在莱迪思FPGA中实现 DC-SCM

莱迪思半导体白皮书

2022年4月

了解更多：

www.latticesemi.com

在线联系我们

www.latticesemi.com/contact
www.latticesemi.com/buy

V. 1 WP0031C

目录

第一节	|	摘要	P3
第二节	|	DC-SCM是什么？	P3
第三节	|	为什么要使用DC-SCM？	P3
第四节	|	DC-SCM架构	P4
第五节	|	DC-SCM LTPI	P5
第六节	|	莱迪思LTPI	P5
第七节	|	莱迪思DC-SCM的安全实现	P9
第八节	|	莱迪思DC-SCM的控制实现	P10
第九节	|	莱迪思产品革新：一种方案三种关键特性	P10
第十节	|	支持DC-SCM的莱迪思产品	P11
第十一节	|	使用莱迪思SupplyGuard™实现端到端的保护	P11
第十二节	|	结论	P11
第十三节	|	参考文献	P12

摘要

DC-SCM是OCP硬件管理项目的一个子项目。DC-SCM实施模块化服务器管理，包含了已存储在典型处理器主板上的所有的固件状态。DC-SCM通常将三个关键功能转移到一个标准尺寸模块（CFM）中。

- 管理——BMC功能和一个新的LTPI接口（低电压差分信号通道协议和接口）
- 安全
- 控制

本文描述了DC-SCM的LTPI（服务器管理）、安全和控制三个方面。DC-SCM 2.0的所有三个关键功能都已经在莱迪思半导体的单个FPGA中实现。

DC-SCM 2.0规范的一个重要变化就是引入了低电压差分信号通道协议和接口（LTPI）。本文描述了DC-SCM及其在莱迪思FPGA解决方案中的LTPI实现。

DC-SCM的安全模块称为ROT（可信根），可以用来解决黑客在保密固件的闪存中安装恶意代码的安全问题。莱迪思PFR（平台固件保护恢复）解决方案可以作为DC-SCM的ROT，避免数据中心服务器中的此类漏洞。

莱迪思FPGA还包括了DC-SCM定义的控制功能，提供数据中心服务器所需的时序重置和电源管理功能。

DC-SCM是什么？

开放计算项目（OCP）是一个在公司之间共享服务器和数据中心产品设计和最佳实践的组织。DC-SCM（Datacenter-ready Secure Control Module）是OCP硬件管理项目的一个子项目。它提供了将常见的服务器管理、安全和控制功能从主板转移到标准尺寸模块（CFM）的指南。

DC-SCM架构定义了与CPU板互操作的输入/输出端口。DC-SCM服务器在HPM（主机处理器模块）板上只有基本的中央计算元件（CPU）、高速存储器和IO连接器，其他所有组件均在模块化DC-SCM（安全、控制、管理）板上。

为什么要使用DC-SCM？

DC-SCM有诸多益处：

- DC-SCM能轻松实现CPU/存储器的设计和部署，因为管理、安全和控制功能都独立于CPU/存储器板的开发。
  - 将BMC和RoT实施与服务器分离，实现独立的开发和创新
  - 通过将管理电路转移到更小、更低价的PCB，从而节省成本
  - 在多个项目和架构中使用通用的DC-SCM设计，节省验证时间
  - 简化HPM电路板布局，缩短开发时间

使用DC-SCM之后，拓展机箱只需根据CPU和SoC供应商的指南进行简单的常规开发即可

- 系统管理和安全性能不断发展且独立于CPU的更新换代。
  - DC-SCM可以在一代产品内在平台上部署管理和安全升级，无需重新设计更复杂的组件

- DC-SCM使用开源模块化方法，轻松实现互操作性。
  - 标准化的常用模块
  - 采用高速互连（PCIe）等通用接口
- DC-SCM的优势之一体现在服务器报废时。模块化设计的好处是可以单独销毁安全模块，出售或回收报废的服务器不会泄露安全数据/密钥。

