BootCore™ SC

Safety-Critical Firmware for Intel's Tiger Lake SoC

FEATURES AND BENEFITS

- Safety-critical boot firmware that provides chipset initialization and launches a pre-OS boot payload
- Small storage footprint results in smaller flash size requirements
- Quick boot times
- Designed with security as a priority
- Modular design to allow
  - Extensibility to add custom features
  - Functional reliability that can be trusted in safety-critical deployments
- Configurability to meet the needs of customer programs

INTRODUCTION

CoreAVI's BootCore™ SC is a safety-critical boot firmware that provides functionality for hardware chipset initialization and payload launch to boot an operating system. Central to BootCore SC is a modular design which allows a clear separation between initialization and launch. This separation and modularity allow quick boot times while maintaining functional reliability, extensibility, configurability, and a small footprint. BootCore SC is ideal for all safety-critical applications in industries such as aerospace, defense, automotive, IoT, and many others. BootCore SC is offered independently but is part of CoreAVI's Platforms for Safety-Critical Applications, also consisting of VkCore® SC, VkCoreGL® SC, and ComputeCore™ products. It is available with the required safety data packages for the highest levels of safety certification.

BootCore SC is integral to CoreAVI's SBC3005 Single Board Computer; however, BootCore SC may also be licensed for other hardware solutions such as those developed by the customer in-house.

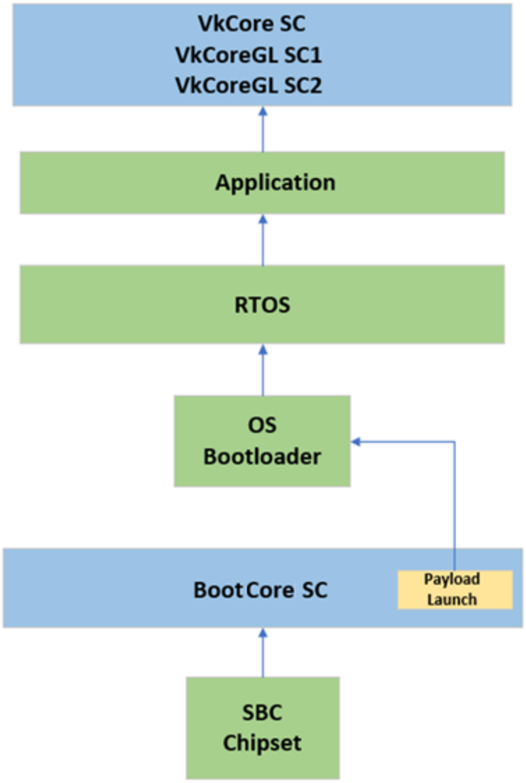

Figure 1: BootCore SC Boot Process

SECURITY

BootCore SC provides available support for trusted platform modules (TPM), verified boot on Intel Tiger Lake products, and measured boot. These features verify firmware components before execution to ensure system boot is not compromised.

MODULAR DESIGN

BootCore SC employs a modular design that allows the addition of features specific to a customer program, such as program specific splash screens or new functionality. Feature development is performed in conjunction with CoreAVI engineering services.

CONFIGURABILITY

BootCore SC can be configured during the build process to enable or disable firmware functionality. Some features that are configurable are:

- Security features
- Firmware boot device order
- Launch payload to boot an operating system
- Splash screen
- Custom functionality

CERTIFICATION SUPPORT

CoreAVI's BootCore SC supports FAA DO-178C /EASA ED-12C Level A certification with data packages to aid in FAA DO-178C / EASA ED-12C avionics software safety certification. BootCore SC also supports ISO 26262 ASIL D safety compliance, and for functional safety support in industrial automation and robotics applications, BootCore SC provides support for IEC 61508 support up to SIL3.

For more information, please contact Sales@CoreAVI.com.