Laird™

CONNECTIVITY

Securing Your Medical Device Starts with a Secure Communications Module

In today’s technological landscape, securing your device is an increasingly complex goal that requires more comprehensive approaches.

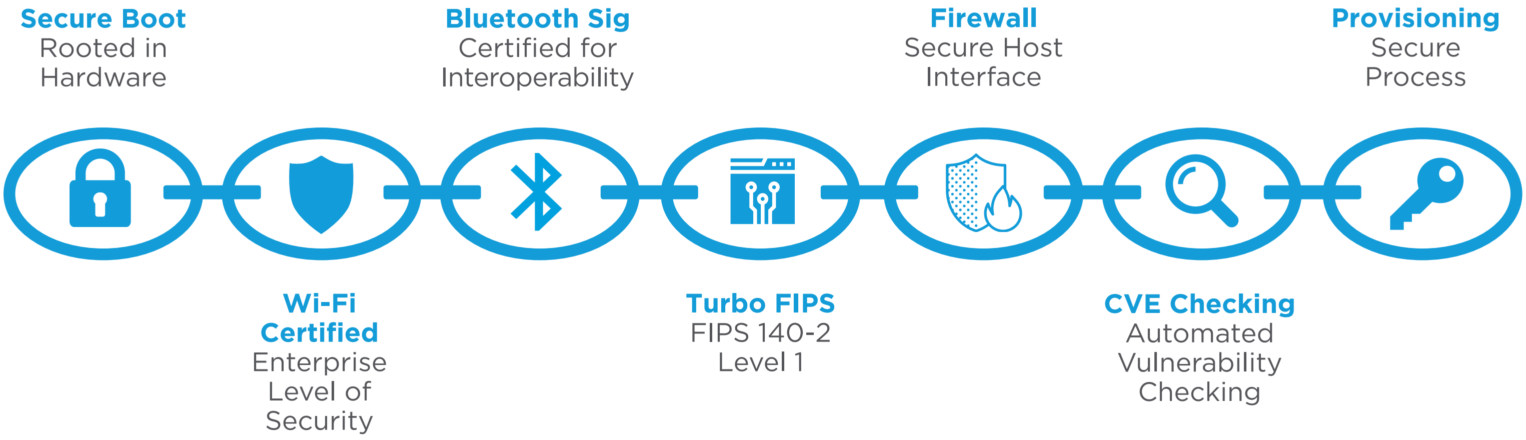
Securing Your Medical Device Starts with a Secure Communications Module

Understanding Laird Connectivity's Chain of Trust Architecture

In today's technological landscape, securing your device is an increasingly complex goal that requires more comprehensive approaches.

The best and most effective approaches to device security address the vulnerabilities at every level, isolate subcomponents to firewall potential damage, and rigorously test to stay ahead of malicious activities. Devices leveraging an embedded OS, such as Linux, require security to be designed at the point of product creation and hardened to a sufficient level prior to leaving the factory.

Laird Connectivity is introducing its latest line of Enterprise Performance and Security modules based on the 60 Series SOM. These modules use the Chain of Trust architecture which is rooted in hardware to ensure only authorized software is loaded and executed on the device. This makes it much more difficult to leverage the 60 SOM-based communication module to compromise its host or attack other devices on the same network. The 60 SOM-based communication module is also designed to be securely updated to quickly remediate any vulnerabilities found in the future.



Secure Boot Rooted in Hardware

Wi-Fi Certified Enterprise Level of Security

Bluetooth Sig Certified for Interoperability

Turbo FIPS FIPS 140-2 Level 1

Firewall Secure Host Interface

CVE Checking Automated Vulnerability Checking

Provisioning Secure Process

Chain Of Trust – Verified At Every Layer

Laird Connectivity's Chain of Trust architecture, in combination with secure production provisioning, secures software images running on the 60 SOM. For customers utilizing the 60 SOM as the wireless communications module, this architecture protects from attacks using vulnerabilities exploited on the module to further attack the hosted platform. For devices utilizing the 60 SOM as the host for the main application, the Chain of Trust provides a mechanism to provision and update software with signed images, preventing unauthorized or rogue software from loading into the device.

Over time, unpatched connected devices become one of the largest potential attack surfaces given that their security vulnerabilities become well-known and easily exploited.