DC-SCM架构

DC-SCM架构主要包括以下几个部分：

- BMC：基板管理控制器
- BMC闪存：使用一个或等多个闪存器件（通常是两个）来存储BMC固件镜像
- BIOS闪存：使用一个或等多个闪存器件（通常是两个）来存储BIOS固件镜像
- DC-SCM CPLD：包含特定应用逻辑和LTPI 接口的可编程逻辑器件（DC-SCM 2.0 中引入了新的LVDS通道协议和接口）
  RoT安全处理器： 负责验证系统上的BMC、BIOS和/或其他固件镜像的安全处理器
- 可信任平台模块（TPM）：可选的专用微控制器，通过集成的加密密钥保护硬件

下图是DC-SCM规范中所定义的DC-SCM架构模块框图：

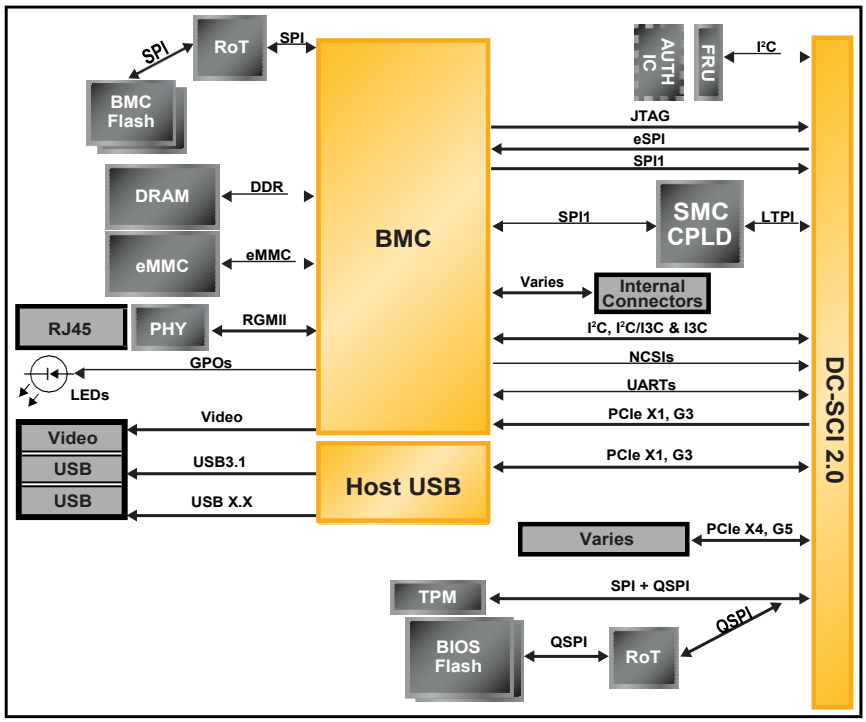

图 1

DC-SCM LTPI

DC-SCM 2.0规范的一个重要变化是引入了低电压差分信号通道协议和接口（LTPI）。LTPI解决了DC-SCM 1.0中的串行GPIO接口的缺点。

- LTPI比GPIO延迟更低
- 它允许主机平台模块和DC-SCM模块之间的多个管理接口进行通道通信（为 I2C、SMBus、UART、数据自定义协议提供通道）

