FORD LDM Localization - 功能 #3353

Task # 3240 (进行中): FORD文档输出

功能 # 3349 (进行中): SWQA文档

TDR_RQT_003701_705377 Software Design Best Practices

2025-03-04 09:49 - 力常 张

状态:	已解决	**开始日期:**	2025-03-17
优先级:	普通	**计划完成日期:**	2025-03-27
指派给:	力常 张	**% 完成:**	66%
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

Software Design Best Practices
软件技术设计评审的完成和/或以下设计规则的符合性应符合本RQT：
.DR-003701-707963 全局变量（Global Variables）
.DR-003701-707965 运行时边界检查（Run Time Boundary Checking）
.DR-003701-707966 软件循环（Software Loops）
.DR-003701-707964 动态内存分配（Dynamic Memory Allocation）
.DR-003701-707967 低层接口软件实现（Software Implementing a Low-Level Interface）
.DR-003701-708184 软件配置（Software Configuration）

需求分析
福特要求软件设计团队实施稳健的软件设计以确保软件/系统行为的可靠性，这包含旨在应对非预期交互与环境条件的防御性技术（defensive techniques）。福特定义了以下设计规则作为软件设计最佳实践的最低要求。

在全局作用域（global scope）声明变量会增加风险，因其允许整个程序对其进行修改。**DR-003701-707963 全局变量（Global Variables）**限制了福特车辆软件中全局变量的使用。

实施运行时边界检查（run-time boundary checking）可提升健壮性。DR-003701-707965 运行时边界检查（Run Time Boundary Checking）明确了判定关键数据的方法，并强制要求纳入运行时边界检查机制。

陷入软件循环（software loop）可能导致程序呈现甚至实际停止运行的异常状态。**DR-003701-707966 软件循环（Software Loops）规范了福特车辆软件中循环结构的使用准则。

动态内存分配（dynamic memory allocation）可能导致软件非确定性（non-deterministic）风险。DR-003701-707964 动态内存分配（Dynamic Memory Allocation）列出了福特车辆软件中允许与禁止使用动态内存分配的条件。

当所需接口的硬件不可用时，可通过通用输入/输出引脚（general-purpose input/output pins）实现功能。DR-003701-707967 低层接口软件实现（Software Implementing a Low-Level Interface）定义了在专用外设I/O硬件不可用时实现接口的约束条件。

风险声明：
未能实施这些设计规则将导致模块不可恢复性无响应。

子任务:

功能 # 3380: TDR_RQT_003701_705377 001 Global Variables	**进行中**
功能 # 3381: TDR_RQT_003701_705377 002 运行时边界检查（Run Time Boundar...	**进行中**
功能 # 3382: TDR_RQT_003701_705377 003 软件循环（Software Loops）	**进行中**
功能 # 3383: TDR_RQT_003701_705377 004 动态内存分配（Dynamic Memory All...	**已关闭**
功能 # 3384: TDR_RQT_003701_705377 005 低层接口软件实现（Software Impleme...	**已关闭**
功能 # 3385: TDR_RQT_003701_705377 006 软件配置（Software Configuration）	**进行中**

历史记录

#1 - 2025-03-04 09:50 - 力常 张

Software Design Best Practices

#2 - 2025-03-04 09:50 - 力常 张

- 主题 从 RQT_003701_705377 变更为 RQT_003701_705377 Software Design Best Practices

#3 - 2025-03-04 09:58 - 力常 张

- 主题 从 RQT_003701_705377 Software Design Best Practices 变更为 TDR_RQT_003701_705377 Software Design Best Practices

Software Design Best Practices

#4 - 2025-03-04 10:14 - 力常 张

- 计划完成日期 从 2025-03-05 变更为 2025-03-31

#5 - 2025-03-11 09:47 - 力常 张

需求正文
任何包含以下类型软件的电子控制模块均需满足指定设计规则：
非AUTOSAR操作系统（Non-AUTOSAR OS）
AUTOSAR Classic平台
AUTOSAR Adaptive平台
第三方软件

需符合的设计规则
.DR-003701-707963 全局变量（Global Variables）
.DR-003701-707965 运行时边界检查（Run Time Boundary Checking）
.DR-003701-707966 软件循环（Software Loops）
.DR-003701-707964 动态内存分配（Dynamic Memory Allocation）
.DR-003701-707967 低层接口软件实现（Software Implementing a Low-Level Interface）
.DR-003701-708184 软件配置（Software Configuration）

DV/证据：软件技术设计评审
软件技术设计评审的完成和/或以下设计规则的符合性应符合本RQT：
.DR-003701-707963 全局变量（Global Variables）
.DR-003701-707965 运行时边界检查（Run Time Boundary Checking）
.DR-003701-707966 软件循环（Software Loops）
.DR-003701-707964 动态内存分配（Dynamic Memory Allocation）
.DR-003701-707967 低层接口软件实现（Software Implementing a Low-Level Interface）
.DR-003701-708184 软件配置（Software Configuration）

需求分析
福特要求软件设计团队实施稳健的软件设计以确保软件/系统行为的可靠性，这包含旨在应对非预期交互与环境条件的防御性技术（defensive techniques）。福特定义了以下设计规则作为软件设计最佳实践的最低要求。

在全局作用域（global scope）声明变量会增加风险，因其允许整个程序对其进行修改。**DR-003701-707963 全局变量（Global Variables）**限制了福特车辆软件中全局变量的使用。

实施运行时边界检查（run-time boundary checking）可提升健壮性。DR-003701-707965 运行时边界检查（Run Time Boundary Checking）明确了判定关键数据的方法，并强制要求纳入运行时边界检查机制。

陷入软件循环（software loop）可能导致程序呈现甚至实际停止运行的异常状态。**DR-003701-707966 软件循环（Software Loops）规范了福特车辆软件中循环结构的使用准则。

动态内存分配（dynamic memory allocation）可能导致软件非确定性（non-deterministic）风险。DR-003701-707964 动态内存分配（Dynamic Memory Allocation）列出了福特车辆软件中允许与禁止使用动态内存分配的条件。

当所需接口的硬件不可用时，可通过通用输入/输出引脚（general-purpose input/output pins）实现功能。DR-003701-707967 低层接口软件实现（Software Implementing a Low-Level Interface）定义了在专用外设I/O硬件不可用时实现接口的约束条件。

风险声明：
未能实施这些设计规则将导致模块不可恢复性无响应。

#6 - 2025-03-14 17:18 - 力常 张

- 描述 已更新。

#7 - 2025-03-17 11:20 - 力常 张

- 状态 从 新建 变更为 已解决