DC-SCM Implementation in Lattice FPGA

A Lattice Semiconductor White Paper.

May 2022

Learn more:

www.latticesemi.com

Contact us online:

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

TABLE OF CONTENTS

Abstract

DC-SCM is a sub-project of the OCP (Open Compute Project) Hardware Management Project. DC-SCM implements modular server management that contains all the FW (Firmware) states previously housed on a typical processor motherboard. DC-SCM moves three key elements to a common form factor module.

- Management -BMC functions plus a new interface LTPI (Low voltage differential signaling tunneling protocol and interface)
- Security
- Control

The paper describes the LTPI (server management), Security, and Control aspects of DC-SCM. All three key functions of DC-SCM 2.0 have been implemented in a single FPGA from Lattice Semiconductor.

One of the significant changes in the DC-SCM 2.0 specification is the introduction of Low-voltage differential signaling Tunneling Protocol & Interface (LTPI). This paper below describes the DC-SCM and its implementation of LTPI in the Lattice FPGA solution.

DC-SCM also describes a security module as ROT (Root of Trust), to address a security problem, where hackers can surreptitiously install malicious code in a privileged firmware's flash memory. Lattice PFR (Platform Firmware Resiliency) solution implemented as a ROT device for DC-SCM can eliminate this vulnerability in data center servers.

The Lattice FPGA also includes the control functions as defined by DC-SCM, providing reset sequencing and power management functions required for data center servers.

What is DC-SCM?

The Open Compute Project (OCP) is an organization that shares designs of servers and data center products and best practices among companies. DC-SCM (Datacenter-ready Secure Control Module) is a sub-project of the OCP Hardware Management Project. The sub-project provides the guideline that moves the common server management, security, and control features from a typical motherboard onto a common form factor module.

The DC-SCM architecture defines input/output ports for interoperability with CPU boards. A DC-SCM server has just the essential central compute element (CPU), high-speed Memory, and IO Connectors in the HPM (Host Processor Module) board, and everything else in the modular DC-SCM (Security, Control, Management) board.

Why DC-SCM

There are various benefits to DC-SCM:

- DC-SCM enables the design and deployment of CPU/Memory complexes with ease as management, security and control are independent of CPU/Memory board development.
  - Decouples BMC and RoT (Root of Trust) implementation from the server, allowing innovation at different rates
  - Saves cost by moving the management circuit to a smaller, less expensive PCB
  - Saves validation time by having a common DC-SCM design across multiple programs and architectures
  - Enables simpler HPM board layout and reduces development time
  - With Dc-SCM, Expansion Chassis can be a simple routine development based on guidelines from CPU and SoC suppliers.

- System management and security are constantly evolving and independent of CPU generation.
  - DC-SCM enables the deployment of management and security upgrades on platforms within a generation without redesigning more complex components.
- DC-SCM targets interoperability with ease using an open-source modular approach
  - Standardized common blocks
  - An adopted common interface like High-speed Interconnect (PCIe)
- One of the advantages of DC-SCM is the decommissioning of servers. Modular designs allow crushing/destroying the security module and the decommissioned server can be sold or recycled without exposing security data/keys.

DC-SCM Architecture

DC-SCM architecture consists of the following primary elements:

- BMC – The Baseboard Management Controller
- BMC Flash – One or more (typically two) flash devices are used to contain the BMC firmware image.
- BIOS Flash – One or more (typically two) flash devices used to contain the BIOS firmware image
- DC-SCM CPLD – A programmable logic device that contains application-specific logic and LTPI interface (LVDS Tunneling Protocol & Interface introduced in DC-SCM 2.0)
- RoT Security Processor – A security processor responsible for attesting the BMC, BIOS, and/or other firmware images on the system.
- TPM – Trusted Platform Module – An optional dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

The block diagram below is an architectural building block of a DC-SCM, as defined in the DC-SCM spec:

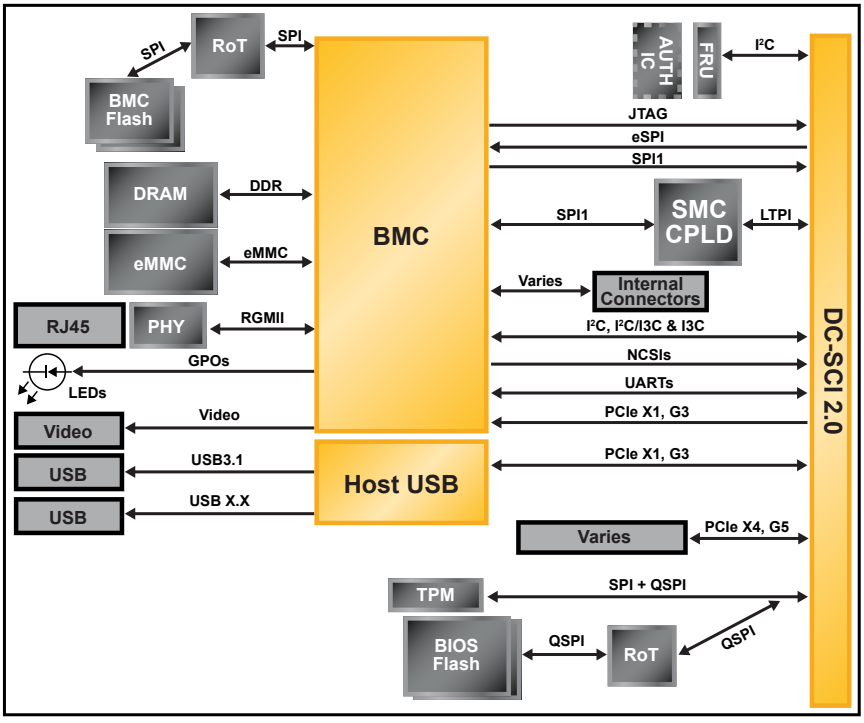

Figure 1

DC-SCM LTPI

One of the significant changes in the DC-SCM 2.0 specification is the introduction of Low-voltage differential signaling Tunneling Protocol & Interface (LTPI). The LTPI addresses shortcomings of the Serial GPIO interface used in DC-SCM 1.0.

- LTPI has much lower latency for GPIO
- It allows tunneling of multiple management interfaces between the Host Platform Module and DC-SCM module (provides a tunnel for I2C, SMBus, UART, Data-Custom Channels)

DC-SCM LTPI Architecture

The LTPI interface is implemented with two FPGA/CPLD devices as shown below

- HPM FPGA – providing a bridging of local HPM interfaces to LTPI
- SCM CPLD – providing an LTPI bridging to local SCM interfaces