DC-SCM LTPI架构

如下图所示，LTPI接口采用了两片FPGA/CPLD器件实现。

- HPM FPGA——提供本地HPM接口到LTPI的桥接
- SCM CPLD——提供LTPI到本地SCM接口的桥接

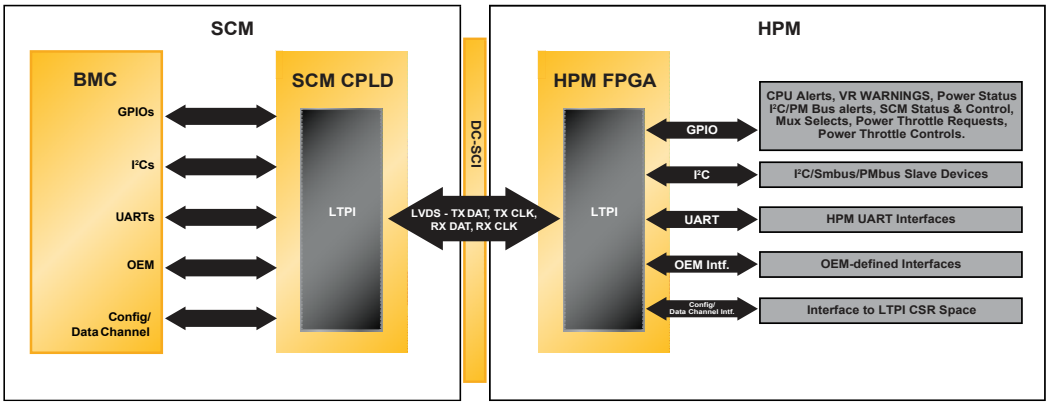

图 2

LTPI接口用于在HPM和SCM之间传输各种低速信号。LVDS接口比DC-SCM 1.0中的SGPIO接口提供更高的带宽和更好的扩展性。它不仅支持GPIO，还支持SMBus、I2C和UART等低速串行接口的通道传输。它还可以通过额外的专有OEM接口进行扩展，并为HPM CPLD和SCM CPLD之间的原始数据通道传输提供支持。

莱迪思LTPI

莱迪思DC-SCM LVDS通道协议和接口IP核是兼容OCP、DC-SCM标准的解决方案。莱迪思LTPI IP全面支持符合DC-SCM 2.0协议规范的接口和协议。该LTPI IP具有以下特性：

- 符合DC-SCM 2.0协议规范
  - 链路初始化、发现和协商
- 支持多通道串行接口
  - 支持GPIO、I²C、UART、OEM和数据通道聚合
  - 总共支持多达7个通道的聚合/解聚合
- 最高支持64位GPIO通道，采样率高达90kHz（低延迟GPIO可达5 MHz）
- 对于I2C/SMBus接口，每一个接口都可以配置为主控、从动或同时配置为主控/从动（用于多主控）
- 支持LVDS和sub-LVDS
- LFMXO5器件LVDS数据速率高达1000Mbps

莱迪思LTPI通道架构

在DC-SCM　LTPI规范的基础上，莱迪思使用时分复用（TDM）高速LVDS全双工链路在SCM和HPM之间发送和接收LTPI通道数据。

如下图所示，对于每个相等的时隙 T_N（下图的示例帧T_{+1}），都有一个LTPI帧在传输。在每个LVDS通道中都有部分LVDS帧在进行双向传输。通过LTPI接口发送的每个帧中分配给特定通道的比特数与每个通道专用的LTPI带宽成正比。

