



Embedded Cybersecurity for Industrial Control Systems: Putting Protection Where It Matters Most



Summary

Operational technology gets smarter and more connected each year. As the amount of data generated and processed within OT networks continues to grow, new opportunities have arisen for threat actors—ranging from individual cybercriminals to nation states—to wreak havoc on critical systems.

OT operators need assurance that their devices are protected and securely reporting data. Maintaining that assurance has grown increasingly difficult. Even systems that are not directly targeted can bear the cost of collateral damage, due to the rapid pace of development in new threats that specifically target ICS systems.

The solutions available to protect OT assets and devices have become problematic. Industrial firewalls, in particular, are complex to implement and maintain, and are the most common point of failure in a successful cyber attack. An incorrect setting in an industrial firewall creates a paradox where the very device asset owners rely upon to protect their network introduces new vulnerabilities. Moreover, tuning and updating firewalls drives head count and high operating expenses while delivering questionable return on investment to the asset owners.

To manage the growing threats, OT operators are shifting to a model in which cybersecurity is built directly into OT devices, rather than added on after the fact. Embedded, hardware-enforced security technology provides stronger protection and simpler administration than any other approach.

More connectivity, more risk

Industry 4.0—the ongoing move toward interconnectivity and automation in industrial process control—has opened a world of new possibilities for critical infrastructure operators.

For the first time, systems and devices at the lowest levels of the industrial network, like actuators, sensors, and switches, are gaining network connectivity on a broad scale. These newly-smart devices give critical infrastructure operators an unprecedented ability to monitor and adjust system performance in real time.

Increased connectivity creates not only opportunities to optimize performance, but additional vulnerabilities as well. Of particular concern is the fact that network connectivity exposes low-level industrial devices to attackers. Devices that were previously inaccessible, except through direct physical contact, can now be attacked over the network.

The consequences of a successful attack at the control or process level are potentially much more severe than those of a breached workstation or server. In addition to the financial damage that follows any security breach, disruptions at these levels can lead to physical damage and even loss of life.

In response to these new threats, industrial network owners are seeking alternatives to the existing cybersecurity paradigm and looking for ways to reap the operational efficiencies that come with the delivery and analysis of rich performance data, without exposing industrial devices to critical security threats.

Hardware vs software-based security

Software-based industrial firewalls are inherently high maintenance and vulnerable to sophisticated attacks. Hardware-based security technology provides more reliable protection and requires little to no maintenance, and has gained wide adoption among critical infrastructure organizations.

Why are software-based firewalls vulnerable?

Like any other form of software, industrial firewall software relies on a central processing unit (CPU) for its operation. A CPU has no built-in restrictions on what it will and will not do— if malicious code reaches the CPU, the CPU will execute it.

Adding to the risk is the fact that most software-based industrial firewalls are designed to run on commonly-used commercial operating systems. These operating systems have been studied by threat actors for years (or decades), and an enormous number of vulnerabilities have been documented and exploited.

The result is that threat actors are constantly creating and deploying new forms of malicious code to use in attacks against critical infrastructure systems. Software providers and security teams are forced into a continuous cycle of reactive protection, patching and updating their systems to protect against the emerging threats.

This pattern places a burden on every security operation, but is uniquely challenging for critical infrastructure operators, due to the time-consuming and expensive nature of testing and deploying new patches for mission critical systems.

Hardware-based security: simpler and stronger

Hardware-based security technology provides a cheaper, more secure alternative. Hardware security solutions can be designed so that it is physically impossible for a component to operate in an unintended way, or to perform any function other than the one it was designed to perform.

Implementing security based on Field Programmable Gate Array (FPGA) chips, rather than general purpose CPUs, can reduce or even eliminate the potential for unintended execution. An FPGA can still implement very complex logical functions, but unlike a regular CPU, it can be restricted to a finite number of possible states. This makes it possible to enforce strict protocol validation and firewall rules that cannot be disabled or modified through software manipulation or other conventional attack techniques.

Why embed?

