ICS 43.060.50
CCS R 16

团 体 标 准

T/CEATEC XXX—2026

车用发动机电子控制单元(ECU)功能安全与故障诊断规范

Vehicle engine electronic control unit (ecu) functional safety and fault diagnosis specification

2026-X-XX 发布 2026-X-XX 实施

中国欧洲经济技术合作协会 发布

目　　次

前言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件主要起草单位：。

本文件主要起草人：。

本文件为首次编制。

车用发动机电子控制单元(ECU)功能安全与故障诊断规范

1 范围

本文件规定了车用发动机电子控制单元(ECU)的功能安全要求、故障诊断要求以及验证与确认要求。

本文件适用于装配于道路车辆、以汽油机、柴油机或混合动力发动机为控制对象的车用发动机电子控制单元，包括发动机管理系统（EMS）或动力控制模块（PCM）中承担发动机控制功能的ECU。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 34590.1 道路车辆 功能安全 第1部分：术语

GB/T 34590.5 道路车辆 功能安全 第5部分：产品开发：硬件层面

GB/T 34590.6 道路车辆 功能安全 第6部分：产品开发：软件层面

GB/T 34590.9 道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析

ISO 11452-2 道路车辆——窄带辐射电磁能引起的电气干扰部件试验方法——第2部分：吸波内衬屏蔽室（ALSE）（Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy — Part 2: Absorber-lined shielded enclosure）

3 术语和定义

GB/T 34590.1界定的以及下列术语和定义适用于本文件。

3.1

发动机电子控制单元 engine electronic control unit

用于实现发动机控制功能的车载电子控制单元，包括硬件、软件、诊断与通信接口。

3.2

功能安全 functional safety

系统在规定条件下避免危险反应的能力。

3.3

故障诊断 diagnostics

识别、定位和记录故障的过程，包括故障检测、故障判定、故障定位、故障记录与故障上报。

4 功能安全要求

4.1 安全完整性等级划分

ECU应根据其功能对车辆安全的影响程度，按照GB/T 34590.9的方法进行风险评估，确定对应的ASIL等级，具体划分要求见表1。

表1 ECU控制功能与ASIL等级对应关系

ECU 控制功能类别	汽车安全完整性等级（ASIL）	ASIL 等级判定依据	核心安全目标与要求
燃油喷射控制、点火控制	ASIL C	故障可能导致发动机熄火、非预期加速，严重度 S3，暴露概率 E3，可控性 C2	避免发动机失控运行，确保故障时平稳停机或降功率运行
可变气门正时（VVT）控制、怠速控制	ASIL B	故障可能导致动力下降、排放超标，严重度 S2，暴露概率 E3，可控性 C2	维持发动机基本运行能力，控制排放在限值内
排气再循环（EGR）控制、燃油蒸发控制	ASIL A	故障主要影响排放性能，严重度 S1，暴露概率 E3，可控性 C1	提示故障状态，不影响发动机核心运行安全

注：严重度（S）、暴露概率（E）、可控性（C）的分级按照GB/T 34590.9的规定执行，S3为可能导致重伤或死亡，S2为可能导致轻微伤害，S1为无人员伤害；E3为高暴露概率（正常使用中频繁出现）；C2为驾驶员难以控制，C1为驾驶员可有效控制。