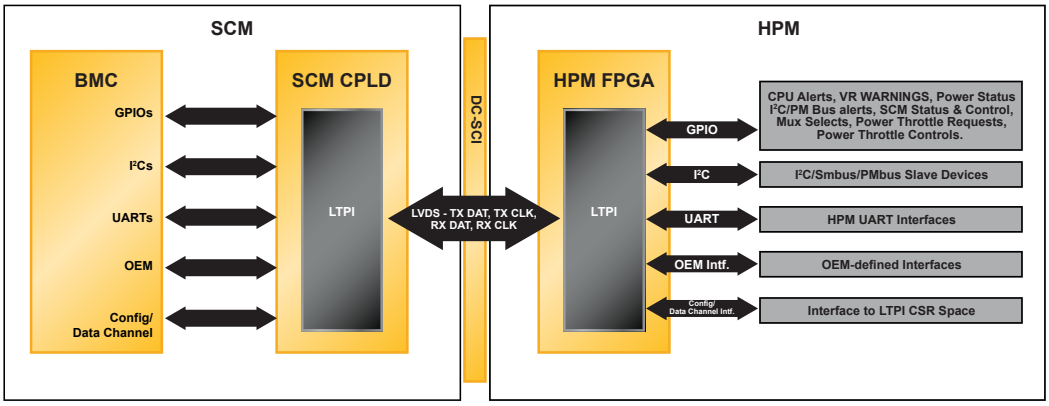

Figure 2

LTPI interface is designed for tunneling various low-speed signals between the HPM and SCM. The LVDS interface provides higher bandwidth and better scalability than the SGPIO interface introduced in DC-SCM 1.0. It allows for tunneling of not only GPIOs but also low-speed serial interfaces such as SMBus, I2C, and UART. It is also extensible with additional proprietary OEM interfaces and provides support for raw Data tunneling between HPM CPLD and SCM CPLD.

Lattice LTPI

The Lattice DC-SCM LVDS (Low Voltage Differential Signaling) Tunneling Protocol and Interface (LTPI) IP Core is an OCP, DC-SCM Standards compatible solution. Lattice LTPI IP fully supports the interface and protocol compliant with DC-SCM Protocol Specifications 2.0. The LTPI IP has the following features:

- Compliant with DC-SCM Protocol Specifications 2.0
  - Link initialization, discovery, and negotiation.
- Supports Multi-Channel Serial Interface
  - Supports GPIO, I²C, UART, OEM, and Data channel aggregation
  - Supports up to 7 channels of aggregation/disaggregation in total
- Supports up to 64-bit GPIO channels, with a sampling rate of up to 90 kHz (~ 5MHz for Low latency GPIO)
- For I²C/SMBus interface, each can be configured as master, slave, or Master/Slave (for multi-master).
- Supports LVDS and sub-LVDS
- Supports up to 1000Mbps LVDS data rate for LFMXO5 devices

Lattice LTPI Architecture

Based on the DC-SCM LTPI spec, Lattice uses Time Division Multiplexing (TDM) of a high-speed LVDS full-duplex link to transmit and receive LTPI channels between SCM and HPM.

As shown below, for every equal time slot TN (example Frame T+1 below) there is one LTPI Frame being transmitted. Each LVDS channel is being provided with a portion of the LVDS Frame transported in each direction. The number of bits assigned to a specific channel in each frame sent over the LTPI interface is directly proportional to the LTPI bandwidth dedicated for each channel.

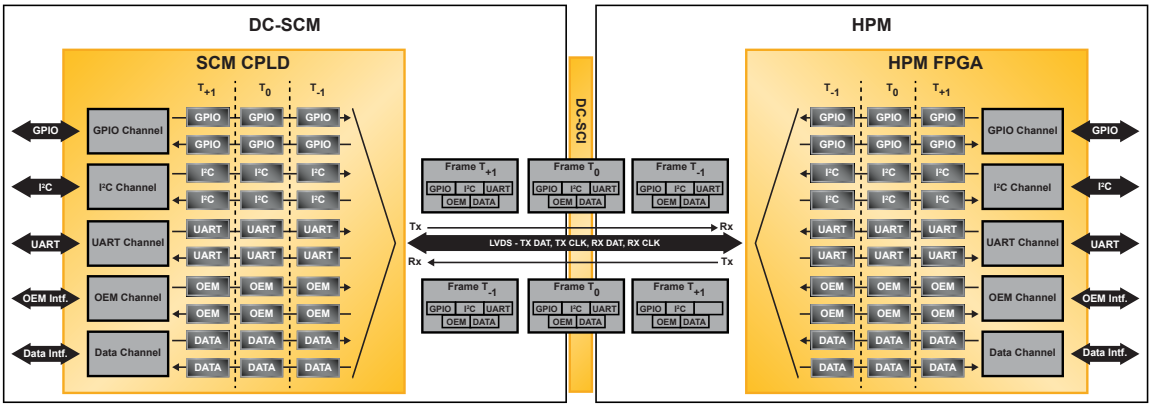

Figure 3

Lattice LTPI Channel Block Diagram

A high-level Channel diagram of the Lattice LTPI reference design is shown below. Data received from external channels are aggregated and transmitted between the Secure Control Module (SCM) and the Host Processor Module (HPM) through the Low Voltage Differential Signaling (LVDS) interface. Incoming data from the LVDS interface are remapped to the corresponding target external channel.

