OpenTitan Integrated
A RISC-V Open-Source Silicon Root-of-Trust for large SoCs

Robert Schilling[1], Samuel Ortiz[1], Ravi Sahita[1], Andreas Kurth[2]

[1]Rivos Inc.
[2]lowRISC CIC

Abstract

Modern System-on-Chips (SoCs) rely on a secure Root of Trust (RoT) as the foundation for all security services. Compromise of the RoT can have catastrophic consequences, undermining the security of the entire system.

This paper presents OpenTitan Integrated, an open-source silicon RoT based on RISC-V specifically tailored for integration into the complex security subsystems of large SoCs. OpenTitan Integrated extends the functionality of the discrete OpenTitan implementation by addressing the specific needs of integrated deployments. Key contributions include: 1) a clear interface trust boundary, defining secure communication paths and preventing privilege escalation; 2) a robust and standardized communication interface, enabling seamless interaction with other SoC components; and 3) a flexible register isolation mechanism, protecting sensitive registers in the system from unauthorized access and modification. These additions enable secure interaction with other SoC components and prevent unauthorized access, enhancing the overall security posture of the SoC.

Furthermore, OpenTitan Integrated's open-source nature, available on GitHub under a permissive license, facilitates community review, independent verification, and enhances the overall security and trustworthiness of the design. This collaborative approach allows for rapid identification and mitigation of potential vulnerabilities, leading to a more robust and secure RoT.

Introduction

Large SoCs increasingly rely on integrated Root-of-Trust (RoT) solutions to provide crucial security services, ranging from secure boot and attestation to debug authorization. However, integrating a secure and trustworthy RoT into complex SoC architectures presents significant challenges. Traditional, closed-source RoT solutions can be costly, difficult to integrate, and lack transparency and do not provide the necessary flexibility for the integration. This paper introduces OpenTitan Integrated, an open-source integrated RoT based on RISC-V designed to address these challenges. Building upon the proven OpenTitan project [1], we introduce enhancements specifically for integrated deployments, including a secure and trusted communication interface, isolated register accesses, and a comprehensive secure debug authorization mechanism. *Darjeeling*, our open-source reference implementation of OpenTitan Integrated, is illustrated in Figure 1 and is available under GitHub [2].

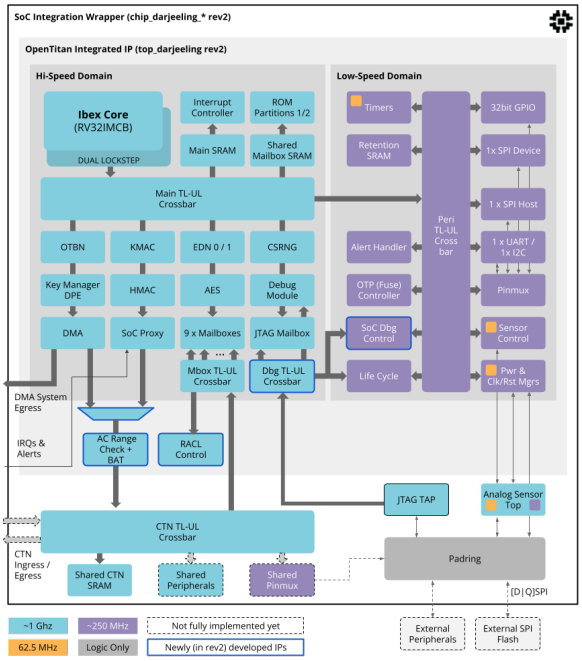

Figure 1: *OpenTitan Integrated Architecture.*

Integrated Communication Interface

Secure communication between the SoC and the OpenTitan Integrated Root of Trust (RoT) is paramount. To achieve this, OpenTitan Integrated leverages two distinct communication interfaces enforcing the principle of least privilege. First, multiple Data Object Exchange (DOE)-compatible mailboxes provide a controlled and secure mechanism for loading data from the SoC into the RoT. Critically, the RoT rigorously verifies all requests, including data access permissions, ensuring only legitimate operations are executed. The mailbox interface serves as the *sole* communication

pathway between the SoC and OpenTitan Integrated, enforcing a strong trust boundary and preventing unauthorized access. Responses can be sent directly via the mailbox or, for larger data transfers, through a dedicated DMA controller. A key innovation in OpenTitan Integrated is the DMA's support for inline hashing. This feature automatically computes hash values of transferred data, enabling efficient and robust integrity verification of critical images, such as those used during the secure boot process.