If hardware-based security is preferable to software-based security, embedded hardware security is the most advantageous approach of all.

Building security into industrial devices, rather than attempting to add security after the fact, provides a range of benefits for operators, designers, and manufacturers of industrial and critical infrastructure controllers and safety systems.

Recent innovations make it possible for hardware-based security to be built-into modular platforms, such as sensors, programmable logic controllers, SCADA devices, and network switches. This technology provides highly secure, deterministic, data flow management between industrial equipment and external networks.








Stronger protection

Embedded hardware security, by definition, places security technology at a lower level in the industrial network, providing more effective protection against attacks with the greatest potential to do harm.

Software-based firewalls are designed to protect against attacks targeted at higher network levels, such as engineering workstations or human-machine interfaces. These types of attacks are generally launched by criminals seeking monetary gain. In many cases, the threat actors are not particularly sophisticated, but by using widely available tools, techniques, and procedures, even an unskilled attacker can overcome firewall defenses.

Attacks that aim lower in the network—at programmable logic controllers or remote terminal units, for example—are even more difficult to execute and block. These attacks are typically carried out by nation states or nation-affiliated groups with resources and capabilities beyond those of even advanced cyber criminals. Their attacks are intended to destroy data, damage equipment, and create disruption for political or military purposes. The custom code used in these attacks is often sophisticated enough to defeat any software-based firewall.

Embedded hardware security, however, provides a deterministic filter that blocks any malicious code—no matter how advanced—and allows only predefined data types to travel through. This approach provides maximum protection where the consequences of a security failure are most severe.

Network Level		Cyber Attack Profile	
4	Business & Logistical Planning		<ul style="list-style-type: none">• Threat actors are typically cybercriminals• Attacks are motivated by monetary gain• Attack tools and methods are easily available• Consequences are typically limited to financial loss
3	Site operations		
2	Supervisory Controls		
1	Basic Controls		<ul style="list-style-type: none">• Threat actors are typically nation states• Attacks are motivated by political or military goals• Attacks require advanced capabilities• Consequences can include physical damage and loss of life
0	Physical Processes		

Lower Cost

Industrial controls with embedded cybersecurity can decrease both capital and operational expenses for network owners.

Typically, the initial cost of an industrial control with built-in security is equivalent to, or lower than, the cost of buying a non-secured industrial control and an external firewall solution to protect it. When costs for additional rack space and peripheral equipment (neither of which are needed for embedded solutions), the initial cost of embedded security is likely to be lower in almost every case.

Once installed, an embedded hardware security module can be expected to function properly throughout the lifespan of the device it protects. Conventional industrial firewall solutions—since they're built on commercial-grade, rather than industrial-grade, platforms—have an expected lifespan of only a few years, after which they must be upgraded or replaced.

Embedded security provides even greater operational expense savings. In contrast to the resource-intensive patching and updating that software-based solutions require, embedded security modules need minimal ongoing maintenance. Organizations that adopt embedded security can expect a dramatic reduction in personnel costs related to security maintenance, along with reductions in power consumption due to the modules' small size and resource demands.

Simplified administration

Unlike conventional industrial cybersecurity solutions, embedded hardware security modules do not depend on software and are not vulnerable to conventional zero-day exploits. As a result, the technology does not require frequent updates in order to consistently enforce security policies.

Embedded modules can be designed to meet the exact requirements of each use case, eliminating the need for custom configurations that are often needed when security is added after the fact.

Benefits for OEMs

By directly embedding cybersecurity modules into PLCs, IIoT devices, and other OT devices, manufacturers and vendors can deliver a high level of assurance and differentiate themselves from the competition.

