

FORD LDM Localization - 功能 #3381

Task # 3240 (进行中): FORD文档输出

功能 # 3349 (进行中): SWQA文档

功能 # 3353 (已解决): TDR_RQT_003701_705377 Software Design Best Practices

TDR_RQT_003701_705377 002 运行时边界检查 (Run Time Boundary Checking)

2025-03-17 08:59 - 力常 张

状态:	进行中	开始日期:	2025-03-17
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-003701-707965 Run Time Boundary Checking ” 本设计规则支持 RQT-003701-705377 《软件设计最佳实践》，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， 第三方软件 并作为该RQT的合规性实施方法。 必须对输入参数及关键数据实施有效性校验，其边界值应严格遵循设计阶段定义值。 ——功能安全相关数据会进行数据传递的校验 设计规则说明 关键数据 - 通过FMEA（失效模式分析）、FTA（故障树分析）、HARA（危害分析与风险评估）等方法识别的数值，用于确保ECU的安全用例(safety case)及核心任务实现。 实施运行时边界检查可增强系统健壮性。鉴于程序中任何位置访问无效符号或数据均可能引发功能异常，要求每次使用前均进行有效性校验并不现实。本规范将有效性校验和/或合理性检查限定于输入参数与关键数据。通过在数据输入阶段确保数值处于定义区间，并对超限值实施处置，可消除重大错误面（error surface），否则极可能导致系统故障。对于被标识为任务关键和/或安全关键（safety-critical）的符号，应实施同等验证。 分析/讨论 本设计规则支持 RQT-003701-705377 《软件设计最佳实践》，适用于所有含软件实现的电子控制模块，并作为该RQT的合规性实施方法。 技术规范：设计规则的闭环以完成软件技术设计评审（Technical Design Review, TDR）为标志，具体通过 “ SWQA通用TDR检查单 ” 中的下列问题项落实： IIP15008 A) 除EEPROM/数据闪存(Data Flash)数据外，列出所有需实施边界检查的关键数据变量。 B) 对于被标识为"关键数据"的每个数据结构，需通过硬件-软件接口规范（HW <-> SW Interface Specification）或等效文件说明： i) 该数据结构被识别为关键数据的依据 ii) 其数值、索引或地址的上下限值是否已文档化 iii) 当检测到关键数据无效时采取的措施（示例：忽略、进入跛行回家策略、使用默认值 INV09005 A) 列出所有法规要求及关键软件配置标志 B) 哪些数据项采用冗余存储？ C) 是否存在因数据损坏导致系统停用的项目？ D) 哪些项目属于安全关键项（如：电动车窗、安全气囊）？——近光 i) 针对所有安全关键项，描述其故障对系统的影响 E) 哪些项目设有默认值？ i) 使用默认项时的功能限制（如：功能降级） ii) 是否支持通过自学习算法等方式实现默认值恢复？ IIP15017 针对每个输入源（GPIO、网络、外设等）的说明要求需阐述以下内容：输入数据合理性校验方法，对非合理数据的处置机制，接收超范围数据时系统采用的数据交付策略			

历史记录

#1 - 2025-03-17 09:16 - 力常 张
- 状态 从 新建 变更为 已解决

#2 - 2025-03-17 09:17 - 力常 张
- 目标版本 从 H005_SW0007169.A003.2 变更为 FORD_TDR_Documents

#3 - 2025-03-17 09:18 - 力常 张
- % 完成 从 0 变更为 100

#4 - 2025-03-24 15:08 - 稚媛 黄
- 主题 从 DR-003701-707965 运行时边界检查 (Run Time Boundary Checking) 变更为 TDR_RQT_003701_705377 002 运行时边界检查 (Run Time Boundary Checking)

#5 - 2025-03-24 15:21 - 稚媛 黄
- 描述 已更新。

#6 - 2025-03-25 10:44 - 涛 陆
- 描述 已更新。
- 状态 从 已解决 变更为 进行中
- 指派给 从 力常 张 变更为 希星 柯
- % 完成 从 100 变更为 50

列出功能安全相关的数据结构

#7 - 2025-06-03 12:56 - 希星 柯

```
tLbPara Lb : Lb灯信息
typedef struct LbPara {
uint8 lbSig;
uint8 lbHwSig;
uint8 lbHwPsnSig;
uint16 lbHwFailCnt;
uint8 lbHwFailFlag;
uint8 lbNtcFlt;
uint8 lbRbinFlt;
uint8 lbChnFlt;
uint8 lbChnFltReport;
uint8 lbOFAF;
uint8 lbFanOff;
} tLbPara

tLbSig LbSigInfo:Lb点灯信息
typedef struct tLbSig {
uint8 LbSig;
uint8 CheckVal;
}tLbSig

tAdc adcInfo:adc信息
typedef struct tAdc {
uint16 AdcVal;
uint16 CheckVal;
}tAdc

tNtc ntc_ad_val : Ntc信息
typedef struct tNtc {
uint16 NtcVal;
uint16 CheckVal;
}tNtc

tBat BatVoltInfo
typedef struct tBat {
uint16 BatVol;
uint16 CheckVal;
}tBat

tTempInfo tempInfo : buck温度信息
typedef struct{
uint8 tempVal;
uint8 checkVal;
}tTempInfo;
```

```
tboostInfo boostInfo : boost电压信息
typedef struct{
uint8 boostVal;
uint8 deltVal;
}tboostInfo;
```