RISC-V Server Platform Specification

Server Platform Task Group

Version v0.0.0, 2023-11-30: Draft

Table of Contents

Preamble

This document is in the Development state

Assume everything can change. This draft specification will change before being accepted as standard, so implementations made to this draft specification will likely not conform to the future standard.

Copyright and license information

Contributors

This RISC-V specification has been contributed to directly or indirectly by (in alphabetical order):

Andrei Warkentin, Ved Shanbhogue

Chapter 1. Introduction

The RISC-V Server Platform specification defines a standardized set of hardware and sofware capabilities, that portable system software, such as operating systems and hypervisors, can rely on being present in a RISC-V server platform.

A server is a computing system designed to manage and distribute resources, services, and data to other computers or devices on a network. It is often referred to as a 'server' because it serves or provides information and resources upon request. Such computing systems are designed to operate continually and have higher requirements for capabilities such as RAS, security, performance, and quality of service. Examples of servers include web servers, file servers, database servers, mail servers, game servers, and more. This specification focuses on defining requirements for general-purpose server computing systems that may be used for one or more of these purposes.

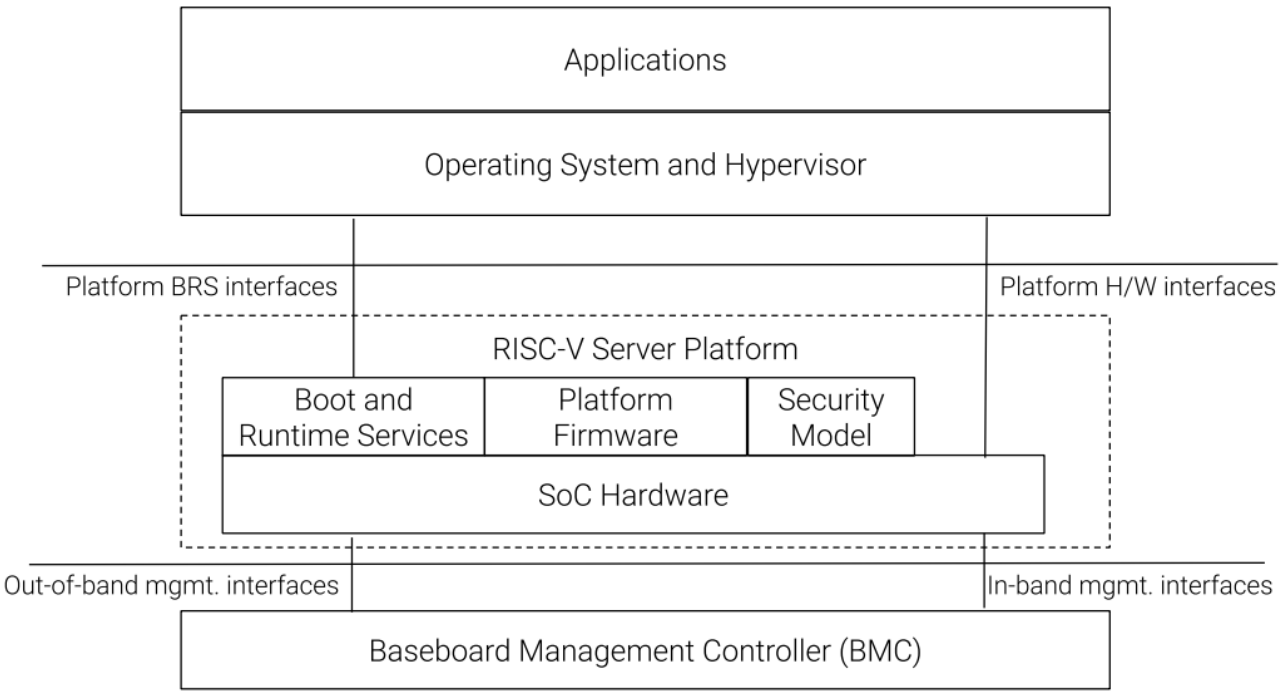

Figure 1. Components of a RISC-V Server Platform

The RISC-V server platform is defined as the collection of SoC hardware, peripherals, platform firmware, boot/runtime services, and platform security services. The platform provides hardware interfaces (e.g., harts, timers, interrupt controllers, PCIe root ports, etc.) to portable system software. It also offers a set of standardized boot and runtime services based on the UEFI and ACPI standards. To support provisioning and platform management, it interfaces with a baseboard management controller (BMC) through both in-band and out-of-band (OOB) management interfaces. The in-band management interfaces support the use of standard manageability specifications like MCTP, PLDM, IPMI, and Redfish for provisioning and management of the operating system executing on the platform. The OOB interface supports the use of standard manageability specifications like MCTP, PLDM, Redfish, and IPMI for functions such as power management, telemetry, debug, and provisioning. The platform security model includes guidelines and requirements for aspects such as debug authorization, secure/measured boot, firmware updates, firmware resilience, and confidential computing, among others.

The platform firmware, typically operating at privilege level M, is considered part of the platform and is usually expected to be customized and tailored to meet the requirements of the SoC hardware (e.g., initialization of address decoders, memory controllers, RAS, etc.), boot/runtime services and platform security.

