同济大学
TONGJI UNIVERSITY

硕士学位论文

(专业学位)

车用机电复合传动控制系统功能安全分析与验证

姓　　名：严洪江

学　　号：1231640

所在院系：汽车学院

职业类型：工程硕士

专业领域：车辆工程

指导教师：钟再敏　博导

副指导教师：张剑锋　高工

二〇一六年一月

同濟大學
TONGJI UNIVERSITY

A dissertation submitted to

Tongji University in conformity with the requirements for

the degree of Master of Engineering

Functional Safety Analysis and Validation of Electromechanical Complex Transmission Control System Used by Vehicle

Candidate: Yan HongJiang

Student Number: 1231640

School/Department:School of Automotive Studies

Discipline: Engineering Master

Major: Automotive Engineering

Supervisor: Zhong Zaiming

Jan, 2016

车用机电复合传动控制系统功能安全分析与验证

严洪江

同济大学

学位论文版权使用授权书

本人完全了解同济大学关于收集、保存、使用学位论文的规定，同意如下各项内容：按照学校要求提交学位论文的印刷本和电子版本；学校有权保存学位论文的印刷本和电子版，并采用影印、缩印、扫描、数字化或其它手段保存论文；学校有权提供目录检索以及提供本学位论文全文或者部分的阅览服务；学校有权按有关规定向国家有关部门或者机构送交论文的复印件和电子版；在不以赢利为目的的前提下，学校可以适当复制论文的部分或全部内容用于学术活动。

学位论文作者签名：

年　　月　　日

同济大学学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，进行研究工作所取得的成果。除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人创作的、已公开发表或者没有公开发表的作品的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。本学位论文原创性声明的法律责任由本人承担。

学位论文作者签名：

年　　月　　日

摘要

混合动力汽车是应对能源短缺、环境污染并推动汽车工业可持续发展的重要技术发展方向。国内外已经实现量产的车型有：大众 Jetta 的 HEV、现代 Sonata 的 HEV、上汽的 E550、比亚迪的秦等。

将混合动力汽车新增的动力源电机与原有传动系统的集成是其关键技术之一，当前已从初期的变速器与电机离散结构向变速器和电机一体化结构发展，本文将至少集成一个电机的变速器装置定义为机电复合传动机构。其控制系统定义为机电复合传动控制系统。它承担了扭矩解析、扭矩分配、传动系统控制、模式切换等多项复杂功能。控制单元的些微设计缺陷或失效可能会导致重大的安全事故，使用户的生命受到威胁。如何确保控制系统的电控单元的安全性成为混合动力汽车开发的另一项关键技术。传统的方法已经难以满足电控单元设计开发的需要，引入专门的功能安全研究方法成为必然。

本论文对电控单元硬件开发需要遵循的功能安全方法进行了深入的研究，包括技术安全需求分析、系统设计、硬件安全需求分析、硬件架构度量评估、随机失效违反安全目标评估、硬件集成测试等。在此基础上，以某混合动力汽车（PHEV）的机电复合传动控制系统为例，对其控制系统进行功能安全分析并将功能安全需求逐步分解到技术安全概念。结合电控单元硬件设计方案评估其硬件架构度量和随机硬件失效的概率度量，验证了硬件设计和满足一定功能安全目标之间的关系。

本论文设计了机电复合传动控制系统及其控制单元，并用功能安全的方法进行了评估，例如系统架构、微处理器电路、供电电路、传感器信号采集电路、电磁阀驱动电路、总线通讯电路。设计搭建了硬件在环测试环境，创建了测试用例。给出了电控单元硬件设计满足功能安全目标的验证结果。

最后本文得出了所有和扭矩相关的功能均为安全相关的、技术安全需求规范起到上承功能安全需求下启技术安全概念的重要作用、每一个实施安全相关功能的部件都存在违反安全目标的硬件失效模式的结论。

关键词：机电复合传动，功能安全，硬件失效，硬件在环

ABSTRACT

Hybrid vehicle is one of solution to resolve energy and climate issues and promote the sustainable development of automobile industry. There are some mass products in the automobile market, such as Jetta HEV of VW, Sonata HEV of Hyundai, E550 PHEV of SAIC, Qin PHEV of BYD.

The key point of hybrid vehicle is to integrate transmission and E-motor. This is called "Electromechanical Complex Transmission". Its electrical control system is called "Electromechanical Complex Transmission Control System". It will execute the functions of torque resolution, torque distribution, transmission control and mode shift. The failure of the system will direct lead to accident and threaten the life of user. How to guarantee the safety of the system became another key technique of hybrid vehicle. It has been difficult to fulfil the development of its complex electrical and electronic system, using of functional safety became necessary.

This study focus on the key phase of ISO26262, e.g. technical safety requirement analysis, system design, hardware safety requirement analysis, evaluation of hardware architectural metrics, evaluation of violation of the safety goal due to random hardware failures, hardware integration test. Base on one type of electromechanical complex transmission control system of PHEV. An effectively evaluation method of functioanl safety is derived and the way from functional safety requirements to the hardware technical safety concept is dedicated. Base on the hardware design the hardware architectural metrics and the random hardware failures metrics are evaluated, and the relationship between hardware design and functional safety goal is analysed.

An electromechanical complex transmission control system and its control unit had been designed and evaluated by functional safety, such as system architectural, microprocessor, power supply, sensor signal process, valve drive, bus communication. This study use HIL testing to validate the target of functional safety.

The conclusions of this study are "all torque related functions are safety related", "the technical safety requirement specification is derived from functional safety requirement and can educe the technical safety concept".

Key Words: Electromechanical complex transmission, Functional safety, Hardware failures, Hardware in loop

目录

第 1 章 引言

1.1 概述

随着能源短缺、环境污染问题的日益严峻，新能源汽车已经成为国家战略。目前国内已经实现批量化生产的新能源汽车主要有：纯电动汽车（PEV）[1]、混合动力汽车（HEV）[2,3]和插电式混合动力汽车（PHEV）[4]。其中插电式混合动力汽车的动力系统结构最为复杂。为了适应插电式混合动力汽车的动力系统特点，传统的传动系统已经无法满足新的需求，集成电机、离合器和减速机构的车用机电复合传动系统成为国内外汽车厂商及零部件供应商研究开发的重点。该系统可匹配插电和非插电的混合动力汽车，如果移除离合器则适用于纯电动汽车[5,6]。

当前汽车工程师面临两大挑战：1、汽车的功能变的越来越复杂，特别是新能源汽车。以插电式混合动力汽车动力系统的扭矩控制为例，传统汽车一般只需要 EMS 和 TCU 两大控制单元互相配合，而插电式混合动力汽车则增加了整车控制单元 VCU、电机控制单元 MCU、电池管理系统 BMS。插电式混合动力汽车动力系统的控制单元越来越多，相应的其失效的概率相比传统汽车也大大增加。2、人的安全成为汽车设计开发中首先需要考虑的问题，且被放到了最重要的位置。传统的被动安全和主动安全显然已经无法应对这两大挑战[7,8]，为此国际标准化组织提出了功能安全的概念。

功能安全涵盖了如辅助驾驶、发动机控制、自适应巡航和变速箱控制等功能。功能安全关注系统故障后的行为，而不是系统的原有功能或性能。以机电复合传动控制系统为例，离合器位置信号是动力系统输出扭矩主要决定因素，若该信号发生故障使其指示位置偏离实际位置，则可能导致动力系统输出扭矩过大或偏小，造成车辆发生非驾驶员期望的加减速，这是一个功能安全风险。从设计上采取措施，使该位置信号发生故障时动力系统扭矩仍然可控，则提高了动力系统的安全性。由此可见功能安全对于汽车产品设计的指导意义。

本论文通过对功能安全标准的研究学习，特别是对系统和硬件设计阶段的深入探讨，对一种机电复合传动控制系统的功能安全进行分析，希望进行一些有益的探索，为公司在该领域的开发工作提供一定的帮助，也为国内汽车工程设计人员提供一些功能安全理论结合实际的有益探索。

通过研究功能安全的开发流程和分析方法，包括系统功能、外部接口、相关项定义、安全目标、功能安全需求并识别技术安全需求、系统环境，确认和认可措施的要求等，对机电复合传动控制系统进行功能安全分析，基于分析结果设计

并优化功能安全相关的安全措施，以期将系统的风险降到可接受的范围内，从而提高系统的安全性。结合实际的硬件设计评估其硬件架构度量和随机硬件失效的概率度量，研究硬件设计和满足一定功能安全目标的关系。最后使用硬件在环测试设备来验证功能安全的目标。

本论文工作被限制在 ISO26262 系统和硬件设计阶段的主要环节，主要原因为：ISO26262 完整实施是非常大的任务，这需要大量人员的参与，如功能安全管理、系统风险、实现、验证及售后等多个开发环节；本论文工作只持续 20 周时间，ISO26262 完全实施需要远大于 20 周的时间，所以完整实施功能安全从时间上来说也是不可能的； ISO26262 提供了一种名为脱离环境的安全原件开发（SEooC）的方法，这种方法可以假设系统的使用范围、功能和接口，如：该系统适用于整备质量小于 1800kg 的前轮驱动车辆、该系统可以满足最大道路坡度为 35%；当驾驶员在一定车速下请求时激活功能、当驾驶员请求时关闭功能。该方法还可以假设相关项定义、安全目标、功能安全需求，如：当车速大于一定值时系统不会激活功能（ASIL X）；为探测到驾驶员请求时系统不会关闭功能（ASIL Y）。对系统使用环境的假设如：一个外部资源将按照要求的 ASIL 等级提供驾驶员请求信息或其他车辆状态信息（ASIL Z）。这一方法在实际的汽车产品开发中被广泛的应用，很多零部件厂商在开发产品时并不明确最终的车辆使用环境，当假设的条件与最终用户环境不一致时，变化的部分如果涉及功能安全将被重新分析讨论。这一方法的好处是可以节约大量的开发时间和资源[15, 16]。

1.2 机电复合传动系统技术现状

机电复合传动系统作为混合动力汽车的关键技术，国内外各大汽车企业都投入大量人力物力进行技术研发，目前已经推出了一批量产的产品。

1、大众 Jetta 混合动力系统

2012 年德国大众发布了基于 P2 模块和 7 速双离合变速器的混合动力产品 Jetta HEV。P2 是指将电机置于离合器和变速箱之间的方案。P2 系统最重要的要求之一就是减小整个系统的空间尺寸。原则上，可以将减震系统或离合器集成到电机转子内。通过评估各种需求和尺寸大小，更进一步的方案是将离合器集成到转子内。离合器及转子的轴承以及离合器的操纵都布置在变速箱侧。混合动力模块预先安装在变速箱壳体之内。P2 系统最大的优点是只需要对变速箱的壳体和连接处做局部修改，不涉及齿轴的变更，可以最大限度的保留双离合器原有的部件和产线。同时继承了双离合变速器良好的换挡品质。但是由于无法将电机和变速器高度集成，P2 系统布置在 A 级及以下的车型比较困难。

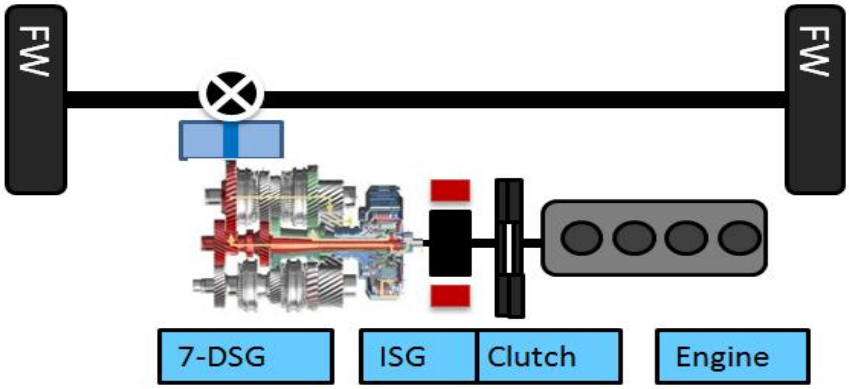

图 1.1 大众 Jetta HEV 传动系统结构图

表 1.1 大众 Jetta HEV 关键参数

基本参数	数值
整备质量	1505kg
变速箱类型	7 速 DSG
发动机类型	L4 1.4L TSI
发动机最大扭矩	250Nm
发动机最大功率	110kW
电机类型	PM
电机峰值功率	20kW
电机峰值扭矩	150Nm
电池容量	5Ah
电池能量	1.1kWh
电池额定电压	220V
电池类型	锂离子电池

2、现代 Sonata 混合动力系统

2012 年韩国现代发布了基于 BSG/ISG 和自动变速器的混合动力产品 Sonata HEV。该方案修改了前端轮系用于集成 BSG 电机，取消液滤变矩器，将 ISG 电机置于离合器和 AT 之间。该系统最大的优点是只需要对变速箱的连接处做局部修改，不涉及齿轴的变更，可以最大限度的保留 AT 原有的部件和产线。同时继承了 AT 优良的换挡品质。但是由于无法将电机和变速器高度集成，系统布置在 A 级及以下的车型比较困难，同时还要涉及发动机前端轮系的更改。

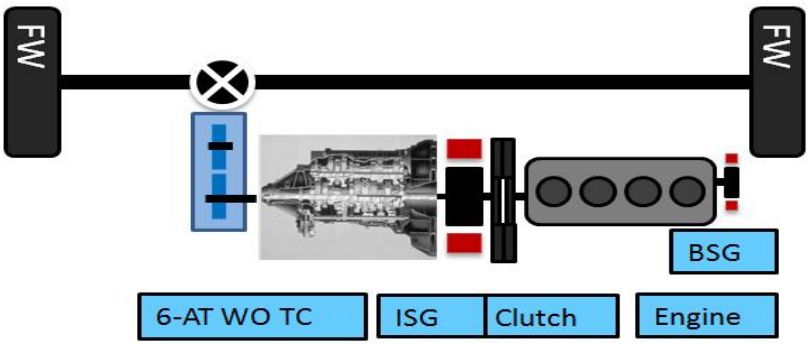

图 1.2 现代 Sonata HEV 传动系统结构图

表 1.2 现代 Sonata HEV 关键参数

基本参数	数值
整备质量	1591kg
变速箱类型	6AT
发动机类型	L4 Atkinson cycle engine
发动机最大扭矩	210 Nm
发动机最大功率	119 kW
电机类型	PM
电机峰值功率	35kW
电机峰值扭矩	205Nm
电池容量	5.3Ah
电池能量	1.4kWh
电池额定电压	270V
电池类型	锂离子电池

3、荣威 E550 插电混合动力系统

2013 年上汽荣威发布了基于 TM/ISG 和两档变速结构的插电混合动力产品荣威 E550 PHEV。该系统将 TM/ISG 电机和一个专门开发的 2 挡变速箱高度集成。该系统最大的优点是结构紧凑，效率高，可以最大限度的利用手动变速器的部件和产线。同时具有良好的换挡品质。

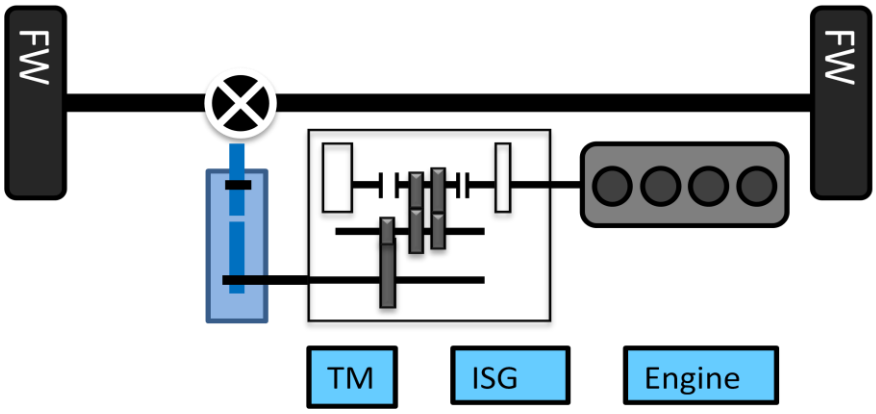

图 1.3 荣威 E550 PHEV 传动系统结构图

表 1.3 荣威 E550 PHEV 关键参数

基本参数	数值
整备质量	1699kg
变速箱类型	2 速 AMT
发动机类型	L4 1.5L VCT
发动机最大扭矩	136Nm
发动机最大功率	80kW
电机类型	PM
电机峰值功率（TM、ISG）	44kW、24kW
电机峰值扭矩（TM、ISG）	317Nm、150Nm
电池容量	40Ah
电池能量	11.8kWh
电池额定电压	294V
电池类型	磷酸铁锂电池

1.3 功能安全技术现状

为了适应道路车辆的电子电器系统的特殊应用领域，国际标准化组织在IEC61508 标准的基础上修编，于 2011 年发布了 ISO26262 标准[9-16]，这是专为汽车工业制定的新标准，它定义了汽车电气系统功能安全问题。而 IEC61508 起源于工业自动化，并不是专为汽车工业制定的[17,18]。这一修编适用于由电子、电器和软件组成的安全相关的系统在安全生命周期内的所有活动。

ISO26262 标准定义一个工作，以及该工作过程应该如何被做，如硬件设计架构、软硬件接口、单元测试、集成测试等每一个环节都必须关注功能安全的目标是否满足并得到验证。

ISO26262 不对任何用户实际使用的功能提出规定，如换档 map 该如何设置，TCU 和 EMS 之间的扭矩干预机制该如何定义，混动模式该如何切换等。相反，ISO26262 规定了应该如何开发安全的电子电气控制系统。如为了避免扭矩传递失效的发生，它规定了应该如何开发扭矩监控系统。除了安全相关的功能开发，开发这些功能所需要的流程和满足安全目标的证据也将得到强化。ISO26262 通过适当的需求和流程提供指导以避免系统失效和随机硬件失效带来的风险。

越来越严峻的功能安全问题促使国际标准化组织制定属于汽车工业自己的功能安全标准（ISO26262）。ISO26262 专注于电子电器系统的功能安全，但是基于其他技术手段的安全相关的系统也可以借鉴其架构。其他技术手段如机械、液压、气动等。ISO26262 提供汽车安全生命周期并支持生命周期内活动可按需裁减；提供汽车专用的基于风险的方法以确定汽车安全完整性等级（ASIL）；使用 ASIL 来规范 ISO26262 的应用需求以避免不合理的残余风险；提供验证和确认方法的需求以确保可以达到可接受的安全等级；功能安全受到开发流程、产品、服务和管理流程的影响。

ISO26262 专著应用于安装在最大整备质量不超过 3500kg 的量产乘用车上的由电子电器系统组成的安全相关的系统。在 ISO26262 正式发布前开发的系统和产品不受标准地约束，但是如果有功能更改，则更改部分需要遵循 ISO26262。遵循 ISO26262 的目的就是车辆制造商，甚至最终客户，可以知道车辆是在一种特定方式下开发车辆或零部件，该方式聚焦在功能安全，如遵从规则、开发的方法以及交付物等。

ISO26262 应对由安全相关的电子电器系统的错误行为导致的危害，但是不包含应对诸如：电击、火灾、烟雾、热辐射、有毒物、可燃物、化学反应、腐蚀物、能量释放等危害。ISO26262 不包含应对电子电器系统名义上的性能，如：主动或被动安全系统、制动系统、自适应巡航。

1、 国外功能安全标准的实施状态

在国外由于其汽车工业的基础较好，功能安全的理念在很多零部件及整车企业得到

很好的贯彻执行[19,20]。在标准的制定、安全认证、流程培训、产品研发等方面，汽车工业最发达的德国均走在了前列。如 TUV 南德公司作为标准的制定者之一，在功能安全培训 、产品认证方面已经成为业内标杆。以整车制造商为例，梅赛德斯-奔驰公司 2000 年之前就成立了专门的功能安全机构，负责研究汽车安全并将 ISO26262 标准转化为公司的企业标准-方法手册，经过对方法手册的裁剪进一步细化到项目手册。梅赛德斯-奔驰公司反馈的意见经过标准组织的确认可以进入 ISO26262 的后续版本。其他的如大众、宝马也都相应的成立机构以应对 ISO26262 标准的实施。在零部件企业中 Bosch 作为标准的制定者之一，标准的很多内容均来自 Bosch 的开发流程和技术规范。Bosch 的专利产品，电子车身稳定系统（ESP）就是典型的需要符合功能安全标准的产品，其批量生产的时间早于 ISO26262 标准的发布时间本身就说明了 Bosch 在功能安全领域的地位。另一家零部件巨头 Schaeffler 从 2012 年起就成立了功能安全技术中心，负责开发和执行 Schaeffler 规范，来诠释功能安全相关的标准、流程、方法、工具、指南并提供项目开发中工程和管理上安全相关的支持。在日本，以 Honda 和 Denso 为例，两家企业均成立了功能安全机构以应对 ISO26262 标准的实施。

2、国内功能安全标准的实施现状

在国内，功能安全方面的分析研究工作局限在少数大型整车企业、高等院校和科研机构内[21,22]，国内完全遵循 ISO26262 要求设计流程并满足该标准的产品目前还很少。值得注意的是，随着中国汽车工业的快速发展，国内的汽车保有量大幅度增加，促使各大汽车厂商不得不关注功能安全，对功能安全的研发投入大幅增加，同时大量的研发人员投入到对汽车功能安全的研究中。ISO26262 功能安全标准提出的功能安全分析方法，在理论上为国内厂商提供了目标和方法，但是如何将理论和实际的工程开发相结合还是国内汽车工程设计人员的短板。由中国汽车技术研究中心牵头组织的道路车辆功能安全标准研究制定工作组目前承担了中国功能安全标准的编制工作。上汽、一汽、东风、比亚迪、奇瑞、吉利、泛亚等整车企业参与了编制小组，东软、科世达、舍夫勒（中国）等零部件企业参与了编制小组。小组的主要工作包括功能安全国家标准的撰写、召开功能安全国际研讨会、收集国内企业的意见和建议、跟踪欧美日标准化组织的最新动态。编制小组的整体工作思路和目标分为以下 5 个阶段。

第一阶段，2013 年至 2016 年，基于 ISO26262，充分理解其内涵，在政府管理部门的指导下，根据我国汽车行业的特点和实际情况，加入特定要求，制定出符合我国汽车电子产业发展需求的标准，即修改采用该标准，形成符合我国国情的基础通用标准 GB/T《道路车辆 功能安全》。

第二阶段，2015 年至 2020 年，开展 GB/T《道路车辆 功能安全》具体操作研究，为满足行业的实际需要，加强标准的可操作性，对标准的各部分进行细化完善，形成操作规范/指南/指导性文件/标准。

第三阶段，2016 年至 2020 年，形成基于整车层面的功能安全相关的关键电控系统的汽车安全完整性等级（ASIL）划分和安全目标定义的规范/指南/指导性文件/标准。

第四阶段，2016 年至 2020 年，形成行业通用的电控系统功能安全流程开发体系和评估准则，形成整车和关键电控系统功能安全技术评估测试评价体系。

第五阶段，2016 年至 2020 年，形成相对完善的道路车辆功能安全标准体系，将前几个阶段的工作成果拓展到道路车辆电子电气系统和产品，完善已有标准中与功能安全相关的内容。

2014 年上汽乘用车有限公司成立了功能安全和 FMEA 小组，专门负责制定动力系统的安全需求规范、流程、工具、指南等工作。公司新开发的动力系统均遵循 ISO26262 标准，目前正在进行部分产品的安全认证工作。以混合动力系统的关键零部件为例，如发动机控制单元、变速箱控制单元、电机控制单元，联合电子开发的新一代产品均承诺遵循 ISO26262 标准，并获得 TUV 南德公司的认证。公司可以根据客户的系统需求提供相应 ASIL 等级的产品。

1.4 汽车电子硬件功能安全分析和应用

汽车电子的硬件功能安全分析的核心是电控单元。在国际上，各大电控单元的生产商如德国 Bosch 和大陆、美国 Delphi 和 TRW、日本电装等控制了电控单元的核心技术，特别是底盘控制、动力系统控制等技术复杂，可靠性要求高的电控单元，已经被上述汽车零部件巨头垄断。为了满足电控单元的功能安全设计，需要相应的微处理器芯片、电源芯片、驱动芯片等核心器件，目前汽车电子器件的核心技术均掌握在英飞凌、恩智浦、意法半导体、瑞萨、德州仪器等国际半导体公司。

英飞凌公司推出的32位多核架构，可以有效地满足ISO26262标准。其设计、应用和技术资料都符合最高的汽车安全完整性等级（ASIL D）。这种全新架构是英飞凌满足未来汽车动力总成和安全应用需求的基础，其包含三个处理器内核（TriCore）通过交叉开关进行互连，以 CPU 全速运行，避免硬件竞争，并引入锁步核和增强型硬件安全机制。三个核中的两个具备可独立配置的额外锁步核。其他安全技术包括：安全内部通信总线、总线监控单元和位于所有内存中的误码检测码/纠正码。分布式内存保护系统可在内核、总线和外设层级运行。具备独立读取接口的多个程序闪存模块。

恩智浦和意法半导体针对汽车电子的各种安全应用，联合推出 32 位双核处理器 MPC564xL 系列，符合 ISO26262 标准。该系列支持电动转向控制、主动式悬架控制、主动巡航雷达控制等各种安全应用。其采用 32 位 Power Architecture

