

FORD LDM Localization - 功能 #3418

Task # 3240 (进行中): FORD文档输出

功能 # 3349 (进行中): SWQA文档

功能 # 3366 (新建): TDR_RQT_003701_705923 Software Support of ELCOMP NVM Requirements

TDR_RQT_003701_705923 008 Avoid NVM Wear-out

2025-03-24 16:39 - 稚媛 黄

状态:	进行中	开始日期:	2025-03-24
优先级:	普通	计划完成日期:	
指派给:	希星 柯	% 完成:	50%
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-003701-708289 Avoid NVM Wear-out 1. NVM存储单元寿命限制 禁止在车辆使用寿命内耗尽任何单个NVM存储单元的使用寿命。具体耐久性定义参见设计规则说明部分的“耐久性定义（Durability Definition）”。 2. 复位后的NVM缓冲区管理 微控制器在复位后，必须能够仅基于NVM中存储的信息确定哪个NVM缓冲区最旧。 3. 多缓冲区数据一致性设计 NVM管理器设计必须包含处理多缓冲区数据一致性问题的机制（例如：不完整的多缓冲区更新），同时避免存储单元过早损耗（尤其是在微控制器频繁复位的情况下）。 4. 序列号（Sequence Number）管理 若采用递增或递减序列号，必须确保序列号在超过两倍车辆使用寿命前不会发生翻转（上溢或下溢）。 设计规范 5. 频繁修改数据的特殊豁免 对于频繁修改的数据项（由功能规范定义或经福特批准），可豁免“50ms内启动NVM更新”的要求。 关于“50ms内启动NVM更新”的详细要求，请参考设计规则 DR-003701-708350《管理NVM更新》。 设计规范 福特对NVM磨损的定义是：在车辆使用寿命期间，任一NVM存储单元的使用寿命被耗尽。NVM存储单元指单次擦除操作中可清除的最小字节单位。该定义简化了系统测试，因其未规定超出使用寿命后的处理方式（而是通过识别NVM故障并制定纠错方法来应对）。 注：耐久性/车辆使用寿命数据详见RQT-030000-010326文件。 为避免磨损，需明确车辆生命周期内每个NVM数据项的修改次数。供应商应与福特软件工程师共同评审各NVM数据项支持的修改次数上限。需特别注意，数据项的多次修改极易被忽视，且每个数据项的变更可能源自多个触发源。 避免磨损的技术方案：每个NVM存储单元的可修改次数存在上限。若需求要求频繁修改某一数据项，则需分配更多NVM存储单元以分散写入压力，但由此将引发新问题：复位后如何识别哪个存储单元包含最新数据。以下列出潜在解决方案（供应商可不限于这些实施方案，但必须在设计评审时提交设计方案）。 该技术方案要求开发者为每个NVM数据分配特定地址范围，因此调整数据位置或应对高频使用时需重新映射多个NVM数据项（或将非连续数据项拼接处理）。 序列号是每次修改NVM存储单元时更新的数据值，有时可直接利用现有数据作为序列号（例如里程表读数）。 一种序列号采用单向递增（或递减）且永不溢出（或下溢）的数值，另一种则允许溢出/下溢（循环编码）。 以下为复位后确定下次写入位置的简易方法：本例使用允许循环递增的8位无符号序列号（seqA、seqB和seqC），其核心逻辑是找出数值最小的序列号（同时兼容循环溢出处理）。常量THRESHOLD定义了参与循环计算的数值上限临近范围，该阈值越大，对多次复位的容错性越强。 关键序列号使用规则包括：优先使用已擦除缓冲区；必须按固定顺序循环使用缓冲区；若采用单向递增/递减序列号，其溢出/下溢临界值必须超过2倍车辆使用寿命（此方案以增加NVM开销为代价降低算法复杂度）；若采用循环序列号（允许溢出/下溢），软件在确定覆写单元时必须考虑循环特性（此方案减少NVM占用但增加软件复杂度及代码空间）；对于多单元缓冲区，设计需检测部分使用状态并制定应对策略，特别要快速响应连续复位情况。 多缓冲区与空缓冲区管理需遵循：			

clipboard-202503312002-l5dg0.png

该技术方案同样要求开发人员为每个NVM数据分配特定的地址范围，因此调整数据位置或应对高频使用时需要重新映射多个NVM数据项（或将非连续数据项进行拼接处理）。

该方案采用多缓冲区机制，通过已擦除缓冲区标识下一次更新的写入位置，此时唯一需要确保的是始终存在可用擦除缓冲区。例如，若策略规定在擦除下一缓冲区（如图中的缓冲区3）之前先向空缓冲区写入数据，则遭遇突发复位时可能导致所有缓冲区均被占用。因此必须在执行写入前确保至少保留两个已擦除缓冲区（注：采用五个及以上缓冲区可确保冗余性）。

当使用多存储单元结构时，处理数据一致性（部分更新或未完成更新）会显著增加系统复杂度：对于部分更新的数据结构，若选择擦除会加速单元老化，若不擦除则可能因多次微复位耗尽所有缓冲区并损毁有效数据副本。该问题没有简单解决方案，可能的应对措施包括延迟数秒执行NVM写入，但这可能导致重要故障诊断码（DTC）丢失，再次强调该问题具有固有复杂性。

空缓冲区管理核心规则包括：

优先使用已擦除缓冲区；写入前必须确保存在2个已擦除缓冲区；最少配置5个缓冲区（2个擦除态+3个使用态）；必须按固定顺序循环使用缓冲区；对于多单元缓冲区，策略需检测部分使用状态并制定应对方案（需注意重复擦除会加速单元老化），特别要解决快速重

复复位问题。

其他应用场景：

还存在类似内存管理器的NVM管理技术——允许数据任意写入存储位置且支持多次写入，但仅使用堆栈中最新信息。该技术要求更多前期工作及更强数据处理能力，但消除了地址依赖性并便于扩展NVM数据项，仍需建立数据最后写入位置的追踪机制及数据一致性保障方法，且会大幅增加验证设计是否符合车辆使用寿命要求的复杂度。

当需要掉电后快速写入NVM数据时，必须配置预擦除内存专用区域以确保即时可用，同时更难保证在保持电力耗尽前完成擦写周期。

高频修改NVM数据的例外处理规定：

频繁修改的数据可能快速耗尽NVM寿命。此类数据项可在规范中特别标注，允许供应商针对这些特定数据项豁免"50毫秒内启动NVM更新"的要求（详见设计规则《NVM更新管理》中关于50毫秒更新启动要求的具体说明）。

供应商也可主动向福特申报其他应纳入例外清单的数据项，所有例外申请将按照分析/讨论章节规定的流程进行评审。建议供应商积极提报所有符合例外条件的数据项以供评估。

历史记录

- #1 - 2025-03-31 20:01 - 力常 张
- 描述 已更新。
 - 状态 从 新建 变更为 进行中
- #2 - 2025-03-31 20:02 - 力常 张
- 文件 clipboard-202503312002-l5dg0.png 已添加
 - 描述 已更新。
- #3 - 2025-03-31 20:08 - 力常 张
- 描述 已更新。
- #4 - 2025-04-08 10:36 - 涛 陆
- 指派给 从 力常 张 变更为 希星 柯
 - % 完成 从 0 变更为 50
- 评估是否满足主机需求

文件

clipboard-202503312002-l5dg0.png	35 KB	2025-03-31	力常 张
----------------------------------	-------	------------	------