

# 团 体 标 准

T/CSICE 033.3-2025

## 柴油发动机电控单元 第 3 部分：基础软件开发

Diesel engine electronic control unit—Part 3: Basic software development

2025-12-26 发布

2025-12-26 实施

中国内燃机学会 发布



目 次

前言 ..... II

引言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 符号和缩略语 ..... 1

5 技术指标 ..... 2

    5.1 一般要求 ..... 2

    5.2 操作系统健康度 ..... 2

    5.3 系统安全 ..... 2

6 开发过程 ..... 2

    6.1 基础软件需求分析 ..... 2

        6.1.1 系统需求 ..... 2

        6.1.2 技术要求 ..... 2

        6.1.3 实施步骤 ..... 2

    6.2 基础软件架构设计 ..... 3

        6.2.1 技术要求 ..... 3

        6.2.2 实施步骤 ..... 3

    6.3 基础软件单元设计与实现 ..... 3

        6.3.1 技术要求 ..... 3

        6.3.2 实施步骤 ..... 4

    6.4 基础软件单元测试 ..... 4

        6.4.1 技术要求 ..... 4

        6.4.2 实施步骤 ..... 4

附录 A（资料性） 基础软件需求规格书..... 5

附录 B（资料性） 基础软件架构设计说明书..... 6

附录 C（资料性） 基础软件单元详细设计说明书..... 7

附录 D（资料性） 基础软件单元测试总结报告..... 8

## 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。

T/CSICE 033-2025《柴油发动机电控单元开发》已经或计划发布7个部分。

- 第1部分：需求开发。
- 第2部分：应用软件开发。
- 第3部分：基础软件开发。
- 第4部分：硬件设计。
- 第5部分：软件集成。
- 第6部分：软件测试。
- 第7部分：硬件验证。

本文件为T/CSICE 033-2025第3部分。

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。

本文件由中国内燃机学会标准管理部提出。

本文件由中国内燃机学会归口。

本文件起草单位：潍柴动力股份有限公司、潍柴新能源商用车有限公司、山东大学、潍柴雷沃(潍坊)农业装备有限公司、中国重型汽车集团有限公司、济南汽车检测中心有限公司、南岳电控(衡阳)工业技术股份有限公司。

本文件主要起草人：史家涛、陈娜娜、于惠、余浪、孙柯、代萍、季宇杰、刘晓波、王华杰、王飞、王健、王志新、李园、王梦、丁才云。

本文件于2025年首次发布。

## 引 言

T/CSICE 033-2025《柴油发动机电控单元》是指导柴油发动机电控单元如何自上而下进行正向开发。它涉及柴油发动机电控单元开发的原则、流程、设计、集成和验证的行业标准，由7个部分组成。

- 第1部分：需求开发。
- 第2部分：应用软件开发。
- 第3部分：基础软件开发。
- 第4部分：硬件设计。
- 第5部分：软件集成。
- 第6部分：软件测试。
- 第7部分：硬件验证。

T/CSICE 033-2025的第1部分规定了柴油发动机电控单元需求开发的术语和定义、一般要求和需求开发过程要求。第2部分规定了柴油发动机电控系统中基于模型的应用软件开发流程的要求。第3部分规定了柴油发动机电控单元中基础软件的技术指标及开发过程。第4部分规定了柴油发动机电控单元中硬件需求说明、架构设计、元器件及芯片选型、电路原理图设计和印刷电路板（PCB）设计需要遵循的基本指导方法和规则。第5部分规定了柴油发动机电控单元中软件集成的技术要求及实施步骤。第6部分规定了柴油发动机电控单元系统测试过程的要求。第7部分规定了柴油发动机电控单元硬件验证过程中试验条件、试验工况、试验方法及判定依据的要求。

