什么情况下网络安全远远不够？

Microchip Technology Inc.
FPGA 业务部
技术主管
Tim Morin

什么情况下网络安全问题会变成物理安全问题？换句话说，什么情况下半导体必须具有内置篡改检测器？

在广泛的非国防市场，有些人认为网络安全完全可以满足他们的需求。毕竟，他们设置了栅栏、大门、警卫、摄像头和防火墙，并且由他们自己的员工来制造和/或生产自己的系统，从而实现了“物理”安全。这可能就足够了。但大家扪心自问，在什么条件下任何人（可能是员工）都可以访问一台设备，他们的哪些做法可使设备所具备的功能被利用或被秘密提取？

这势必需要公司回答以下问题：我的供应链管理是否安全？设备或货物是否曾“丢失”？设备如何停用？谁负责维修设备，设备如何升级？“谁可以在设备的使用寿命期间访问该设备，他们可以如何处理该设备？”这些问题的答案将有助于推动组织的决策过程。

下面是需要考虑的关键安全主题：

生产（制造印刷电路板）、配置和测试

- 在任何非易失性器件的编程过程中，公司是否使用了经过哈希运算且已签名的映像？是否存在记录已配置内容、已配置的电路板数量以及未通过出厂测试的电路板数量的可审核日志？这些日志是否经过哈希运算且已签名？
- 是否禁止了调试端口？

发货给客户

- 组织能否对发货件数与客户收到的件数进行核对？大多数客户会立即说“嘿，少了一件！”。但是，如果客户因为某种原因丢失了一件，该怎么办？这家公司不得不假定有一件设备流落在外。
- 公司及其客户能否验证交付设备的完整性？他们能否验证设备在运输过程中未遭到篡改？

已部署设备

- 设备上是否有防篡改密封？
- 是否只允许获得授权的技术人员维修设备？
- 是否允许远程更新？

  - 如果允许，经过验证后，这些映像是否是完整的和真实的？
  - 是否有适当的机制来防止回滚？
- 设备停用时是否执行零值化？是否使其无法操作？是否将其销毁？

如果对上述任何一个问题的回答都是“否”，那么组织应该认真考虑内置防篡改对策的半导体，这样他们便可根据设备在其生命周期内可能出现的风险情况为其量身定制篡改响应。例如，FPGA 产品应该具有可用于定制威胁响应的多种防篡改功能（图 1）。示例包括：

- 足够数量的数字篡改标志
- 多个模拟窗口电压检测器，可为您提供每个关键电源（Vdd、Vdd18 和 Vdda25）的高/低跳变点
- 数字窗口温度，可为您提供高/低管芯温度
- 来自内置温度检测器的原始电压和温度值
- 系统控制器慢速时钟，用于指示系统控制器的欠压条件
- 数字总线（至少 5 位），用于指示器件复位源（已触发 DEVRST 引脚、篡改宏输入、系统控制器看门狗和安全锁定篡改检测器，以及任何其他复位）

