MSL FPGA INC 晶片參數

芯片概述

CEC1712H-S2-I/SX 是来自MSL FPGA INC美时龙的一款安全加密嵌入式控制器，专为防范恶意软件和实现硬件级安全启动设计，主要应用于 5G 基础设施、汽车电子及工业控制领域。以下是其关键信息：

核心参数

安全架构：基于 Arm Cortex-M4处理器，集成硬件信任根（Root of Trust），
支持安全启动功能，可验证外部 SPI 闪存中的固件完整性。
符合NIST 800-193标准，提供密钥撤销和代码回滚保护，确保固件更新安全。

功能特性

加密功能：内置 Soteria-G2 定制固件，在预启动阶段检测并阻止恶意程序，缩短开发周期。
支持多处理器验证（最多两个应用处理器，每个处理器配两个闪存组件）。

应用场景

5G 与数据中心：保护操作系统免受预启动阶段的恶意攻击。
汽车电子：用于 ADAS（高级驾驶辅助系统）等需高安全性的场景。