Register Access Control

An SoC must provide differentiated security on access to registers in the SoC and the CPU. In OpenTitan Integrated, we provide a generic solution to this problem and introduce Register Access Control (RACL). In RACL, each processing element is assigned a role, which is transmitted alongside with the register access on the bus fabric. At the register level, this role is compared against the allowed set of roles (policy) for this register (read and write accesses support a different role set). If the transmitted role of the processing element is within the policy, the register access is allowed. Otherwise, the access is denied, a bus error is returned, and the denied access is logged in dedicated error registers.

In OpenTitan Integrated, we integrated this framework purely based on HJSON files. Integrators that use this framework define their roles and policies in a single configuration file acting as a single source of truth. Furthermore, they define on a per-instance basis, the mapping of allowed roles per registers, also in the form of an HJSON file. The SoC-generator tool of OpenTitan *topgen* picks up these configuration files and automatically generates the necessary hardware, without use interaction. As illustrated in Figure 2, this methodology ensures minimal user interaction, easy auditability, and prevents duplication by generating everything from the HJSON specification. Furthermore, the tool also create verification environments and a documentation collateral, which is equally important as the functionality itself.

Debug Control and Authorization

Debug mechanisms are essential in complex SoCs, particularly those with numerous embedded processing cores. However, uncontrolled debug access can pose a significant security risk. OpenTitan Integrated addresses this challenge with a dedicated *Debug Control Module*. This module acts as the central authority for managing the debug state of the entire SoC, distributing a dedicated debug bus to control debug capabilities across the chip. This granular control allows for enabling or disabling debug access on a per-component

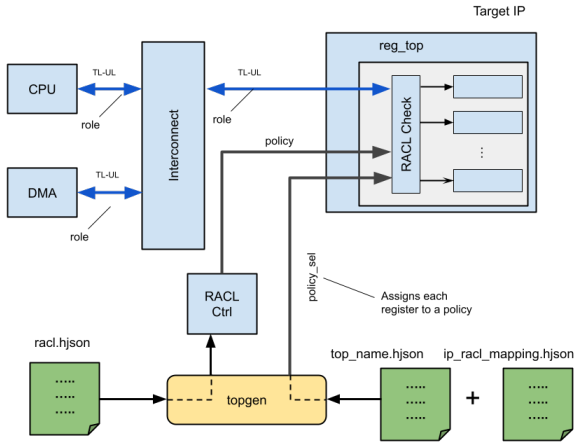

Figure 2: *RACL Tooling in OpenTitan.*

basis. While debugging might be permissible during development, production deployments typically require restricted access to certain components. OpenTitan Integrated implements a robust, cryptography-based debug authorization flow, enabling trusted operators to securely authorize and selectively enable debug features for specific components even after deployment. This ensures secure debug access while protecting sensitive components in production.

Discussion

This work has presented OpenTitan Integrated, an open-source silicon Root of Trust designed specifically for the integrated use case in large SoC designs. Building upon the robust foundation of OpenTitan, we have enhanced both the design and tooling to meet the unique requirements of seamless SoC integration. A core principle of this project is *transparency*. OpenTitan Integrated, including the reference implementation *Darjeeling*, is developed openly on GitHub, fostering community participation and scrutiny. We believe that this open and collaborative approach not only strengthens the RISC-V ecosystem by providing a high-quality, auditable RoT, but also significantly improves the security of this critical component. By leveraging the collective expertise of the open-source community, we can identify and address potential vulnerabilities more effectively, ultimately leading to a more secure and trustworthy RoT for a wide range of applications.

References

[1] OpenTitan Contributors. *OpenTitan: Open Source Silicon Root of Trust*. `https://opentitan.org/`. [Online; accessed 07-Feb-2025]. 2025.

[2] OpenTitan Contributors. *OpenTitan OpenSource Implementation*. `https://github.com/lowRISC/opentitan`. [Online; accessed 07-Feb-2025]. 2025.