The Chain of Trust is based on a Secure Boot process that begins with an embedded Hardware Root of Trust. The Secure Boot process enables the Root of Trust to be chained to all executable code for the 60 SOM enabling verification of every bit of code running on the module. Secure Boot also controls the available boot sources. Insecure boot paths such as serial or USB ports are disabled permanently during the production process.

During the production provisioning process, a secure symmetric key is programmed into the hardware. The first external boot code that is executed by the 60 SOM is stored in the onboard flash. This boot code is encrypted with the same symmetric key during provisioning thus ensuring the contents remain secret and can be verified as trustworthy. The device will not boot unless the code and data loaded from the flash memory matches the unique pre-determined hash generated during production. This proprietary and secure implementation protects against modifications to the 60 SOM, preventing the loading of insecure images or the enabling of external boot processes.

Security can be increased further by enabling each individual device to be programed with a unique encryption key. If one device is ever compromised, that key cannot be used to attack multiple devices. At a minimum, we anticipate providing unique keys on a per customer or customer device type basis.

The Laird Connectivity Chain of Trust architecture includes an Encrypted File System on the 60 SOM to store confidential information such as network credentials, passwords, or other configuration details deemed sensitive by the end user or hospital where the unit is deployed. This protects any stored credentials or configuration details from exposure to hackers and intruders.

Designing and building secure products is only the beginning. Software and image updates are required over the life of the product to improve performance, add features, and fix security vulnerabilities. Over time, unpatched connected devices become one of the largest potential attack surfaces given that their security vulnerabilities become well-known and easily exploited. The reason is simple – an attacker can scan a network to find devices with old firmware, then simply take advantage of well-known, well-documented vulnerabilities without having to first do the hard work of discovering how to attack the device. This type of attack is so simple that it can be fully automated and deployed by amateur hackers.

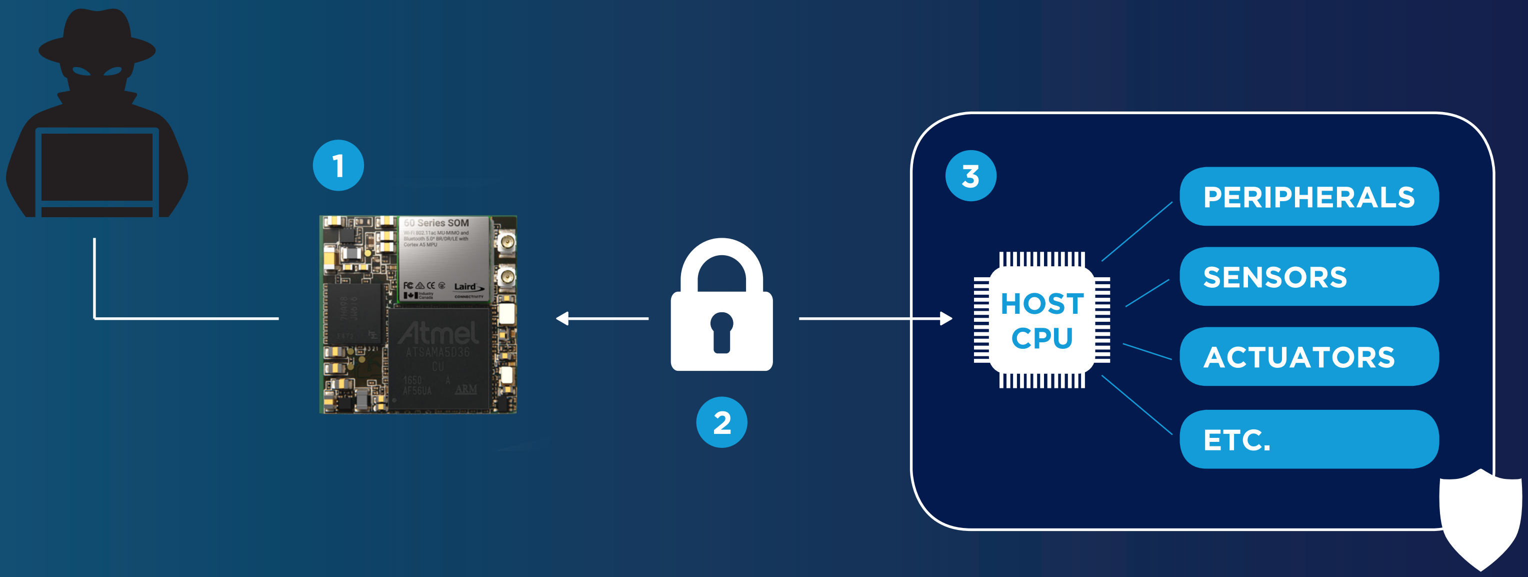
By working in partnership with our customers, it is possible to ensure all devices are up to date. This may include Laird Connectivity managing the update process to connected devices in the field via a web service, as well as making updates available to our customers and end users where a physical update of the device may be required.

