# Embedsec Secerned

QVLx

Security on Lock.

## Myth

Classical cybersecurity covers embedded system security.

## Truth

Classical cybersecurity is broader than the required specificity.

## Introduction

This document is intended to address a common misconception that classical security sufficiently covers the embedded domain.

We deem this notion to be a inaccurate and aim to shed light on this subject. We also hereby coin the term *embedsec*, for brevity and to highlight distinction of the field. We will use the term henceforth.

## Explication

We see embedsec in a similar manner to the field of dentistry. Patients don't go to a cardiologist when they have a toothache. Even though cardiology and dentistry both fall under the tree of medicine and have the same ultimate goal of human care, they are not to be confused. Otherwise, patients will not receive proper care for ailments or adequate preventative measures.

It is important that the embedsec domain be recognized as being distinct and specialized. If one hires a traditional cybersecurity professional solely for the protection of an embedded system, they likely won't provide the depth that the system requires.

This is because of the following differentiating aspects:

- Embedsec involves a unique set of software technologies and protocols.
- Embedsec has to conform to notable embedded systems limitations such as power and memory.
- Embedsec frequently considers an attacker's physical access to fielded devices.
- Embedsec relies heavily on intricate hardware and firmware knowledge.

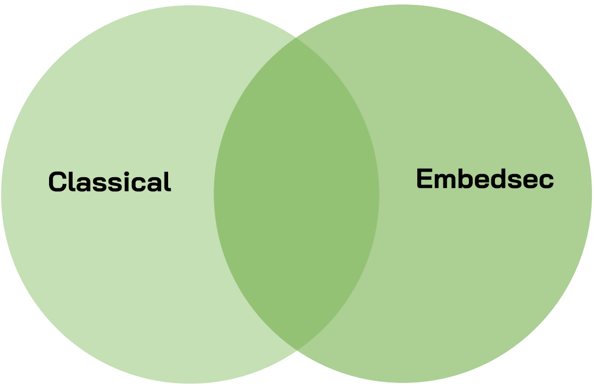

*Figure 1. Overlapping Security Domains*

Embedsec involves unique technologies and protocols that distinguish the field from classical security. Technologies such as RTOSes, MQTT, Zigbee, Mil-Std-1553, SpaceWire, and CANbus are typical to embedded contexts. It is imperative that the parties responsible for the protection of embedded devices understand how to meet the requirements centered around these technologies and protocols.

Power, memory, and other limitations entail that embedded systems need to be secured in such a way that considers these restrictions. Embedded systems may not have access to the breadth of countermeasures that desktop and other computing devices can utilize. An example of this is machine learning. Unless a board is one of the few shipped with AI co-prossessors on it, machine-learning will typically be too expensive of a computation to be a viable intrusion detection mechanism.

Embedsec considers physical attack vectors more often than classical cybersecurity because assets are often times performing functions out in the field, where they are physically accessible. They may be subject to certain side-channel attacks, glitching attacks, and tamper techniques that rely on physical device access. Such close-proximity actions must be considered by embedsec professionals in addition to remote attacks.

Embedded systems are a topology of hardware components that can constitute attack surface and/or countermeasures. These must be understood, protected, and/or leveraged. Because of this required expertise, the first and foremost level of protection is provided by hardware vendors.

Which leads us to make a crucial point: without proper hardware capability, there is only a very minimal level of security that can be guaranteed for a device. This protection is inadequate for most situations unless the device is not connected to a network, doesn't use radio frequency communications, and is floating in the remoteness of space. Even then, one would need to ensure that initially loaded software is verified when it runs, which cannot be enforced without proper hardware constructs.

Software TEEs that claim to secure devices through partitioning or separation of memory and other resources, don't provide adequate protection without the use of hardware. Most commercially available RTOSes and bare-metal hypervisors will utilize hardware security measures to varying degrees. Hence, OS providers are a solid source of embedsec capability to be considered along with hardware vendors.

A third source for embedsec services are specialized firms like QVLx. These firms provide penetration testing and consultation to ensure that hardware, firmware, OS/hypervisor, and other aspects are being properly chosen and utilized. QVLx provides Red-Blue Security Services, Secure Boot Services, and Qualified Vendor Services to meet program requirements. Furthermore, QVLx provides the Salvum© Security Engine. In addition to a secure shell powering hundreds of diverse embedsec modules, Salvum includes a Host Environment Hardening Guide that addresses the hardware and OS related topics mentioned in this document and ensures that embedded targets only come in contact with trusted hosts.

As the cyber domain matures, the distinction of embedsec will grow more pronounced. There are currently no noteworthy certifications for embedsec and there exist only a handful of training programs, including QVLx offerings. But more training will arise in the future and if certification methods for embedsec emerge, they will likely be specific to hardware context. This field is both formally young and increasingly important due to the growth of IoT and other ubiquitous computing paradigms. Be excited to see embedsec expand with time. Watch this space.

# About QVLx

*QVLx is a disruptive supplier of critical embedded systems expertise, products, and innovation. Our company helps customers develop complex, robust, and elegant solutions to meet their most demanding requirements in excellence.*

*QVLx is headquartered in Huntsville, Alabama.*

*For more information, visit qvlx.com*