## 柴油发动机电控单元 第3部分：基础软件开发

### 1 范围

本文件规定了柴油发动机电控单元中基础软件的技术指标及开发过程。  
本文件适用于柴油发动机电控单元，其他电控单元可参照本文件执行。

### 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 11457 信息技术 软件工程术语

GB/T 32421 软件工程 软件评审与审核

T/CSICE 033.1-2025 柴油发动机电控单元 第1部分：需求开发

### 3 术语和定义

GB/T 11457和GB/T 32421界定的以及下列术语和定义适用于本文件。

#### 3.1

##### **基础软件 basic software**

电控系统的基础软件包括操作系统、微控制器驱动、板载芯片驱动、输入输出接口、内存服务、通讯协议栈、系统服务、复杂驱动、功能安全、信息安全、引导程序等。

#### 3.2

##### **应用软件 application software**

实现电控系统控制策略的软件集合。

#### 3.3

##### **软件模块 software module**

具备独立功能的最小软件单元。

#### 3.4

##### **引导程序 boot loader**

电控系统上电后执行的第一段程序，用于跳转到应用程序或更新应用程序。

### 4 符号和缩略语

下列缩略语适用于本文件。

EEPROM：电可擦除可编程只读存储器（erasable programmable read-only memory）

Flash：闪存（flash memory）

RAM：随机存取存储器（random access memory）

## 5 技术指标

### 5.1 一般要求

基础软件开发的一般要求如下：

- a) C 代码应符合 MISRA-C:2012，汇编代码遵循各企业的汇编语言编程规范；
- b) 通过软件分层、模块化、标准接口等方式实现基础软件的可移植性；
- c) 代码具备可读性，每行不超过 81 个字符，每个函数不超过 200 行；
- d) 能够对代码注释率、资源使用情况进行统计。

### 5.2 操作系统健康度

操作系统健康度是衡量软件运行状态的重要指标，基础软件应提供操作系统健康度检查功能，对整个电控系统软件的具体要求如下：

- a) 单个任务最大执行时间不超过 300  $\mu$ s，保证高优先级任务的实时响应性；
- b) 能够监控周期任务的执行间隔，任务未按预期执行时触发错误处理机制；
- c) 为处理极限情况下的并发任务，CPU 最高负荷不超过 85%；
- d) 堆栈使用率不超过 80%，防止堆栈溢出引起程序崩溃；
- e) 电控单元从上电至应用软件开始运行的时间不超过 300 ms，以满足整车通讯首帧报文的发出时间需求；
- f) 单片机定时器偏差不得超过 0.1%，以满足操作系统心跳时钟偏差不得超过 0.1%的要求；
- g) CAN 总线负荷率建议低于 40%，最大不应超过 60%，避免因过载导致数据冲突或丢失。

### 5.3 系统安全

系统安全是软件正常运行的重要保障，具体要求如下：

- a) 看门狗超时时间不超过关键任务运行周期的三倍；
- b) 能够记录复位原因及复位时上下文信息；
- c) 能够对程序与数据的一致性进行检查；
- d) 电控系统刷写失败时，重新上电应停止在 BootLoader 再次刷写；
- e) 采用 E2E、SecOC 等技术，确保通讯的安全性；
- f) 刷写过程采用数字签名、安全启动、密钥安全存储等技术保证安全刷写；
- g) 软件复位后，应停留在引导程序中执行复位保护机制；
- h) 应用程序与引导程序相互跳转前，应先将芯片的各模块恢复到默认状态。

## 6 开发过程

### 6.1 基础软件需求分析

#### 6.1.1 系统需求

系统需求应满足 T/CSICE 033.1-2025。

#### 6.1.2 技术要求

基础软件需求应实现条目化，每条需求应包含需求编号、需求名称、需求描述、需求优先级及验证方式。需求描述应具备完整性、正确性、可行性、必要性及可验证性，具体内容如下。

- a) 功能定义。明确该需求实现的具体功能。
- b) 约束。根据需求的具体内容，确认实现该需求要遵循的约束条件。
- c) 外部接口。软件模块与其他软件模块之前的接口，包括接口的用途、格式等。
- d) 异常处理要求。故障或异常情况下的软件处理策略。
- e) 性能要求。如控制精度、动态响应性等。

#### 6.1.3 实施步骤

基础软件需求分析按照以下步骤进行：

- a) 根据系统需求分析基础软件层面的需求，完成基础软件需求规格书，规格书格式可参考附录 A；
- b) 从需求的完备性、准确性、可行性、必要性及可验证性等方面对基础软件需求规格书进行评审并出具评审报告。

6.2 基础软件架构设计

6.2.1 技术要求

基础软件架构应满足基础软件需求、具备可扩展性、可维护性及可重用性。  
基础软件架构设计需确定基础软件模块之间的结构关系和数据流程，分为静态架构设计和动态架构设计。