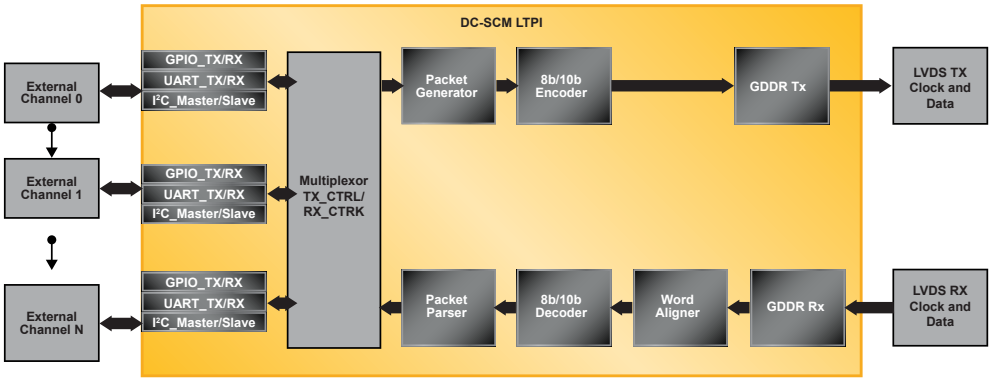

Figure 4

DC-SCM/HPM LTPI IP consists of Multiplexor, Frame/Packet Generator/Parser, 8b/10b Encoder/ Decoder, Word Aligner/Link Synchronizer, and GDDR Transmit and Receive modules. Multiplexor

Multiplexor

Multiplexor interfaces with the external channels. After link training and feature negotiation, the P. The multiplexor module switches sampling between each channel to form the payload.

Packet Generator and Parser

Frame generator and parser generate the required packets for link training and negotiations. Frame generator is used by TX to generate the frames to be sent over to communicating receiver. Frame parser is used by RX to parse the received frame

8b/10b Encoder/Decoder

LTPI IP performs 8b/10b encoding/decoding for data transmitted/received to/from receiving host. For TX, 8-bit data is converted to 10-bit data based on encoding specified in IEEE Standard 802.3.

GDDR Serializer/De-serializer

Data is transmitted to receiving host in serial form. IP serializes the data through generic DDR interface x5 (10bit: 1bit) for the LFXMO5 device and DDR interface x4 (8bit: 1bit) for MachXO3L/LF/D device. Likewise, for the RX mode, data is de-serialized through the DDR interface.

Lattice LTPI Interface Channels

The following channels are defined for the Lattice LTPI Interface

- GPIO Channel: This tunnels the GPIO signals from HPM to SCM and from SCM to HPM. The GPIO Channel allows for differentiation between Low Latency and Normal Latency GPIOs (Serialized GPIO) to allocate more bandwidth for time-critical GPIO Signals and allow for scalability in extending the number of tunneled GPIOs.
- I^2C/SMBus Channel: Tunnels I^2C/SMBus Links from SCM to HPM and HPM to SCM.
- UART Channel: Tunnels Full-Duplex UART interfaces with flow control support between SCM and HPM.

GPIO Interfaces

The GPIO channel defines Low Latency and Normal Latency GPIOs as defined in the DC-SCM spec (please see the figure below). This is a part of the Lattice IP configuration where each instance of these interface modules utilizes one channel with an IO width of up to 64 bits. For a successful transmission and reception, the PID (Packet Identifier) of the transmitting channel for either the SCM or HPM should match the PID of the receiving channel, which is instantiated on the transmitting module.