技术，可选择锁步或解耦并行处理模式等安全架构。

瑞萨电子开发的面向汽车应用的 V850 系列处理器中的面向底盘和安全应用的 P 系列，符合 ISO26262 标准，并达到 ASIL D 水平。P 系列具有高效片上诊断功能，包括带有对比单元的冗余 CPU 子系统、逻辑和存储器的内置式自测试以及所有片上存储器的误差检验与校正码保护。主要应用于电动转向控制、电机控制、电池管理等安全系统。

德州仪器的 TMS570 是一款基于两个相同的 Cortex-R4 内核的对称型双核处理器，每个处理器内核的性能均可以达到 300MIPS。用运行于锁步模式的双核处理器架构来比较处理结果。主存储器和本地存储器以及总线流量上实施错误校正代码和奇偶校验码保护机制。CPU 具有逻辑内置自检，存储器内置自检，循环冗余校验器模块。

在国内，符合 ISO26262 标准的电控单元的开发还处在起步阶段，除联合电子、大陆（中国）、Delphi（中国）外，恒润、联创等本土企业正尝试开发符合安全标准的电控单元。汽车电子器件的核心技术则完全受制于国际半导体公司。

1.5 论文主要内容

论文的主要内容如下：

第 1 章“引言”，主要阐述了研究本论文的背景、国际国内对于机电复合传动系统及功能安全的研究现状。

第 2 章“硬件开发功能安全标准实施”，主要介绍了功能安全标准的架构及内容，重点阐述产品开发阶段的系统层和硬件层如何实施功能安全。

第 3 章“机电复合传动控制系统需求设计”，首先阐述了本论文的研究对象，车用机电复合传动控制系统，定义了相关项，提出了系统设计的功能安全需求和非功能安全需求。

第 4 章“机电复合传动控制系统功能安全设计”，首先基于功能安全需求进行技术安全需求分析，得出技术安全需求规范，进行技术安全概念分析得到技术安全概念。完成控制单元的硬件设计。

第 5 章“控制单元硬件功能安全分析”，首先基于技术安全概念进行硬件功能安全需求分析，得到硬件技术的安全机制和诊断覆盖率。基于硬件设计的实际案例进行硬件架构度量计算和随机硬件失效概率度量计算。最后通过硬件在环测试对实际的机电复合传动控制系统进行测试验证。

第 6 章“结论与展望”，首先总结了通过本论文的研究得到的结论，然后点明了未来需要进一步研究的内容。

第 2 章 硬件开发功能安全标准实施

2.1 功能安全标准

ISO26262 的标准分成 10 个部分，如下图 2.1 所示，每个流程都包含一些条款，通常这些条款由目标、综述、输入、推荐需求、输出等内容组成。这些条款极大的规范了产品开发的流程使得车辆制造商，零部件供应商甚至最终客户，可以知道车辆是在这种特定方式下开发的，该方式聚焦在功能安全，如遵从规则等。

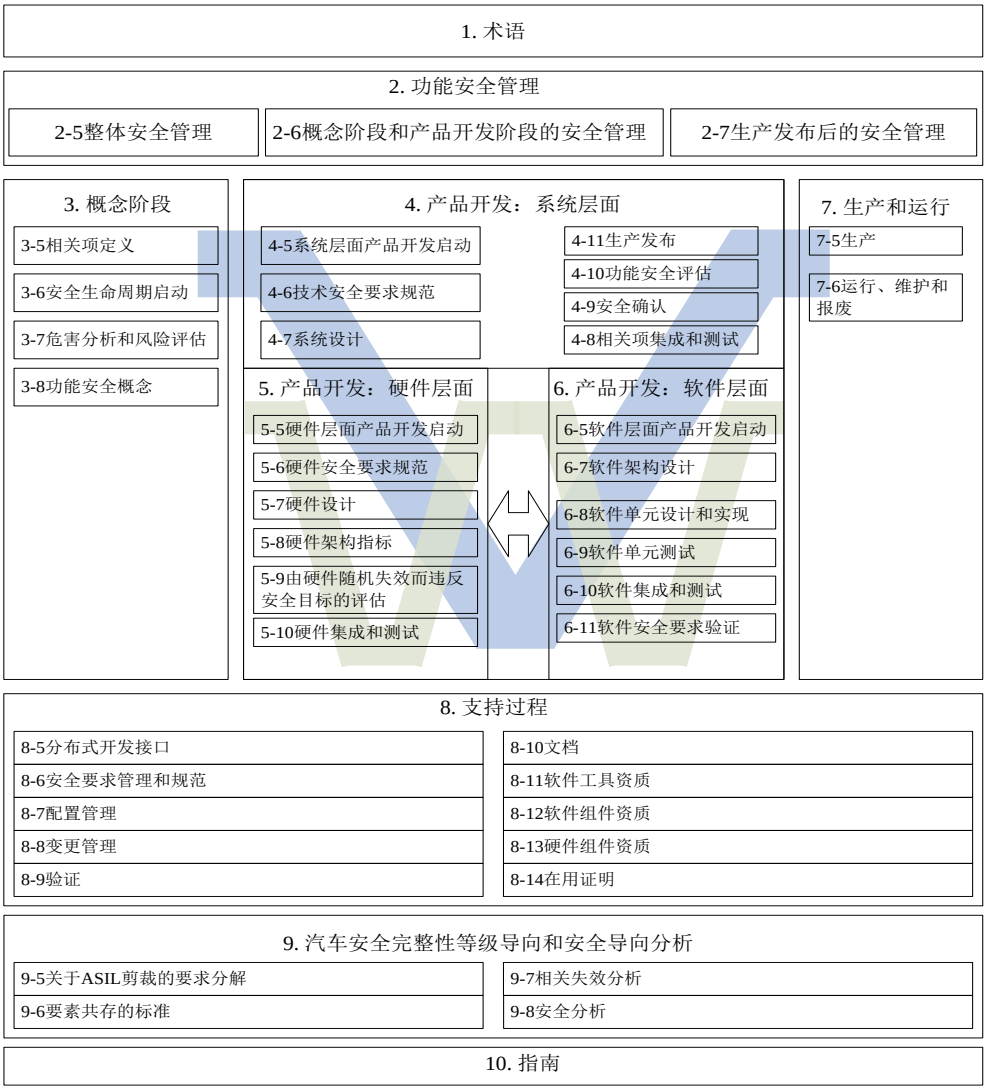

图 2.1 功能安全标准模型

2.2 功能安全系统层面

功能安全系统阶段的工作分成 7 个小的阶段,分别是系统层面初始化产品开发、技术安全需求规范、系统设计、相关项集成测试、安全确认、功能安全评估、产品发布，几个小阶段的相互关系如下图 2.2 所示[11]。

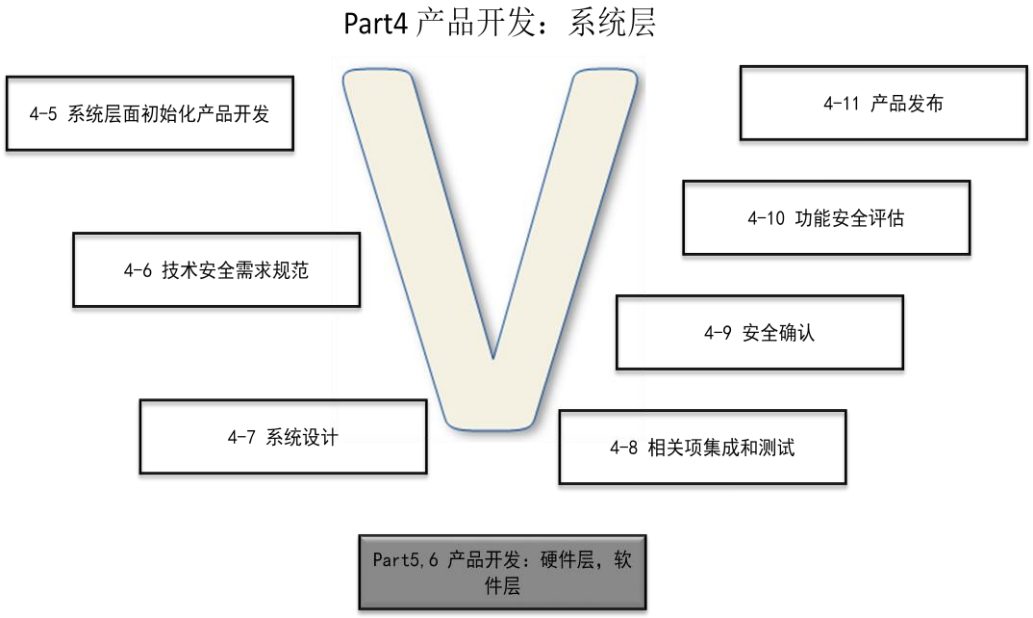

图 2.2 系统阶段模型

对系统开发关键条款的详细描述见表 2.1。

表 2.1 系统阶段

序号	条款	目的	前置条件	工作交付物
4-6	技术安全需求规范	1、定义技术安全需求，提炼功能安全概念； 2、分析核实技术安全需求符合功能安全需求；	功能安全概念 确认计划	技术安全需求规范 系统验证报告 确认计划
4-7	系统设计	1、开发相关项系统设计和技术安全概念； 2、验证系统设计和技术安全概念符合技术安全技术规范；	相关项集成测试计划 技术安全需求规范	技术安全概念 系统设计规范 硬件软件接口规范

2.2.1 技术安全需求规范

在整个开发生命周期中，技术安全需求作为执行功能安全概念的技术需求是必须的，它是相关项层面功能安全需求向系统层面技术安全需求的细化。

1、技术安全需求规范

技术安全需求应该基于功能安全概念、相关项初始架构假设、外部接口（如通讯和用户界面）、系统参数（如环境参数，车重和功能参数，最大扭矩）、系统配置需求(如 HEV 中机电复合传动控制系统可以匹配 1.0T 或 1.5T 的发动机)。

概念阶段的相关项初始架构假设和本条款的假设的一致性必须确保。如果其它功能或需求要被本系统或它的部件执行，那么这些功能或需求应该被列入规范或参考。技术安全需求应为安全相关的，在系统和相关项原件之间以及相关项和其它系统之间有相关性。

2、安全机制

技术安全需求应指定本系统或原件的响应，这些响应的促进因素会影响安全目标的完成。包括失效和结合相关运行模式及系统状态定义的促进因素的组合。例如自适应巡航控制系统在获知车辆稳定控制功能失效时会关闭自适应巡航功能达到其安全目标。

技术安全需求应指定安全机制，包括：a、和探测、指示、控制系统自身错误的方法，这些方法包含：系统或原件的自我监控以探测随机硬件失效，如可能也要探测系统失效；通讯通道的失效模式的探测和控制方法；b、和探测、指示、控制和系统存在相互影响的外部设备的错误相关的方法，外部设备包含：其它 ECU、供电、通讯模块；c、使能系统以达到或维持安全状态的方法，这些方法包含：当安全机制的优先次序以及机制冲突时的逻辑仲裁；d、细化及执行报警和限功能概念的方法；e、防止潜在故障的方法，这些方法包含：上电时的测试，如行驶前检查、运行时周期测试、下电时的测试，如行驶后检查、日常维护检查。

每一个使能相关项以达到或维持一个安全状态的安全机制应指定：a、安全状态的转变，包含对执行器的控制需求；b、容错时间间隔，可以用车辆测试或实验方法测定；c、如安全状态无法立刻达到，需要一个紧急运行间隔，可以用车辆测试或实验方法测定，如急停开关从触发到进入安全状态的时间；d、维持安全状态的方法，如驻车功能的安全机制依赖于电子驻车系统（EPS），同时传动系统应具备驻车锁止机构。

3、ASIL 分解

如果技术安全需求需要进行 ASIL 分解，则需要依照 ISO26262-9-条款 5。

4、避免潜在故障

应用于 ASILs（A）、（B）、C、D，相应的安全机制需要制定以防止潜在故障，对于随机故障，只有多点故障才会包含潜在故障。通过不同运行模式下，如：上电、下电、运行时或其它测试模式的在线测试，就是一种通过验证部件状态来探测潜在故障的安全机制。应用于 ASILs（A）、（B）、C、D 时，为避免多点失效，应为每一个安全机制规定故障探测间隔。多点故障的探测间隔应考虑以下因素：硬件部件的可靠性及其在架构中的角色、暴露于相应危害事件的概率、因硬件随机失效导致违反安全目标的最大概率目标值、相关安全目标分配的 ASIL。应用于 ASILs（A）、（B）、C、D 时，对于防止双点故障残余的安全机制应遵循：

对于 ASIL D 的系统，其“防止双点故障残余的安全机制”的安全等级应为 ASIL B、对于 ASIL B、C 的系统，其“防止双点故障残余的安全机制”的安全等级应为 ASIL A、对于 ASIL A 的系统，其“防止双点故障残余的安全机制”的安全等级可按工程经验设定。

2.2.2 系统设计

系统设计和技术安全概念的开发是基于源自功能安全概念的技术安全需求规范。为了开发系统架构设计，功能安全需求、技术安全需求和非安全相关需求应被执行，因此此阶段的安全相关和非安全相关需求在一个流程中被处理。

1、系统设计规范和技术安全概念

系统设计应基于功能概念、初步的架构假设和技术安全需求。在 ISO26262-3 中的初步的架构假设和此处的初步架构假设的一致性需要确保。技术安全需求应分配到系统设计原件。系统设计应执行技术安全需求。关于技术安全需求的执行，系统设计应考虑：a、对系统设计的验证能力；b、达到功能安全需要使用的硬件和软件设计的技术能力；c、系统集成时的测试能力。

2、系统架构设计条件

系统和子系统架构应遵从技术安全需求及其各自的 ASILs。每一个原件应继承技术安全需求所执行的最高的 ASIL。如果原件由被分配了不同 ASILs 的子原件或由非安全相关和安全相关子元件组成，那么每一个子元件应被当做最高 ASIL 的原件来对待，除非存在符合 ISO26262-9-条款 6 说所的共存条件。安全相关的原件的内部和外部接口应被定义，以避免其它有害的安全相关原件影响它。系统设计中如果安全需求用到 ASIL 分解，应该依照 ISO26262-9-条款 5。

3、避免系统失效的方法

系统设计中识别系统失效原因和系统故障影响的安全分析应被应用。识别出来的内部系统失效原因应被消除或减轻他们的不利影响。识别出的外部系统失效原因应被消除或减轻他们的不利影响。为减少系统失效，可信的汽车系统设计原则需要应用，如：a、可信的技术安全概念复用；b、可信的原件设计的复用，包含硬件和软件部件；c、可信的探测和控制失效的机制的复用；d、可信的标准化接口的复用。为了确认可信的设计原则或原件在新的相关项中是合适的，其应用的结果应被分析，同时在复用前要检查最基本的假设。影响分析包括：确定的诊断能力和可行性、环境参数、时间参数、确定的资源的通用性、系统设计的鲁棒性。当需求应用于 ASIL D 时，应不去复用可信的设计原则。应用于 ASILs（A）、（B）、C、D 时，为避免因系统太复杂而导致失效，系统架构设计遵循：模块化、足够的层次颗粒度、简单的原则。模块化设计方法可以参考表 2.2。

表 2.2 模块化系统设计资产

资产		ASIL			
		A	B	C	D
1	分等级设计	+	+	++	++
2	精确设计的接口	+	+	+	+
3	避免软硬件模块不必要的复杂性	+	+	+	+
4	避免不必要的复杂接口	+	+	+	+
5	检修时的可维护性	+	+	+	+
6	开发及运行时的可测性	+	+	++	++

4、运行时控制随机硬件失效的方法

探测、控制或消除随机硬件失效的方法应规定且符合系统设计规范和技术安全概念。这类方法可以是硬件诊断功能以及通过诊断探测随机硬件失效。应用于 ASILs（B）、C、D 时在相关项层面的评估时应规定单点故障度量和潜在故障度量的目标值。应用于 ASILs（B）、C、D 时需要选择一个随机硬件失效导致违反安全目标的评估流程，同时在相关项层面的评估时应规定一个随机硬件失效目标值。应用于 ASILs B、C、D 时，原件层面恰当的失效率和诊断覆盖率目标值应规定以符合：ISO26262-5-条款 8 的目标值、ISO26262-5-条款 9 的流程。应用于 ASILs（B）、C、D 时，对于分布式开发，得到的目标值都应传递给每一个相关方。

5、分配给硬件和软件

技术安全需求应直接或细微改良后分配给硬件、软件或两者。如果技术安全需求被分配到具备可编程能力的客户硬件单元，那么结合 ISO26262-5,6 的需求的开发流程应被定义和执行。系统设计应遵循分配和分割的原则。

6、硬件软件接口规范（HSI）

HSI 规范应指定硬件和软件的交户并且和技术安全概念一致。HSI 规范应包含部件的可被软件控制的硬件设备和支持软件运行的硬件资源。HSI 规范应包含以下的参数：a、硬件设备的相关运行模式和配置参数。运行模式如默认、初始、测试或超级。配置参数如增益控制、带通频率、时钟预设；b、硬件特征需确保原件和分割的支持软件之间的独立性；c、共享和专属的硬件资源。如内存映射、寄存器分配、定时器、中断、I/O 端口；d、硬件设备访问机制。如串行、并行、从式、主从式；e、为每一个涉及到技术安全概念的服务定义计时参数。相关的硬件诊断能力和相应的软件应用应在 HSI 规范中指定。a、硬件诊断功能应被定义。如过流、短路、过温的探测；b、需要软件执行的硬件诊断功能应被定义。HSI 应在系统设计阶段指定，在硬件开发和软件开发时被重新定义。

2.3 功能安全硬件层面

功能安全硬件阶段的工作分成 6 个小的阶段,分别是硬件层面初始化产品开发、硬件安全需求规范、硬件设计、硬件架构度量、由于随机硬件失效导致的违反安全目标的评估、硬件集成和测试,几个小阶段的相互关系如下图 2.3 所示[12]。

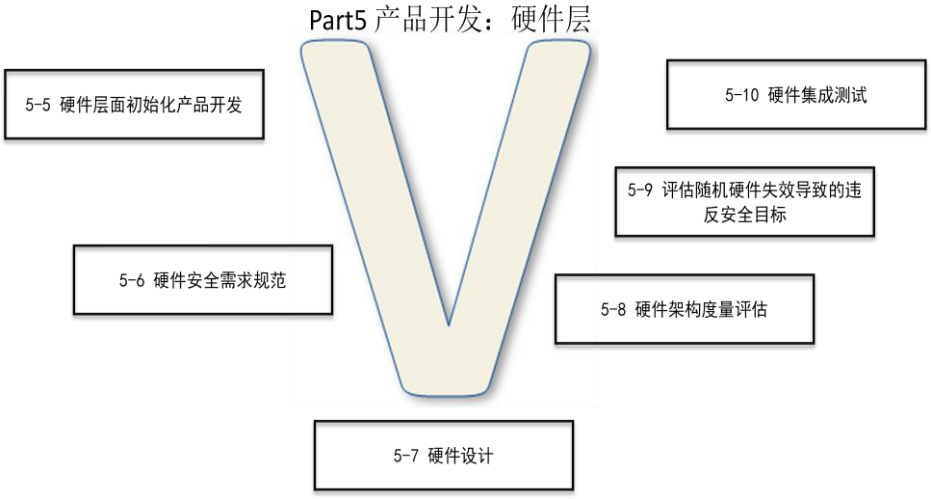

图 2.3 系统阶段 V 模型

硬件开发关键条款的详细描述见表 2.2。

表 2.2 硬件开发阶段说明

序号	条款	目的	前置条件	工作交付物
5-6	硬件安全需求规范	1、定义硬件安全需求； 2、核实硬件安全需求符合技术安全概念和系统设计规范； 3、细化硬件软件接口规范	安全计划修订 技术安全概念 系统设计规范 硬件软件接口规范	硬件安全需求规范 硬件软件接口规范修订 硬件安全需求验证报告
5-8	硬件架构度量评估	评估相关项的硬件架构符合硬件架构度量描绘的错误处理需求	硬件安全需求规范 硬件设计规范 硬件安全分析报告	分析相关项架构应对随机硬件失效的有效性 分析相关项架构应对随机硬件失效的有效性的检查报告
5-9	评估随机硬件失效导致的违反安全目标	为由相关项的随机硬件失效导致的违反安全目标的残余风险是否足够低提供合理可用的评判标准	硬件安全需求规范 硬件设计规范 硬件安全分析报告	由于随机硬件失效导致违反安全目标的分析 硬件专用方法规范 由于随机硬件失效导致违反安全目标的评估检查报告
5-10	硬件集成和测试	通过测试确保开发的硬件符合硬件安全需求	安全计划修订 相关项集成和测试计划修订 硬件安全需求规范 硬件设计规范	硬件集成和测试报告

2.3.1 硬件安全需求规范

技术安全需求被分配给硬件和软件。同时涉及硬件和软件的需求被进一步分解到只和硬件相关的安全需求。硬件安全需求需要进一步细化，考虑设计参数和

设计参数对硬件的影响。

1、相关项的硬件原件的硬件安全需求规范源自分配给硬件的技术安全需求。

2、硬件安全需求规范应包含和安全相关的每一个硬件安全需求，包括：a、硬件安全需求和相关的安全机制的属性可以控制硬件原件的内部失效，包括覆盖瞬时故障的内部安全机制，如果有关联的话；b、确保原件的硬件安全需求和相关的安全机制的属性可以容忍原件外部的失效。例如 ECU 的功能表现必须容忍输入电路开路等外部失效事件；c、硬件安全需求和相关的安全机制的属性遵从其它原件的安全需求。如执行器和传感器的诊断；d、硬件安全需求和相关的安全机制的属性可以对内部或外部失效进行探测并发送信号。例如一个安全机制的硬件部件规定的错误响应时间和容错时间间隔的一致性；e、硬件安全需求不指定具体的安全机制。

3、需求应用于安全目标 ASILs（B）、C、D。当取得相关项硬件原件的度量值时，依照 ISO26262-4-条款 7 而规定的 ISO26262-5-条款 8 的度量的目标值应考虑。

4、需求应用于安全目标 ASILs（B）、C、D。当取得相关项硬件原件的度量值时，依照 ISO26262-4-条款 7 而规定的 ISO26262-5-条款 9 的度量的目标值应考虑。

5、硬件安全需求应依照 ISO26262-8-条款 6。

6、应指定相关项或原件的硬件设计验证判断标准，包括环境条件（温度、震动、电磁干扰），指定运行环境（供电电压、工况），指定硬件特殊的需求，包括：a、通过认证中等复杂的硬件部件来验证的话，判断标准应符合 ISO26262-8-条款 13；b、通过测试来验证的话，判断标准应依照 ISO26262-5-条款 10。

7、硬件安全需求应遵循 ISO26262-4-条款 6 规定的安全机制的容错时间间隔。

8、硬件安全需求应遵循 ISO26262-4-条款 6 规定的多点故障探测间隔。当安全目标为 ASILs C、D 且对应的安全概念没有指示明确的值，那么多点故障探测间隔可以指定为小于或等于相关项上电到下电的周期。适当的多点故障探测间隔也可以通过对随机硬件失效发生的定量分析证明。

9、硬件安全需求应遵循 ISO26262-8-条款 6, 9 以提供证据来证明：a、技术安全概念、系统设计规范和硬件规范的一致性；b、技术安全需求分配到硬件原件的完整性；c、与相关软件安全需求的一致性；d、正确性和精确性。

10、HSI 应被充分的重定义以便软件可以准确的控制和使用硬件，同时应描述每一个安全相关的硬件和软件之间的依赖性。

11、硬件和软件开发的人员应联合负责验证重新定义的 HSI 规范是否充分。

2.3.2 硬件设计

硬件设计包含硬件架构设计和硬件详细设计。硬件架构设计描绘所有硬件部件和它们之间的相互作用。硬件详细设计是电气原理层面对于组成硬件的元器件之间的连接关系的描述。为开发一个单独的硬件设计，硬件安全需求和非安全需求都需要遵循。因此在这个阶段安全和非安全需求将用同一个开发流程来处理。

1、硬件架构设计

硬件架构应执行 ISO26262-5-条款 6 定义的硬件安全需求。每一个硬件部件应继承它所执行的硬件安全需求的最高 ASIL，即硬件部件的每一个特征应继承它所执行的硬件安全需求的最高 ASIL。在硬件架构设计时，如果 ASIL 分解被应用于硬件安全需求，ASIL 分解应依照 ISO26262-9-条款 5。如果一个硬件部件由不同的 ASILs 的部件，或未分配 ASIL 的部件和安全相关的部件组成，那么每一个部件应按照最高 ASIL 处理，除非遇到符合 ISO26262-9 的共存条件。

硬件安全需求和它们的执行之间的可追溯性应被维持到最低的硬件部件层。为避免由于高度复杂导致的失效，硬件架构设计应显出下列的原则和表 2.3 的资产:a、模块化；b、充分的层级颗粒度；c、简单。非功能导致的安全相关的硬件部件的失效应在架构设计中考虑，包括以下影响：温度、震动、水、灰尘、电磁干扰、来自于硬件架构其它部件或环境的窜扰。

表 2.3 模块化硬件设计资产

资产		ASIL			
		A	B	C	D
1	分等级设计	+	+	++	++
2	精确定义安全相关的硬件部件的接口	+	+	+	+
3	避免不必要的复杂接口	+	+	+	+
4	避免软硬件部件不必要的复杂性	+	+	+	+
5	检修时的可维护性	+	+	+	+
6	开发及运行时的可测性	+	+	++	++

