

FORD LDM Localization - 功能 #3387

Task # 3240 (进行中): FORD文档输出

功能 # 3349 (进行中): SWQA文档

功能 # 3359 (已解决): TDR_RQT_003701_705381 Supervision of Unused Executable Memory

TDR_RQT_003701_705381 001 (Unused Memory Execution)

2025-03-17 13:29 - 力常 张

状态:	新建	开始日期:	2025-03-17
优先级:	普通	计划完成日期:	
指派给:	力常 张	% 完成:	100%
类别:		预期时间:	0.00 小时
目标版本:	FORD_TDR_Documents	耗时:	0.00 小时
描述 参考软件 “ DR-003701-707985 Unused Memory Execution ” 需求描述 本设计规则支持 RQT-003701-705381 《未使用内存执行监控（Unused Memory Execution）》，适用于包含以下类型软件的所有电子控制模块： 非AUTOSAR操作系统（Non-AUTOSAR OS） AUTOSAR Classic 平台 AUTOSAR Adaptive 平台 并作为该RQT的合规性实施方法。 核心要求： 若执行未使用的可执行内存地址，必须在执行监控器（execution supervisor，如看门狗）超时时间的2倍时间内触发微控制器硬件复位，且此时间需进一步受功能安全要求约束。 若程序计数器（program counter）取值超出编程地址范围（programmed address range），微控制器硬件复位（microcontroller hardware reset）是最安全的恢复方法。仅通过执行全部或部分程序初始化序列（program initialization sequence）作为运行时恢复措施（runtime recovery action）而不进行硬件复位是不充分的，因为程序计数器损坏（program counter corruption）属于根本性故障（fundamental fault），无法在发生损坏的同一电源周期（power cycle）内信任程序化异常处理（programmatic exception handling）。 微控制器硬件复位及后续冷启动初始化（cold boot initialization）是应对并防止运行环境级异常（operating environment level exceptions）复发的稳健、普适且场景适配的恢复方法。 注：子微控制器（sub-microcontroller）的数据或可执行映像不属于未使用内存——其应被视为大型数据表（large data table）的类比。 强制复位实现方法（当执行未使用内存时）： 由于内存对齐（memory alignment）可能引发问题，仅允许使用与对齐无关的指令。依赖执行监控器（execution supervisor）超时的策略不可用，因为当程序执行超出范围（fundamental error）时无法保证监控器的正常运行。福特核准的强制复位技术如下（其他技术须按"分析/讨论"章节的例外流程实施）： 将内存填充为SWI指令。在SWI中强制执行复位。 分析/讨论 本设计规则支持所有带软件的电子模块的RQT-003701-705381 “未使用的内存执行”，是符合RQT的一种方法。 设计规则关闭机制：这些设计规则的关闭是软件技术设计的完成 审查（TDR），并通过“SWQA常见TDR检查表”问题解决： IRH08004 A) 您如何确保在重置时初始化未使用的RAM？ B) 如何确保RAM变量在重置时初始化？ IRH08012 RAM可执行性（RAM Executability） A) RAM是否可执行？（包含堆栈） B) 若未使用的可执行RAM被执行，MCU复位的最大延迟时间（最坏情况时间）是多少？ C) 若在MCU堆栈中发生执行，描述您系统的反应。			

历史记录

- #1 - 2025-03-24 14:58 - 稚媛 黄
- 指派给 被设置为 力常 张
- #2 - 2025-03-24 15:30 - 稚媛 黄
- 主题 从 DR-003701-707985 未使用内存执行（Unused Memory Execution） 变更为 TDR_RQT_003701_705381未使用内存执行（Unused Memory Execution）
- 描述 已更新。
- #3 - 2025-03-24 15:30 - 稚媛 黄
- 主题 从 TDR_RQT_003701_705381未使用内存执行（Unused Memory Execution） 变更为 TDR_RQT_003701_705381 001未使用内存执行（Unused Memory Execution）

#4 - 2025-03-25 15:45 - 稚媛黄

- 主题 从 TDR_RQT_003701_705381 001未使用内存执行 (Unused Memory Execution) 变更为 TDR_RQT_003701_705381 001 (Unused Memory Execution)