is managing director for embedded security at Maxim Integrated