ICS 43.040.10
T 36

中华人民共和国国家标准化指导性技术文件

GB/Z 33013—2016

道路车辆　车用嵌入式软件开发指南

Road vehicles—Development guidelines for motor vehicle embedded software

(ISO/TR 15497:2000, Road vehicles—
Development guidelines for vehicle based software, NEQ)

2016-10-13 发布　　2017-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

本指导性技术文件使用重新起草法参考 ISO/TR 15497:2000《道路车辆　车用嵌入式软件开发指南》编制，与 ISO/TR 15497:2000 的一致性程度为非等效。

本指导性技术文件与 ISO/TR 15497:2000 的主要差别如下：

——将完整性等级由 ISO/TR 15497:2000MISRA 的概念“安全完整性等级”代替为 ISO 26262 的相关概念及其分级表格；

——参考 ISO 26262 增加严重性参数概念及其表格；

——参考 ISO 26262 增加暴露率参数概念及其表格；

——删除了不适用的国外法律条款及相关事宜；

——删除了部分缩略语。

本指导性技术文件由国家发展和改革委员会提出。

本指导性技术文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本指导性技术文件起草单位：中国电子技术标准化研究院、上海计算机软件技术开发中心、中国汽车技术研究中心。

本指导性技术文件主要起草人：张展新、丁志刚、许秀香。

道路车辆　车用嵌入式软件开发指南

1　范围

本指导性技术文件规定了道路车辆软件开发过程及相关要求。

本指导性技术文件适用于道路车辆软件的开发、验证和管理。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 19001—2008　质量管理体系　要求(ISO 9001:2008,IDT)

GB/T 19003—2008　软件工程　GB/T 19001—2000 应用于计算机软件的指南(ISO/IEC 90003:2004,IDT)

ISO 26262-3:2004　道路车辆　功能安全　第 3 部分:方案阶段定义(Road vehicles—Functional safety—Part 3:Concept phase)

3　软件生存周期

3.1　汽车软件设计准则

汽车软件安全性方面的设计准则考虑如下：

a)　安全性必须是明确可以看到的。

b)　风险越大需要提供的信息就越多。

c)　软件的健壮性、可靠性和安全性，如同质量一样，应是内建的而不是附加的。

d)　当人身安全和财产安全要求发生冲突时，人身安全必须优先。

e)　系统设计应同时考虑随机性的和系统性的故障。

f)　无论是否存在失效，应能证明其健壮性。

g)　安全性的考虑应适用于贯穿于整个产品设计、制造、运行、服务和报废弃的每个阶段。

3.2　项目计划

3.2.1　项目定义

3.2.1.1　使用软件会在成本、灵活性和功能性方面具有很多益处。然而，由于软件复杂度会引发很多问题，只有确实需要这些益处时，才将软件包含到系统中。

3.2.1.2　本章规定的方法可以同时应用于整车系统层和软件系统层。

3.2.1.3　项目启动前，宜制定清晰的项目目标。

示例：批量生产系统与研究和开发原型产品的项目目标是不同的。

3.2.1.4　项目定义宜包含要实现的特性和功能的列表。汽车制造商相关部门应达成一致并制定文件，使得在具体工作开始前设计和开发团队可使用该定义。

3.2.1.5　项目定义宜包括任何现有的法规要求、项目设想和非功能性需求。