Firewall – Isolating Subcomponents For Greater Security

Compartmentalization is used commonly for physical security within buildings with the use of separate, secure rooms. If a person enters the building or room, they are separated from the main building or secure area via locked doors until building security clears them. Laird Connectivity's 60 SOM leverages its Firewall in the same way, with the use of barriers implemented at the hardware level to enforce isolation between the software components of the system, preventing security vulnerabilities or breaches in one software component proliferating to other areas of the system. The use of compartmentalization in a system design increases the strength in depth of security within the design. The use of the 60 SOM to provide secure and robust communications immediately delivers additional protection within the product, protecting any mission critical applications running within the host processor of the product from attacks launched against the outwardly facing 60 SOM communications module.

Additional compartmentalization techniques within the 60 SOM Secure Communications Module utilize the hardware memory management unit of the processor and Linux system processes to further enhance security.

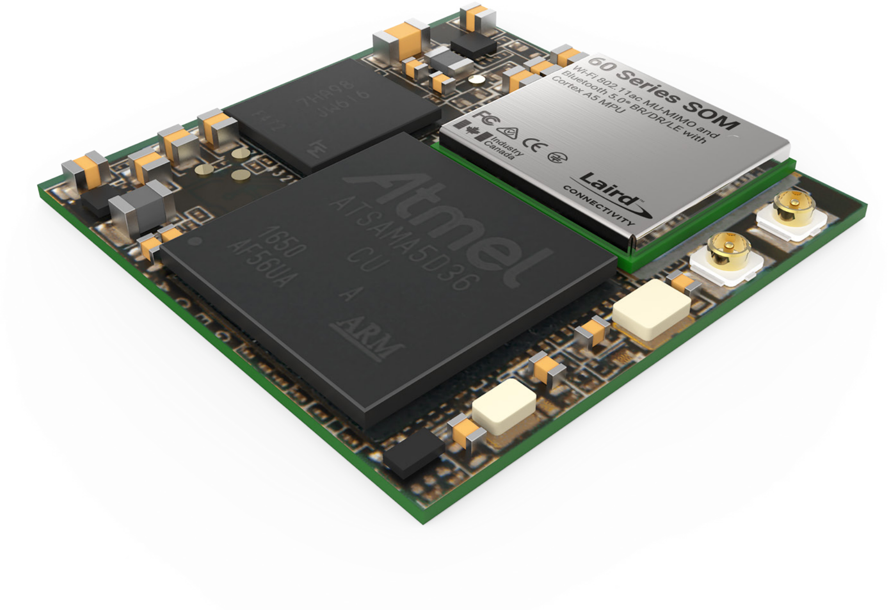
To aid customer products to implement the Firewall within their designs using the 60 SOM secure communications module, Laird Connectivity provides a secure communications link to the host via a software library/API. This allows the product host processor to control, configure, and communicate data through the 60 SOM secure communications module using a cryptographically secured communications channel. If the 60 SOM loses connection to the host via this secure connection for whatever reason, it will disable wireless access to the network.



1 **A malicious attack on the system can be intercepted by the 60 SOM, which functions as a basic firewall for the host system.**

2 **The host system communicates with the 60 SOM only over a secured connection via Laird Connectivity's DCAL library, restricting access from outside actors.**

3 **The isolation allows the host device to remain safe in the event of attacks on the 60 SOM and allows mission-critical operations to take place unrestricted.**



Common Vulnerabilities

Laird Connectivity continually monitors software packages utilizing Laird Connectivity's Linux distribution process, ensuring that new vulnerabilities are analyzed and addressed as soon as they are identified. This is achieved through an automated set of tools which monitors the publicly available CVE database, alerting Laird Connectivity when new vulnerabilities are announced. Laird Connectivity is committed to working with 60 SOM customers on a process to alert them of new vulnerabilities and informing them of steps to mitigate their impact within the installed base.