This specification standardizes the requirements for hardware and software interfaces and capabilities by building on top of relevant RISC-V standards, such as the Server SoC, Boot and Runtime Services and Platform Security specifications for server software executing on the application processor harts at privilege levels below M. It enables OS and hypervisor vendors to support such platforms with a single binary OS image distribution model. The requirements posed by this specification represent a standard set of infrastructural capabilities, encompassing areas where divergence is typically unnecessary and where novelty is absent across implementations.

To be compliant with this specification, the server platform MUST support all mandatory requirements and MUST support the listed versions of the specifications. This standard set of capabilities MAY be extended by a specific implementation with additional standard or custom capabilities, including compatible later versions of listed standard specifications. Portable system software MUST support the specified mandatory capabilities to be compliant with this specification.

The requirements in this specification use the following format:

ID#	**Requirement**
CAT_NNN	The `CAT` is a category prefix that logically groups the requirements and is followed by 3 digits - `NNN` - assigning a numeric ID to the requirement. The requirements use the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" that are to be interpreted as described in RFC 2119 [1] when, and only when, they appear in all capitals, as shown here. When these words are not capitalized, they have their normal English meanings.
A requirement or a group of requirements may be followed by non-normative text providing context or justification for the requirement. The non-normative text may also be used to reference sources that are the origin of the requirement.	

This specification groups the requirements in the following broad categories:

- Hardware
- Firmware
- Security

1.1. Glossary

Most terminology has the standard RISC-V meaning. This table captures other terms used in the document. Terms in the document prefixed by 'PCIe' have the meaning defined in the PCI Express (PCIe) Base Specification [2] (even if they are not in this table).

Table 1. Terms and definitions

Term	Definition
ACPI	Advanced Configuration and Power Interface [3].
BMC	Baseboard Management Controller. A motherboard resident management controller that provides functions for platform management.
Guest	Software in a virtual machine.
Hypervisor	Software entity that controls virtualization.
ID	Identifier.
OS	Operating System.
SoC	System on a chip, also referred as system-on-a-chip and system-on-chip.
UEFI	Unified Extensible Firmware Interface. [4]
VM	Virtual Machine.

Chapter 2. Server Platform Hardware Requirements

2.1. RISC-V SoC

A RISC-V server platform is based on a RISC-V SoC with RISC-V application processors.

ID#	Requirement
HSOC_010	The RISC-V SoC MUST comply to the Server SoC specification [5].
The Server SoC specification is still under construction. This specification should be updated once the specification versioning info is finalized.	
HSOC_020	All peripherals that are intended for assignment to a VM or a user space device driver must be based on PCIe.

2.2. Peripherals

ID#	Requirement
HPER_010	For remote-access and system engineering purposes, a fully 16550-compatible [6] UART MUST be implemented.
This specification does not provide guidance around how the UART is physically exposed, i.e. via RS232 signalling or via a BMC	
HPER_020	The implemented UART MUST support: • Interrupt-driven operation using a wired interrupt. • Flow control.
HPER_030	If a USB controller is implemented, it MUST comply to XHCI 1.2 or later [7].
HPER_040	Implemented XHCI controllers must: • Support 64-bit addressing (AC64 = '1'). • Support a 4K PAGESIZE.
HPER_050	If a SATA controller is implemented, it must comply to AHCI 1.3.1 or later [8].
HPER_060	Implemented AHCI controllers must: • Support 64-bit addressing (S64A = '1').

Chapter 3. Server Platform Firmware Requirements

ID#	Requirement
FIRM_010	The RISC-V SoC MUST comply to the BRS-I recipe described in the Boot and Runtime Service specification [9].
The Boot and Runtime Services specification is still under construction. This specification should be updated once the specification versioning info is finalized.	

Chapter 4. Server Platform Security Requirements

Bibliography

[1] “Key words for use in RFCs to Indicate Requirement Levels.” [Online]. Available: datatracker.ietf.org/doc/html/rfc2119.

[2] “PCI Express® Base Specification Revision 6.0.” [Online]. Available: pcisig.com/pci-express-6.0-specification.

[3] “Advanced Configuration and Power Interface (ACPI) Specification.” [Online]. Available: uefi.org/specifications.

[4] “Unified Extensible Firmware Interface.” [Online]. Available: uefi.org/specifications.

[5] “RISC-V Server SoC Specification.” [Online]. Available: github.com/riscv-non-isa/server-soc.

[6] “National Semiconductor PC16550D UART Datasheet.” [Online]. Available: www.scs.stanford.edu/10wi-cs140/pintos/specs/pc16550d.pdf.

[7] “eXtensible Host Controller Interface for Universal Serial Bus 1.2.” [Online]. Available: www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/extensible-host-controler-interface-usb-xhci.pdf.

[8] “Advanced Host Controller Interface (AHCI).” [Online]. Available: www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/serial-ata-ahci-spec-rev1-3-1.pdf.

[9] “RISC-V Boot and Runtime Services Specification.” [Online]. Available: github.com/riscv-non-isa/riscv-brs.