life.augmented

AN4729
应用笔记
STM32L0/L4 防火墙概述

前言

防火墙是 STM32 L0 和 L4 系列微控制器提供的附加保护系统。它用于保护 Flash 或 SRAM 存储器中的部分代码或数据，使其不受意图转贮代码或获取相关敏感数据的攻击。防火墙可检测到对这些受保护区域的每次非法访问，并相应地产生复位，中断任何入侵。

防火墙能够保护三个不同的可配置区域，通常叫做段：

- 位于 Flash 或 SRAM 存储器中的代码段；
- 位于 Flash 存储器中的非易失性的数据段；
- 位于 SRAM 存储器中的易失性的数据段。

防火墙打开时，每个段均可被 CPU 访问 （允许的访问类型取决于执行访问的段）。当防火墙关闭时，不能访问这些受保护的段。每次访问都触发一个复位。

要打开防火墙，需要执行一个叫做 “ 调用门 ” 的特殊序列。它是打开防火墙并解锁对受保护代码和数据区域的访问 （以及执行受保护代码）的唯一入口点。从调用门函数返回会将其关闭。

防火墙可用于保护来自第三方的敏感代码以及保护 OEM 应用软件不受攻击。

将防火墙性能和其他保护机制 （像专利代码读出保护或读保护， PCROP 或 RDP）结合起来，可实现高级保护。

根据目标安全限制、软件架构和开发阶段的相关工作模型，可考虑不同的应用方案。

若需完整解决方案的更详细信息，请联系您本地的 ST 销售代表。

1 版本历史

表 1. 文档版本历史

日期	版本	变更
2015 年 8 月 25 日	1	初始版本。

表 2. 中文文档版本历史

日期	版本	变更
2017 年 6 月 30 日	1	中文初始版本。

重要通知 - 请仔细阅读

意法半导体公司及其子公司 （“ST”）保留随时对 ST 产品和 / 或本文档进行变更、更正、增强、修改和改进的权利，恕不另行通知。买方在订货之前应获取关于 ST 产品的最新信息。 ST 产品的销售依照订单确认时的相关 ST 销售条款。

买方自行负责对 ST 产品的选择和使用， ST 概不承担与应用协助或买方产品设计相关的任何责任。

ST 不对任何知识产权进行任何明示或默示的授权或许可。

转售的 ST 产品如有不同于此处提供的信息的规定，将导致 ST 针对该产品授予的任何保证失效。

ST 和 ST 徽标是 ST 的商标。所有其他产品或服务名称均为其各自所有者的财产。

本文档中的信息取代本文档所有早期版本中提供的信息。