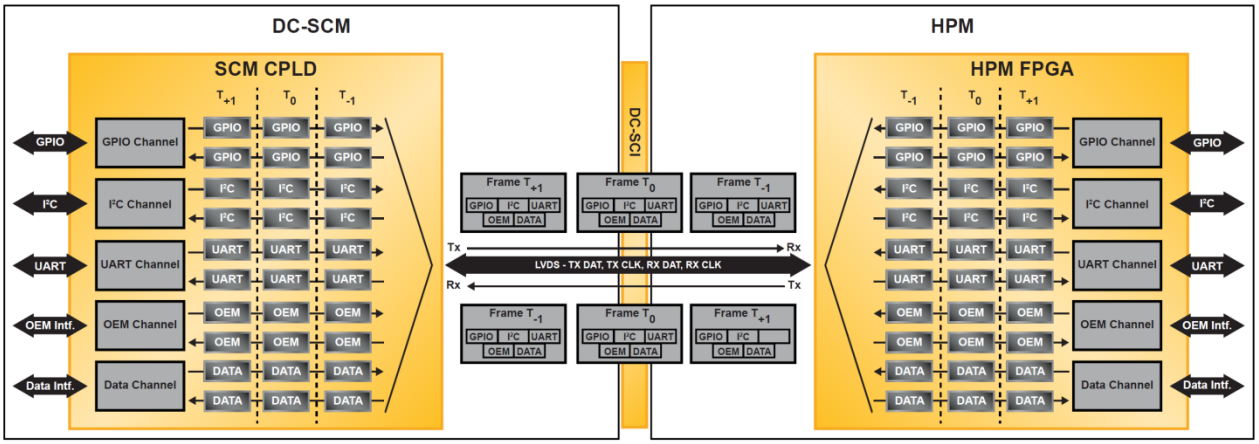

图 3

莱迪思LTPI通道框图

莱迪思LTPI参考设计的上层通道框图如下所示。从外部通道接收的数据通过低压差分信号（LVDS）接口在安全控制模块（SCM）和主机处理器模块（HPM）之间聚合和传输。来自LVDS接口的输入数据被重新映射到相应的目标外部通道。

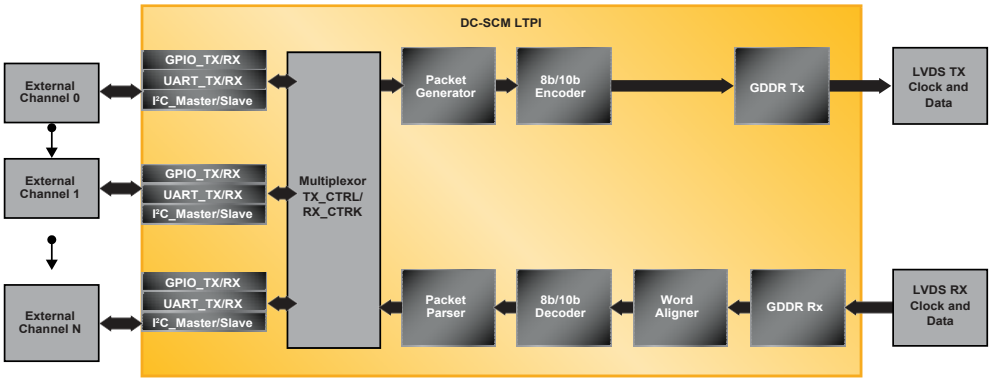

图 4

DC-SCM/HPM LTPI IP由多路复用器、帧/数据包生成器/解析器、8b/10b编码器/解码器、字对齐器/链路同步器以及GDDR发送和接收模块组成。

多路复用器

多路复用器连接外部通道。在链路训练和特性协商之后，多路复用器模块在每个通道之间切换采样，形成有

效载荷。

数据包生成器/解析器

帧生成器和解析器生成链路训练和协商所需的数据包。TX使用帧生成器来生成要发送到通信接收器的帧。RX使用帧解析器来解析接收到的帧。

8b/10b编码器/解码器

LTPI IP对发送到接收主机/从接收主机接收到的数据执行8b/10b编码/解码。对于TX，8位数据会根IEEE 802.3标准中指定的编码规则转换为10位数据。

GDDR串行器/解串器

数据以串行方式发送到接收主机。IP通过LFXMO5器件的通用DDR接口x5（10 bit：1 bit）和MachXO3L/LF/D器件的DDR接口x4（8 bit：1 bit）对数据进行串行化。同样，在RX模式下，数据通过DDR接口进行解串。

莱迪思LTPI接口通道

莱迪思LTPI接口定义了以下通道：

- GPIO通道：该通道实现了GPIO信号在HPM和SCM之间的互传。GPIO通道可以区分低延迟和正常延迟GPIO（串行GPIO），从而为对时序要求严格的GPIO信号分配更多带宽，并扩展传输的GPIO数量。
- I²C/SMBus通道：将I2C/SMBus链路数据从SCM传输到HPM，以及从HPM传输到SCM。
- UART通道：传输全双工UART接口，支持SCM和HPM之间的流控制。

GPIO接口

正如DC-SCM规范中的定义，GPIO通道定义了低延迟和正常延迟GPIO（参见下图）。这是莱迪思IP配置的一部分，这些接口模块的每个实例都使用一个64位的通道。为了成功进行发送和接收，SCM或HPM的发送通道的PID（数据包标识符）应与接收通道的PID相匹配，该PID在发送模块上实例化。