Penetration Testing

Laird Connectivity utilizes the 60 SOM and other aspects of Laird Connectivity's technologies within our stand-alone products such as gateways and communication dongles. Laird Connectivity is actively performing penetration testing of these units to check for exploitable vulnerabilities. This will be followed by action plans and design activities to further harden the devices against exploits. Information and expertise captured through this process can be applied to the 60 SOM and confidentially shared with integration customers as needed. Laird Connectivity actively works with customers to support penetration testing of complete units that leverage our secure communication modules.

> Laird Connectivity is committed to working with 60 SOM customers on a process to alert them of new vulnerabilities and informing them of steps to mitigate their impact within the installed base.

Wi-Fi Certification – Enterprise Level Of Security

Wi-Fi CERTIFIED™ is an internationally-recognized seal of approval for products indicating that they have met industry-agreed-upon standards for interoperability, security, and a range of application specific protocols. Whether deploying a new infrastructure or integrating new equipment into an existing infrastructure, using Wi-Fi CERTIFIED products ensures interoperability of Wi-Fi products from multiple vendors. Fewer network problems and support calls are often additional advantages of using Wi-Fi CERTIFIED products. Laird Connectivity is pursuing Wi-Fi certification on the 60 SOM series for 802.11ac Wave-2. The solution will also be WPA\2 certified and offer a software roadmap to WPA3 certification. In terms of authentication types, Laird Connectivity goes beyond most vendors by supporting enhanced authentication methods.

Authentication Support - Laird Connectivity's Enhanced EAP Supplicant

Laird Connectivity provides an enhanced EAP Supplicant within our embedded Linux package. The Laird Connectivity supplicant manages the connection state machine and supports the standard supplicant and security role. The Laird Connectivity supplicant supports additional EAP types versus those found in most open source supplicants. Laird Connectivity has gone through extensive testing and optimization of the supplicant including modifications to tune and optimize supplicant behavior, ensuring the best performance in the field. An example would be taking advantage of Laird Connectivity's signature fast scan and roam capabilities for the Enterprise. Support for Cisco Centralized Key Management (CCKM) is also included for greater interoperability and performance on Cisco's network architecture.

FIPS 140-2 Turbo - On-Board Cryptographic Engine

Within the Laird Connectivity 60 SOM, we are implementing FIPS 140-2 Turbo functionality, which allows you to satisfy federal security requirements for encrypting data in motion and rest without sacrificing enterprise network performance. The 60 SOM's hardware acceleration will be directly NIST certified for FIPS 140-2 Level 1. The 60 SOM certification facilitates end products meeting the FIPS requirements without the need for the end product to go through the certification process directly. The solution will contain capabilities for power-on self-testing and encryption key management. As an added security benefit, the module will support full encryption of onboard network parameters and other information to maintain security of the local network. The hardware accelerator will be accessible via an API interface, allowing its use within the application for things such as encrypting data at rest. This dedicated hardware accelerator allows excellence in cryptographic generation without compromising the rest of the device's resources and without impacting your application performance.

Laird Connectivity's Secure Communications Modules

Healthcare providers and executives around the globe know it is imperative that patients' health information is accurate, accessible and captured in near real-time. Connecting smart medical devices to the network to provide data interchange with EMR and like hospital systems is transforming hospital operations; increasing efficiency and accuracy of data capture. However, to minimize the exposure of patient and other critical data, this must be done in a secure environment. Laird Connectivity begins the process of securing the medical device with a secure communications module with security built in from production and maintained through the update process. Laird Connectivity's Chain of Trust architecture is designed with multiple layers of verification, signing, encryption, and isolation to ensure the device only runs trusted software and isolating the host application from intrusion attempts. This, in combination with Laird Connectivity's dedication to identifying and fixing vulnerabilities proactively, is the strength that the 60 SOM presents – a comprehensive, multi-level approach that ensures your device is secured in the event of a malicious attack.

For more on the Laird Connectivity 60 SOM module and the Chain of Trust architecture, contact CS-Sales@lairdtech.com.