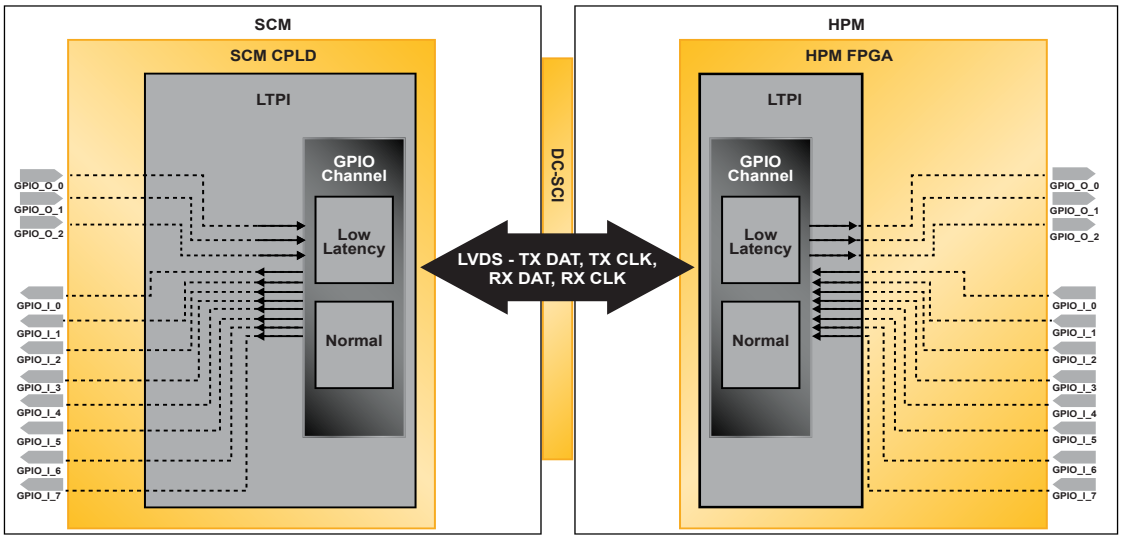

Figure 5

UART Interfaces

UART interfaces are sent through GPIO interfaces and require an instance of at least one GPIO TX and one GPIO RX channel.

I²C Interface

Lattice LTPI IP uses the I²C/SMBus Channel to tunnel I²C/SMBus buses through the LTPI interface for the links where there is only one Controller either on SCM or on the HPM. The primary use case addressed by the DC-SCM LTPI I²C/SMBus tunneling is as presented in the Figure below where BMC on SCM acts as the controller of the I²C/SMBus links with Target devices located on the HPM. Each instance of these interface modules utilizes one channel. For a successful transmission and reception, the PID of the I²C Master channel for either the SCM or HPM should match the PID of the I²C Slave channel that is instantiated on the other module.