静态架构见图1，具体技术要求如下：

- a) 分级层次的软件结构；
- b) 多核的电控系统，应描述各个核负责的功能；
- c) 多单片机的电控系统，应描述各个单片机负责的功能；
- d) Flash、RAM、EEPROM 等各种资源的分配情况；
- e) 数据类型及其特征参数；
- f) 软件模块的外部接口；
- g) 软件的安全机制。

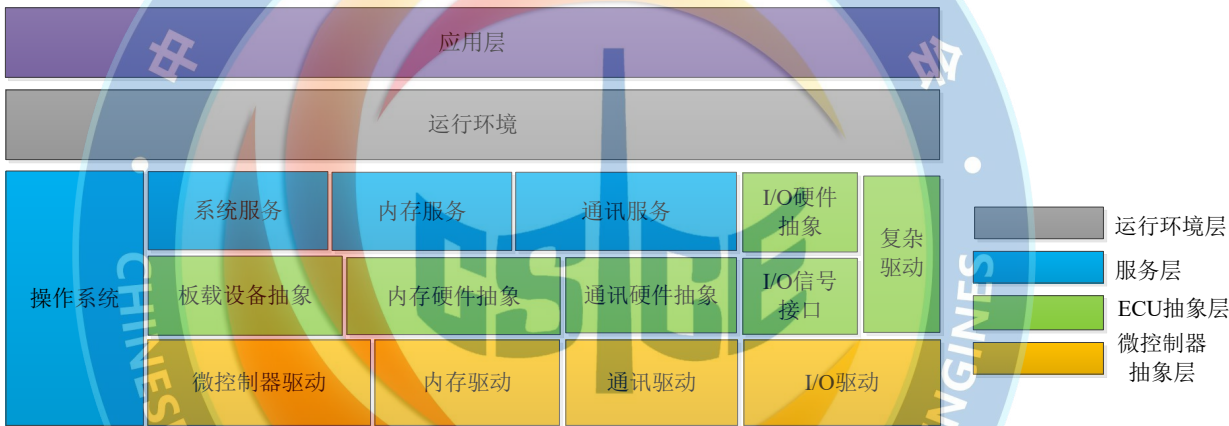


图 1 基础软件静态架构框图

动态架构设计技术要求如下：

- a) 周期任务和中断任务的优先级、触发方式等；
- b) 单片机的上电、下电、休眠、唤醒的时序图；
- c) 软件运行的状态机流程图；
- d) 软件模块间的数据流；
- e) 对外接口的数据流。

6.2.2 实施步骤

基础软件架构设计应按照以下步骤进行：

- a) 根据基础软件需求规格书，遵照 6.2.1 中的技术要求进行基础软件架构设计，完成基础软件架构设计说明书，设计说明书格式可参照附录 B；
- b) 对基础软件架构设计说明书进行评审并出具评审报告。

6.3 基础软件单元设计与实现

6.3.1 技术要求

基础软件单元设计与实现需以软件模块为对象，包括以下内容。

- a) 需求追踪。明确基础软件模块的软件设计与软件需求之间的追踪关系，确保实现该软件模块的所有需求。

- b) 软件模块框图。描述本模块的组成以及与其他模块之间的接口交互情况。
- c) 功能概述。描述基础软件模块所实现的整体功能，必要时应当包含原理性的介绍。
- d) 函数原型及功能、逻辑说明。函数原型应该包含函数名称、输入参数的定义及范围、输出参数的定义及类型、返回值的定义及类型，函数功能描述应以条目化的形式进行，函数实现逻辑可以流程图的形式进行。
- e) 时序关系。描述基础软件模块函数的调用关系。
- f) 静态、动态配置参数说明。描述参数名称、含义及数据类型等。

### 6.3.2 实施步骤

基础软件单元设计与实现应按照以下步骤进行：

- a) 根据基础软件架构设计说明书，遵照 6.3.1 中的要求和建议进行基础软件单元设计，完成基础软件单元设计说明书，设计说明书格式可参考附录 C；
- b) 对基础软件单元设计说明书进行评审并出具评审报告；
- c) 根据基础软件单元设计说明书、编程语言编码规范以及编程语言标识符命名规范进行基础软件源代码层面的实现；
- d) 对基础软件源代码进行代码审查。