2、硬件详细设计

为避免共因设计失效，相关的经验教训应依照 ISO26262-2-条款 5 被应用。非功能导致的安全相关的硬件器件的失效应在详细设计中考虑，包括以下影响：温度、震动、水、灰尘、电磁干扰、来自于硬件部件其它器件或环境的窜扰。

硬件详细设计中使用的器件的运行条件应遵从它们的环境和操作限制规范。鲁棒性设计原则应考虑。鲁棒性设计原则可以通过基于质量管理（QM）的检查清单来体现，例如部件的保守的规范。

3、安全分析

在硬件设计中识别失效原因和故障影响的安全分析应依照表 2.4 和 ISO26262-9-条款 8 来应用。安全分析最初的目的是支持硬件设计的规范，慢慢

的也被用于硬件设计的验证。在支持硬件设计规范时，定性分析是恰当和足够的。

表 2.4 硬件设计安全分析

方法		ASIL			
		A	B	C	D
1	演绎分析，典型的有故障树分析（FTA）	O	+	++	++
2	归纳分析，典型的有故障模式和效应分析（FMEA）	++	++	++	++

需求应用于安全目标 ASILs（B）、C、D。对于每一个安全相关的硬件部件或器件，安全分析应为安全目标识别：a、安全故障；b、单点故障或残余故障、多点故障（感知的、探测的、潜在的）。大多数情况下，可以只对双点故障进行分析，但是有时侯多点故障也和技术安全概念相关，例如执行冗余安全机制的时候。识别双点故障的意图不是要系统的分析任意两个硬件故障的每一种可能的组合，但是至少要考虑来自技术安全概念的组合，如一个故障影响安全相关的部件，另一个故障影响对应的达成或维持安全状态的安全机制。

需求应用于安全目标 ASILs（B）、C、D。避免单点故障的安全机制的有效性证据应被提供。为此：a、安全机制保持在安全状态或安全的转换到安全状态能力的证据应提供，特别是在故障容错时间间隔内恰当的失效缓解能力；b、残余故障的诊断覆盖率应被评估，一个故障可能出现在任何时候（不仅在上电时）并且其诊断测试间隔加上相关的安全机制的故障响应时间比相应的故障容错时间间隔长的话，则不能被认为是有效的覆盖。如果是那种能被证明只会出现在上电时且其出现在车辆运行时的可能性可以忽略的故障那么只执行上电后的启动测试是可以接受的。FMEA 分析和故障树分析可以用于制定逻辑依据。依赖于硬件原件的失效模式和在更高层面上它们造成的后果的知识，可以采用对硬件原件全局诊断覆盖率的评估或采用更细的失效模式覆盖率评估。ISO26262-5，附件 D 可以用于由恰当的逻辑依据支撑的诊断覆盖率的评估起始点。

需求应用于安全目标 ASILs（B）、C、D。避免残余故障的安全机制的有效性证据应被提供。为此：a、故障探测和通知驾驶员的能力包括潜在故障可接受的多点故障探测间隔的证据应被提供以判断哪些故障保持潜在，哪些故障不再潜在；b、潜在故障的诊断覆盖率应被评估，一个故障不能被认为是有效覆盖，如果其诊断测试间隔加上相关的安全机制的故障响应时间大于相应得潜在故障的多点故障探测间隔。FMEA 分析和故障树分析可以用于制定逻辑依据。ISO26262-5，附件 D 可以用于由恰当的逻辑依据支撑的诊断覆盖率的评估起始点。依赖于硬件原件的失效模式和在更高层面上它们造成的后果的知识，可以采用对硬件原件全局诊断覆盖率的评估或采用更细的失效模式覆盖率评估。

需求如果被应用，硬件设计独立的遵从其需求的证据需要被提供，它基于对非独立失效的分析，依照 ISO26262-9。

被硬件设计引入的新的危害没有被原有的安全目标覆盖，他们应该被引入和评估，实现方法是通过依照 ISO26262-8 的更改管理流程的危害分析和风险评估。

2.3.3 估算硬件架构的度量

硬件架构度量用于评估相关项的架构应付随机硬件失效的效力。ISO26262 描述了单点故障度量和潜在故障度量两种硬件架构度量，度量及其关联的目标值应用到整个相关项的硬件并和 ISO26262-5-条款 9 所描述的因随机硬件失效引起的违反安全目标的评估是互补的。

硬件架构度量所描述的随机硬件失效被限定在某些相关项的安全相关的电子电器硬件部件，也就是那些对于违反安全目标或达到安全目标起到显著作用的部件以及单点故障、残余故障、潜在故障的部件。对于机电一体的部件，只考虑电气的失效模式和失效率。

硬件架构度量在硬件架构设计和硬件详细设计中可以被重复应用。硬件架构度量依赖于整个相关项的硬件。通过符合硬件架构度量得到的目标值可以达到相关项所涉及的每一个安全目标。

硬件架构度量可达到以下目的：a、可以被客观的评估：度量是可考证的并且足够精确的以识别不同的架构；b、支持最终设计的评估；c、提供 ASIL 相关的硬件架构通过/失败的判断标准；d、显示硬件架构中防止单点或残余故障风险的安全机制的覆盖率无论如何是足够的（单点故障度量）；e、显示硬件架构中防止潜在故障风险的安全机制的覆盖率无论如何是足够的（潜在故障度量）；f、描述单点故障、残余故障、潜在故障；g、对不确定的硬件失效率确保其鲁棒性；h、被限定于安全相关的原件；i、支持用于不同的原件层级。为了减轻分布式开发的难度，目标值可以分配到微处理器或控制器。

1、需求应用于安全目标 ASILs（B）、C、D。依照 ISO26262-5，附件 C，诊断覆盖率、单点故障度量、潜在故障度量的概念应应用于以下 2 至 9 的需求。

2、需求应用于安全目标 ASILs（B）、C、D。残余故障和相关的潜在故障的安全机制对安全相关的硬件部件的诊断覆盖率应被评估。为此 ISO26262-5，表格 D. 1 至 D. 14 可被用作宣称合理的逻辑依据支持诊断覆盖率的起始点。

3、需求应用于安全目标 ASILs（B）、C、D。分析使用的硬件部件的估算失效率应被定义：a、使用来自被认可的工业界资料提供者的硬件失效率数据。例如 IEC/TR62380，IEC61709 , MIL HDBK217F 注释 2，EN50129：2003，ISO26262-5，附件 C，IEC62061：2005，附件 D 等。来自这些数据库的数据一般被认为较悲观；b、使用现场反馈或测试的统计数据。这种情况下，估算的失效率需要具备可接受的置信水平；c、使用建立在定性或定量论证的基础上的基于工程方法的专家

判断。专家判断作为这类判断的基础应依照总体的评判标准被使用。估计的失效率制定前先要设置这些评判标准。专家判断的评判标准包括：现场经验、测试、可靠性分析、设计创新。

4、需求应用于安全目标 ASILs（B）、C、D。如果单点故障和潜在故障计算出的失效率无法提供充足的证据，其它可选的方法需要提出，如增加安全机制来探测和控制这个故障。充足的证据意指通过 ISO26262-5-条款 8 所列的方法确定失效率来给出的证据。

5、需求应用于安全目标 ASILs（B）、C、D。针对每一个安全目标，如 ISO26262-4-条款 7 所要求的单点故障定量的目标值应基于以下参考目标值来源：a、来自应用于相似的可信设计原则的硬件架构度量计算，两个具备相似功能、相似安全目标、相同 ASIL 的设计；b、来自于表格 2.5。表中的指标试图提供设计指导和设计遵从安全目标的证据。

表 2.5 取得单点故障度量目标值的可能来源

	ASIL B	ASIL C	ASIL D
单点故障度量	≥90%	≥97%	≥99%

6、需求应用于安全目标 ASILs（B）、C、D。针对每一个安全目标，如 ISO26262-4-条款 7 所要求的潜在故障定量的目标值应基于以下参考目标值来源：a、来自应用于相似的可信设计原则的硬件架构度量计算，两个具备相似功能、相似安全目标、相同 ASIL 的设计；b、来自于表格 2.6。表中的指标试图提供设计指导和设计遵从安全目标的证据。

表 2.6 取得潜在故障度量目标值的可能来源

	ASIL B	ASIL C	ASIL D
潜在故障度量	≥60%	≥80%	≥90%

7、需求应用于安全目标 ASILs（B）、C、D。针对每一个安全目标，相关项的所有硬件应遵循以下可选方案之一：a、满足单点故障度量目标值；b、满足硬件原件层面规定的恰当值，该值由需求 5 给定，其对于遵从硬件原件层的目标值是合理的，对于遵从分配到相关项的整个硬件的单点故障度量目标值是足够的。

如果一个相关项包含具有明显不同的失效率水平的不同类型的硬件原件，遵从硬件架构度量所存在的风险仅聚焦在那些具有最高等级失效率的硬件原件上。为每一种硬件规定一个恰当的度量目标值有助于对高失效率原件的关注。

当预期瞬时故障和所采用的技术是相关的。可以制定和验证一个专门的单点故障目标值来要求瞬时故障，也可以基于证实内部安全机制覆盖瞬时故障的执行效力来定性其合理性。

如果单点故障度量不能满足目标值，需要评估设计达成安全目标的合理性。

在定义单点故障度量时，部分或全部的安全目标的运用可以一起考虑，但是

这里只考虑那些具备最高 ASIL 的安全目标的度量目标值。

8、需求应用于安全目标 ASILs（B）、（C）、D。针对每一个安全目标，相关项的所有硬件应遵循以下可选方案之一：a、满足潜在故障度量目标值；b、满足硬件原件层面规定的恰当的值，该值由需求 6 给定，其对于遵从硬件原件层的目标值是合理的，对于遵从分配到相关项的整个硬件的潜在故障度量目标值又是足够的；c、对于潜在故障，和需求 6 给出的潜在故障度量目标值一样需要满足诊断覆盖率的目标值，以上适用于每一个含有会导致安全机制无效的故障的硬件原件。这一可选的应用是基于故障探测的，当安全机制的无效会直接导致安全目标的违反。

选项 c 被限定在那些每一个安全机制都是基于故障探测的案例。它假设案例中某功能可能的潜在故障可以灵敏的通过安全机制的探测被发现。在别的案例中选项 c 不可以应用，只能应用选项 a 和 b。

在可以应用选项 c 的案例中，度量不再被计算，只需要估计硬件原件的潜在故障被安全机制覆盖的诊断覆盖率。

如果一个相关项包含具有明显不同的失效率水平的不同类型的硬件原件，遵从硬件架构度量所存在的风险仅聚焦在那些具有最高等级失效率的硬件原件上。为每一种硬件规定一个恰当的度量目标值有助于对高失效率原件的关注。

如果潜在故障度量不能满足目标值，需要评估设计达成安全目标的合理性。

在定义潜在故障度量时，部分或全部的安全目标的运用可以一起考虑，但是这里只考虑那些具备最高 ASIL 的安全目标的度量目标值。

9、需求应用于安全目标 ASILs（B）、C、D。对于需求 7 和 8 的验证检查需要执行以提供设计符合 ISO26262-8-条款 9 要求的技术准确性和完整性的证据。

对单点故障度量的验证检查可以确保那些安全相关的硬件原件的失效率被考虑，所以得到的度量不会因为不必要的不存在潜在单点故障或残余故障的安全相关的硬件原件而有不恰当的偏离。例如为安全机制添加不必要的硬件原件。

2.3.4 评估随机硬件失效导致的安全目标的违反

有两种可选的方法被推荐用于评估违反安全目标的残余风险是否足够低。两种方法均可以评估由于单点故障、残余故障、双点故障导致的违反安全目标的残余风险。在分析中，对于残余和双点故障需要考虑安全机制的覆盖率，对于双点故障还需要考虑暴露持续的时间。

第一种方法使用概率度量，称为随机硬件失效概率度量（PMHF），可以评估对相关安全目标的违反。第二种方法单独评估每一个单点和残余故障，以及导致违反相关安全目标的每一个双点失效。这一分析方法也可以看成是子集分析。

两种方法在硬件架构设计和硬件详细设计中可以被重复应用。其范围被限定在相关项的随机硬件失效。分析中考虑的部件是电子电器硬件部件。对于机电一体的部件，只考虑电气的失效模式和失效率。

1、需求应用于安全目标 ASILs（B）、C、D。相关项应符合需求 2 或 3。

2、评估随机硬件失效概率度量

需求应用于安全目标 ASILs（B）、C、D。如 ISO26262-4-条款 7 所要求的随机硬件失效导致的违反每一个安全目标的最大概率的定量的目标值需通过以下参考目标值资料来源来定义：a、来自于表格 2.7；b、来自相似的可信设计原则的现场数据；c、来自应用于相似可信设计原则所使用的失效率的定量分析技术。这些来自资料来源 a，b，c 的定量目标值没有任何绝对的意义，只是用于新旧设计之间的对比。它们试图提供确保残余风险足够低的设计指导，并提供设计符合安全目标的证据。

表 2.7 取得随机硬件失效目标值的可能来源

ASIL	随机硬件失效目标值
D	$<10^{-8}h^{-1}$
C	$<10^{-7}h^{-1}$
B	$<10^{-7}h^{-1}$

需求应用于安全目标 ASILs（B）、C、D。上一需求得到的定量目标值应表述为相关项运行生命周期内每小时的故障平均发生概率，当相关项处于下电关闭模式时，该时间不被计算在每小时的故障平均发生概率中。

需求应用于安全目标 ASILs（B）、C、D。对于硬件架构的单点、残余、双点故障的定量分析应提供违反每一个安全目标的最大概率的定量的目标值达到的证据。这一定量分析应考虑：a、相关项的架构；b、每一个可能导致单点故障或残余故障的硬件部件的失效模式的失效率估计；c、每一个可能导致双点故障的硬件部件的失效模式的失效率估计；d、安全相关硬件部件被安全机制覆盖的诊断覆盖率；e、双点故障的暴露持续时间。

定量分析时那些能导致安全相关的硬件原件失效的硬件原件的失效模式及其安全机制同时被考虑。它们可以是单点故障、残余故障、多点故障。

暴露持续时间从故障可被探测开始，包括：a、与每一个安全机制关联的多点故障探测间隔时间，在故障不向驾驶员指示时则探测间隔时间为车辆的生命周期；b、当驾驶员被要求停留在安全的方式时，探测时间间隔为一个驾驶周期的最大持续时间，平均的驾驶周期持续时间一般为 1 小时；c、当驾驶员被提醒去维修车辆时，探测时间间隔为车辆进入维修车间的平均时间间隔，车辆维修的平均时间和故障类型有关，一般影响舒适性的为 200 个驾驶周期，如空调系统，影响辅助驾驶功能的为 50 个驾驶周期，如倒车雷达，亮黄色警告灯或影响驾驶行

为的为 20 个驾驶周期，如 ABS 系统，亮红灯的为一个驾驶周期，如发动机故障。

因此，暴露持续时间依赖于所涉及的监控的类型（持续监控、周期性自检、驾驶员监控、无监控）和探测到故障时的响应的种类。根据探测到故障后触发一个转换到安全状态的需求不同，暴露持续时间可以短到几个毫秒，也可以长到车辆的生命周期。

如果失效概率不能满足目标值，需要评估设计达成安全目标的合理性。

依赖于硬件原件的失效模式和在更高层面上它们造成的后果的知识，可以采用对硬件原件全局诊断覆盖率的评估或采用更细的失效模式覆盖率评估。对于使用集成诊断的安全机制，ISO26262-5-附件 D 可以用于由恰当的逻辑依据支撑的诊断覆盖率的评估起始点。

需求应用于安全目标 ASILs C、D。只有当专有的方法被采用时才可以考虑接受一个单点故障出现在硬件部件。专用的方法包括：a、硬件部件的过设计或物理隔离；b、来料的特殊抽样测试以降低出现这种失效模式的风险；c、老化测试；d、专用的控制安排作为控制计划的一部分；e、分配安全相关的特殊参数。

需求应用于安全目标 ASILs C、D。如果硬件部件的诊断覆盖率小于 90%则需要上一节提到专用方法去处理硬件部件。在定义安全机制的覆盖率时可以考虑硬件部件的安全故障的比例。在硬件部件层面而非相关项层面，计算诊断覆盖率的处理方式和计算单点故障度量近似。

需求应用于安全目标 ASILs（B）、C、D。分析所用的硬件部件失效率应根据 ISO26262-5-条款 8 估算。

需求应用于安全目标 ASILs（B）、C、D。为避免量化失效率时出现偏差，如果失效率来源是结合的，它们应该使用缩放因子来按比例缩放以保持一致性。可以参考 ISO26262-5-附件 F

3、评估违反安全目标的每一个原因

图 2.4 和 2.5 描述了分析随机硬件失效导致的违反安全目标的每一个原因的方法。每一个单点故障用故障出现的评判标准来评估。每一个残余故障用故障出现结合安全机制的效力的评判标准来评估。

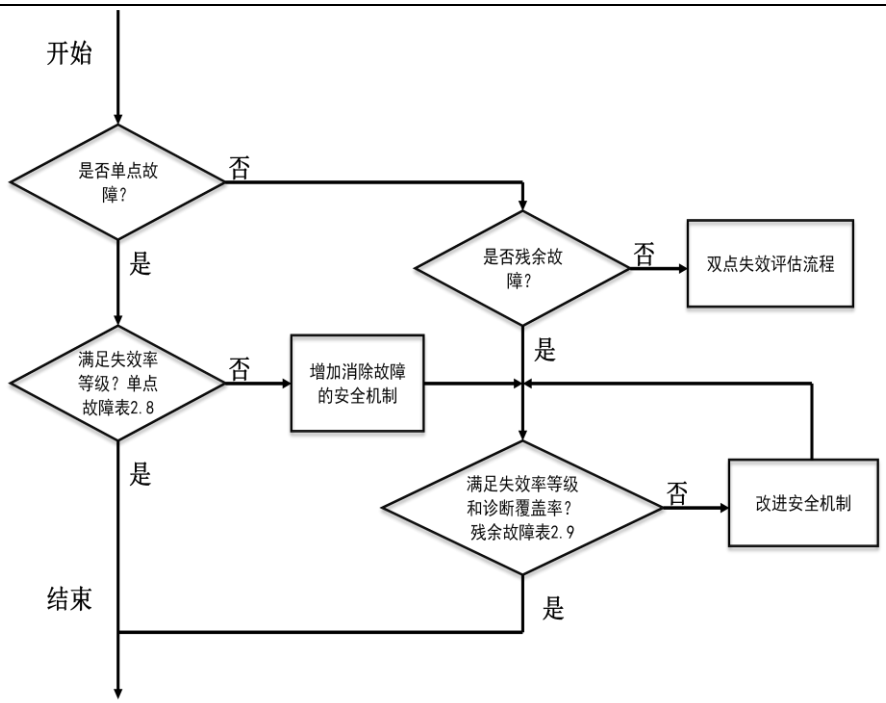

图 2.4 单点和残余故障的评估流程

如果双点失效是确认的，那么导致失效的故障将用故障的出现结合安全机制的覆盖率的评判标准来评估。

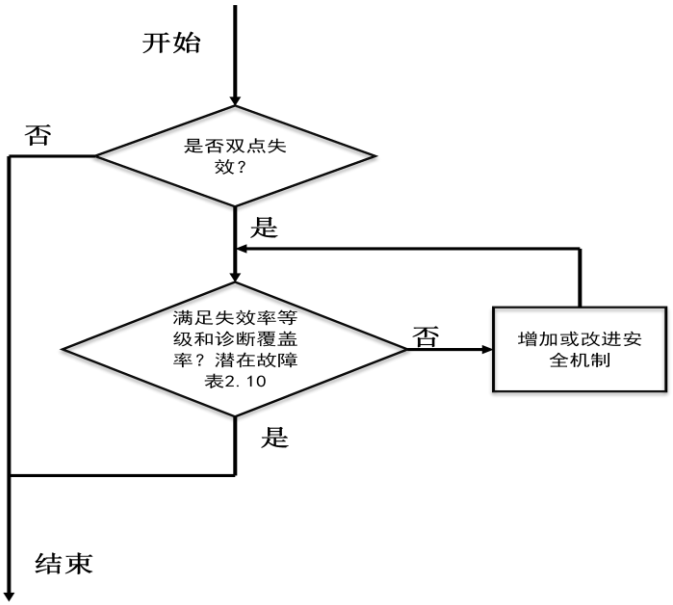

图 2.5 双点失效的评估流程

需求应用于安全目标 ASILs（B）、C、D。在硬件部件层面上对于每一个单点故障、残余故障、双点失效违反安全目标的单独的评估应被实施。此评估应提供每一个单点故障、残余故障、双点失效违反安全目标可以被接受的证据。

需求应用于安全目标 ASILs（B）、C、D。硬件部件失效率的等级分类应被

确定，失效率等级 1,2,3 和 FMEA 所使用的等级是类似的，等级 1 表示失效模式出现的概率最低：a、和等级 1 对应的失效率应小于随机硬件失效目标值定义的 ASIL D 的目标除以 100；b、和等级 2 对应的失效率应小于等于 10 倍的等级 1 对应的失效率；c、和等级 3 对应的失效率应小于等于 100 倍的等级 1 对应的失效率；d、和等级 i（i>3）对应的失效率应小于等于 10（i-1）倍的等级 1 对应的失效率。

如果可以提供逻辑依据，则等级 1 的分级计算可以除以一个小于 100 的数。

需求应用于安全目标 ASILs（B）、C、D。如果相应的硬件部件的失效率等级符合表 2.8 的目标值，则其出现的单点故障可以考虑被接受。

表 2.8 硬件部件关于单点故障的失效率等级目标

ASIL	失效率等级
D	失效率等级1+专用方法
C	失效率等级2+专用方法或失效率等级1
B	失效率等级2或失效率等级2

需求应用于安全目标 ASILs（B）、C、D。如果相应的硬件部件的诊断覆盖率和失效率等级符合表 2.9 的目标值，则其出现的残余故障可以考虑被接受。失效率只考虑硬件部件的失效率而不考虑安全机制的效力。

表 2.9 给定诊断覆盖率的硬件部件关于残余故障的最大失效率等级

ASIL	残余故障的诊断覆盖率			
	≥99.9%	≥99%	≥90%	<90%
D	失效率等级4	失效率等级3	失效率等级2	失效率等级1+专用方法
C	失效率等级5	失效率等级4	失效率等级3	失效率等级2+专用方法
B	失效率等级5	失效率等级4	失效率等级3	失效率等级2

需求应用于安全目标 ASILs C、D。对于失效率等级 i（i>3），如果一个残余故障的诊断覆盖率大于等于[100-10(3-i)]%，则对于 ASIL D 可以考虑接受，或则大于等于[100-10(4-i)]%，则对于 ASIL C 可以考虑接受。

需求应用于安全目标 ASILs D。一个双点失效在以下情况下应被考虑为真：a、如果一个或两个涉及的硬件部件的诊断覆盖率（针对残余故障）小于 90%；b、如果双点失效的双点故障之一保持潜伏的时间比故障探测间隔时间长的话。

需求应用于安全目标 ASILs C。一个双点失效在以下情况下应被考虑为真：a、如果一个或两个涉及的硬件部件的诊断覆盖率（针对残余故障）小于 80%；b、如果双点失效的双点故障之一保持潜伏的时间比故障探测间隔时间长的话。

需求应用于安全目标 ASILs C、D。一个双点失效不被认为是真的，则考虑将其和安全目标共存，这样也是可以接受的。

需求应用于安全目标 ASILs C、D。相应的硬件部件遵从表 2.10 给定的失效率等级和诊断覆盖率目标值则一个双点故障出现在硬件部件并产生一个双点失效应考虑被接受。失效率只考虑硬件部件的失效率而不考虑安全机制的效力。

表 2.10 硬件部件关于双点故障的失效率等级和诊断覆盖率目标

ASIL	潜在故障的诊断覆盖率		
	≥99%	≥90%	<90%
D	失效率等级4	失效率等级3	失效率等级2
C	失效率等级5	失效率等级4	失效率等级3

需求应用于安全目标 ASILs（B）、C、D。用于分析的硬件部件失效率的失效率等级分类应通过失效率资料来源来证明。如果分析使用的失效率数据资料来源有多个，那么每个失效率的比例因子需要采用。

4、验证检查

需求应用于安全目标 ASILs（B）、C、D。源于需求 2 和 3 的分析结果的验证检查应实施以提供设计符合 ISO26262-8-条款 9 的技术准确性和完整性证据。

2.3.5 硬件集成测试

硬件集成测试活动的目标是集成硬件元件并测试硬件设计以验证其符合硬件安全需求和相应的 ASIL 等级。

硬件集成和测试活动应依照 ISO26262-8-条款 9 被执行。

硬件集成和测试活动应与 ISO26262-4-5 的相关项集成测试计划相互配合。

测试设备应受到质量监控体系的管控。

测试用例应源自表 2.11 的方法的恰当的组合。

表 2.11 硬件集成测试方法

方法		ASIL			
		A	B	C	D
1	需求分析	++	++	++	++
2	分析内部和外部接口	+	++	++	++
3	完善和分析类似的设计	+	+	++	++
4	分析边界值	+	+	++	++
5	基于错误猜测的经验和知识	++	++	++	++
6	功能相关分析	+	+	++	++
7	分析关联故障的共因限制条件、先后次序、来源	+	+	++	++
8	分析环境条件和操作使用案例	+	++	++	++
9	标准	+	+	+	+
10	分析重大的变型	++	++	++	++