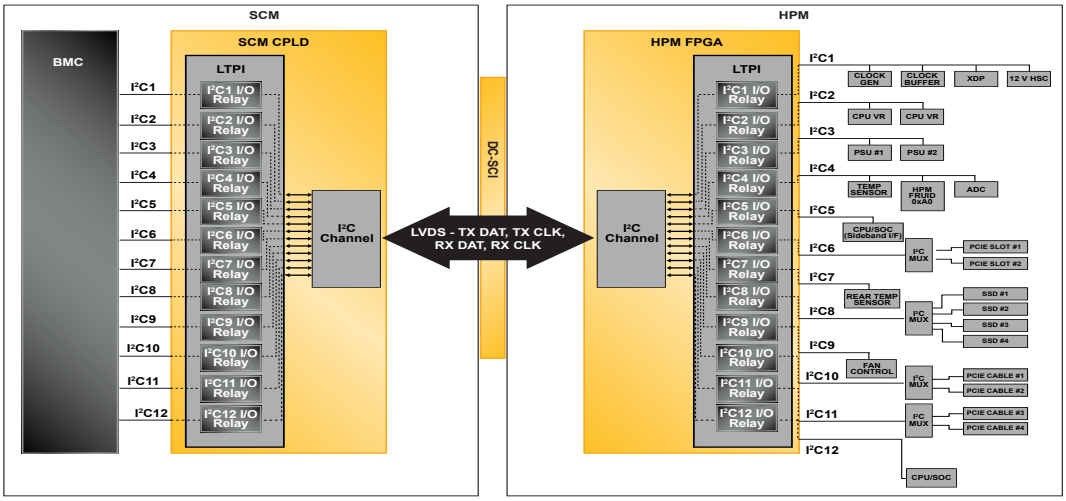

Figure 6

Lattice LTPI Channel Assignment:

Lattice LTPI Channels provide a functional classification of specific types of interfaces used in communication between SCM and HPM. Lattice LTPI allows for flexibility in the mapping of the interfaces. An example of design flexibility with LTPI is presented below (reference from DC-SCM LTPI spec). In this example, the GPIO channel is converted into an SGPIO interface with additional logic within SCM CPLD.

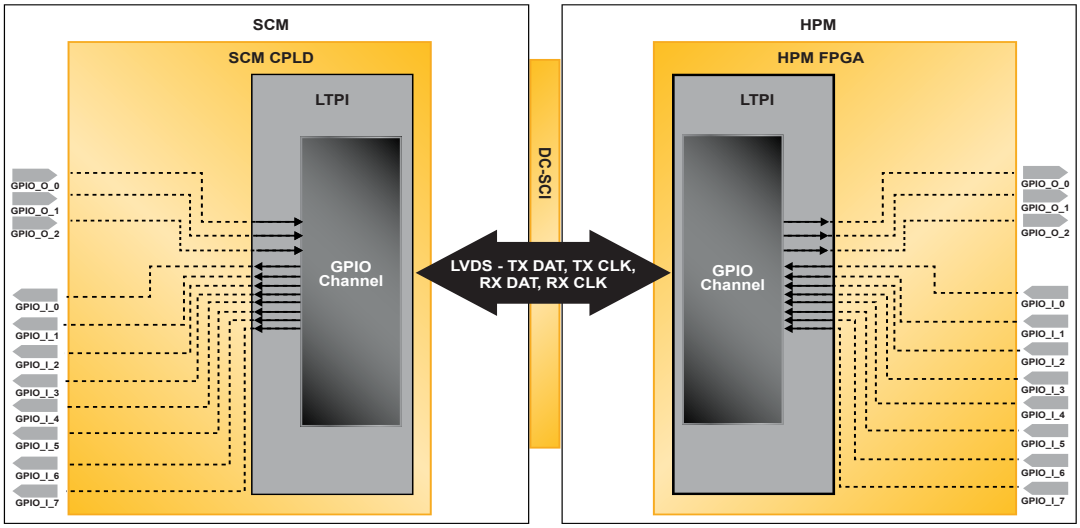

Figure 7

Lattice Security Implementation for DC-SCM

A typical enterprise server contains multiple processing components, each having its own non-volatile SPI flash memory storage for storing its firmware. Through unauthorized access to firmware, hackers can surreptitiously install malicious code in a component's flash memory. DC-SCM specification calls for a security processor responsible for attesting the BMC, BIOS, and/or other privileged firmware images on the system.