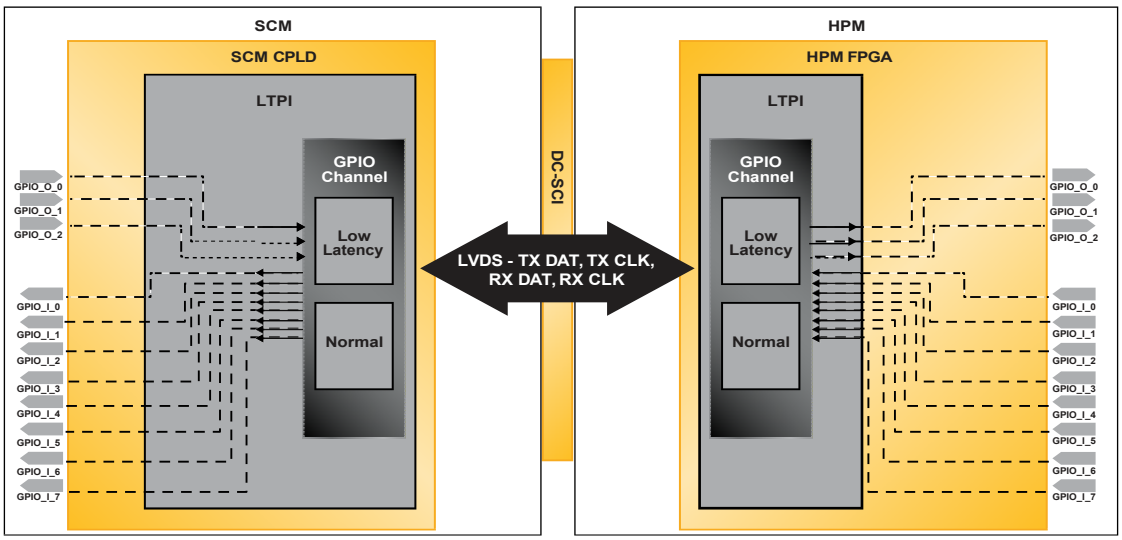

图 5

UART接口

UART接口通过GPIO接口发送，需要至少一个GPIO TX和一个GPIO RX通道的实例。

I²C接口

莱迪思LTPI IP使用I2C/SMBus通道通过LTPI接口为那些在SCM或HPM上只有一个控制器的链路传输I2C/SMBus总线数据。DC-SCM LTPI I2C/SMBus的主要用例如下图所示，SCM上的BMC充当目标器件位于HPM上的I2C/SMBus链路的控制器。这些接口模块的每个实例都使用一个通道。为了成功进行发送和接收，SCM或HPM的I2C主控通道的PID应与另一个模块上实例化的I2C从通道的PID相匹配。