硬件集成测试活动应验证安全机制的执行应对硬件安全需求的完整性和正确性，具体方法见表 2.12。

表 2.12 硬件集成测试验证安全机制应对硬件安全需求的完整性和正确性

方法		ASIL			
		A	B	C	D
1	功能测试	++	++	++	++
2	故障注入测试	+	+	++	++
3	电气测试	++	++	++	++

硬件集成测试活动应验证硬件抵抗外部压力的鲁棒性，具体方法见表2.13。

表 2.13 硬件集成测试验证安全机制应对硬件安全需求的完整性和正确性

方法		ASIL			
		A	B	C	D
1	环境测试带功能测试	++	++	++	++
2	扩展功能测试	O	+	+	++
3	统计测试	O	O	+	++
4	最坏情况测试	O	O	O	+
5	超限测试	+	+	+	+
6	机械测试	++	++	++	++
7	加速寿命测试	+	+	++	++
8	机械耐受试验	++	++	++	++
9	电磁干扰、抗干扰、静电防护测试	++	++	++	++
10	化学测试	++	++	++	++

2.4 本章小结

本章阐明了功能安全标准的架构和各个部分之间的关系，实施系统开发和硬件开发的 V 模型及各个阶段的条款、目的、前置条件、需求/推荐和交付物。明晰了功能安全系统开发的重点是技术安全需求分析和技术安全概念分析，功能安全硬件开发的重点是硬件架构度量评估、随机硬件失效导致的违反安全目标的评估和硬件集成测试。

第 3 章 机电复合传动控制系统需求设计

3.1 传动控制系统相关项定义

机电复合传动系统是指一种集成驱动电机的插电式混合动力传动系统，该系统的机械部分主要由驱动电机、起动/发电/助力电机、离合器 C1、离合器 C2、1 档速比齿轮组、2 档速比齿轮组、主减速器构成，如图 3.1 所示。从动力系统的结构可以知道，通过系统几个主要动力源的不同组合，可以有 3 种工作模式，分别是纯电动模式、串联模式与并联模式。

该系统的 3 种工作模式通过控制离合器 C1 与 C2 来实现。当 C1 断开 C2 闭合时，系统工作在纯电动模式，在这种模式下，发动机与起动/发电/助力电机均停止工作，车辆由驱动电机单独驱动。当发动机工作并带动发电电机发电时系统进入串联模式。当 C1 和 C2 同时闭合时，系统进入并联模式[4,23]。

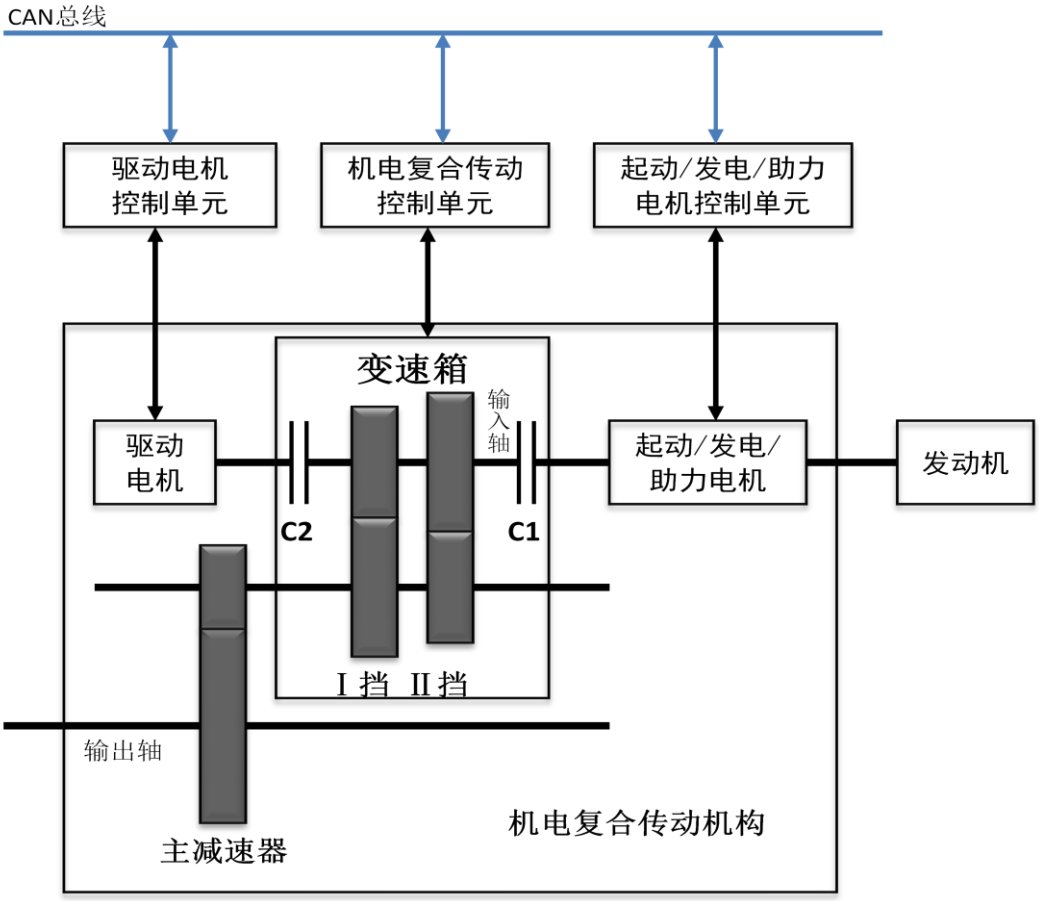

图 3.1 机电复合传动系统结构图

机电复合传动控制系统是关键，后面的讨论都限制在这一相关项。所谓相关项是指：那些应用 ISO26262 并在整车层面执行功能的系统或系统的组合。车用机电复合传动控制系统是指：由机电复合传动控制单元、传感器、执行器、电机、传动系统线束几个系统所组合而成的相关项，但是不包含发动机、发动机控制单元、电机控制单元、整车供电系统、整车线束所实现的功能。

机电复合传动控制系统实现的主要功能如表 3.1[24,25]。

表 3.1 机电复合传动控制系统主要功能

功能	描述
上下电管理	低压上下电； 主接触器控制； 电机模式控制；
混动系统运行模式管理	默认模式：车速为零，系统自检完成且无故障； 爬行模式：油门和制动踏板都释放，车辆以一定的车速行驶； 纯电行驶模式：在 SOC 允许时，以驱动电机为动力，发动机不参与工作； 助力/并联模式：发动机、驱动电机/助力电机共同驱动车辆； 发动机模式：在发动机工况良好且不需要充电时可以由发动机单独驱动； 智能充电模式：当发动机效率较低且 SOC 允许时，为提高效率可以在发动机驱动时让发电电机发电； 串联模式：在 SOC 较低时，由于低车速输入轴和发动机的速差较大，需要通过发动机带动发电电机发电，并由驱动电机驱动车辆； 滑行模式：当车速较高时，驾驶员松开油门，发动机进入断油状态，车辆滑行减速，如果 SOC 太低，在保证减加速度值不超过限值时可以通过驱动电机发电进行能量回收，C1 离合器的状态和 SOC 关联； 制动能量回收模式：一定车速下，驾驶员有制动需求时，通过驱动电机进行能量回收，C1 离合器的状态和 SOC 关联；
能量管理	车辆运行时依据电池的参数和实际工况，实现能量的管理；
驾驶员意图解释	对加速踏板信号进行解释； 对制动踏板信号进行解释； 对驾驶模式开关信号进行解释； 从 CAN 信号获取换挡杆的信号；
扭矩分配与驾驶性	将驾驶员的扭矩需求根据不同工况分配给发动机、驱动电机或助力电机； 通过对扭矩的闭环控制和平滑处理提高驾驶性； 通过扭矩监控逻辑提高安全性；
扭矩干预	响应 ESP 的扭矩干预； 换挡时对发动机和电机扭矩实现干预； 提供动力系统输出扭矩支持 EPB 自动释放功能；
换挡 map 及换挡控制	制定换挡 map； 根据驾驶员意图实现档位控制； 根据实际工况实现档位控制；
离合器控制	根据实际工况实现离合器的控制；
巡航控制	当车身控制器单元读取到驾驶员的指令后将指令通过 CAN 发送给本控制单元，实现巡航的禁用、使能、挂起、车速设定等。在检测到制动踏板信号时挂起；
液压系统压力管理	根据蓄能器压力调节油泵电机的转速，维持合理的压力区间；
信号输入与输出	物理输入信号采集、转换； 物理输出信号转换、驱动； CAN 信号处理模块；
附件管理	电空调能量协调管理； 发动机除霜除雾需求管理； 辅助发动机自学习及碳罐管理； 辅助电机自学习管理；

续表

功能	描述
诊断管理与安全	根据发动机控制单元发送的故障信息制定相应策略； 根据电机控制单元（含 DCDC）发送的故障信息制定相应策略； 根据电池管理系统发送的故障信息制定相应策略； 根据车身其它控制单元发送的故障信息制定相应策略； 实现机电复合传动系统控制单元硬件故障诊断及处理； 实现机电复合传动系统各传感器的故障诊断和处理； 实现油泵电机的故障诊断和处理； 实现电磁阀的故障诊断和处理； 实现 CAN 通讯模块的故障诊断和处理； 车辆碰撞后限制扭矩需求为零；

为了更好的讨论系统功能，需要对系统进行一定的假设，见表 3.2。

表 3.2 系统假设

假设	描述
能量回收为全制动能量回收	当制动时优先采用电机回收能量，机械制动只在系统无法回收能量时介入
采用电子稳定系统（ESP）	机电复合传动控制单元需要响应 ESP 的扭矩干预，如：禁止换挡、快速升扭矩、快速降扭矩
倒车时禁止能量回收	由于倒车时的车速一般很低，可回收的能量有限
倒车时使用驱动电机驱动	由于本系统没有单独的倒档，倒车只能通过驱动电机的反转实现
车辆为前轮驱动	拖车救援及车辆维护时需注意
系统以外的功能全部正常	机电复合传动控制系统外的所有系统功能正常

3.2 传动控制系统危害分析

通过对已知车辆危害的识别，筛选出和控制系统相关的危害[28]，见表 3.3。

表 3.3 危害识别

危害类型	危害	危害描述
电的	直接接触带电部件导致触电	直接或间接接触到带电的高压部件。电器通过空气产生电弧放电，导致人员伤害。满足 GB/T 18384-2001，由于篇幅的限制，本论文不对相关的内容展开讨论[29,30,31]
	非直接接触带电部件导致触电	
	电弧放电触电	
	电磁辐射对医学部件的危害	由于驱动电机等大功率部件的电磁辐射对特定的人员造成的伤害，如带心脏起搏器的人员。满足 GB/T 18387-2013，由于篇幅的限制，本论文不对相关内容展开讨论[32]
	电气过载起火	例如负载存在故障，发热起火
	短路烧毁起火	例如线束出现短路，过流发热起火
热的	高压电池热损坏	不属于本论文的讨论范围
	热源辐射烧毁	
化学的	有害气体/液体释放	
	可燃物质释放起火	
功能的	非预期车辆加速	错误的扭矩被传递到轮端，导致车辆持续一定时间的非预期加速
	非预期车辆减速	错误的扭矩被传递到轮端，导致车辆持续一定时间的非预期减速
	停止或低速下非预期车辆加速	错误的扭矩被传递到轮端，导致车辆持续一定时间的非预期加速
	非预期的可接触部件旋转	维修时，错误的扭矩被传递到发动机，导致维修人员伤害
	驾驶员无法看清周边环境及道路	有除霜除雾需求时无法起动发动机
	失去转向能力或转向过度	不属于机电复合传动控制系统的讨论范围
	失去制动能力	
	失去提醒其他交通参与者的能力	
	倒车雷达和影像失效	

危害事件用 ASIL 来分类，分成 A、B、C、D 四类，最低级危害为 ASIL A，最高级危害为 ASIL D。除以上四类危害事件之外的为 QM，它表示该功能不是一个安全关键功能。当确定了某个危害事件的暴露度、严重度和可控度这三个方面的程度后，就可通过表 3.4 查出该危害的 ASIL 等级。暴露度是指危害事件的暴露程度；严重度是指相关项的故障行为产生的后果。可控度是指驾驶员或其它潜在处于风险的人员能够充分控制危害事件以避免特定伤害的能力，即对事故的预防行为。

表 3.4 ASIL 确定表

严重度	暴露度	可控度		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

结合表 3.3 筛选出的和机电复合传动控制系统相关的危害和表 3.1 的相关项进一步分析得到危害事件、危害事件等级、安全目标、安全状态、安全需求。本文简化了分析过程[33]，结果见表 3.5。

表 3.5 危害事件分析

危害事件	ASIL	安全目标	安全状态	描述
与前方车辆剧烈碰撞	C	避免因为非预期车辆加速导致与前方车辆剧烈碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
与前方车辆碰撞	B	避免因为非预期车辆加速导致与前方车辆碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C2
与前方车辆轻微碰撞	QM	-	-	S1、E4、C1
与后方车辆剧烈碰撞（反向）	C	避免因为非预期车辆加速导致与后方车辆剧烈碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
与后方车辆剧烈碰撞	C	避免因为非预期车辆减速导致与后方车辆剧烈碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
与后方车辆碰撞（反向）	B	避免因为非预期车辆加速导致与后方车辆碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C2
与后方车辆碰撞	B	避免因为非预期车辆减速导致与后方车辆碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C2
与后方车辆轻微碰撞（反向）	QM	-	-	S1、E4、C1
与后方车辆轻微碰撞	QM	-	-	S1、E4、C1
剧烈碰撞前方行人	C	避免因为非预期车辆加速导致剧烈碰撞前方行人	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
碰撞前方行人	B	避免因为非预期车辆加速导致碰撞前方行人	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C1

续表

危害事件	ASIL	安全目标	安全状态	描述
轻微碰撞前方行人	A	避免因为非预期车辆加速导致轻微碰撞前方行人	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C1
剧烈碰撞后方行人（反向）	C	避免因为非预期车辆加速导致剧烈碰撞后方行人	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
碰撞后方行人（反向）	B	避免因为非预期车辆加速导致碰撞后方行人	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C1
轻微碰撞后方行人（反向）	A	避免因为非预期车辆加速导致轻微撞后方行人	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C1
与前方设施剧烈碰撞	C	避免因为非预期车辆加速导致与前方设施剧烈碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
与前方设施碰撞	A	避免因为非预期车辆加速导致与前方设施碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C2
与前方设施轻微碰撞	QM	-	-	S1、E4、C1
与后方设施剧烈碰撞（反向）	C	避免因为非预期车辆加速导致与后方设施剧烈碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E4、C2
与后方设施碰撞（反向）	A	避免因为非预期车辆加速导致与后方设施碰撞	输出扭矩为 0，发出故障灯、警示灯点亮请求	S2、E4、C2
与后方设施轻微碰撞（反向）	QM	-	-	S1、E4、C1
车辆快速起火并爆炸	A	避免车辆快速起火爆炸	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E1、C3
车辆快速起火	A	避免车辆快速起火	输出扭矩为 0，发出故障灯、警示灯点亮请求	S3、E1、C3
车辆有异味或缓慢起火	QM	-	-	S3、E1、C1
发动机旋转伤人	QM	-	-	S3、E1、C1
无法除霜除雾	QM	-	-	S1、E3、C1

以上分析将危害事件按照危害发生的剧烈程度进行区分，替代了复杂的情景分析。例如，不管车辆在什么天气、道路、交通状况下行驶，只要是与前方车辆碰撞的危害事件，可以归结为剧烈、一般、轻微三种程度，这一方法可以极大地简化情景分析的过程，可以快速的得到危害事件及其等级。

3.3 传动控制系统功能安全需求

一个典型的车辆驱动过程为：加速踏板-加速踏板位置传感器-线束-机电复合传动控制单元-CAN 总线-驱动电机控制单元/发动机控制单元-驱动电机/发动机-变速箱-轮端。

一个典型的车辆制动能量回收的过程为：轮端-变速箱-驱动电机-驱动电机控制单元。

扭矩信号的传递如图 3.2 黑色箭头所示，扭矩的传递路径如图 3.2 红色箭头所示。

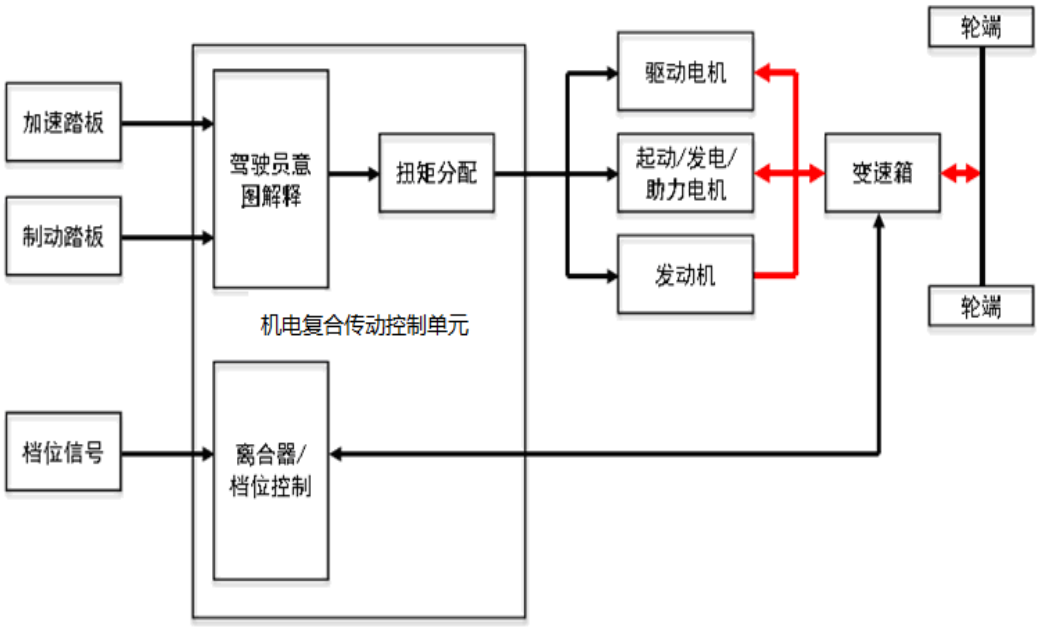

图 3.2 车辆驱动/能量回收示意

以表 3.5 中“避免因为非预期车辆加速导致与前方车辆剧烈碰撞”这一安全目标为例进行分析。车辆出现非预期加速的原因是轮端产生了驾驶员需求扭矩以外的扭矩，从机电复合传动系统和功能安全的范畴考虑，产生这一后果可能是因为：1、加速踏板传感器故障；2、线束故障；3、机电复合传动控制单元硬件故障；4、机电复合传动控制单元软件故障；5、CAN 总线故障；6、电机故障；7、变速箱电气故障；8、制动踏板传感器故障；9、供电系统。

再以表 3.5 中“避免因为非预期车辆加速（反向）或减速导致与后方车辆剧烈碰撞”为例进行分析。车辆出现非预期加速（反向）的原因是轮端产生了驾驶员需求扭矩以外的扭矩，或轮端扭矩小于驾驶员的需求扭矩，产生这一后果可能是因为：1、加速踏板传感器故障；2、线束故障；3、机电复合传动控制单元硬件故障；4、机电复合传动控制单元软件故障；5、CAN 总线故障；6、电机故障；7、变速箱电气故障；8、制动踏板传感器故障；9、供电系统。

再以表 3.5 中“避免传动系统快速起火爆炸”为例进行分析，传动系统快速起火的原因是部件过热起火并引燃了易燃易爆的物品，产生的原因可能是因为：1、线束故障；2、机电复合传动控制单元硬件故障；3、机电复合传动控制单元软件故障；4、电机故障；5、变速箱电气故障；9、供电系统。

进一步分析变速箱电气故障，其中对扭矩产生影响的部件有：电磁阀、油泵电机、油压传感器、位置传感器、转速传感器。

通过对表 3.5 中的每一个安全目标进行分析后，提炼组合得到表 3.6 的功能安全需求列表，这些需求可以用于系统功能安全设计[34]。

表 3.6 功能安全需求

序号	需求	ASIL	状态
1	机电复合传动系统低压供电功能必须满足功能安全	C	接受
2	机电复合传动系统电气连接功能必须满足功能安全	C	接受
3	机电复合传动系统扭矩的 CAN 通讯功能必须满足功能安全	C	接受
4	机电复合传动系统的扭矩需求的解析功能必须满足功能安全	C	接受
5	机电复合传动系统的扭矩分配功能必须满足功能安全	C	接受
6	机电复合传动系统的电机驱动功能必须满足功能安全	C	接受
7	机电复合传动系统的电机发电功能必须满足功能安全	C	接受
8	机电复合传动系统的扭矩传递功能必须满足功能安全	C	接受
9	机电复合传动系统的制动需求解析功能必须满足功能安全	C	接受

关于其它功能安全相关的需求分析，可以分析表 3.2 中的系统假设。可见在 ESP 发出扭矩干预的请求时需要机电复合传动控制单元的响应。外部的功能安全需求见表 3.7。

表 3.7 外部功能安全需求

序号	需求	ASIL	状态
1	机电复合传动系统响应 ESP 的功能必须满足功能安全	C	接受

接受的理由是，外部的扭矩请求对于机电复合传动控制单元来说只是扭矩来源的差别，可以将这个需求的功能安全分析和表 3.6 的需求合并。其原因和巡航功能的安全需求被分解到表 3.6 的需求是一样的，差别在于驾驶员的扭矩需求是通过加速踏板输入的，而 ESP 的扭矩干预和巡航功能的扭矩需求是通过 CAN 总线输入的，其功能安全可以归结为 CAN 通讯的功能安全。

3.4 传动控制系统非功能安全需求

传动控制系统主要由机电复合传动控制单元、供电系统、驾驶员意图采集（如加速踏板传感器、制动踏板传感器、模式开关）、变速箱信号采集（如油压传感器、油温传感器、输入轴转速传感器、输出轴转速传感器、档位位置传感器）、变速箱执行机构（如油泵电机、C1 电磁阀、C2 电磁阀、安全压力阀、换挡流量控制阀、换挡压力控制阀）、CAN 通讯总线组成[26,27]。

1、电源

混合动力车辆的低压供电系统一般由 DC/DC、蓄电池、电缆、保险丝、整车线束、负载、接地组成。

控制单元作为机电复合传动控制系统中的控制中枢，系统内部的负载均由控制单元提供电源，控制单元应至少提供两个引脚用于电源，每个引脚可以压接 $2mm^2$ 的导线，这样一方面可以分担较大的电流负荷，另一方面在一个引脚失效的时候，控制单元可以降低负荷运行，避免系统失效。控制单元在下电后消耗的电流应小于 1mA。控制单元的供电模式见表 3.8。

表 3.8 控制单元供电模式

模式	电压范围（V）	注释
工作电压	9-16	控制单元的所有功能应正常
额定电压	13.5	DC/DC 正常工作时的电压，控制单元的所有功能应正常
过低电压	6-8.5	控制单元关闭大功率负载，其他功能正常，记录电压低故障
过高电压	16.5-18	控制单元关闭大功率负载，其他功能正常，记录电压高故障
起动电压	18-24	1 分钟内控制单元无损坏，关闭大功率负载，其他功能正常，记录电压高故障
抛负载电压	<32	10 秒钟内控制单元无损坏，关闭大功率负载，其他功能正常，不记录电压高故障
反向电压	-14	控制单元无损坏

2、接地

控制单元应至少提供三个引脚用于接地，每个引脚可以压接 $2mm^2$ 的导线，这样一方面可以分担较大的电流负荷，另一方面在一个引脚失效的时候，控制单元可以降低负荷运行，避免系统失效。地偏移应小于正负 0.5V，接地电阻应小于 15mΩ。

3、传感器供电

控制单元应提供两路独立的 9V 电源为速度传感器供电，接地同样独立。电压精度达到正负 0.15V,每路应提供大于 20mA 的电流。控制器唤醒时电源使能。电源可以通过处理器独立控制开闭。

控制单元应提供三路独立的 5V 电源为传感器供电，接地同样独立。电压精度达到正负 0.15V，每路应提供大于 90mA 的电流。控制器唤醒时电源使能。电源可以通过处理器独立控制开闭。

4、油温传感器信号输入

控制单元应提供一路 12 位分辨率的模拟量输入采集油温传感器信号，传感器的电阻值范围为 $56<R_S<55000\Omega$，消耗电流小于 2mA。

5、油压传感器信号输入

控制单元应提供一路 12 位分辨率的模拟量输入采集油压传感器信号，传感器的输出电压值范围为 $0<V_O<5$ V，5V 供电，消耗电流小于 2mA。

6、制动踏板位置传感器信号输入

控制单元应提供一路 12 位分辨率的模拟量输入，采集制动踏板位置传感器信号，传感器的输出电压值范围为 $0<V_O<5$ V，5V 供电，消耗电流小于 6mA。

7、加速踏板位置传感器信号输入

控制单元应提供两路 12 位分辨率的模拟量输入，采集加速踏板位置传感器信号，传感器 1 的输出电压值范围为 $1<V_{O1}<4.5$V，传感器 2 的输出电压值范围为 $0.5<V_{O2}<2.25$ V，5V 供电，总消耗电流小于 15mA。