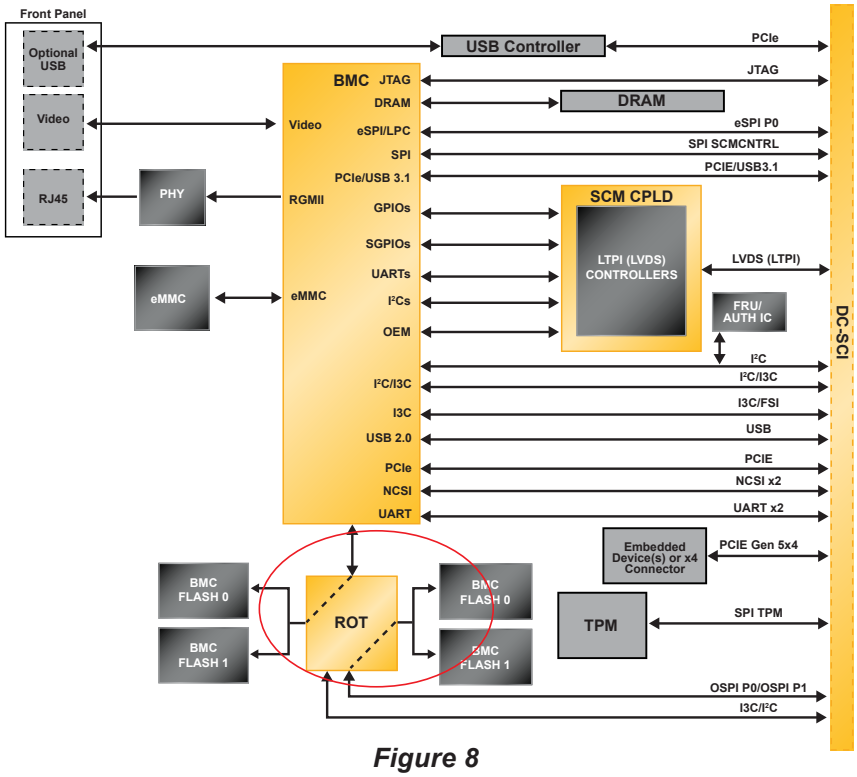

Figure 8

Lattice Security/RoT (Root of Trust) Implementation Overview

To address this security problem, where hackers can install malicious code in a privileged firmware's flash memory, the National Institute of Standards and Technology (NIST) released the NIST SP 800 193 specifications in 2018, which defines a uniform protection mechanism known as Platform Firmware Resilience (PFR). Lattice has a PFR solution that can be implemented as an RoT device for DC-SCM which addresses this vulnerability of enterprise servers. Lattice RoT is implemented based on three guiding principles:

- Protection – Lattice has demonstrated state machine-based algorithms that offer nanosecond response time in detecting security breaches into the SPI memory. This prevents unauthorized access to modify any of the firmware in SPI memory. The solution is customizable through simple easy-to-use databases. Using secure communication with the PFR algorithm, the BMC will be able to authorize modifications to SPI memory to support in-system updates.
- Detection – Elliptic Curve Cryptography (ECC) based measurements made on the firmware stored in each of the SPI memory detect all unauthorized modifications to it. The detection method is independent of the existing firmware security approaches used in that design. Using the integrated board power management function, it is possible to detect any unauthorized modifications to firmware before the board is started up.

- Recovery – If a security breach is detected, Lattice's implementation provides a customizable recovery mechanism. This mechanism can perform a simple rollback to a previous version of firmware, or a full-blown recovery to the latest authorized version of the firmware. The Power Management and Control PLD algorithm can be customized to respond to the nature of the breach to implement the full trusted recovery process for any Board.

Implementation Features

Lattice's PFR solution has many desired customers and developers' features. Some of the features are:

- Scalable – Protect, with nanosecond level response all firmware on the board. The solution can also protect other add-in subsystems through secure communication with the corresponding roots of trust
- Non-By-passable – As this solution implements the full power sequencing for the server board along with the PFR implementation, it cannot be bypassed
- Self-Protecting – The PFR implementation uses a revolutionary Root-of-Trust FPGA as an anchor. This FPGA can dynamically control its attack surface and protects itself from external attacks
- Self-Detecting – The Root-of-Trust FPGA can detect any security breach of its configurations by using a non-by-passable cryptographic hardware block.
- Self-Recovery – The Root-of-Trust FPGA can switch over to the known good image automatically when it discovers a breach to its active configuration

Lattice Control Implementation for DC-SCM

Almost all servers today use the Lattice FPGA devices for control PLD functions, such as power/reset sequencing, various types of serial busses (I2C, SPI, eSPI, SGPIO, etc.), debug ports, LED drives, FAN PWM driver, front panel switches sensing and other general GPIO functions. Lattice FPGA devices support 1V signaling, which enables them to perform out-of-band signal integration without the need for external GTL transceivers.