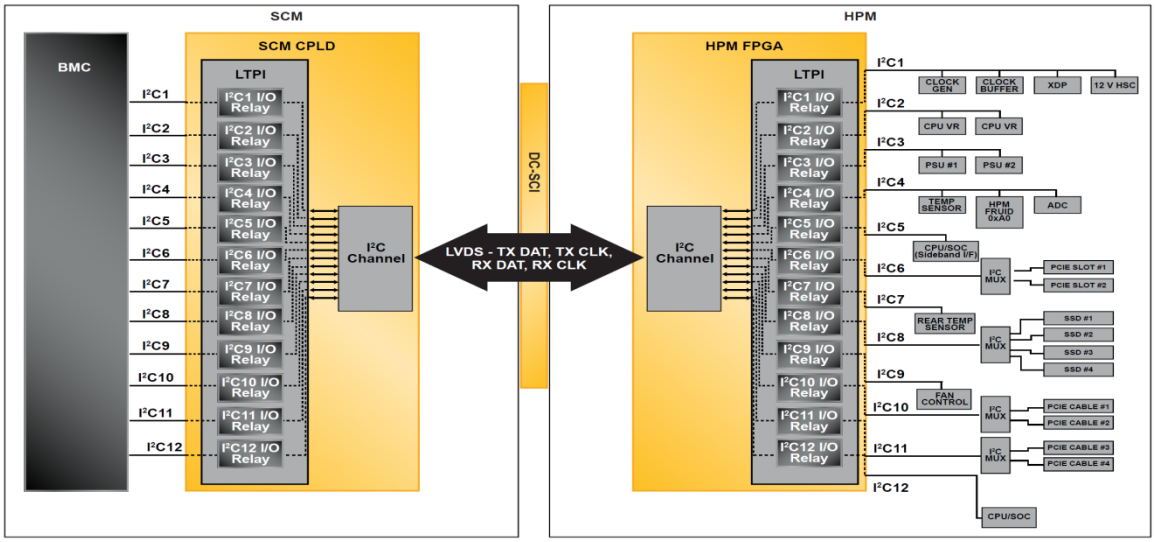

图 6

莱迪思LTPI通道分配

莱迪思LTPI通道可对用于SCM和HPM之间通信的特定类型接口进行功能分类。莱迪思LTPI还能实现接口映射的灵活性。LTPI的设计灵活性示例如下图所示（参考DC-SCM LTPI规范）。在此示例中，GPIO通道被转换为SGPIO接口，并在SCM CPLD中增加了额外的逻辑。

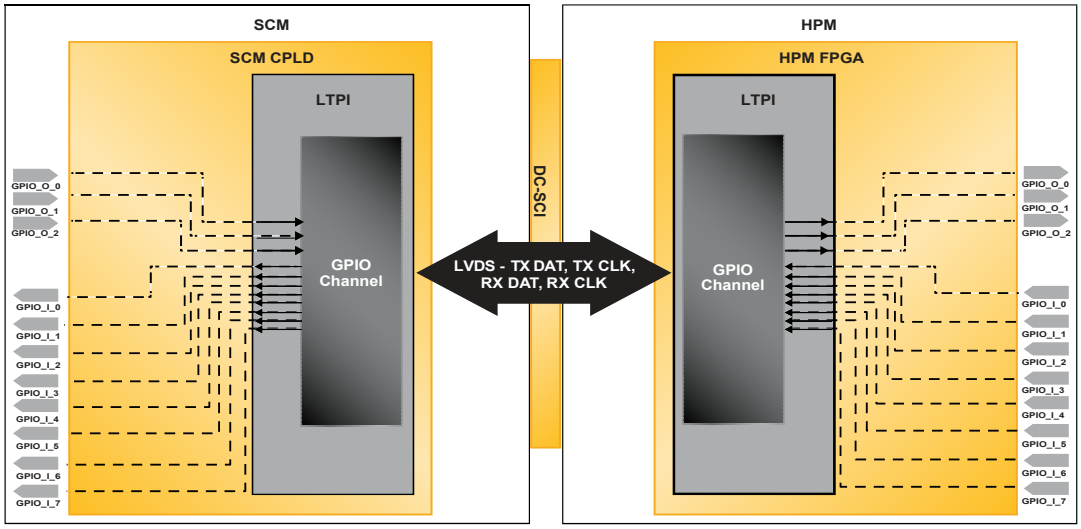

图 7

莱迪思DC-SCM安全实现

企业服务器通常包含多个处理组件，每个组件都有自己的非易失性SPI闪存缓存，用于存储其固件。黑客通过未经授权访问固件，可以暗中在组件的闪存中安装恶意代码。DC-SCM规范要求使用安全处理器来验证系统的BMC、BIOS和/或其他保密的固件镜像。