8、唤醒和点火继电器信号输入

控制单元应提供两路高有效的数字量输入端口，用以唤醒控制单元，唤醒信号的状态和钥匙的关系见表 3.9。

表 3.9 控制单元唤醒模式

唤醒信号	钥匙状态			
	OFF	ACC	RUN	CRANK
唤醒	Low/High（Function Requirement）	High	High	Low
点火继电器	Low/High（Function Requirement）	Low/High（Function Requirement）	High	High

9、模式开关信号输入

控制单元应提供一路高有效地数字量输入端口，用以识别驾驶员的模式切换请求。开关为触发式，常按无效。

10、制动踏板开关信号输入

控制单元应提供一路高有效地数字量输入端口，用以识别制动踏板开关信号。

11、输入/输出轴转速信号输入

控制单元应提供两路可测量 PWM 频率信号的输入，霍尔转速传感器的输出频率小于 12kHz，9V 供电，每路消耗电流小于 20mA。

12、位置传感器信号输入

控制单元应提供一路可测量 PWM 信号占空比的输入，位置传感器的输出频率为 1kHz，5V 供电，占空比范围为 10%-90%（0-25mm），消耗电流小于 20mA。

13、电磁阀高边驱动

设计电磁阀高边驱动的目的是在低边驱动发生故障时可以可靠的关闭电磁阀，为了节约成本，电磁阀可以共用高边驱动，所以控制单元应至少提供三路高边驱动，控制安全压力阀、换挡压力阀/C2 压力阀、换挡流量阀/C1 压力阀的高边，每路应提供大于 3A 的电流并且可以通过处理器独立控制开闭。

14、电磁阀低边驱动

控制单元应提供五路低边驱动，控制安全压力阀、换挡压力阀、C2 压力阀、换挡流量阀、C1 压力阀的低边，每路应提供大于 1.5A 的电流并且可以通过处理器独立控制开闭。

15、油泵电机驱动

控制单元应提供无刷直流电机的三相控制驱动，电机的额定电压 13.5V，额定电流小于 15A，最大电流小于 50A，最大电流持续时间小于 200mS，最大转速小于 3500rpm。

16、霍尔位置传感器输入

控制单元应提供三路可测量 PWM 频率信号的输入，霍尔位置传感器的输出频率小于 60Hz，5V 供电，每路消耗电流小于 20mA。

17、CAN 总线

为了最大限度的不改变整车信号，并保证总线的负载率不超出合理范围。控制单元应提供两路高速 CAN 总线接口，总线速率为 500kbps。

非安全相关的系统原理如图 3.3 所示。

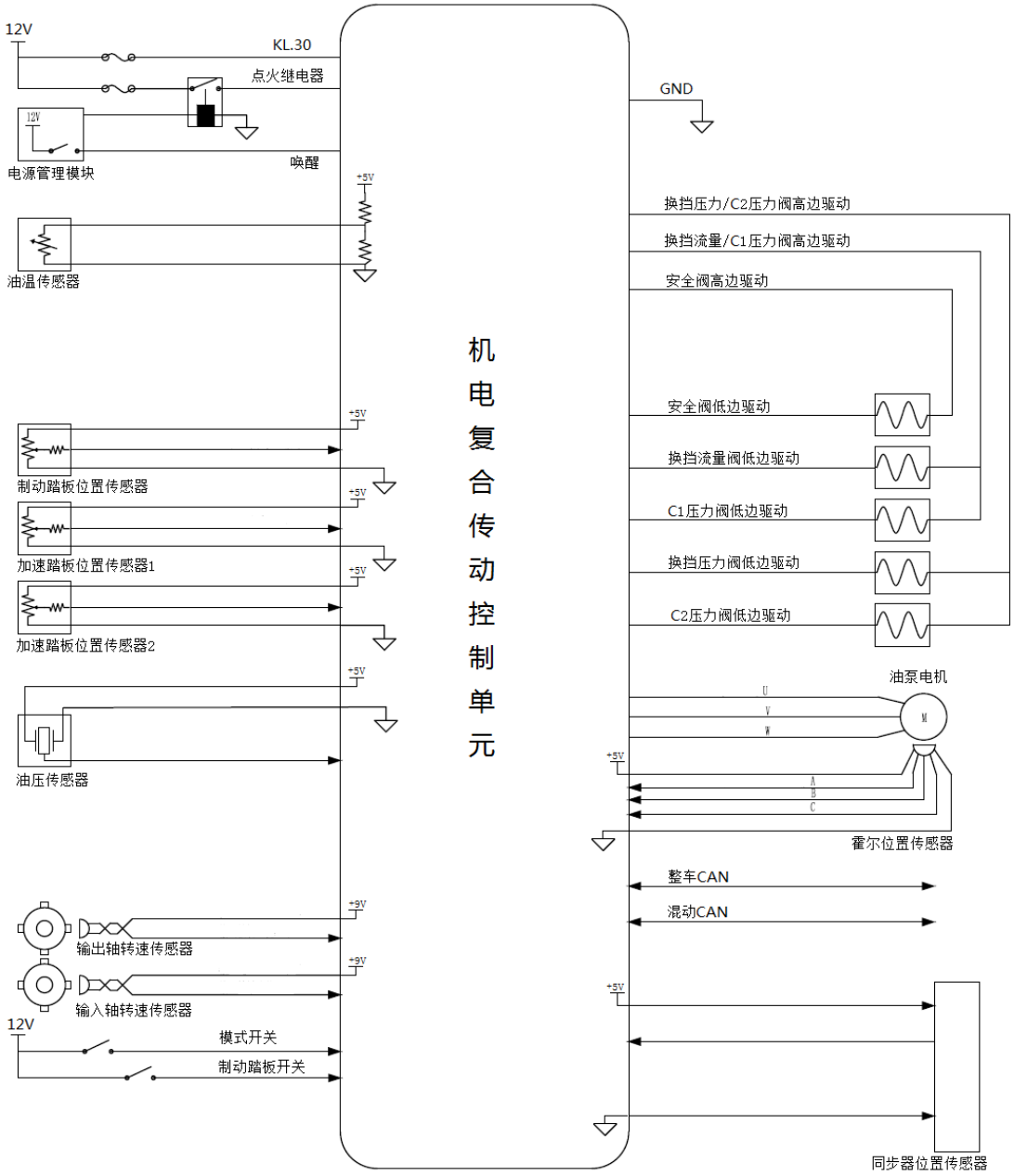

图 3.3 机电复合传动控制系统

3.5 本章小结

本章说明了一种机电复合传动控制系统的结构和功能列表，通过对已知车辆危害的识别和分析，筛选出与研究对象相关的危害事件，运用功能安全的方法分析危害事件，制定了所有功能安全相关和非功能安全相关的系统需求。

第 4 章 机电复合传动控制系统功能安全设计

系统功能安全设计主要包括技术安全需求规范、功能安全系统设计、功能安全硬件设计。技术安全需求规范的目标是基于功能安全需求，定义相应的技术安全需求；功能安全系统设计的目标是设计符合技术安全规范的技术安全概念和系统；功能安全硬件设计则对控制单元内部的关键电路进行研究并提出设计方案。

4.1 技术安全需求

将功能安全需求用功能安全的方法逐条分析，如安全机制分析、避免潜在故障分析，最终完成技术安全需求规范。

为了简化分析过程且不违反功能安全的要求，假设和功能安全需求相关的部件都继承了需求的 ASIL 等级。例如和“机电复合传动系统的扭矩传递功能”相关的部件的 ASIL 等级均为 C，安全机制的安全等级为 ASIL A。

1、低压供电功能安全

假设相关项以外的功能全部正常，因此对于机电复合传动控制系统的低压供电我们只需要分析控制单元的低压供电功能安全[35,36]。

控制单元的低压供电功能的失效可以分为：内部电源芯片失效、内部供电电路失效[34]；

对应的安全机制为：a、监控蓄电池电压，当电压超出 9-16V 的正常范围时，发出点亮蓄电池故障灯请求以提醒驾驶员，当电压超出 6-24V 的工作范围时，系统进入安全状态并关闭电源芯片；b、监控电路监控电源芯片的输出电压，当电压超出正常范围时，系统进入安全状态并关闭电源芯片；c、监控在上电、下电、运行时实施，故障响应时间小于 20ms（任务时间为 10ms）；由表 3.4 可知供电功能相关的安全状态为“输出扭矩为 0，发出故障灯、警示灯点亮请求”和“传动系统不会快速起火”，关闭电源芯片可以防止电路过流发热，确保传动系统不会快速起火，关闭的方法有：主动关闭（如数据接口和硬线使能）和被动关闭（蓄电池电压过低）。对于主动关闭则可以在关闭前进入安全状态“控制输出扭矩为 0 并发出故障灯、警示灯点亮请求”；对于被动关闭则控制单元来不及控制输出扭矩和发送请求，需要外部相关项的安全机制进入安全状态，详见 3 的描述。

对于如何避免多点故障的潜伏，需要对安全机制的硬件随机失效进行分析，以上所有的安全机制均是基于 CPU 没有失效的前提，为了避免多点故障的潜伏，需要增加看门狗监控 CPU，当探测到 CPU 故障时，复位 CPU，此时 CAN 发送中断。或者需要一个完全独立的从 CPU 及运行环境，对主 CPU、蓄电池电压和电源芯片输出电压的监控机制（使用独立的监控电路）。当监控到故障时，从 CPU 关闭 CAN 发送功能。上述安全机制还可以通过使用双核或以上的处理器来实现，核 0 为主处理器，核 1 除了承担部分的运算任务外，还可以与核 0 互相监控。

2、电气连接功能安全

机电复合传动系统各部件的电气连接功能由整车线束、传动系统线束、各部件接插件组成。机电复合传动控制系统中除了供电（含接地）、加速踏板、制动踏板、CAN 总线的电气连接功能由整车线束完成外，其它的传感器和执行器的连接由传动系统线束完成，假设系统以外的功能全部正常，因此对于机电复合传动控制系统的电气连接我们只需要分析传动系统线束、传动系统各部件接插件的功能安全。

传动系统线束和接插件的失效可以分为：连接断路、连接短路、连接断续。其中连接短路又可以分为：信号对电源短路、信号对地短路、信号间短路、电源对地短路[34]。

安全机制为：a、系统的接插件带自锁装置；b、系统的接插件具有防错插的功能；c、系统的接插件满足 IP6K9K 的要求；d、系统线束满足环境温度规范；e、系统线束满足震动规范；f、除电源和地以外的导线发生短路时其电流被限制在电路设计电流以下。安全机制 a、b、c、d、e 将有效地降低断路、短路、断续等随机硬件失效的概率，在后续的分析中将进一步讨论。

电气连接功能相关的安全状态为“输出扭矩为 0，发出故障灯、警示灯点亮请求”和“传动系统不会快速起火”，安全机制 f，可以防止电路过流发热，确保传动系统不会快速起火。故障响应时间小于 1ms。

由于电气连接功能是为了实现其它功能而产生，探测多点故障潜伏的安全机制可以在讨论其它功能安全需求时进行分析，例如探测电源对地短路多点故障潜伏的安全机制已包含在 1 中[27]。

3、扭矩相关的通讯功能安全

CAN 通讯是一个网络，其硬件和底层软件的设计需要遵循 ISO11898 和 Bosch CAN2.0 的标准，业界一般认为满足标准的设计为 ASIL QM。为了达到 ASIL C 的安全等级，需要更多的安全机制。

信号的最小传输单位为信号帧，每一个连接到 CAN 总线的通道为一个节点，总线上可以有多个节点。从应用层来说，CAN 通讯功能的失效分为：信号帧丢

失、节点丢失、总线关闭、帧数据错误或数据过时。

对应的安全机制为：a、接收节点探测到含扭矩和警示灯点亮请求的信号帧丢失后，开始计时，过程中如果帧恢复，则停止计时并复位计时器，当计时达到一个标定值后（故障响应时间），默认收到的扭矩为 0 并点亮故障灯、警示灯；b、关于节点丢失的安全机制同 a；c、关于总线关闭，传动系统控制单元探测到故障后，开始计时，当计时达到一个标定值后（故障响应时间），由于 CAN 总线关闭故障的最小恢复时间大于 500ms，期间接收节点无法收到任何传动系统控制单元发送的信号，默认收到的扭矩为 0 并点亮故障灯、警示灯；d、采用 Check-sum 和 Rolling-counter 机制，探测数据错误和数据过时故障，当接收节点探测到含扭矩和警示灯点亮请求的信号帧存在 Check-sum 或 Rolling-counter 故障时，开始计时，过程中如果故障恢复，则停止计时并复位计时器，当计时达到一个标定值后（故障响应时间），默认收到的扭矩为 0 并点亮故障灯、警示灯。以上安全机制可以探测 CAN 通讯的多点故障潜伏，覆盖 2 未覆盖的故障[37, 38, 39]。

4、扭矩需求解析功能安全

车辆的扭矩需求来源包含：加速踏板位置信号、巡航功能、ESP 的扭矩干预请求。加速踏板位置传感器将驾驶员的扭矩需求以电压的形式输入机电复合传动控制单元，控制单元将电压信号转换为输出电压和电源电压的百分比，并根据车速查表得到一个扭矩需求值。巡航时控制单元根据当前车速和目标车速计算得到一个扭矩需求值。控制单元收到 ESP 的扭矩干预请求后，计算出一个相应的扭矩结果。

扭矩需求解析功能可能的失效为：加速踏板位置传感器故障、传感器信号采样电路故障、CPU 硬件故障、信号转换和扭矩算法故障[34]；

对应的安全机制为：a、监控加速踏板位置传感器的输出信号；b、CPU 硬件的自检和监控；c、用独立的第二种信号转换和扭矩算法监控第一种算法；d、监控在上电、下电、运行时实施，故障响应时间小于 20ms（任务时间为 10ms）；相关的安全状态为“输出扭矩为 0，发出故障灯、警示灯点亮请求”。

对于如何避免多点故障的潜伏，需要对安全机制的硬件随机失效进行分析，对于上述的安全机制 a，其无法探测信号值处于合理区间的失效，因此需要一个完全独立的加速踏板位置传感器信号进行，信号的合理性判断，当无法确定任何一路信号的有效性时，输出扭矩为 0 并发出故障灯、警示灯点亮请求，故障响应时间为小于 20ms；对于安全机制 b，需要增加看门狗监控 CPU，当探测到 CPU 故障时，复位 CPU，此时 CAN 发送中断。或者需要核 1 对核 0 监控，当监控到故障时，核 1 关闭 CAN 发送功能。对于安全机制 c，需要核 1 用独立的第三种信号转换和扭矩算法监控第二种算法，因此加速踏板位置信号需要输入给核 1，

当探测到核 0 的算法故障时，核 1 关闭 CAN 发送功能。

5、扭矩分配功能安全

扭矩分配功能可能的失效为：CPU 硬件故障、扭矩算法故障[34]；

对应的安全机制为：a、CPU 硬件的自检和监控；b、用独立的第二种扭矩算法监控第一种算法；c、监控在上电、下电、运行时实施，故障响应时间小于 20ms（任务时间为 10ms）；相关的安全状态为“输出扭矩为 0，发出故障灯、警示灯点亮请求”。

对于如何避免多点故障的潜伏，需要对安全机制的硬件随机失效进行分析，对于上述的安全机制 a，需要增加看门狗监控 CPU，当探测到 CPU 故障时，复位 CPU，此时 CAN 发送中断。或者需要核 1 对核 0 监控，当监控到故障时，核 1 关闭 CAN 发送功能。对于安全机制 b，需要核 1 用独立的第三种扭矩算法监控第二种算法，当探测到核 0 的算法故障时，核 1 关闭 CAN 发送功能。

6、电机驱动功能安全

电机驱动功能可能的失效为：电机控制单元故障、电机本体故障[34]；由于电机控制单元的功能安全分析和机电复合传动系统控制单元的分析类似，并且其不属于机电复合传动控制系统，本文不再详细展开，假设其功能正常。电机本体故障又可以分为：扭矩相关故障和非扭矩相关故障。

当机电复合传动控制单元接收到电机扭矩相关的故障，则输出的扭矩为 0 并发出故障灯、警示灯点亮请求。当机电复合传动控制单元探测到含电机扭矩的信号帧丢失后，开始计时，过程中如果帧恢复，则停止计时并复位计时器，当计时达到一个标定值后（故障响应时间），默认输出的扭矩为 0 并发出故障灯、警示灯点亮请求。

7、电机发电功能安全

电机发电功能可能的失效为：电机控制单元故障、电机本体故障；由于电机控制单元的功能安全分析和机电复合传动系统控制单元的分析类似，并且其不属于机电复合传动控制系统，本文不再详细展开，假设其功能正常。电机本体故障又可以分为：扭矩相关故障和非扭矩相关故障。

当机电复合传动控制单元接收到电机扭矩相关的故障，则输出的扭矩为 0 并发出故障灯、警示灯点亮请求。当机电复合传动控制单元探测到含电机扭矩的信号帧丢失后，开始计时，过程中如果帧恢复，则停止计时并复位计时器，当计时达到一个标定值后（故障响应时间），默认输出的扭矩为 0 并发出故障灯、警示灯点亮请求。

在电机发电用于能量回收的情况下，全能量回收功能失效，完全由机械制动提供制动的需求。

8、扭矩传递功能安全

扭矩传递功能可能的失效为：电磁阀故障、电磁阀控制电路故障、油泵电机故障、油泵电机控制电路故障、油压传感器故障、油压传感器信号采样电路故障、位置传感器故障、位置传感器信号采样电路故障、转速传感器故障、转速传感器信号采样电路故障、CPU 硬件故障、变速箱控制算法故障[27,34]；

对应的安全机制为：a、监控电磁阀的状态；b、监控油泵电机的状态；c、监控油压传感器的输出信号；d、监控位置传感器的输出信号；e、监控转速传感器的输出信号；f、CPU 硬件的自检和监控；g、用独立的第二种变速箱控制算法监控第一种算法；h、监控在上电、下电、运行时实施，故障响应时间小于 20ms（任务时间为 10ms）；相关的安全状态为“输出扭矩为 0，发出故障灯、警示灯点亮请求”。

对于如何避免多点故障的潜伏，需要对安全机制的硬件随机失效进行分析，对于上述的安全机制 c，其无法探测油压信号值处于合理区间的失效，因此需要结合油泵电机的运行状态和算法，进行信号的合理性判断；对于安全机制 e，其无法探测转速信号值处于合理区间的失效，因此需要结合车速信号或电机转速信号和算法，进行信号的合理性判断；对于安全机制 d，其无法探测位置信号值处于合理区间的失效，因此需要独立的位置传感器信号，进行信号的合理性判断；当确定上述故障时，输出扭矩为 0 并发出故障灯、警示灯点亮请求，故障响应时间为小于 20ms；对于安全机制 a，b，f，需要增加看门狗监控 CPU，当探测到 CPU 故障时，复位 CPU，此时 CAN 发送中断。或者需要核 1 对核 0 监控，当探测到核 0、电磁阀或油泵电机的故障时，核 1 关闭 CAN 发送功能。对于安全机制 g，需要核 1 用独立的第三种信号转换和扭矩算法监控第二种算法，因此加速踏板位置信号需要输入给核 1，当探测到核 0 的算法故障时，核 1 关闭 CAN 发送功能。

9、制动需求解析功能安全

制动需求解析功能可能的失效为：制动踏板开关、开关信号采样电路故障、CPU 硬件故障、开关信号算法故障[27,34]；

对应的安全机制为：a、CPU 硬件的自检和监控；b、用独立的第二种信号算法监控第一种算法；c、监控在上电、下电、运行时实施，故障响应时间小于 20ms（任务时间为 10ms）；相关的安全状态为“输出扭矩为 0，发出故障灯、警示灯点亮请求”。

对于如何避免多点故障的潜伏，需要对安全机制的硬件随机失效进行分析，上述的安全机制无法探测制动踏板开关及其采样电路的失效，因此需要另外一个有效值相反的开关信号或一个模拟信号，进行信号的合理性判断，当两路信号值

不一致时，输出扭矩为 0 并发出故障灯、警示灯点亮请求，故障响应时间为小于 20ms；对于安全机制 a，需要增加看门狗监控 CPU，当探测到 CPU 故障时，复位 CPU，此时 CAN 发送中断。或者需要核 1 对核 0 监控，当探测到核 0 故障时，核 1 关闭 CAN 发送功能。对于安全机制 b，需要核 1 用独立的第三种信号算法监控第二种算法，因此制动踏板位置信号需要输入给核 1，当探测到核 0 的算法故障时，核 1 关闭 CAN 发送功能。由于制动踏板开关没有被有效的诊断覆盖，为了不违反安全目标，可将制动踏板位置传感器的 ASIL 等级定义为 C，并增加安全机制探测其失效。

4.2 容错时间间隔

容错时间间隔是指：从故障发生到系统进入安全状态的时间间隔[11]。

对于安全机制“传动系统不会快速起火”，根据工程经验，其容错时间间隔为 100ms。

对于安全机制“输出扭矩为 0，发出故障灯、警示灯点亮请求”，假设车重 M=1500kg，发动机+电机的最大扭矩 T_1=400N.m，轮胎半径 r=0.312m，轮端打滑的扭矩为 T_2=2100N.m，一档速比 R=5.8。车辆的加速度为 a(m/s^2)，最高车速为 V(m/s)，容错时间间隔为 t(s)，移动的距离为 S（m）。根据工程经验，当静止的车辆由于非预期的轮端扭矩达到的最高车速小于 1m/s 时，移动距离小于 0.1m 时认为是安全的。这一最高车速小于人的正常行走速度。

$$T_1 \times R > T_2 \tag{4.1}$$

$$a = T_2 \div r \div M \tag{4.2}$$

$$V = a \times t \tag{4.3}$$

加速度 a=4.48m/s^2，达到最高车速 1m/s 所需的时间 t=223ms，因此选取容错时间间隔为 200ms。

$$S = 0.5a \times t \times t \tag{4.4}$$

计算得到车速 V=0.896m/s，小于 1m/s，移动距离 S=0.0896m，小于 0.1m，满足功能安全需求。

4.3 技术安全需求规范

综合以上分析，得到技术安全需求见表 4.1。

表 4.1 中，拒绝需求 6、10、11、13 的原因是这些需求的实现需要超出了本文定义的相关项范围。

表 4.1 技术安全需求规范

序号	技术安全需求	ASIL	状态
1	蓄电池电压超出 6-24V 时，系统进入安全状态并关闭电源芯片	C	接受
2	电源芯片输出电压超出 $Vo_{+/-1V}$ 时（Vo=5V，3V），系统进入安全状态并关闭电源芯片	C	接受
3	监控在上电、下电及运行时实施	C	接受
4	监控到蓄电池电压、电源芯片输出电压及核 0 故障时系统进入安全状态并关闭电源芯片	A	接受
5	核 1 具备独立的运行能力	A	接受
6	电源被动关闭时，系统可以进入安全状态	C	拒绝
7	系统的接插件带自锁装置，有防错插的功能，满足防水防尘的规范	C	接受
8	系统线束满足环境温度规范和震动规范	C	接受
9	电源和地以外的导线短路时电流被限制在设计电流以下	C	接受
10	其它接收节点探测到含扭矩和警示灯点亮请求的信号帧丢失后系统进入安全状态	A	拒绝
11	其它接收节点探测到含扭矩和警示灯点亮请求的节点丢失后系统进入安全状态	A	拒绝
12	传动系统控制单元探测到总线关闭、帧丢失、节点丢失或数据错误、数据过时故障后系统进入安全状态	A	接受
13	其它接收节点探测到数据错误和数据过时故障后系统进入安全状态	A	拒绝
14	探测到 CPU 硬件故障后系统进入安全状态	C	接受
15	探测到加速踏板位置传感器的输出信号故障后系统进入安全状态	C	接受
16	探测到信号转换和扭矩算法故障后系统进入安全状态	C	接受
17	探测到加速踏板位置传感器信号合理性故障后系统进入安全状态	A	接受
18	监控到核 0 的信号转换和扭矩算法故障后系统进入安全状态	A	接受
19	机电复合传动控制单元接收到电机扭矩相关的故障后系统进入安全状态	C	接受
20	探测到电磁阀故障后系统进入安全状态	C	接受
21	探测到油泵电机故障后系统进入安全状态	C	接受
22	探测到油压传感器故障后系统进入安全状态	C	接受
23	探测到位置传感器故障后系统进入安全状态	C	接受
24	探测到转速传感器故障后系统进入安全状态	C	接受
25	探测到油压传感器信号合理性故障后系统进入安全状态	A	接受
26	探测到转速传感器信号合理性故障后系统进入安全状态	A	接受
27	探测到位置传感器信号合理性故障后系统进入安全状态	A	接受
28	监控到电磁阀、油泵电机及核 0 故障时系统进入安全状态	A	接受
29	探测到制动踏板位置传感器故障后系统进入安全状态	C	接受
30	探测到制动踏板信号合理性故障后系统进入安全状态	A	接受
31	传动系统不会快速起火的容错时间间隔为 100ms	C	接受
32	输出扭矩为 0，发出故障灯、警示灯点亮请求的容错时间间隔为 200ms	C	接受

4.4 功能安全系统设计

基于技术安全需求和系统非安全相关的需求开展系统设计。由于非功能安全需求在前面已经讨论过，此处不再赘述。

4.4.1 技术安全概念

进一步分析如何实现技术安全需求可以得到相应的技术安全概念，技术安全概念需要考虑系统设计的可验证（安全机制是可验证的或有第三方提供的安全手册）、技术能力（所有的安全机制都是目前的技术水平可以实现的）、系统集成可