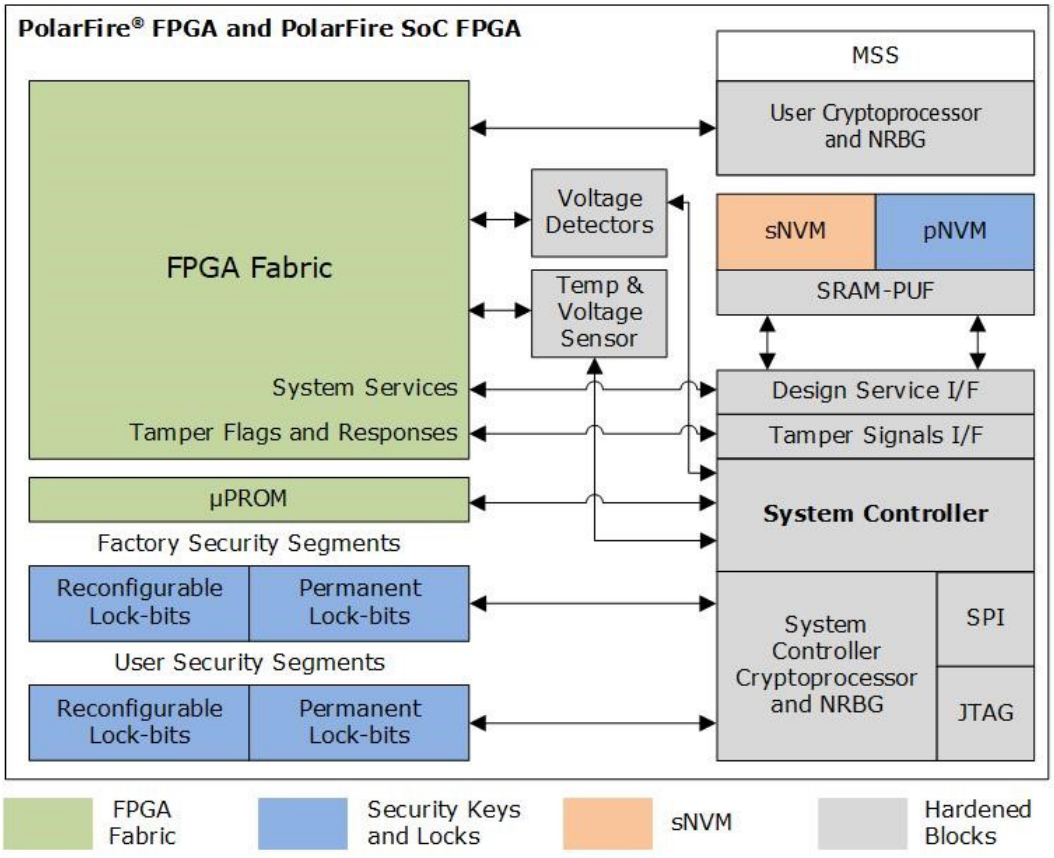

图 1. Microchip PolarFire® FPGA 和 PolarFire SoC FPGA 器件的设计和数据安全属性

篡改检测和响应

在对 FPGA 设计的篡改宏进行实例化时，应该可以使用多种类型的篡改标志。每个标志都有自己的用途：

标志 [31:0]	标志名称	说明
1	MESH_ERROR	有源网篡改标志。每当有源安全网发现实际金属网输出与预期输出不匹配时，将此标志置为有效。此举可防止侵入式攻击，例如使用聚焦离子束（FIB）技术对某个较高级别金属层的有源金属网的走线进行切割和探测。
2	CLOCK_MONITOR_GLITCH	每当时钟毛刺监视器检测到脉冲宽度超限时置为有效。
3	CLOCK_MONITOR_FREQUENCY	每当时钟频率监视器发现 160 MHz 和 2 MHz RC 振荡器之间的频率不匹配时置为有效。
4	LOW_1P05	当 1.05V 电源（VDD）低于系统控制器 1.05V 检测器的低阈值时置为有效。
5	HIGH_1P8	当 1.8V 电源（VDD18）高于系统控制器 1.8V 检测器的高阈值时置为有效。
6	HIGH_2P5	当 2.5V 电源（VDD25）高于系统控制器 2.5V 检测器的高阈值时置为有效。
7	保留	保留。
8	SECDED	当系统控制器的内部存储器中出现 2 位误差时置为有效。这是导致 POR 的致命条件。
9	SCB_BUS_ERROR	当在系统控制器总线上检测到错误时置为有效。
10	WATCHDOG	当系统控制器的看门狗复位即将触发时置为有效。
11	LOCK_ERROR	当在受到持续监视的安全锁定段中检测到单位或双位误差时置为有效。
12	保留	保留。
13	DIGEST	当请求的摘要检查失败时置为有效。
14	INST_BUFFER_ACCESS	当使用 JTAG/SPI 接口对系统控制器的共享缓冲区执行读/写访问时，将该标志置为有效。

15	INST_DEBUG	当执行调试指令时置为有效。
16	INST_CHECK_DIGESTS	当请求外部摘要检查时置为有效。
17	INST_EC_SETUP	当使用椭圆曲线从指令时置为有效。
18	INST_FACTORY_PRIVATE	当执行工厂 JTAG/SPI 指令时置为有效。
19	INST_KEY_VALIDATION	当请求密钥验证协议时置为有效。
20	INST_MISC	当执行未分类的 SPI 从指令时置为有效。
21	INST_PASSCODE_MATCH	当尝试匹配密码时置为有效。
22	INST_PASSCODE_SETUP	当启动一次性密码协议时置为有效。
23	INST_PROGRAMMING	当使用外部编程指令时置为有效。
24	INST_PUBLIC_INFO	当发出器件公共信息请求时置为有效。
25	保留	保留。
26	INST_PASSCODE_FAIL	当密码匹配失败时置为有效。
27	INST_KEY_VALIDATION_FAIL	当密钥验证失败时置为有效。
28	INST_UNUSED	当执行未使用的指令操作码时置为有效。
29	BITSTREAM_AUTHENTICATION_FAIL	当比特流身份验证失败时置为有效。
30	IAP_AUTO_UPDATE	如果发生 IAP 更新（通过 IAP 系统服务或在器件引导时自动更新），则置为有效。
31	IAP_AUTO_RECOVERY	如果发生 IAP 恢复程序，则置为有效。

响应与检测同等重要。如果在单个事件、一系列事件或其中的任何事件组合发生期间，公司决定因未经授权的篡改而采取行动，则随着时间的推移，应针对事件对响应进行调整。或者，组织可以打击违例行为，强化安全部分。示例包括：

IO 禁止

禁止所有用户 IO。将 IO 重置为由其 SEU 抗扰配置位定义的状态。专用（JTAG、SPI 和 XCVR 等）IO 或未通过配置位配置的 IO 除外。只要将 IO_DISABLE 置为有效，即会禁止 IO。

安全锁定

所有用户锁都设置为其锁定状态。

复位

向系统控制器发送复位信号以开始掉电和上电周期。

零值化

将任何或所有配置存储元件清零并进行验证。将内部易失性存储器（例如LSRAM、uSRAM和系统控制器RAM）清零并进行验证。零值化完成后，可以使用JTAG/SPI从指令检索零值化证书，以确认零值化过程成功。如果使能系统控制器挂起模式，则此篡改响应不可用。用户可以选择在零值化后进入两种不同的状态：

- 出厂状态——器件恢复到交付前的状态。
- 不可恢复。甚至公司也无法访问器件的内部。

零值化完成后，可以通过专用JTAG/SPI端口导出零值化证书，向外部实体保证器件确实已执行零值化。

在当今竞争激烈的环境中，网络安全还远远不够。公司制造的设备有可能会落入其竞争对手和危险分子的手中。半导体产品必须具有各种内置的防篡改功能，组织可以利用这些功能来定制其对这些威胁的响应。如需了解更多信息，请访问 https://www.microchip.com/en-us/products/fpgas-and-plds