Hitless I/O

To enable zero downtime, Lattice implemented a feature called Hitless I/O. Typically, Control PLDs enable the designers to significantly reduce time-to-market and enable them to meet the market pressures of bringing out new customized hardware within the allotted time. Sometimes, there could be bugs in the implementation of the control function or the overall system architecture that may require a new function. A common approach to accomplish a modification to the design is through an in-system update and power cycling of the system to bring the newly programmed image into service. To ensure the continuous operation of high availability systems, the Lattice FPGA devices can hold the I/Os unchanged, while the configuration refresh occurs, and the new configuration initializes.

Lattice Evolution - Three Key functions in One Solution

Lattice FPGA offers the unique possibility of three key functions of DC-SCM integrated into a Lattice solution:

- LTPI (management function)
- Security (Dynamic, Real-Time, End-to-End Protection) and
- Control (Programmable system control)

Lattice FPGAs are highly reliable and lead the industry for low-power FPGA-based applications and offer up to 100X better SER (soft error rate) performance than comparable CMOS technologies. Lattice FPGA has Robust Standards & DC-SCM Protocol Compliance. The available Propel tool provides developers with an easy configuration of the Drag & Drop Interface.

Lattice Products Supporting DC-SCM

Lattice is very committed to DC-SCM. Lattice has a portfolio of FPGA products that supports DC-SCM as well as Root of trust and user power control logic. Below is a list of existing products that support DC-SCM.

Lattice Products	DC-SCM	RoT	Control
MachXO3D	✓	✓	✓
Mach-NX	✓	✓	✓
MachXO5-NX	✓	✓	✓
MachXO3	✓		✓

Table 1

Lattice End-to-End Protection with SupplyGuard™

Lattice is very committed to DC-SCM. Lattice has a portfolio of FPGA products that supports DC-SCM as well as Root of trust and user power control logic. Below is a list of existing products that support DC-SCM.

Lattice SupplyGuard™ assigns a unique ordering part number to each customer. The unique part number corresponds to the encryption credentials which lock the Lattice FPGA and extend Platform root of trust protection to the entire supply chain, from IC manufacture through final product end of life. Some of the useful features that Lattice SupplyGuard™ are

- Protection against overbuilding, cloning, counterfeiting, and unauthorized hardware modification.
- Ability to track devices through the supply chain.
- No special high-security programming equipment, processes, or facilities are needed for OEMs or ODMs.
- Authentication credentials of external ICs are programmed onto Lattice as part of the customer's encrypted configuration bitstream. This securely transfers cryptographic ownership of the Lattice FPGAs in the system to the customer during factory programming

Conclusion

Lattice Semiconductor is dedicated to the DC-SCM 2.0 rollout. Lattice implemented and optimized three key DC-SCM functions with a viable single-chip solution

Lattice has fully validated DC-SCM reference designs available for broader DC-SCM customers and board designers who can implement DC-SCM with ease. Lattice's tightly integrated solution can enable board designers to have a unified single FPGA solution instead of a portfolio of different solutions for LTPI, Security, and Control. Lattice's cohesive DC-SCM solution can improve performance and reduce power consumption as well as occupy a small footprint on the board.

Lattice has a framework of GUI and non-GUI-based tools for these three key DC-SCM functions. System architects and Board designers can easily implement features from a drop-down list of choices. Our integrated design tools can give the architect/designers a single pane of glass view of a single solution to three major DC-SCM features.

References

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

Learn more:

www.latticesemi.com

Contact us online:

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