测试（安全机制是可测的）。技术安全概念的分析结果如表 4.2 所示。

表 4.2 技术安全概念

技术安全需求	系统设计	测试方法
1	机电复合传动控制单元通过 A/D 口读取蓄电池电压，诊断软件判断电压超出 6-24V 时，控制系统进入安全状态并通过使能端口关闭电源芯片；	通过硬件在环测试设备调节电池电压超限；
2	机电复合传动控制单元通过 A/D 口读取电源芯片输出电压，诊断软件判断电压超出 $Vo_{+/-1V}$ 时（Vo=5V，3V），控制系统进入安全状态并关闭电源芯片；	通过控制单元的软件模拟电源电压超限；
3	监控软件在上电、下电时调用，运行时实施的调用任务周期为 10ms；	通过控制单元的软件模拟故障；
4	核 1 通过 A/D 口监控蓄电池电压和电源芯片输出电压，其软件判断超出合理范围并且监控到核 0 的故障时，关闭 CAN 通讯并通过使能端口关闭电源芯片；	模拟电池电压超限并使核 0 失能；
5	机电复合传动控制单元为核 1 提供输入信号；	核 0 失效，核 1 能正常工作；
6	--	--
7	系统的接插件带自锁装置，有防错插的功能，满足防水防尘的规范；	通过 DV 试验；
8	系统线束满足环境温度规范和震动规范	通过 DV 试验；
9	机电复合传动控制单元内除电源和地以外的电路短路时，电流被限制在设计电流以下，不会引起电路毁坏；	短路故障注入；
10	--	--
11	--	--
12	机电复合传动系统控制单元探测到总线关闭、帧丢失、节点丢失或数据错误、数据过时故障，控制系统进入安全状态；	CAN 总线故障注入；
13	--	--
14	CPU 自检，探测故障；CPU 硬件复位； 独立的模块（外部看门狗）探测 CPU 故障；CPU 硬件复位；	通过 CPU 供应商的安全手册提供安全证据；
15	通过诊断软件，探测加速踏板位置传感器的输出信号故障，控制系统进入安全状态；	模拟加速踏板位置传感器故障；
16	信号转换和扭矩算法故障探测（一级监控）；独立的软件模块探测信号转换和扭矩算法故障，控制系统进入安全状态；核 0 软件复位（二级监控）；	软件故障注入；
17	通过诊断软件，探测加速踏板位置传感器信号合理性故障，控制系统进入安全状态；	模拟加速踏板位置传感器故障；
18	核 1 监控核 0 的信号转换和扭矩算法故障，关闭 CAN 通讯；（三级监控）；	软件故障注入；
19	机电复合传动控制单元接收到电机扭矩相关的故障，控制系统进入安全状态；	模拟电机故障信号帧；
20	通过诊断软件，探测电磁阀故障，控制系统进入安全状态；	模拟电磁阀故障；
21	通过诊断软件，探测油泵电机故障，控制系统进入安全状态；	模拟油泵电机故障；
22	通过诊断软件，探测油压传感器故障，控制系统进入安全状态；	模拟油压传感器故障；
23	通过诊断软件，探测位置传感器故障，控制系统进入安全状态；	模拟位置传感器故障；
24	通过诊断软件，探测转速传感器故障，控制系统进入安全状态；	模拟转速传感器故障；
25	通过诊断软件，探测油压传感器信号合理性故障，控制系统进入安全状态；	模拟油压传感器合理性故障；
26	通过诊断软件，探测转速传感器信号合理性故障，控制系统进入安全状态；	模拟转速传感器合理性故障；
27	通过诊断软件，探测位置传感器信号合理性故障，控制系统进入安全状态；	模拟位置传感器合理性故障；
28	核 1 监控电磁阀、油泵电机及核 0 故障，关闭 CAN 通讯；	模拟电磁阀、油泵电机故障并使核 0 失能；
29	通过诊断软件，探测制动踏板位置传感器故障，控制系统进入安全状态；	模拟制动踏板位置传感器故障；
30	通过诊断软件，探测制动踏板信号合理性故障，控制系统进入安全状态；	模拟制动踏板位置信号合理性故障；
31	硬件设计的故障响应时间小于 100ms；	故障注入；
32	软件可标定的故障响应时间为小于 200ms；	故障注入；

系统部件与技术安全需求的关系如表 4.3 所示。可见控制单元、电源、CAN 总线、线束是涉及技术安全需求最多的部件，减少它们的失效可以有效地控制整个系统的失效。

表 4.3 技术安全需求与系统部件关系矩阵

技术安全需求	系统部件																	
	机电复合传动控制单元		控制器电源	加速踏板位置传感器	制动踏板位置传感器	输入轴转速传感器	输出轴转速传感器	油压传感器	制动踏板开关	同步器位置传感器	油泵电机	CAN总线	主油压电磁阀	离合器C1电磁阀	离合器C2电磁阀	换挡压力电磁阀	换挡流量电磁阀	线束
	硬件	软件																
1	●	●	●									●						●
2	●	●	●									●						●
3	●	●	●									●						●
4	●	●	●									●						●
5	●		●															●
6																		
7																		●
8																		●
9	●																	
10																		
11																		
12	●	●	●									●						●
13																		
14	●	●	●									●						●
15	●	●	●	●								●						●
16	●	●	●									●						●
17	●	●	●	●								●						●
18	●	●	●									●						●
19	●	●	●									●						●
20	●	●	●									●	●	●	●	●	●	●
21	●	●	●								●	●						●
22	●	●	●					●				●						●
23	●	●	●							●		●						●
24	●	●	●			●	●					●						●
25	●	●	●					●			●	●						●
26	●	●	●			●	●					●						●
27	●	●	●							●		●						●
28	●	●	●								●	●	●	●	●	●	●	●
29	●	●	●		●							●						●
30	●	●	●		●				●			●						●
31	●																	●
32	●	●	●									●						●

4.4.2 系统架构设计约束

所有系统部件都执行了 ASIL C 的技术安全需求，所以部件相应的继承了相关技术安全需求的 ASIL C。系统与外部的接口为：1、供电电源；2、CAN 总线；3、线束；系统部件之间的接口为内部接口，由线束完成。

4.4.3 避免系统失效的方法

系统部件中机电复合传动控制单元、供电电源、CAN 总线、线束和绝大部分的技术安全需求相关，因此避免系统失效首先需要降低这些部件的失效率。

由于供电电源、CAN 总线、线束是系统的外部接口，其他相关项的失效可能通过这些接口引起系统的失效，复用可靠地部件和设计可以有效的避免此类失效。例如：1、使用标准的总线接口：成熟的商业化 CAN 协议软件；2、使用成熟的部件如接插件、控制单元电路设计；3、使用成熟的诊断或探测方法。

系统模块化有助于避免系统失效，例如：1、机电复合传动控制单元为核心模块；2、传感器为输入模块；3、各类执行器为输出模块。

系统简化有助于避免系统失效，例如：1、为了简化外部接口，机电复合传动控制单元作为系统供电的唯一接口；2、机电复合传动控制单元和其他相关项的接口均通过 CAN 总线；3、为了简化内部接口，所有传感器和执行器均连接到机电复合控制单元。

4.4.4 实施时控制随机硬件失效的方法

探测和控制或消除随机硬件失效的方法可参考表 4.2。通过前面的分析可得单点故障度量目标值为≥97%，潜在故障度量目标值为≥80%。

随机硬件失效评估的方法为“随机硬件失效概率度量（PMHF）”。通过前面的分析可得，随机硬件失效目标值为$<10^{-7}h^{-1}$。

4.4.5 分配到硬件和软件

技术安全需求分配到软件的部分由机电复合传动控制单元的 CPU 完成，硬件的部分由机电复合传动控制系统完成。详细的分配参见表 4.3。

4.4.6 硬件-软件接口

结合系统安全和非安全相关的功能需求，评估机电复合传动控制单元的软件规模、运算需求，确定 CPU 的主频、易失性内存（RAM）、非易失性内存（Flash）的需求。

根据总线信号的数据量和传输速率确定 CAN 总线的速率，确定内部总线的类型（SPI、I^2C）。

根据 I/O 需求，确定 A/D 转换通道的数量（信号输入，诊断输入），确定 PWM 输入通道的数量，确定输出端口的数量，确定输入输出电路。

确定操作系统的任务周期，数据一致性方案，系统初始化方案，软件刷新方案，节点是否有网络唤醒功能，内存管理方案，实时计数器方案。

4.5 功能安全硬件设计

1、微处理器模块

微处理器采用英飞凌 Tricore 系列的 TC275，看门狗采用 STM706，芯片的接口设计如图 4.1 所示。

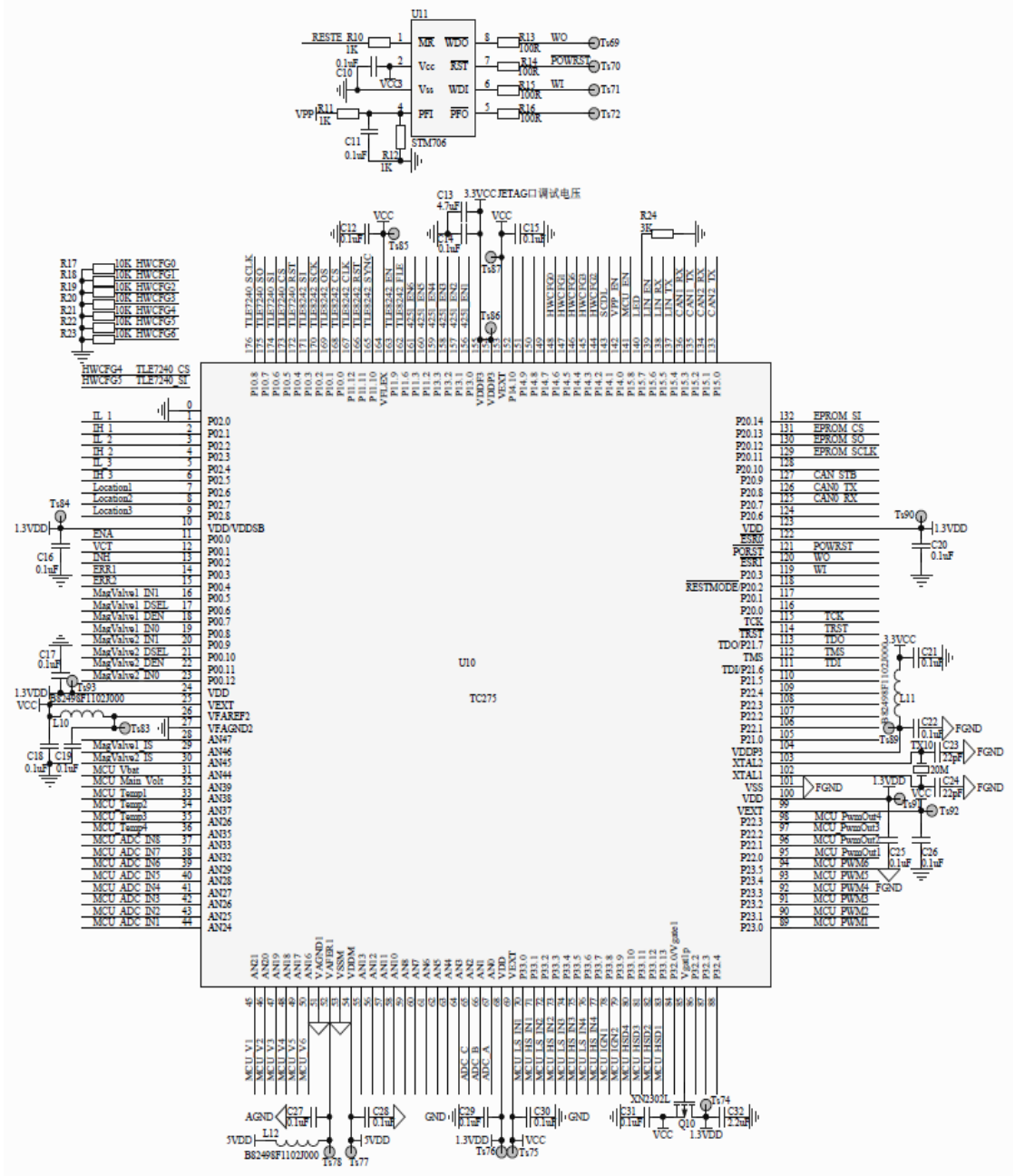

图 4.1 微处理器模块电路原理图

2、电源模块

电源设计分为 12V 电源输入及监控、控制单元唤醒电路、5V 电源输入及监控、9V 电源输出及监控、5V 电源输出及监控。详细设计如图 4.2 所示。

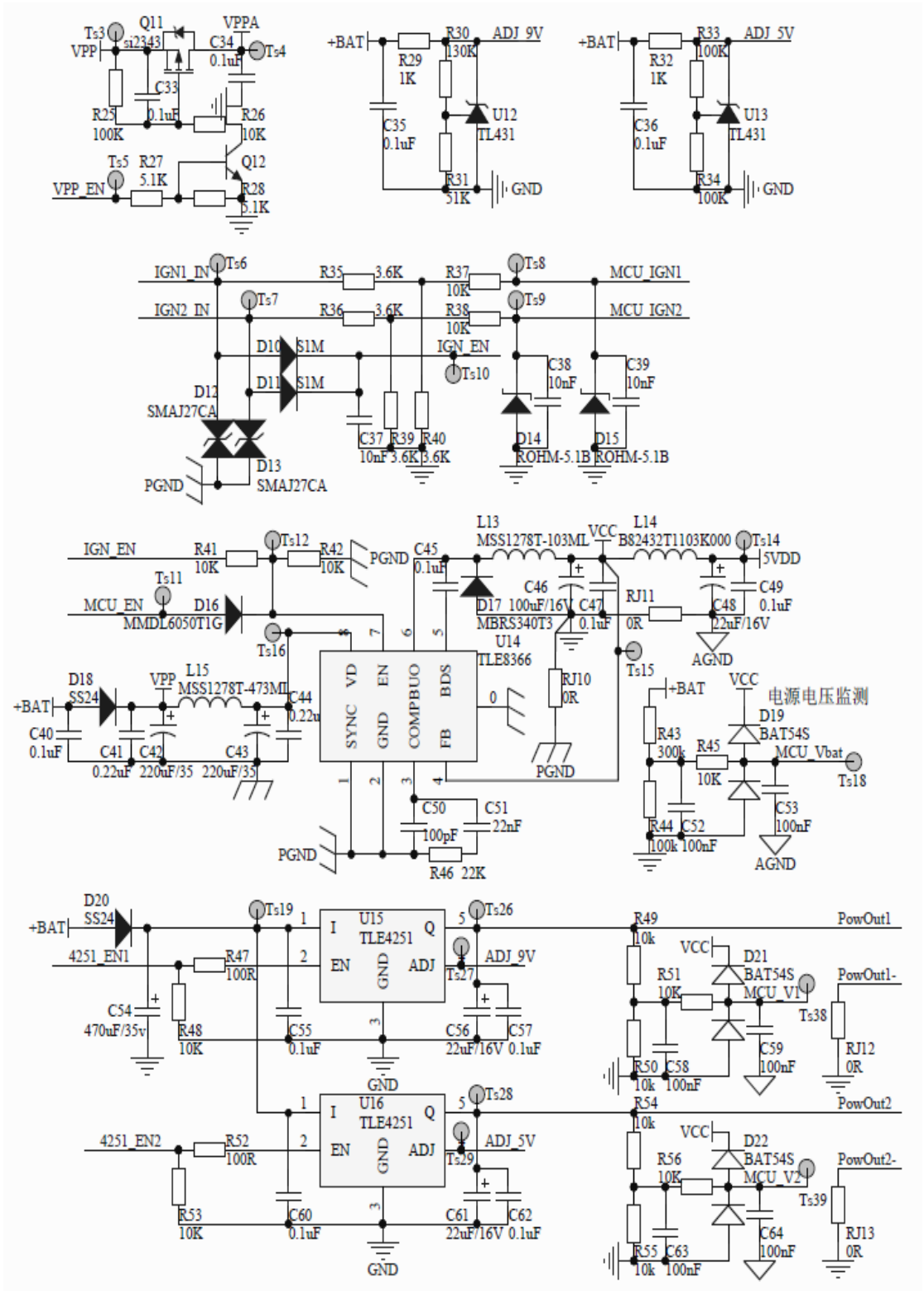

图 4.2 电源模块电路原理图

3、模拟信号采集模块

单路模拟信号采集的电路如图 4.3 所示。

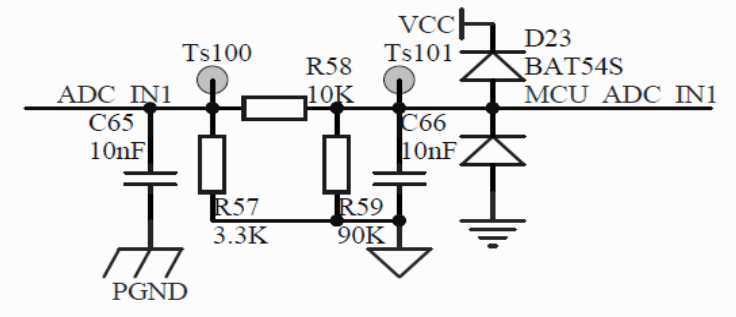

图 4.3 模拟信号采集模块电路原理图

4、电磁阀驱动模块

电磁阀驱动由高边驱动及监控和低边驱动及监控两部分组成，详细设计如图 4.4 所示。

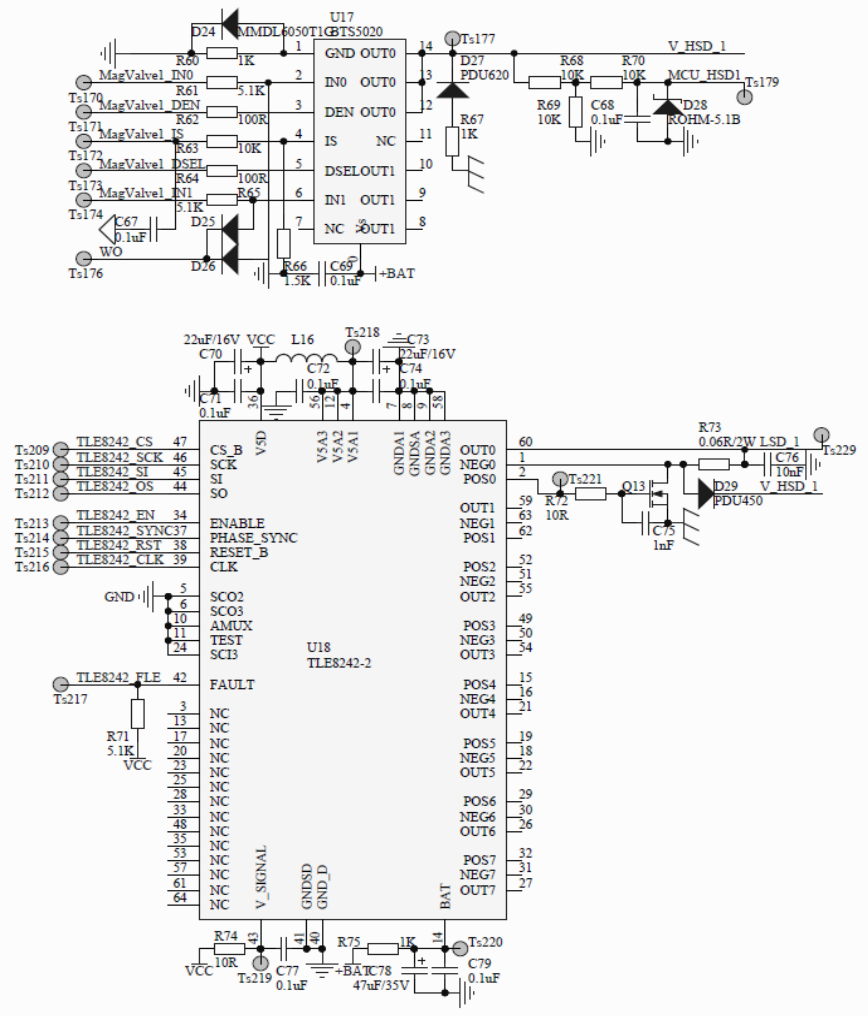

图 4.4 电磁阀驱动模块电路原理图

5、CAN 通讯驱动模块

CAN 通讯驱动模块集成在微处理器中，CAN 驱动电路如图 4.5 所示。

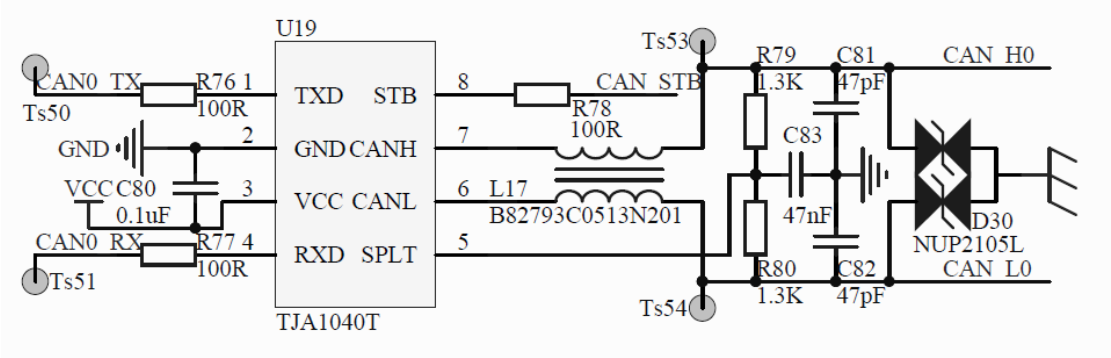

图 4.5 CAN 通讯驱动模块电路原理图

4.6 本章小结

本章通过技术安全需求分析，定义了系统的 ASIL 等级。通过技术安全概念分析，定义了系统的实现方法。定义了实现系统功能安全设计目标的评估指标：单点故障度量目标值为≥97%，潜在故障度量目标值为≥80%，随机硬件失效目标值为$<10^{-7}h^{-1}$。最后按照需求设计了控制单元的微处理器、电源、模拟信号采集、电磁阀驱动、CAN 通讯驱动的电路原理图。

第 5 章 控制单元硬件功能安全分析

控制单元硬件功能安全分析主要包括硬件安全需求分析、估算硬件架构度量、估算随机硬件失效概率度量、控制单元集成测试。硬件安全需求分析的目标是基于技术安全需求，细化相应的硬件安全需求；估算硬件架构度量的目标是评估相关项的架构应付随机硬件失效的效力；估算随机硬件失效概率度量的目标是评估违反安全目标的残余风险是否足够低。控制单元集成测试完成硬件在环测试台架的搭建，创建测试用例，完成测试报告。

5.1 硬件功能安全需求

将机电复合传动控制系统的通用硬件模块化分类后得到图 5.1 所示的示意图。当前的处理器单元一般集成了 RAM 和 ROM，所以将 D.5 RAM 和 D.6 ROM 合并到 D.4 中。

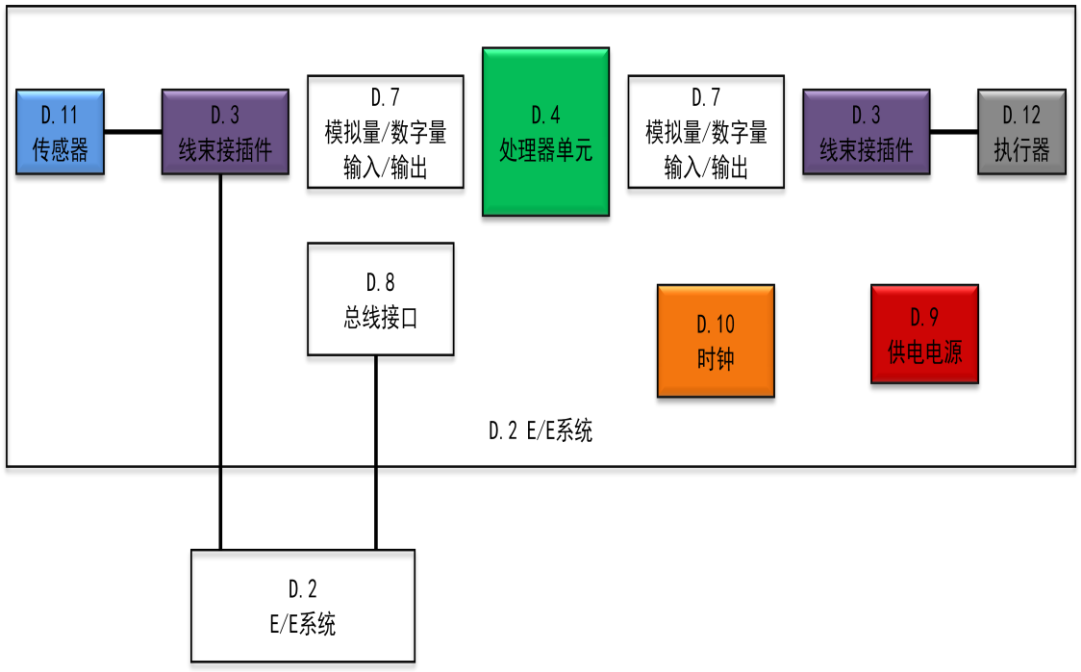

图 5.1 系统通用硬件示意

结合表 4.2，机电复合传动控制系统可选的安全机制/方法、技术目标和硬件技术的典型诊断覆盖率详见表 5.1[40]。其中涉及的由软件实现的安全机制/方法不在本论文讨论范围内。

