面向低功耗工业 4.0 应用的可编程安全功能

Microchip Technology Inc.

资深 FPGA 产品营销工程师

Apurva Peri

安全性是医疗、工业、汽车和通信领域的一个重大问题。许多行业都在采用基于互联智能机器和系统的智能联网机器及工艺，从而优化工艺和流程。这些系统容易受到恶意攻击、未知软件错误的影响，而远程控制甚至可能导致物理安全问题，因此必须防止未经授权的访问或非法控制。

工业发展的最新篇章，也就是常说的第四次工业革命（又称工业 4.0），开创了创新和发展的新纪元，但本身也存在一系列危险和挑战。工业 4.0 定义了系统、网络、机器和人类之间的通信和互联互通，其中包含物联网（IoT），这将复杂性推向了新的高度。虽然互联互通具有提高效率、实时识别和纠正缺陷、预测性维护以及改进各种功能之间的协作等优势，但这些优势也会显著增加智能工厂或自动化生产基地的安全漏洞。“网络”安全不再局限于特定的操作或系统，还会传播到工厂车间或工业网络上的每一台设备。智能工厂里的控制系统（包括 PLC、传感器、嵌入式系统和工业 IoT 设备）受到的安全威胁在全球范围内呈上升趋势。基于云执行的远程管理也带来了篡改、注入恶意内容等物理攻击的风险。

本文概述了 FPGA 如何推进纵深防御方法的发展以开发安全应用程序，这是在第四次工业革命的推动下，满足 IoT 和边缘计算迅速增长的需求的必经之路。本文介绍了安全功能在硬件、设计和数据中的作用，以及如何在安全性的三个要素（机密性、完整性和真实性）基础上构建应用程序。

一个可靠的安全系统必须具备以下三个核心元素：

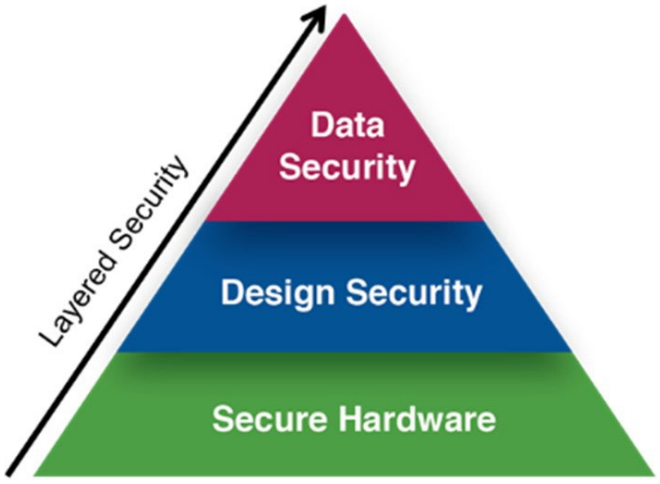
- 可信：保证数据源可靠、获得授权且经过身份验证
- 防篡改：确认设备没有受到任何干扰
- 信息保障：以安全的方式使用、处理和传输系统中的数据

通过 FPGA 实现基于硬件的安全功能

基于软件的单一安全方法在生命周期、可编程性、功耗效率、外形等方面存在不足，在当前的工业 4.0 环境下，不足以达到满足需求的安全等级，因此必须采用纵深防御安全机制，通过安全层加强硬件的防御能力。

如今，大多数安全框架都采用软件实现，其中包含编译为在通用控制器或处理器上运行的加密库。这些软件实现暴露了更大的易受攻击范围以及许多潜在攻击点，例如操作系统、驱动程序、软件协议栈、存储器和软键。此外，软件实现可能未针对性能和功率进行优化，因此会带来设计挑战。在工业系统的整个生命周期中，这些系统需要长期维护，同时协议栈、库等方面也需要经常更新，这些工作十分繁琐且成本高昂。原则上，底层硬件必须在其结构中集成安全功能，以防止静态和动态逆向工程、篡改和伪造攻击。

因此，基于可编程硬件的安全功能已成为一种全面、稳健的解决方案，适用于节能工业 IoT 和边缘应用，尤其是采用 FPGA 的解决方案。除了提高系统的安全性能外，FPGA 还可提高应用程序的安全等级。FPGA 必须将关键安全组件集成到硬件、设计和数据中，以提供真正稳健的解决方案，以下几部分将对此加以讨论。



保证 FPGA 硬件的安全

在制造地点或通过供应链运输的过程中，硬件可能会在部署前或预编程时受到攻击。安全的生产系统支持在不太可信的制造环境中加密和配置 FPGA，控制编程器件的数量，并以加密控制的方式审计制造过程；其结构必须可以避免复制品、恶意编程的 FPGA 和未经验证的器件。

保证 FPGA 设计的安全

设计安全性离不开安全的硬件平台，这类平台既可为设计提供机密性和身份验证，又能监视环境中的物理攻击。边信道攻击（SCA）会破坏烧写到器件中的比特流，因此可能会对集成了加密机制的 FPGA 造成严重威胁。SCA 试图通过测量或分析各种物理参数（如电源电流、执行时间和电磁辐射），从芯片或系统中提取机密信息。无论是非易失性 FPGA 还是 SRAM FPGA，烧写或“加载”FPGA 的过程都需要具备抵御边信道攻击的能力。

主动监视器件环境是另一种防止 FPGA 设计受到半侵入式和侵入式攻击的手段。电压、温度和时钟频率的波动可能表明有人试图进行篡改。防篡改 FPGA 提供可定制的响应来抵御攻击，其中包括完全擦除器件，从而使其对攻击者毫无用处。

保证 FPGA 数据的安全

最后，除了确保硬件和设计的安全，FPGA 还必须提供保护应用程序数据的技术，这包括不同方法的组合：

- 真随机数生成器（TRNG），用于构建符合 NIST 标准的安全协议，并提供随机性来源以生成用于加密操作的密钥
- 通过物理不可克隆功能（PUF）生成根密钥。PUF 可利用在半导体生产过程中自然发生的亚微细粒变化，并赋予每个晶体管略微随机的电气特性和惟一身份，类似于人类的指纹，每一个都独一无二
- 受密钥保护的安全存储器
- 能够执行符合行业标准的非对称、对称和 hashtag 函数的加密功能

结论

工业 4.0 是一场不断深化的革命，其广泛采用依赖于稳健的端到端安全解决方案。基于软件的安全和加密功能实现容易存在弱点并遭到恶意利用。

相比之下，当今基于硬件的解决方案利用了具有内置高级安全可编程功能的 FPGA 以及硬件、设计和数据中的安全层。这可提供旨在防止客户 IP 遭到窃取或过度构建的硬件。这些数据安全功能的示例之一是用于抵御边信道攻击的 DPA 保护功能，这通常是一种获得许可的专利功能。此外，基于物理不可克隆函数（PUF）的安全密钥管理解决方案，以及支持符合行业标准的非对称、对称和 hashtag 函数的软件可编程防边信道攻击加密处理器也同样重要。

基于硬件的解决方案为打造真正灵活、安全的系统铺平了道路。凭借其极高的可编程性、出色的性能和极佳的功耗等优势，基于硬件的 FPGA 安全解决方案将成为实现重要安全性能的不二之选。FPGA 集成了防边信道攻击加密加速器，其中包含防篡改/防御措施，可保护客户的知识产权，并提供可信的供应链管理，为开发安全系统提供一个安全平台。