# FORD LDM Localization - 功能 #3388

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 002 Unused Memory Monitor

2025-03-17 13:30 - 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-003701-707986 Unused Memory Monitor
需求描述
本设计规则支持 RQT-003701-705381《未使用可执行内存监控（Supervision of Unused Executable Memory）》，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。

. 未使用RAM必须被检查，以验证其内容自当前电源周期（power cycle）启动初始化后未发生更改。
. 未使用RAM区域必须监控内存损坏，若发生损坏，系统需采取适当措施（至少需将错误码记录至非易失性存储器（NVM））。
. 未使用RAM必须填充预设值，以便检测非预期写入。禁止使用0xFF和0x00作为填充值。
. 未使用NVM必须被检查，以验证其内容自最后一次批量编程（bulk programmed）后未发生更改。
· 未使用NVM区域必须监控内存损坏，若发生损坏，系统需采取适当措施（至少需将错误码记录至NVM）。
·
未使用NVM必须填充预设值以检测非预期写入。允许值为微控制器专用SWI指令、0x55或0xAA。若需偏离此规则，明确禁止使用"擦除"或"未编程"状态值（通常为0xFF或0x00），因其无法表明内存填充的有意编程写入。（*参见"未使用NVM定义"注释。）
· 需提供软件机制报告未使用NVM的状态（例如：可用、受保护、故障）。
· 未使用ROM区域必须监控内存损坏，若发生损坏，系统需采取适当措施（至少需将错误码记录至NVM）。
·
编程地址范围外的未使用ROM必须填充预设值以检测非预期写入。允许值为微控制器专用SWI指令、0x55或0xAA。若需偏离此规则，明确禁止使用"擦除"或"未编程"状态值，因其通常代表上电默认状态，无法表明有意编程写入。（*参见"未使用ROM定义"注释。）
设计规则说明
若程序访问未使用内存，则表明程序存在缺陷。程序应监控未使用内存区域以检测非预期访问，并在必要时记录故障以便后续调查。若此缺陷未被检测到，可能导致程序流程和/或I/O损坏。

未使用RAM定义：满足以下任一或全部条件的RAM：
. 预留未来使用
. 当前项目或电源周期中未激活
. 堆（heap）、局部临时或"暂存"缓冲区/区域已不再使用或超出作用域

未使用NVM定义：满足以下任一或全部条件的NVM：
. 可通过Method 3编程的校准段（calibration segment）
注： 此类用途的NVM豁免内存填充要求。
. 预留未来使用
. 当前项目或电源周期中未激活
. 未受保护用于其他运行模式（如诊断）

未使用ROM定义：满足以下任一或全部条件的ROM：
. 超出ECU供应商编程地址范围
. 不适用于OTA编程
. 当前项目或电源周期中未激活
注： 此类用途的ROM豁免内存填充要求（因多应用策略如VIN选择可降低制造复杂度），但仍需校验其完整性。
分析/讨论
本设计规则支持RQT-003701-705381“ 未使用可执行存储器的监督 ”，适用于所有带软件的电子模块，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审查（TDR）的完成，并通过“ SWQA通用TDR检查表 ”问题来解决：
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 15:33 - 稚媛 黄**

*- 主题 从 DR-003701-707986未使用内存监视器 变更为 TDR_RQT_003701_705381 001未使用内存监视器*

*- 描述 已更新。*

*- 指派给 被设置为 力常 张*

**#2 - 2025-03-24 16:02 - 稚媛 黄**

*- 主题 从 TDR_RQT_003701_705381 001未使用内存监视器 变更为 TDR_RQT_003701_705381 002未使用内存监视器*

**#3 - 2025-03-25 15:46 - 稚媛 黄**

*- 主题 从 TDR_RQT_003701_705381 002未使用内存监视器 变更为 TDR_RQT_003701_705381 002 Unused Memory Monitor*