表 5.1 硬件技术诊断覆盖率

技术安全需求	安全机制/方法	目标	典型诊断覆盖率
1	监控输入电压	探测输入电压值的错误表现	60%
2	监控输入电压	探测输入电压值的错误表现	60%
3	分配到软件设计	--	--
4	监控输入电压	探测输入电压值的错误表现	60%
5	硬件冗余	通过比较两个处理器产生的内部或外部结果，探测处理单元的失效	99%
6	--	--	--
7	结构设计保护	--	--
8	结构设计保护	--	--
9	电路设计保护	--	--
10	--	--	--
11	--	--	--
12	综合信号冗余、帧计数器、超时监控、发送信息回读	探测总线通讯失效、 探测帧丢失、 探测发送节点和接收节点间的数据丢失、 探测总线通讯失效	99%
13	--	--	--
14	CPU 硬件支持下的自检 配置寄存器测试 整体硬件一致性监控 非易失性存储器 易失性存储器 WD 看门狗	通过处理器内部的硬件加快失效探测的速度和扩展探测范围，探测处理单元和其他部件的失效、 探测处理器内部配置寄存器的失效、 探测处理器内部的非法条件、 探测非易失性存储器的信息失效、 探测易失性存储器的信息失效、 监控程序次序的行为和合理性	90% 99% 99% 99% 99% 90%
15	传感器信号有效范围	探测传感器对地、对电源和开路	60%
16	软件多样化冗余	通过动态软件比较探测处理器失效	99%
17	传感器相互关系	用冗余的传感器探测传感器信号在合理范围内的漂移、偏离	99%
18	硬件冗余	通过比较两个处理器产生的内部或外部结果，探测处理单元的失效	99%
19	分配到软件设计	--	--
20	监控输出 监控	探测外部影响失效，时钟失效地址失效，渐变失效，瞬时失效、 探测执行器的错误运行	99% 99%
21	传感器合理性 测试模式 监控	探测传感器对地、对电源和开路、探测静态失效和窜扰、 探测执行器的错误运行	90% 99% 99%
22	传感器信号有效范围	探测传感器对地、对电源和开路	60%
23	传感器信号有效范围	探测传感器对地、对电源和开路	60%
24	传感器信号有效范围	探测传感器对地、对电源和开路	60%
25	测试模式	测静态失效和窜扰	99%
26	传感器合理性检查	用传感器不同样式的信号探测传感器信号在合理范围内的漂移、偏离	90%
27	传感器相互关系	用冗余的传感器探测传感器信号在合理范围内的漂移、偏离	99%
28	硬件冗余	通过比较两个处理器产生的内部或外部结果，探测处理单元的失效	99%
29	传感器信号有效范围	探测传感器对地、对电源和开路	60%
30	传感器相互关系	用冗余的传感器探测传感器信号在合理范围内的漂移、偏离	99%
31	电路设计保护	--	--
32	分配到软件设计	--	--

5.2 硬件故障分类和失效率计算

5.2.1 故障分类

安全相关硬件故障可以分为：

1、单点故障—同时出现的导致违反安全目标的独立故障点为一的故障；

2、残余故障—未被安全机制覆盖的单点故障；

3、多点故障—同时出现的导致违反安全目标的独立故障点大于一的故障；

4、安全故障—不会导致违反安全目标的故障；

其中多点故障又可以分为：

a、可探测多点故障—失效模式可以被安全机制探测到的多点故障；

b、可感知多点故障—失效模式可以被驾驶员感知到的多点故障；

c、潜在多点故障—失效模式既没有被安全机制探测到，也没有被驾驶员感知到的多点故障；

一般情况下故障点大于 2 的多点失效可以认为是安全故障。

假设所有安全相关的失效率为 λ，则

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S} \tag{5.1}$$

λ_{SPF} 是硬件单点故障相关的失效率；

λ_{RF} 是硬件残余故障相关的失效率；

λ_{MPF} 是硬件多点故障相关的失效率；

λ_{S} 是硬件安全故障相关的失效率；

$$\lambda_{MPF} = \lambda_{MPF,DP} + \lambda_{MPF,L} \tag{5.2}$$

$\lambda_{MPF,DP}$ 是硬件可探测或可感知多点故障相关的失效率；

$\lambda_{MPF,L}$ 是硬件潜在多点故障相关的失效率；

残余故障失效率由安全机制的诊断覆盖率决定，

$$\mathrm{K}_{DC,RF} = \left(1 - \lambda_{RF,est} \div \lambda\right) \times 100 \tag{5.3}$$

$$\lambda_{RF} \le \lambda_{RF,est} = \lambda \times \left(1 - \mathrm{K}_{DC,RF} \div 100\right) \tag{5.4}$$

$\lambda_{RF,est}$ 是残余故障估计的失效率；

$\mathrm{K}_{DC,RF}$ 是以百分比表示的残余故障诊断覆盖率；

潜在故障失效率由避免硬件潜在故障的安全机制的诊断覆盖率决定，

$$\mathrm{K}_{DC,MPF,L} = \left(1 - \lambda_{MPF,L,est} \div \lambda\right) \times 100 \tag{5.5}$$

$$\lambda_{MPF,L} \le \lambda_{MPF,L,est} = \lambda \times \left(1 - \mathrm{K}_{DC,MPF,L} \div 100\right) \tag{5.6}$$

$\lambda_{MPF,L,est}$ 是潜在故障估计的失效率；

$\mathrm{K}_{DC,MPF,L}$ 是以百分比表示的潜在故障诊断覆盖率；

5.2.2 单点故障目标值计算

单点故障度量反映了相关项对于单点和残余故障的鲁棒性。一个较高的度量意味着单点和残余故障在相关项的硬件中所占的比例较低。

单点故障度量的计算公式为：

$$1-\sum_{SR,HW}\left(\lambda_{SPF}+\lambda_{RF}\right)\div\sum_{SR,HW}\lambda \tag{5.7}$$

$\sum_{SR,HW}\lambda_x$ 是安全相关的硬件失效率 λ_x 的总和；

5.2.3 潜在故障目标值计算

潜在故障度量反映了相关项对于潜在故障的鲁棒性。一个较高的度量意味着潜在故障在相关项的硬件中所占的比例较低。

潜在故障度量的计算公式为：

$$1-\sum_{SR,HW}\lambda_{MPF,L}\div\sum_{SR,HW}\left(\lambda-\lambda_{SPF}-\lambda_{RF}\right) \tag{5.8}$$

$\sum_{SR,HW}\lambda_x$ 是安全相关的硬件失效率 λ_x 的总和；

5.2.4 随机硬件失效概率目标值计算

作为硬件架构度量的补充，随机硬件失效概率度量有两种方法，下面以随机硬件失效概率度量为例进行阐述。

随机硬件失效概率度量 $\mathrm{M_{PMHF}}$ 的计算公式为：

$$\mathrm{M}_{PMHF}=\left(\begin{array}{l}\lambda_{m,RF}\times\mathrm{T}_{lifetime}+\lambda_{m,DPF}\times\mathrm{T}_{lifetime}\times0.5\times\\ \left(\lambda_{sm,DPF,latent}\times\mathrm{T}_{lifetime}+\lambda_{sm,DPF,\det ected}\times\Gamma_{SM}\right)\end{array}\right)\div\mathrm{T}_{lifetime} \tag{5.9}$$

$\lambda_{m,RF}$ 是功能块残余故障失效率；

$\lambda_{m,DPF}$ 是功能块双点故障失效率；

$\mathrm{T}_{lifetime}$ 是整车寿命；

$\lambda_{sm,DPF,latent}$ 是安全机制的潜在的双点失效率；

$\lambda_{sm,DPF,\det ected}$ 是安全机制的探测的双点失效率；

Γ_{SM} 是安全机制的多点故障探测间隔；

由于 $\lambda_{m,DPF}\times\lambda_{sm,DPF,\det ected}\times\Gamma_{SM}$ 是表示在 Γ_{SM} 的时间之内功能块和安全机制同时失效的概率，其值小到可以忽略不计，因此以上公式可以简化为：

$$\mathrm{M}_{PMHF}=\lambda_{m,RF}+\lambda_{m,DPF}\times0.5\times\lambda_{sm,DPF,latent}\times\mathrm{T}_{lifetime} \tag{5.10}$$

如果不考虑失效的前后顺序则公式可以进一步简化为：

$$\mathrm{M}_{PMHF}=\lambda_{m,RF}+\lambda_{m,DPF}\times\lambda_{sm,DPF,latent}\times\mathrm{T}_{lifetime} \tag{5.11}$$

假设车辆的整车寿命为 20 年，则 $T_{lifetime}<10^6$h，假设 $\lambda_{m,DPF}<1000$FIT 则 $\lambda_{m,DPF}<10^{-6}$/h，所以 $\lambda_{m,DPF}\times T_{lifetime}<1$恒成立，可以接受上述公式进一步简化为：

$$M_{PMHF}=\lambda_{m,RF}+\lambda_{sm,DPF,latent} \quad (5.12)$$

5.3 硬件设计安全目标评估

1、微处理器和电源模块是机电复合传动控制单元的基础功能，其它功能的运行都基于微处理器和电源模块的正常运行，下面首先计算其硬件单点和残余故障总失效率和潜在故障总失效率[41,42]。

功能描述：监控蓄电池的电压，当蓄电池电压超出合理范围时，控制系统进入安全状态；为微处理器提供受控制的电源；提供控制单元的唤醒电路。

安全状态：输出扭矩为 0，发送故障灯、警示灯点亮请求。

选用安全机制：S1、蓄电池电压合理范围；S2、CPU 硬件自检程序、配置寄存器测试、整体硬件一致性监控、非易失性存储器、易失性存储器；S3、WD 看门狗；S4、核 1 监控核 0。

当安全机制 S2, S3 失效时，安全机制 S4 可以防止 S2, S3 的潜在故障[43]。

表 5.2 微处理器和电源失效模式和失效率计算

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
U10	500	Y	全部	50%	X	S2	0.99	2.5	X	S4	0.99	2.48
			全部	50%								
U11	20	Y	常高	50%					X	S4	0.99	0.1
			常低	50%								
R13	2	Y	开路	90%					X	S4	0.99	0.02
			短路	10%								
R14	2	Y	开路	90%					X	S4	0.99	0.02
			短路	10%								
R15	2	Y	开路	90%					X	S4	0.99	0.02
			短路	10%								
C10	2	Y	开路	20%								
			短路	80%					X	S4	0.99	0.02
C12	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C15	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C16	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
C17	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44

续表

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
C18	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C19	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C20	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
C23	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
C24	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
C25	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
C26	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C27	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C28	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C29	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
C30	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C31	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C32	2	Y	开路	20%								
			短路	80%	X	S3	0.9	0.16	X	无	0	1.44
L10	2	Y	开路	90%	X	S2	0.99	0.02	X	S4	0.99	0.02
			短路	10%								
L12	2	Y	开路	90%	X	S2	0.99	0.02	X	S4	0.99	0.02
			短路	10%								
TX10	2	Y	开路	50%	X	S3	0.9	0.1	X	无	0	0.9
			短路	50%	X	S3	0.9	0.1	X	无	0	0.9
Q10	2	Y	开路	50%	X	S3	0.9	0.1	X	无	0	0.9
			短路	50%	X	S3	0.9	0.1	X	无	0	0.9
电源	20	Y	开路	10%	X	无	0	2				
			短路	20%	X	无	0	4				
			超范围	70%	X	S1	0.6	5.6	X	无	0	8.4
R46	2	Y	开路	90%	X	无	0	1.8				
			短路	10%	X	无	0	0.2				
D17	2	Y	开路	90%								
			短路	10%	X	无	0	0.2				
D18	2	Y	开路	90%	X	无	0	1.8				
			短路	10%								
L13	2	Y	开路	90%	X	无	0	1.8				
			短路	10%								
L14	2	Y	开路	90%	X	S3	0.9	0.18	X	无	0	1.62
			短路	10%								
L15	2	Y	开路	90%	X	无	0	1.8				
			短路	10%								

续表

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
U14	20	Y	全部	50%	X	无	0	10				
			全部	50%								
C40	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C41	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C42	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C43	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C44	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C45	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C46	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C47	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C48	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C49	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C50	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C51	2	Y	开路	20%								
			短路	80%	X	无	0	1.6				
C52	2	Y	开路	20%								
			短路	80%					X	无	0	1.6
C53	2	Y	开路	20%								
			短路	80%					X	无	0	1.6
R43	2	Y	开路	90%					X	无	0	2
			短路	10%								
R44	2	Y	开路	90%					X	无	0	2
			短路	10%								
R45	2	Y	开路	90%					X	无	0	1.8
			短路	10%								
D19	2	Y	开路	90%								
			短路	10%					X	无	0	0.2

安全相关总失效率：$\sum_{SR,HW}\lambda$=658；

单点和残余故障总失效率：$\sum_{SR,HW}\left(\lambda_{SPF}+\lambda_{RF}\right)$=67.2；

潜在故障总失效率：$\sum_{SR,HW}\lambda_{MPF,L}$=37.04；

2、以机电复合传动控制单元的加速踏板踏板位置信号采集模块这一安全相关的功能为例，计算其硬件架构度量和随机硬件失效概率度量。

功能描述：读取加速踏板位置传感器信号，当传感器信号失效时，控制系统

进入安全状态;提供受控制的传感器电源并监控,当传感器电压超出合理范围时,控制系统进入安全状态。

安全状态：输出扭矩为 0，发送故障灯、警示灯点亮请求。

选用安全机制：S1、传感器电源电压合理范围；S2、传感器信号合理范围；S3、传感器信号相互关系。

当安全机制 S1 失效时，安全机制 S3 可以防止 S1 的潜在故障。当安全机制 S2 失效时，安全机制 S3 可以防止 S2 的潜在故障。

由于选用了安全机制 S3 传感器信号相互关系，所以需要两路独立的传感器电源和两路模拟信号采集通道,表 5.3 中直接将传感器电源和模拟信号处理电路的原件失效率加倍。

安全机制 S1 的诊断覆盖率可参照硬件冗余。

表 5.3 加速踏板信号采集失效模式和失效率计算

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
R32	4	Y	开路	90%	X	S1	0.99	0.04	X	S3	0.99	0.04
			短路	10%								
R33	4	Y	开路	90%	X	S1	0.99	0.04	X	S3	0.99	0.04
			短路	10%								
R34	4	Y	开路	90%	X	S1	0.99	0.04	X	S3	0.99	0.04
			短路	10%								
C36	4	Y	开路	20%								
			短路	80%	X	无	0	3.2				
U13	40	Y	全部	50%	X	S1	0.99	0.2	X	S3	0.99	0.2
			全部	50%								
D20	4	Y	开路	90%	X	无	0	3.6				
			短路	10%								
C54	4	Y	开路	20%								
			短路	80%	X	无	0	3.2				
U16	40	Y	全部	50%	X	S1	0.99	0.2	X	S3	0.99	0.2
			全部	50%								
R52	4	Y	开路	90%	X	S1	0.99	0.04	X	S3	0.99	0.04
			短路	10%								
R53	4	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S3	0.99	0
R54	4	Y	开路	90%					X	S3	0.99	0.04
			短路	10%								
R55	4	Y	开路	90%					X	S3	0.99	0.04
			短路	10%								
R56	4	Y	开路	90%					X	S3	0.99	0.04
			短路	10%								
RJ10	4	Y	开路	90%					X	S3	0.99	0.04
			短路	10%								
C60	4	Y	开路	20%								
			短路	80%	X	S1	0.99	0.03	X	S3	0.99	0.03
C61	4	Y	开路	20%								
			短路	80%	X	S1	0.99	0.03	X	S3	0.99	0.03

续表

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
C62	4	Y	开路	20%								
			短路	80%	X	S1	0.99	0.03	X	S3	0.99	0.03
C63	4	Y	开路	20%								
			短路	80%					X	S3	0.99	0.03
C64	4	Y	开路	20%								
			短路	80%					X	S3	0.99	0.03
D22	4	Y	开路	90%								
			短路	10%					X	S3	0.99	0
D23	4	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S3	0.99	0
C65	4	Y	开路	20%								
			短路	80%	X	S1	0.99	0.03	X	S3	0.99	0.03
C66	4	Y	开路	20%								
			短路	80%	X	S1	0.99	0.03	X	S3	0.99	0.03
R57	4	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S3	0.99	0
R58	4	Y	开路	90%	X	S1	0.99	0.04	X	S3	0.99	0.04
			短路	10%								
R59	4	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S3	0.99	0
加速踏板传感器 A	50	Y	超高	20%	X	S3	0.99	0.5	X	S3	0.99	0.5
		Y	超低	20%								
		Y	短电源	20%								
		Y	短地	20%								
		Y	开路	10%								
		Y	漂移	10%								
加速踏板传感器 B	50	Y	超高	20%	X	S3	0.99	0.5	X	S3	0.99	0.5
		Y	超低	20%								
		Y	短电源	20%								
		Y	短地	20%								
		Y	开路	10%								
		Y	漂移	10%								

安全相关总失效率：$\sum_{SR,HW}\lambda$=658+276=934

单点和残余故障总失效率：$\sum_{SR,HW}\left(\lambda_{SPF}+\lambda_{RF}\right)$=67.2+11.75=78.95

潜在故障总失效率：$\sum_{SR,HW}\lambda_{MPF,L}$=37.04+1.97=39.97

由公式（5.7）计算可得单点故障度量值=91.5%

由公式（5.8）计算可得潜在故障度量值=95.3%；

可知潜在故障度量达到 ASIL C 的目标值；而单点故障度量达不到 ASIL C 的目标值。

由公式（5.12）计算可得：

M_{PMHF} =104.31FIT+ 37.7FIT=142.01FIT;

可知结果不满足 ASIL C 小于 100FIT 的要求。

分析发现电路中有许多未被安全机制覆盖的滤波电容，通过减少这些滤波电容或者增加安全机制，可以提高单点故障度量值。

3、以机电复合传动控制单元的电磁阀驱动模块这一安全相关的功能为例，计算其硬件架构度量和随机硬件失效概率度量。

功能描述：为电磁阀提供高边和低边驱动，实时监控高边驱动的电压值和电磁阀的电流值，当高边驱动的电压值超出合理范围或电磁阀的电流超出预期值时，控制系统进入安全状态。

安全状态：输出扭矩为 0，发送故障灯、警示灯点亮请求。

选用安全机制：S1、监控输出电压合理范围；S2、监控输出电流值。

当安全机制 S1 失效时，安全机制 S2 可以防止 S1 的潜在故障。

表 5.4 电磁阀驱动失效模式和失效率计算

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
R60	2	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S2	0.99	0
R61	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R62	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R63	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R64	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R65	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R66	2	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S2	0.99	0
R68	2	Y	开路	90%					X	S2	0.99	0.02
			短路	10%								
R69	2	Y	开路	90%					X	S2	0.99	0.02
			短路	10%								
R70	2	Y	开路	90%						S2	0.99	0.02
			短路	10%								
R71	2	Y	开路	90%					X	S2	0.99	0.02
			短路	10%								
R72	2	Y	开路	90%	X	S2	0.99	0.02	X	S1	0.99	0.02
			短路	10%								
R73	2	Y	开路	90%	X	S2	0.99	0.02	X	S1	0.99	0.02
			短路	10%					X	S2	0.99	0
R74	2	Y	开路	90%	X	S2	0.99	0.02	X	S1	0.99	0.02
			短路	10%								

续表

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
R75	2	Y	开路	90%	X	S2	0.99	0.02	X	S1	0.99	0.02
			短路	10%								
C67	2	Y	开路	20%								
			短路	80%	X	S1	0.99	0.02	X	S2	0.99	0.02
C68	2	Y	开路	20%								
			短路	80%					X	S2	0.99	0.02
C69	2	Y	开路	20%								
			短路	80%	X	S1	0.99	0.02	X	S2	0.99	0.02
C70	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C71	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C72	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C73	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C74	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C75	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C76	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C77	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C78	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
C79	2	Y	开路	20%								
			短路	80%	X	S2	0.99	0.02	X	S1	0.99	0.02
D24	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
D28	2	Y	开路	90%								
			短路	10%					X	S2	0.99	0
D29	2	Y	开路	90%	X	S2	0.99	0.02	X	S1	0.99	0.02
			短路	10%								
L16	2	Y	开路	90%	X	S2	0.99	0.02	X	S1	0.99	0.02
			短路	10%								
U17	20	Y	全部	50%	X	S1	0.99	0.1	X	S2	0.99	0.1
			全部	50%								
U18	20	Y	全部	50%	X	S2	0.99	0.1	X	S1	0.99	0.1
			全部	50%								
电磁阀	50	Y	开路	90%	X	S2	0.99	0.5	X	S1	0.99	0.5
			短路	10%								

安全相关总失效率：$\sum_{SR,HW}\lambda$=658+154=812

单点和残余故障总失效率：$\sum_{SR,HW}\left(\lambda_{SPF}+\lambda_{RF}\right)$=67.2+1.18=68.38

潜在故障总失效率：$\sum_{SR,HW}\lambda_{MPF,L}$=37.04+1.18=38.22

由公式（5.7）计算可得单点故障度量值=91.6%

由公式（5.8）计算可得潜在故障度量值=94.9%；

可知潜在故障度量达到 ASIL C 的目标值；而单点故障度量达不到 ASIL C 的目标值。

由公式（5.12）计算可得：

M_{PMHF} =68.38FIT+ 38.22FIT=106.6FIT；

可知结果不满足 ASIL C 小于 100FIT 的要求。

同上通过减少滤波电容或者增加安全机制，可以提高单点故障度量值。

4、以机电复合传动控制单元的 CAN 总线驱动模块这一安全相关的功能为例，计算其硬件架构度量和随机硬件失效概率度量。

功能描述：为 CAN 控制器提供驱动，实时监控 CAN 信号，当扭矩相关的信号失效时，控制系统进入安全状态。

安全状态：输出扭矩为 0，发送故障灯、警示灯点亮请求。

选用安全机制：S1、探测帧丢失或节点丢失；S2、Check-sum 和 Rolling-counter 机制。当安全机制 S1 失效时，安全机制 S2 可以防止 S1 的潜在故障。

表 5.5 CAN 驱动失效模式和失效率计算

部件	失效率	是否安全相关	失效模式	失效率分布	违反安全目标	安全机制	失效诊断覆盖率	残余或单点故障失效率	多点失效后违反安全目标	防止多点失效潜在安全机制	潜在多点失效诊断覆盖率	潜在多点故障失效率
R76	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R77	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R78	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
R79	2	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S2	0.99	0
R80	2	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S2	0.99	0
C80	2	Y	开路	20%								
			短路	80%	X	S1	0.99	0.02	X	S2	0.99	0.02
C81	2	Y	开路	20%								
			短路	80%	X	S1	0.99	0.02	X	S2	0.99	0.02
C82	2	Y	开路	20%								
			短路	80%	X	S1	0.99	0.02	X	S2	0.99	0.02
C83	2	Y	开路	20%								
			短路	80%	X	S1	0.99	0.02	X	S2	0.99	0.02
D30	2	Y	开路	90%								
			短路	10%	X	S1	0.99	0	X	S2	0.99	0
L17	2	Y	开路	90%	X	S1	0.99	0.02	X	S2	0.99	0.02
			短路	10%								
U19	20	Y	全部	50%	X	S1	0.99	0.1	X	S2	0.99	0.1
			全部	50%								

安全相关总失效率：$\sum_{SR,HW}\lambda$=658+42=700

单点和残余故障总失效率：$\sum_{SR,HW}\left(\lambda_{SPF}+\lambda_{RF}\right)$=67.2+0.26=67.46

潜在故障总失效率：$\sum_{SR,HW}\lambda_{MPF,L}$=37.04+0.26=37.3

由公式（5.7）计算可得单点故障度量值=90.4%

由公式（5.8）计算可得潜在故障度量值=94.1%；

可知潜在故障度量达到 ASIL C 的目标值；而单点故障度量达不到 ASIL C 的目标值。

由公式（5.12）计算可得：

M_{PMHF}=67.46FIT+ 37.3FIT=104.76FIT;

可知结果不满足 ASIL C 小于 100FIT 的要求。

同上通过减少滤波电容或者增加安全机制，可以提高单点故障度量值。

5.4 测试验证

5.4.1 测试设备及原理

为了测试机电复合传动控制系统的功能安全设计，硬件在环测试是常用的方法。组成测试环境的设备见表 5.4。

表 5.6 硬件在环测试设备

设备名称	用途
硬件在环测试设备（VT 设备）（附录 A）	VT1004:输出负载模拟和输出电压测试； VT2004:模拟量输入信号模拟； VT2516:数字量输入输出模拟； VT6104:CAN/LIN 网络信号模拟； 产生机电复合传动控制单元所需的输入输出信号； 产生机电复合传动控制单元测试所需的故障测试信号； 监控机电复合传动控制单元输出信号的电压波形； 监控机电复合传动控制单元总线的数据；
标定设备	INCAR 标定设备、CANoe 设备； 监控机电复合传动控制单元内部变量数值，并记录到计算机 B； 读取机电复合传动控制单元内部故障代码；
机电复合传动控制单元	被测对象；
油泵电机	油泵电机的控制是闭环控制，设备无法模拟，直接用真实的电机测试，为了故障输入，可通过设备转接；
电源 A，B	A 为控制单元供电；B 为硬件在环设备（VT）供电；
计算机 A，B	A 运行硬件在环设备（VT）控制程序；B 运行 INCA 控制程序；