4.2 硬件安全要求

4.2.1 电源电路安全

ECU电源电路应满足GB/T 34590.5的要求，具备过压、欠压、反接保护功能，具体参数如下：

a）工作电压范围：9V～16V（正常工况），支持11V～32V瞬态电压耐受（持续时间≤10s）；

b）过压保护阈值：18V±0.5V，保护响应时间≤100μs，故障排除后自动恢复；

c）欠压保护阈值：6.5V±0.3V，当电压低于该值时，ECU应保存关键数据并进入休眠模式；

d）反接保护：当电源正负极反接时，应通过保险丝或TVS管切断电路，无永久性损坏，保护电流≤5A。

4.2.2 输入/输出接口安全

模拟量输入/输出接口应具备防短路、防干扰能力，具体要求如下：

a）短路保护：输入引脚对地/对电源短路时，接口电路应限流≤10mA，短路解除后功能恢复正常；

b）抗干扰能力：应满足ISO 11452-2的要求；

c）数字量输出接口应具备过载保护功能，过载电流阈值为额定电流的1.5倍，保护响应时间≤200μs。

4.2.3 冗余设计要求

ASIL C等级功能对应的ECU硬件应采用冗余设计，具体要求如下：

a）核心处理器（MCU）：应采用双核心锁步架构，两个核心同步执行指令，指令执行结果偏差≤1个时钟周期时触发故障报警；

b）关键传感器：对曲轴、凸轮轴传感器应采用双路信号输入，两路信号偏差≤5°曲轴转角时判定为正常，偏差＞11°曲轴转角时触发故障码；

c）电源冗余：主电源与备用电源切换时间应≤5ms，备用电源容量应满足ECU完成安全响应所需电能，持续供电时间≥200ms。

4.3 软件安全要求

4.3.1 软件开发流程

ECU软件开发应符合GB/T 34590.6规定的V模型开发流程，涵盖需求定义、架构设计、代码实现、单元测试、集成测试、系统测试等阶段，各阶段应形成完整的测试报告与追溯文档。

4.3.2 软件安全机制

软件安全机制要求如下：

a）代码安全：采用静态代码分析工具进行分析，代码覆盖率应≥95%（ASIL C等级），无未定义行为、数组越界等高危漏洞；

b）数据安全：关键控制参数应进行CRC校验，校验码长度≥16位，数据传输错误率≤1×10^{-9}；

c）任务调度安全：核心控制任务周期抖动应≤5%，任务最坏情况下完成时间≤10ms；

d）故障自恢复：软件发生非致命故障时，应在100ms内完成复位恢复，恢复后关键参数初始化正确，无安全风险。

5 故障诊断要求

5.1 诊断系统架构

ECU故障诊断系统应采用分层架构设计，分为信号采集层、故障判断层、安全响应层、诊断服务层，各层功能如下：

a）信号采集层：应实时采集传感器、执行器及总线信号，采集周期≤10ms，信号滤波时间常数为0.1s～1s；

b）故障判断层：基于阈值判断、逻辑验证、冗余对比等算法识别故障，故障判断准确率应≥99.5%，误报率≤0.1%；

c）安全响应层：应根据故障等级执行对应的安全策略，响应时间≤150ms（ASIL C等级）；

d）诊断服务层：应支持OBD-II诊断协议，提供故障码读取、冻结帧数据、数据流监控等服务，通信波特率≥500kbps（CAN总线）。

5.2 故障类型及诊断方法

5.2.1 传感器故障

常见传感器故障类型及诊断方法应符合表2的规定，诊断阈值应基于传感器技术参数及发动机运行特性确定。

表2 常见传感器故障类型及诊断方法

传感器类型	故障类型	诊断方法	诊断阈值	故障码（DTC）	安全响应
冷却液温度（ECT）传感器	开路故障	电压检测法，监测传感器输出电压	电压＞4.8V 或＜0.2V，持续 200ms	P0117（低电压）/P0118（高电压）	采用默认温度值（80℃），限制发动机转速≤4000rpm
	短路故障	电压检测法，结合电路阻抗分析	电压＜0.2V（对地短路）或＞4.8V（对电源短路），持续 100ms	P0117/P0118	同开路故障响应
	漂移故障	趋势分析法，对比进气温度与冷却液温度变化	冷启动时，ECT 与 IAT 偏差＞15℃，持续 30s	P0119（不稳定）	点亮故障指示灯（MIL），正常运行
曲轴位置（CKP）传感器	信号丢失	脉冲计数法，监测信号脉冲频率	发动机转速＞400rpm 时，连续 5 个发动机循环无脉冲信号	P0335（信号故障）	切断喷油、点火，发动机停机，点亮 MIL
	信号异常	冗余对比法，与凸轮轴位置信号比对	CKP 与 CMP 信号偏差＞11° 曲轴转角，持续 2 个循环	P0016（相关性故障）	降功率运行，转速≤3000rpm，点亮 MIL

节气门位置（TPS）传感器	开路/短路	双路信号比对法，监测两路信号电压	单路电压＞4.8V 或＜0.2V，持续 100ms	P0122（低电压）/P0123（高电压）	采用默认节气门开度（15%），限制加速性能
	信号偏差	双路信号比值验证，正常比值为 2:1	两路信号比值偏差＞±10%，持续 500ms	P0121（性能故障）	点亮 MIL，维持基本运行