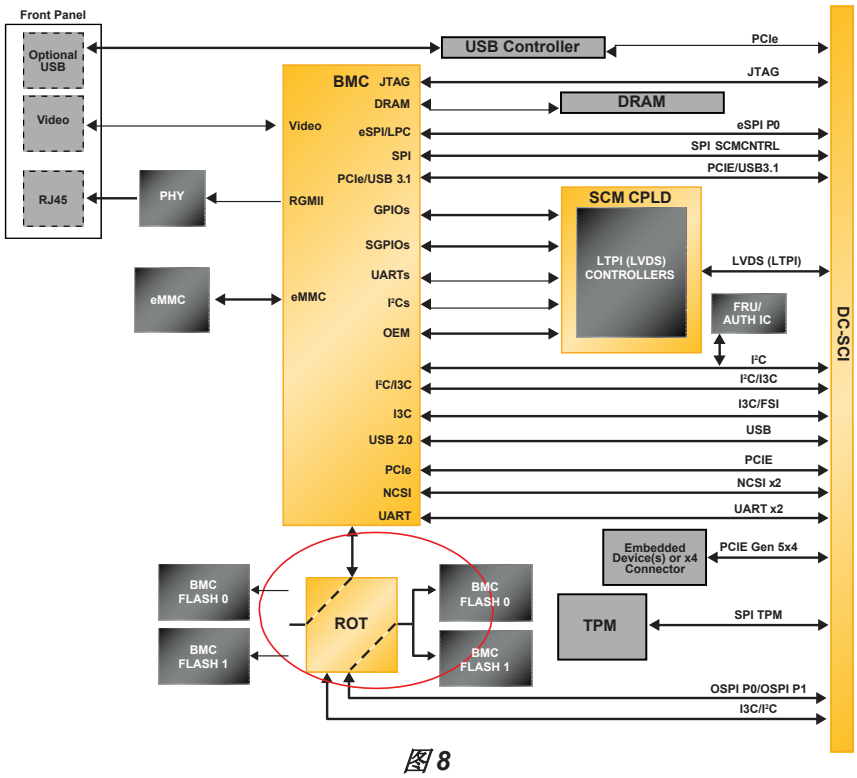

图 8

莱迪思安全/RoT（信任根）实现概述

为了解决黑客在保密固件的闪存中安装恶意代码的安全问题，美国国家标准与技术研究院（NIST）在2018年发布了NIST SP 800 193规范，定义了一种称为平台固件保护恢复（PFR）的统一保护机制。莱迪思的PFR解决方案可以作为DC-SCM的RoT来实现，解决了企业服务器的此类漏洞。莱迪思RoT的实现基于以下三个指导原则：

- 保护——莱迪思已经展示过基于状态机的算法，能以纳秒级响应时间检测SPI存储器的安全漏洞。这可以防止未经授权的访问对SPI存储器中固件的修改。该解决方案可通过简单易用的数据库进行定制。通过使用PFR算法的安全通信，BMC能够授权对SPI存储器的修改以支持在系统更新。
- 检测——对存储在每个SPI存储器中的固件进行椭圆曲线加密（ECC）计算可以检测所有未经授权的修改。检测方法独立于该设计中当前使用的固件安全方法。使用集成的电路板电源管理功能，可以在电路板启动之前检测到所有对固件未经授权的更改。

- 恢复——如果检测到安全漏洞，莱迪思的实现方案提供可定制化的恢复机制。这种机制可以执行简单的回滚操作，恢复到以前的固件版本，或者完全恢复到固件的最新授权版本。还可以自定义电源管理和控制PLD算法，应对不同性质的入侵，对任何电路板实施完全受信任的恢复过程。

方案特性

莱迪思的PFR解决方案拥有许多客户和开发人员期望的特性。例如：

- 可扩展——以纳秒级响应保护板上的所有固件。该解决方案还可以通过与相应信任根的安全通信来保护其他附加的子系统
- 不可绕过——该解决方案实现了服务器主板的完整电源时序以及PFR，因此无法绕过它
- 自我保护——PFR实现革命性地使用了FPGA作为可信根。该FPGA可以动态控制其攻击面并保护自身免受外部攻击
- 自我检测——可信根FPGA通过使用不可绕过的加密硬件模块检测其配置的任何安全漏洞
- 自我恢复——可信根FPGA在发现其活动配置遭到破坏时自动切换到已知完好的镜像

莱迪思DC-SCM的控制实现

当今几乎所有服务器都使用莱迪思FPGA器件来实现控制PLD的功能，例如电源/复位时序、各种类型的串行总线（I2C、SPI、eSPI、SGPIO等）、调试端口、LED驱动器、FAN PWM驱动器、前端面板开关感应和其他通用GPIO功能。莱迪思FPGA器件支持1 V信号，因而能够执行带外信号集成，无需外部GTL收发器。