## 6.4 基础软件单元测试

### 6.4.1 技术要求

基础软件单元测试应当包含以下内容。

- a) 静态单元测试。检查软件模块对编码规范的符合性。
- b) 动态单元测试。对软件模块功能、性能、接口及代码覆盖度的测试。

### 6.4.2 实施步骤

基础软件单元测试应按照以下步骤进行：

- a) 根据编程语言编码规范进行基础软件静态代码检查；
- b) 根据基础软件需求规格书和单元设计说明书进行动态单元测试；
- c) 对上述检查和测试结果进行总结并完成基础软件单元测试总结报告，总结报告可参考附录D；
- d) 对基础软件单元测试总结报告进行评审并出具评审报告。

附录 A  
(资料性)  
基础软件需求规格书

A.1 基础软件需求规格书

基础软件需求规格书格式见表 A.1，且宜包含以下内容。

- a) 需求编号。需求编号 SRS\_DIO\_001 中，SRS 表示基础软件需求，DIO 为模块名称，001 为编号。
- b) 需求描述。每个功能的需求描述要求可参考 6.1.2 的技术要求。
- c) 运行模式。运行模式包括下电、休眠、初始化、正常运行、降级、测试或刷写。
- d) 安全等级。安全等级分为 QM、A、B、C、D。
- e) 优先级。优先级分为高、中、低。
- f) 验证标准。详细描述需求验证通过的标准。
- g) 验证方法。详细描述该需求的测试方法。
- h) 需求状态。需求状态分为新建、已取消、已评审、已发布、已实现、已验证。
- i) 系统需求编号。与系统需求的追溯关系。
- j) 系统架构编号。与系统架构的追溯关系。

表 A.1 基础软件需求格式

| 需求编号 | 需求描述 | 运行模式 | 安全等级 | 优先级 | 验证标准 | 验证方法 | 需求状态 | 系统需求编号 | 系统架构编号 |
|------|------|------|------|-----|------|------|------|--------|--------|
|      |      |      |      |     |      |      |      |        |        |

## 附录 B

(资料性)

### 基础软件架构设计说明书

#### B.1 基础软件架构设计说明书

基础软件架构设计说明书宜包含以下内容。

- a) 范围。
- b) 术语及缩略语。
- c) 相关文档。
- d) 限制与假设。
  - 1) 硬件约束。
  - 2) 软件约束。
  - 3) 其他限制。
- e) 软件架构设计方案。
  - 1) 软件实现方法。
  - 2) 软件架构设计原则。
- f) 基础软件静态架构设计。
  - 1) 软件静态架构。
  - 2) 多核软件架构。
  - 3) 资源分配。
  - 4) 需求分配。
  - 5) 软件组件描述。
  - 6) 软件接口描述。
- g) 基础软件动态架构设计。
  - 1) 任务调度设计。
  - 2) 中断设计。
  - 3) 总时序图。
- h) 安全设计和错误处理。
- i) 软件组件设计。
- j) 非功能性设计。

## 附录 C

(资料性)

### 基础软件单元详细设计说明书

#### C.1 基础软件单元详细设计说明书

基础软件单元详细设计说明书宜包含以下内容。

- a) 范围。
- b) 术语及缩略语。
- c) 相关文档。
- d) 软件需求追踪。
- e) 模块静态设计。
  - 1) 功能概述。
  - 2) 模块框图。
  - 3) 函数接口列表。
  - 4) 变量接口列表。
  - 5) 资源消耗目标。
- f) 模块动态设计。
- g) 函数单元设计。
  - 1) 函数单元1。
  - 2) 函数单元2。
- h) 错误处理。
- i) 变量描述。

附 录 D

(资料性)

基础软件单元测试总结报告

D.1 基础软件单元测试总结报告

基础软件单元测试总结报告格式见表 D.1。

表 D.1 基础软件单元测试总结

| 模块名 | 测试用例总数 | 已执行测试用例数 | 通过的测试用例数 | 测试用例执行率 | 测试用例通过率 | 测试结果 | Fail项原因说明 |
|-----|--------|----------|----------|---------|---------|------|-----------|
|     |        |          |          |         |         |      |           |