5.2.2 执行器故障

执行器故障主要包括驱动电路故障、机械卡滞故障，诊断方法以反馈信号检测和电流监测为主，具体要求如下：

a）喷油器故障：监测喷油器驱动电流，电流＜2A（开路）或＞15A（短路）时触发故障码P0201～P0204，安全响应为切断对应气缸喷油，降功率运行；

b）点火线圈故障：通过次级电压反馈或初级电流监测诊断，初级电流无变化（开路）或电流异常增大（短路）时触发故障码P0351～P0354，安全响应为切断对应气缸点火；

c）VVT电磁阀故障：监测电磁阀驱动电路电压及凸轮轴位置变化，驱动电压异常或凸轮轴位置误差＞7.5°时触发故障码P0010～P0011，安全响应为将VVT锁止在默认位置。

5.2.3 通信故障

ECU与其他控制器的通信故障诊断应符合以下要求：

a）CAN总线故障：总线电平低于1.5V或高于3.5V、错误帧数量＞5帧/秒时触发故障码U0100（通信故障）；

b）通信超时：接收其他控制器信号超时＞100ms时，判定为通信故障，采用默认替代值维持基本功能；

c）安全响应：通信故障发生后，若影响核心安全功能，则降功率运行，否则维持正常运行，点亮MIL。

5.3 故障码管理

5.3.1 故障码存储与清除

故障码应存储在ECU非易失性存储器中，存储容量≥10个故障码，存储时间≥40个驾驶循环，具体要求如下：

a）当前故障码：故障存在时持续存储，故障排除后，经3个连续驾驶循环无复发则自动清除；

b）历史故障码：故障排除后转为历史故障码，可通过诊断仪手动清除或经40个驾驶循环自动清除；

c）冻结帧数据：故障发生时记录关键运行参数，每个故障码对应1组冻结帧数据，数据存储精度≤±5%。

5.3.2 故障指示灯（MIL）控制

MIL控制应符合OBD-II规范，不同故障等级对应的点亮策略如下：

a）A级故障（致命故障，如CKP信号丢失）：故障发生后立即点亮MIL，且持续点亮，直至故障排除；

b）B级故障（严重故障，如喷油器故障）：故障发生后，经2个驾驶循环确认后点亮MIL，故障排除后经3个驾驶循环熄灭；

c）C级故障（轻微故障，如EGR控制故障）：仅存储故障码，不点亮MIL，故障累积超过10个驾驶循环后点亮MIL。

6 验证与确认要求

6.1 功能安全验证

6.1.1 硬件验证

硬件验证应按照GB/T 34590.5的规定执行，验证项目及方法应符合表3的规定。

表3 硬件验证项目及方法

验证项目	验证方法	验收指标	适用 ASIL 等级
硬件故障注入测试	向 MCU、电源电路、I/O 接口注入开路、短路、接地故障	故障检测率≥99%，安全响应时间≤150ms	B/C
电磁兼容性（EMC）测试	按照 ISO 11452 系列标准进行辐射发射、传导抗扰度测试	辐射发射≤40dBμV/m，传导抗扰度耐受电压±200V	A/B/C
温度耐久性测试	在-40℃～125℃环境下持续运行 1000h	无硬件损坏，功能衰减≤5%	A/B/C
冗余功能验证	切断主电源/主传感器，验证备用系统切换功能	切换时间≤5ms，切换后功能正常	C

6.1.2 软件验证

软件验证方法及要求如下：

a）单元测试：对软件模块进行独立测试，采用静态代码分析、控制流分析等方法，语句覆盖率应≥95%（ASIL C），判定条件覆盖率≥90%；

b）集成测试：验证模块间接口兼容性，接口数据传输错误率应≤1×10^{-9}，无死锁、数据竞争问题；

c）系统测试：在HIL（硬件在环）测试台架上模拟各种故障场景，测试软件对故障的诊断与响应能力，测试通过率应≥99.8%。

6.2 故障诊断有效性确认

故障诊断有效性通过实车测试和台架测试确认，测试项目及要求如下：

a）台架测试：在发动机台架上模拟各类故障（传感器开路/短路、执行器卡滞等），每种故障重复测试50次，诊断准确率应≥99.5%，误报率≤0.1%；

b）实车测试：在不同路况（城市道路、高速公路）、不同环境温度（-30℃～40℃）下进行实车测试，累计测试里程≥10000km，故障诊断系统应工作稳定，无漏诊、误诊现象；

c）数据记录：测试过程中记录故障码、冻结帧数据、数据流等信息，数据记录完整性应≥99%，可通过诊断仪正常读取。