无中断I/O

为了实现零停机，莱迪思开发了无中断I/O功能。通常情况下，控制PLD能让设计人员显著缩短产品上市时间，帮助他们应对在规定时间内推出新的定制硬件的市场压力。 有时，控制功能的实现或整个系统架构中可能存在错误，也可能需要引入新功能。完成设计修改的一种常见方法是通过在系统更新和电源重启让新编程的镜像投入使用。为确保高可用性（High Availability ）系统的持续运行，莱迪思FPGA器件可以在进行配置刷新时保持I/O状态不变，然后初始化新配置。

莱迪思产品革新：一种方案三种关键特性

莱迪思FPGA提供了将DC-SCM的三个关键功能集成到莱迪思解决方案中的独特优势：

- LTPI（管理功能）
- 安全（动态、实时、端到端的保护）
- 控制（可编程系统控制）

莱迪思FPGA非常可靠，在基于FPGA的低功耗应用方面处于行业领先地位，其抗软错误率（SER）性能是CMOS技术的100倍。莱迪思FPGA具有可靠的标准并遵循DC-SCM协议规范。Propel工具还为开发人员提供了便捷的拖放操作界面，大大简化了配置。

支持DC-SCM的莱迪思产品

莱迪思非常重视DC-SCM。莱迪思拥有一系列支持DC-SCM、可信根和用户电源控制逻辑的FPGA产品。以下是支持DC-SCM的现有产品列表。

莱迪思产品	DC-SCM	RoT	控制
MachXO3D	✓	✓	✓
Mach-NX	✓	✓	✓
MachXO5-NX	✓		✓

表 1

使用莱迪思SupplyGuard™实现端到端的保护

莱迪思SupplyGuard™为每个客户分配唯一的订购部件编号。这些编号对应锁定莱迪思FPGA的加密凭证并，并将平台可信根保护扩展到整个供应链，从IC制造到产品最终报废。莱迪思SupplyGuard™的特性包括：

- 防止过度制造、克隆、伪造和未经授权的硬件修改
- 能够在整个供应链中追踪器件
- OEM或ODM不需要特殊的高度安全的编程设备、流程或设施
- 外部IC的验证凭证作为客户加密配置位流的一部分被编程到莱迪思器件。这可以在工厂编程期间将系统中莱迪思FPGA的加密所有权安全地转移给客户

结论

莱迪思半导体致力于DC-SCM 2.0的推广。莱迪思通过可行的单芯片解决方案实现并优化了DC-SCM的三个关键功能。

莱迪思拥有经过充分验证的DC-SCM参考设计，可供更广泛的DC-SCM客户和电路板设计人员使用，帮助他们轻松实现DC-SCM。莱迪思紧密集成的解决方案可以为电路板设计人员提供统一的单个FPGA解决方案，而无需针对LTPI、安全和控制提出不同的解决方案组合。莱迪思完善的DC-SCM解决方案可以提高性能，降低功耗，且在电路板上占用很小的空间。

莱迪思针对三个关键的DC-SCM功能提供了一个包括GUI和非GUI工具的框架。系统架构师和电路板设计人员可以从下拉列表中轻松实现特性。我们的集成设计工具可以在一个面板视图中为架构师/设计师提供中整个解决方案，实现DC-SCM的三大特性。

参考文献

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

https://drive.google.com/file/d/14mypJ0Pvej35Q64PkDeK-sixrOIzvnKG/view

https://www.youtube.com/watch?v=SQy7Ztf3nGU

https://www.youtube.com/watch?v=eI9k3j-L-_0&t=8s

https://2020ocpvirtualsummit.sched.com/event/bXZu/dc-scm-base-specification-and-design-details-presented-by-microsoft

https://www.intel.com/content/www/us/en/products/docs/processors/xeon/platform-firmware-resilience.html

了解更多：

www.latticesemi.com

在线联系我们：

www.latticesemi.com/contact
www.latticesemi.com/buy