- **Anticipate customer demands:** Some OT operators already require embedded security in the new devices they purchase. As the industry becomes more aware of the capabilities and benefits of embedded hardware security, more end users will expect and demand that their devices contain native security.
- **Leverage industry-leading technology:** Cybersecurity is a complex and constantly evolving domain. Rather than attempting to build solutions on their own, manufacturers can take advantage of Owl's decades of experience in the field, and offer customers access to technology developed for use in rigorous military and intelligence applications.
- **Be first to market:** Designing, developing, and testing embedded hardware security is a time- and resource-intensive process. OT manufacturers who attempt to create their own embedded security solutions may be years away from a marketable product. By incorporating security modules into their products, OEMs can dramatically reduce development costs and time to market.
- **Win a larger share of the security spend:** Embedded security allows OT operators to reduce their dependence on software-based firewalls and other external security technology. OEMs who embed hardware-based security in their devices can win a larger percentage of customers' total spend, while delivering a lower total cost.

Purpose-driven design

In addition to providing superior protection with lower costs and resource burdens, embedded security technology also makes it possible to create customized configurations and data flows to meet the specific needs of each device, network, and organization.

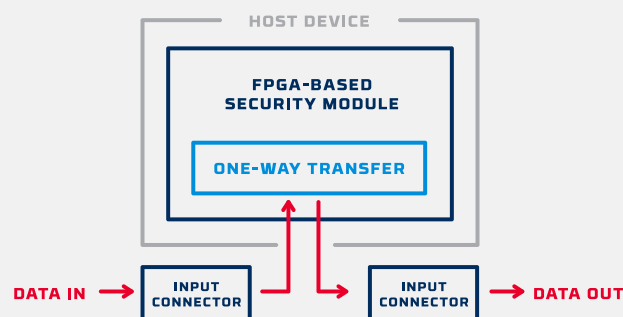
Embedded, hardware-based security provides two dimensions of modular design:

- **Hardware design:** the individual hardware components (such as inputs, outputs, buffers, and FPGA filters) that make up an embedded security device can be selected and laid out to meet the requirements of each use case.
- **Filter logic:** reliable, thoroughly tested functional modules greatly accelerates the process of developing new hardware-based filters. This allows for re-use of filter logic for common data types and reduces the amount of custom development needed to validate a new protocol.

The examples shown below illustrate a few of the possible design patterns that can be implemented with Owl's miniaturized, modular security technology.

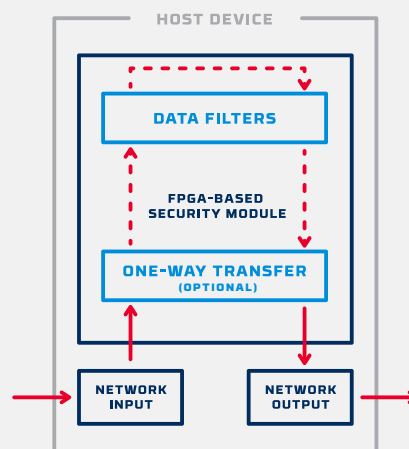
Sample Use Case: One-Way Transfer

- Embeddable security module with copper or SFP connectors
- One-Way Transfer at line rates
- Field upgradable via digitally signed config file
- FPGA code protected against modification or theft
- Will not run malicious code
- Mission-specific networking and data filters



Sample Use Case: One-Way Transfer with Content Filtering

- Embeddable security module with copper or SFP connectors
- One-Way Transfer at line rates
- Field upgradable via digitally signed config file
- FPGA code protected against modification or theft
- Will not run malicious code
- Mission-specific networking and data filters for protocol and data content inspection



Conclusion

The year-over-year rise in cyber attacks against operational technology networks is well documented. Government agencies and cybersecurity research firms unanimously forecast attacks to increase into the foreseeable future. As cybersecurity research firm Mandiant recently put it, “Asset owners need to look at OT security with the mindset that it is not if you will have a breach, but when.”

Given that attackers will inevitably make their way into an organization’s network, it becomes even more important to safeguard devices at the lower levels of the network, where the consequences of a breach would be most severe. Software-based industrial firewalls are simply not able to provide the necessary level of assurance. Hardware-based cybersecurity modules, designed for specific use cases and embedded within industrial control devices themselves, deliver the highest possible assurance that OT devices will remain secure, even when connected to a less-secure network.



Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com



@OwlCyberDefense

203-894-9342 | Sales@owlcyberdefense.com