硬件在环测试设备（VT）可以进行硬件故障的注入测试，如外部供电故障、CAN 总线故障、传感器故障等，因此大部分机电复合传动控制单元 I/O 口的故障验证都可以通过硬件在环测试设备(VT)完成。搭建完成的测试环境如图 5.2。

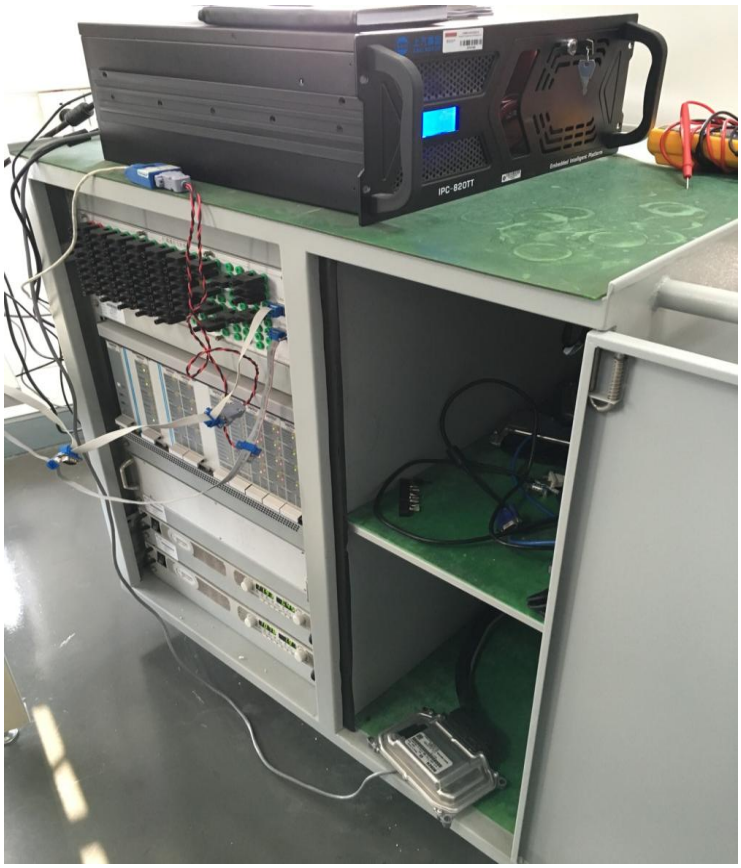

图 5.2 硬件在环测试设备

硬件在环的测试原理如图 5.3 所示。

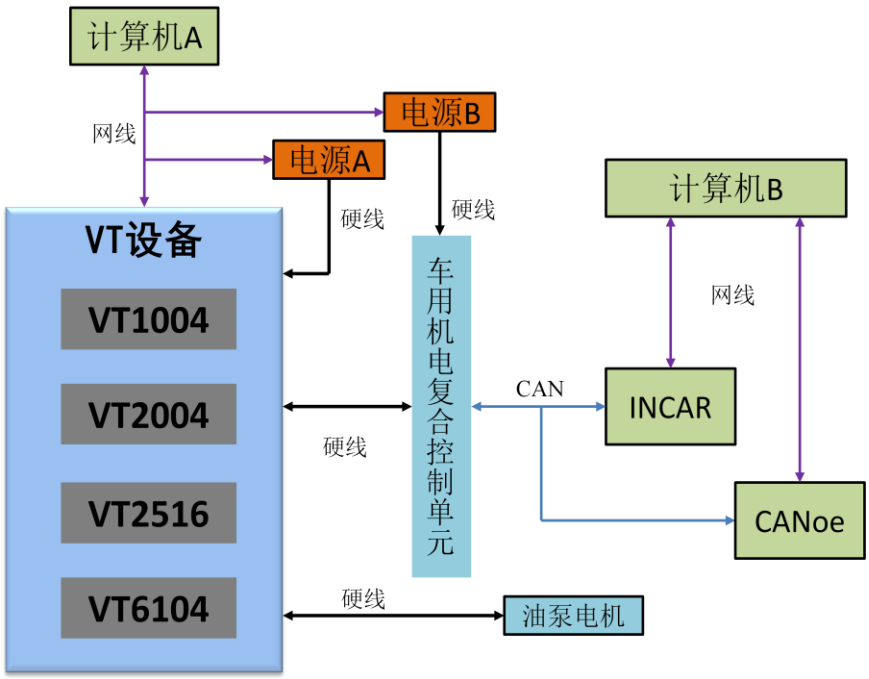

图 5.3 硬件在环测试原理

5.4.2 测试用例和结果

功能安全的测试用例应该覆盖所有的安全机制，针对部件的每一个失效模式，都需要制定一个测试用例去覆盖[44, 45, 46, 47]。

1、电控单元电源电压测试用例

电源电压偏低的测试为，将电控单元的电源电压调到 8V，在 8.5V 时控制器应关闭所有电磁阀的高边驱动端口，控制器的其余功能正常，将电源电压调到 9.5V，在 9V 时控制器应打开所有电磁阀的高边驱动端口，通过 Incar 读取控制器故障码，控制器应记录电源电压低故障。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_626_01_01	HCU shall shut down power stage when voltage drops down to 8.5V and turn on when rise to 9V.			High	Pass
	1	Ignition On	HCU turn on the power stage.		Pass
	2	Decrease battery voltage from 13.5V to 8.1V step by step (0.2V per step).	HCU turn off the power stage when the voltage reaches 8.5V. DFC_PowSupTL_1 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A30 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true.		Pass
	3	Increase battery voltage from 8.1V to 9.5V step by step (0.2V per step).	HCU turn on the power stage when the voltage reaches 9V.		Pass

图 5.4 电控单元电源电压偏低测试用例

电源电压过低的测试为，将电控单元的电源电压调到 5.5V，在 6V 时控制器应关闭 CAN 总线端口，将电源电压调到 7V，在 6.5V 时控制器应打开 CAN 总线端口。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_626_01_01	HCU shall shut down communication when voltage drops down to 6V and turn on when rise to 6.5V.			High	Pass
	1	Ignition On	HCU starts to transmit messages on both Platform CAN and Hybrid CAN within 500ms.		Pass
	2	Decrease battery voltage from 13.5V to 5.5V step by step (0.2V per step).	HCU stops transmiting messages on both Platform CAN and Hybrid CAN when the voltage		Pass
	3	Increase battery voltage from 5.5V to 6.9V step by step (0.2V per step).	HCU starts to transmit messages on both Platform CAN and Hybrid CAN when the voltage reaches 6.5V.		Pass

图 5.5 电控单元电源电压过低测试用例

电源电压偏高的测试为，将电控单元的电源电压调到 17V，在 16.5V 时控制器应关闭所有电磁阀的高边驱动端口，控制器的其余功能正常，将电源电压调到 15.5V，在 16V 时控制器应打开所有电磁阀的高边驱动端口；通过 Incar 读取控制器故障码，控制器应记录电源电压高故障。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_628_01_01	HCU shall shut down power stage when voltage rises to 16.5V and turn on when drops down to 16V.			High	Pass
	1	Ignition On	HCU turn on the power stage.		Pass
	2	Increase battery voltage from 13.5V to 16.9V step by step (0.2V per step).	HCU turn off the power stage when the voltage reaches 16.5V. DFC_PowSupTH_1 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A31 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true.		Pass
	3	Decrease battery voltage from 16.9V to 15.5V step by step (0.2V per step).	HCU turn on the power stage when the voltage reaches 16V.		Pass

图 5.6 电控单元电源电压偏高测试用例

电源电压过高的测试为，将电控单元的电源电压调到 24.5V，在 24V 时控制器应关闭 CAN 总线端口，将电源电压调到 23V，在 23.5V 时控制器应打开 CAN 总线端口。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_628_01_01	HCU shall shut down communication when voltage rises to 24V and turn on when drops down to 23.5V.			High	Pass
	1	Ignition On	HCU starts to transmit messages on both Platform CAN and Hybrid CAN within 500ms.		Pass
	2	Increase battery voltage from 13.5V to 24.3V step by step (0.2V per step).	HCU stops transmiting messages on both Platform CAN and Hybrid CAN when the voltage reaches 24V.		Pass
	3	Decrease battery voltage from 24.3V to 23.1V step by step (0.2V per step).	HCU starts to transmit messages on both Platform CAN and Hybrid CAN when the voltage reaches 23.5V.		Pass

图 5.7 电控单元电源电压过高测试用例

2、加速踏板传感器电源测试用例

5V 电源 1 对电池正极短路的测试为，将电源短接到 12V，通过 Incar 读取控制器故障码，控制器应记录加速踏板传感器电源 1 对电池短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_776_01_04	HCU shall diagnose acceleration pedal position sensor1's power supply short to battery fault.			High	Pass
	1	Ignition ON			Pass
	2	Short-circuit acceleration pedal position sensor1's power supppy (BOB S2pin) to battery supply(KL30).	1)DFC_OutPSSplyASB_2 comes out in VDSM_DFC_Current_DisplyBuffer list. 2)VDHP_InhibitGearShift_flg = true. 3)Raw DTC code=1A81 4)HybElecVehFlt turns to true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off,wait for HCU completely power down.			Pass
	5	Ignition ON.	1)DFC_OutPSSplyASB_2 transfers from VDSM_DFC_Current_DisplyBuffer to VDSM_DFC_History_DisplyBuffer. 2)HybElecVehFlt is false.		Pass
	6	Repeat Step 2 to Step 3.			Pass
	7	Clear fault manually by Set DSMAUX_xClearTrg_C to 255.	Fault is cleared		Pass

图 5.8 加速踏板传感器电源对电池正极短路测试用例

5V 电源 1 对地短路的测试为，将电源短接到地，通过 Incar 读取控制器故障码，控制器应记录加速踏板传感器电源 1 对地故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_776_01_05	HCU shall diagnose acceleration pedal position sensor1's power supply short to ground fault.			High	Pass
	1	Ignition ON			Pass
	2	Short-circuit acceleration pedal position sensor1's power supppy (BOB S2pin) to ground.	1)DFC_OutPSSplyASG_2 comes out in VDSM_DFC_Current_DisplyBuffer list. 2)VDHP_InhibitGearShift_flg = true. 3)Raw DTC code=1A80 4)HybElecVehFlt turns to true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off,wait for HCU completely power down.			Pass
	5	Ignition ON.	DFC_OutPSSplyASG_2 transfers from VDSM_DFC_Current_DisplyBuffer to VDSM_DFC_History_DisplyBuffer. 2)HybElecVehFlt is false.		Pass
	6	Repeat Step 2 to Step 3.			Pass
	7	Clear fault manually by Set DSMAUX_xClearTrg_C to 255.	Fault is cleared		Pass

图 5.9 加速踏板传感器电源对地短路测试用例

5V 电源 1 开路的测试为，将电源断开，通过 Incar 读取控制器故障码，控制器应记录加速踏板传感器电源 1 开路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_776_01_03	HCU shall diagnose acceleration pedal position sensor1's power supply open-pin fault.			High	Pass
	1	Ignition ON			Pass
	2	Set acceleration pedal position sensor1's power supppy (BOB S2pin) open.	1)DFC_OutPSSplyAOP_2 comes out in VDSM_DFC_Current_DisplyBuffer list. 2)Raw DTC code=1A82 3)HybElecVehFlt turns to true.		Pass
	3	Reconnect acceleration pedal position sensor1's power supppy.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off,wait for HCU completely power down.			Pass
	5	Ignition ON.	1)DFC_OutPSSplyAOP_2 transfers from VDSM_DFC_Current_DisplyBuffer to VDSM_DFC_History_DisplyBuffer. 2)HybElecVehFlt is false.		Pass
	6	Repeat Step 2 to Step 3.			Pass
	7	Clear fault manually by Set DSMAUX_xClearTrg_C to 255.	Fault is cleared		Pass

图 5.10 加速踏板传感器电源开路测试用例

3、加速踏板传感器信号测试用例

传感器信号对电源短路的测试为，将传感器信号短接到 5V 或者 12V，通过 Incar 读取控制器故障码，控制器应记录压力传感器信号对电源短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_776_01_01	HCU shall diagnose acceleration pedal position sensor1's output short to battery.			High	Pass
	1	Ignition ON			Pass
	2	Short-circuit acceleration pedal position sensor output(BOB 87pin) to its power supply(BOB 88pin) or battery supply(KL30).	1)DFC_InpPPedalSB_0 comes out in VDSM_DFC_Current_DisplyBuffer list. 2)Raw DTC code=1A21 3)HybElecVehFlt turns to true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off,wait for HCU completely power down.			Pass
	5	Ignition ON.	1)DFC_InpPPedalSB_0 transfers from VDSM_DFC_Current_DisplyBuffer to VDSM_DFC_History_DisplyBuffer. 2)HybElecVehFlt is false.		Pass
	6	Repeat Step 2 to Step 3.			Pass
	7	Clear fault manually by Set DSMAUX_xClearTrg_C to 255.	Fault is cleared		Pass

图 5.11 加速踏板传感器信号对电源短路测试用例

传感器信号对地短路的测试为，将传感器信号短接到地，通过 Incar 读取控制器故障码，控制器应记录压力传感器信号对地短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_776_01_02	HCU shall diagnose acceleration pedal position sensor1's output short to ground fault.			High	Pass
	1	Ignition ON			Pass
	2	Short-circuit acceleration pedal position sensor output(BOB 87pin) to Ground.	1)DFC_InpPPedalSGOP_0 comes out in VDSM_DFC_Current_DisplyBuffer list. 2)Raw DTC code=1A22 3)HybElecVehFlt turns to true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off,wait for HCU completely power down.			Pass
	5	Ignition ON.	1)DFC_InpPPedalSGOP_0 transfers from VDSM_DFC_Current_DisplyBuffer to VDSM_DFC_History_DisplyBuffer. 2)HybElecVehFlt is false.		Pass
	6	Repeat Step 2 to Step 3.			Pass
	7	Clear fault manually by Set DSMAUX_xClearTrg_C to 255.	Fault is cleared		Pass

图 5.12 加速踏板传感器信号对地短路测试用例

传感器信号开路的测试为，将传感器信号开路，通过 Incar 读取控制器故障码，控制器应记录压力传感器信号开路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_776_01_03	HCU shall diagnose acceleration pedal position sensor1's output open-pin fault.			High	Pass
	1	Ignition ON			Pass
	2	Set acceleration pedal position sensor output(BOB 87pin) open.	1)DFC_InpPPedalSGOP_0 comes out in VDSM_DFC_Current_DisplyBuffer list. 2)Raw DTC code=1A22 3)HybElecVehFlt turns to true.		Pass
	3	Reconnect acceleration pedal position sensor output pin.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off,wait for HCU completely power down.			Pass
	5	Ignition ON.	1)DFC_InpPPedalSGOP_0 transfers from VDSM_DFC_Current_DisplyBuffer to VDSM_DFC_History_DisplyBuffer. 2)HybElecVehFlt is false.		Pass
	6	Repeat Step 2 to Step 3.			Pass
	7	Clear fault manually by Set DSMAUX_xClearTrg_C to 255.	Fault is cleared		Pass

图 5.13 加速踏板传感器信号开路测试用例

4、电磁阀高边驱动测试用例

电磁阀高边驱动对电源短路的测试为，将高边驱动短接到 12V，通过 Incar 读取控制器故障码，控制器应记录高边驱动对电源短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_575_03_03	HCU shall diagnose safety valve solenoid power supply circuits short to battery fault.			High	Pass
	1	Short-circuit safety valve solenoid power supply to battery.			Pass
	2	Ignition on	DFC_OutPPSplySB_0 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A72 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off.			Pass
	5	Wait until losing CAN communication with HCU.			Pass
	6	Ignition on.	DFC_OutPPSplySB_0 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to false. VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	7	Ignition off.			Pass
	8	Repeat Step 1 to Step 3.	DFC_OutPPSplyOP_0 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A72 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	9	Clear fault manually.	Fault cannot be cleared.		Pass

图 5.14 电磁阀高边驱动对电源短路测试用例

电磁阀高边驱动对地短路的测试为，将高边驱动短接到地，通过 Incar 读取控制器故障码，控制器应记录高边驱动对地短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_575_03_01	HCU shall diagnose safety valve solenoid power supply circuits short to ground fault.			High	Pass
	1	Ignition ON			Pass
	2	Short-circuit safety valve solenoid power supply to the ground.	DFC_OutPPSplySG_0 comes out in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A70 comes out. HybElecVehFlt turns to true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off.			Pass
	5	Wait until losing CAN communication with HCU.			Pass
	6	Ignition on.	DFC_OutPPSplySG_0 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to false. VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	7	Repeat Step 2 to Step 3.	DFC_OutPPSplySG_0 comes out in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A70 comes out. HybElecVehFlt turns to true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	8	Clear fault manually.	Fault cannot be cleared.		Pass

图 5.15 电磁阀高边驱动对地短路测试用例

电磁阀高边驱动开路的测试为，将高边驱动开路，通过 Incar 读取控制器故障码，控制器应记录高边驱动开路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID	Test Procedure		Expected Results	Priority	
TEST_575_03_02	HCU shall diagnose safety valve solenoid power supply open pin fault.			High	Pass
	1	Disconnect safety valve solenoid power supply from the solenoid.			Pass
	2	Ignition on	DFC_OutPPSplyOP_0 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A71 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	3	Reconnect safety valve solenoid power supply to the solenoid.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off.			Pass
	5	Wait until losing CAN communication with HCU.			Pass
	6	Ignition on.	DFC_OutPPSplyOP_0 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to false. VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	7	Ignition off.			Pass
	8	Repeat Step 1 to Step 3.	DFC_OutPPSplyOP_0 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A71 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	9	Clear fault manually.	Fault cannot be cleared.		Pass

图 5.16 电磁阀高边驱动开路测试用例

5、电磁阀低边驱动测试用例

电磁阀低边驱动对电源短路的测试为，将低边驱动短接到 12V，通过 Incar 读取控制器故障码，控制器应记录低边驱动对电源短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID		Test Procedure	Expected Results	Priority	
TEST_577_01_03	HCU shall diagnose safety valve solenoid output current control circuits short to battery fault.			High	Pass
	1	Ignition on			Pass
	2	Overwite OUTP_EDUSafetyValveCur_mA to be 400mA			Pass
	3	Short-circuit safety valve solenoid output current to battery.	DFC_OutPCcA2SB_4 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1ACF comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	4	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	5	Ignition off.			Pass
	6	Wait until losing CAN communication with HCU.			Pass
	7	Ignition on.	DFC_OutPCcA2SB_4 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to be false.VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	8	Repeat Step 2 to Step 3.	DFC_OutPCcA2SB_4 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1ACF comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	9	Clear fault manually.	Fault can be cleared.		Pass

图 5.17 电磁阀低边驱动对电源短路测试用例

电磁阀低边驱动对地短路的测试为，将低边驱动短接到地，通过 Incar 读取控制器故障码，控制器应记录低边驱动对地短路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID		Test Procedure	Expected Results	Priority	
TEST_577_01_01	HCU shall diagnose safety valve solenoid output current control circuits short to ground fault.			High	Pass
	1	Ignition ON			Pass
	2	Short-circuit safety valve solenoid output current control to the ground.	DFC_OutPPCcA2SG_4 comes out in VDSM_DFC_Current_DisplyBuffer list. DTC code P1ACE comes out. HybElecVehFlt turns to true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	3	Remove short-circuit.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off.			Pass
	5	Wait until losing CAN communication with HCU.			Pass
	6	Ignition on.	DFC_OutPPCcA2SG_4 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to false. VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	7	Repeat Step 2 to Step 3.	DFC_OutPPCcA2SG_4 comes out in VDSM_DFC_Current_DisplyBuffer list. DTC code P1ACE comes out. HybElecVehFlt turns to true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	8	Clear fault manually.	Fault can be cleared.		Pass

图 5.18 电磁阀低边驱动对地短路测试用例

电磁阀低边驱动开路的测试为，将低边驱动开路，通过 Incar 读取控制器故障码，控制器应记录低边驱动开路故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID		Test Procedure	Expected Results	Priority	
TEST_577_01_02	HCU shall diagnose safety valve solenoid output current control open pin fault.			High	Pass
	1	Ignition on			Pass
	2	Disconnect safety valve solenoid output current control from the solenoid.	DFC_OutPCcA2OP_4 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1AD0 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	3	Reconnect safety valve solenoid output current control to the solenoid.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	4	Ignition off.			Pass
	5	Wait until losing CAN communication with HCU.			Pass
	6	Ignition on.	DFC_OutPCcA2OP_4 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to false. VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	7	Repeat Step 2 to Step 3.	DFC_OutPCcA2OP_4 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1AD0 comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	8	Clear fault manually.	Fault can be cleared.		Pass

图 5.19 电磁阀低边驱动开路测试用例

电磁阀电流监控的测试为，将反馈电阻的值从 0.06Ω 改为 1.3Ω，修改电流偏差限制为 1mA，设定输出电流值为 800mA。通过 Incar 读取控制器故障码，控制器应记录输出电流超出合理范围故障，移除故障，故障显示为当前故障，将控制器彻底下电后再上电，故障显示为历史故障，重复上述操作后发送清除故障指令，故障可以清除。

HCU Controller System Test Cases			Test Case Version	1	
Case ID		Test Procedure	Expected Results	Priority	
TEST_577_01_03	HCU shall diagnose safety valve solenoid output current control out of range fault.			High	Pass
	1	Ignition on			Pass
	2	Overwite OutMRstn_resRmn_C[4] to be 1.3Ohm.			Pass
	3	Overwrite OutPCcA2Tolc_iOfsLo_C_[4] to be 0.001A			Pass
	4	Overwite OUTP_EDUSafetyValveCur_mA to be 800mA	DFC_OutPCcA2LOW_4 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A6F comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	5	Disable all the overwriting.	The fault is still in VDSM_DFC_Current_DisplyBuffer list.		Pass
	6	Ignition off.			Pass
	7	Wait until losing CAN communication with HCU.			Pass
	8	Ignition on.	DFC_OutPCcA2LOW_4 transfers into VDSM_DFC_History_DisplyBuffer list. HybElecVehFlt turns to be false. VDHP_InhibitGearShift_flg = false. VDHP_InhibitParallel_flg = false.		Pass
	9	Repeat Step 2 to Step 5.	DFC_OutPCcA2LOW_4 is in VDSM_DFC_Current_DisplyBuffer list. DTC code P1A6F comes out. HybElecVehFlt is true. VDHP_InhibitGearShift_flg = true. VDHP_InhibitParallel_flg = true.		Pass
	10	Clear fault manually.	Fault can be cleared.		Pass

图 5.20 电磁阀电流监控测试用例

6、CAN 总线测试用例

信号帧超时故障确认时间测试，CANoe 模拟单独中止其它节点发送给电控单元的任意一帧报文，待诊断故障代码状态字节变化。测试曲线如图 5.21 所示，坐标 1 为故障发生点，此时 CANoe 停止发送该帧，此时网络上该帧里的信号中断。坐标 2 为故障确认点，帧超时故障状态位置位。坐标 1 和坐标 2 的时间间隔符合规范要求的帧超时故障确认时间。

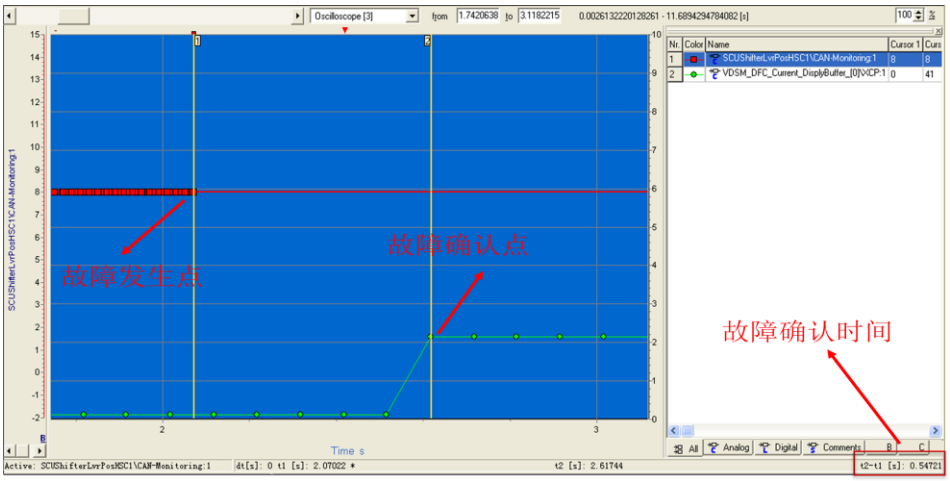

图 5.21 帧超时故障确认测试曲线

信号帧超时故障清除时间测试，CANoe 模拟恢复发送直到诊断故障代码状态字节再次发生变化。测试曲线如图 5.22 所示，坐标 1 为故障恢复点，此时 CANoe 恢复发送该帧，网络上信号恢复发送。坐标 2 为故障清除点，帧超时故障状态位清零。坐标 1 和坐标 2 的时间间隔符合规范要求的帧超时故障清除时间。

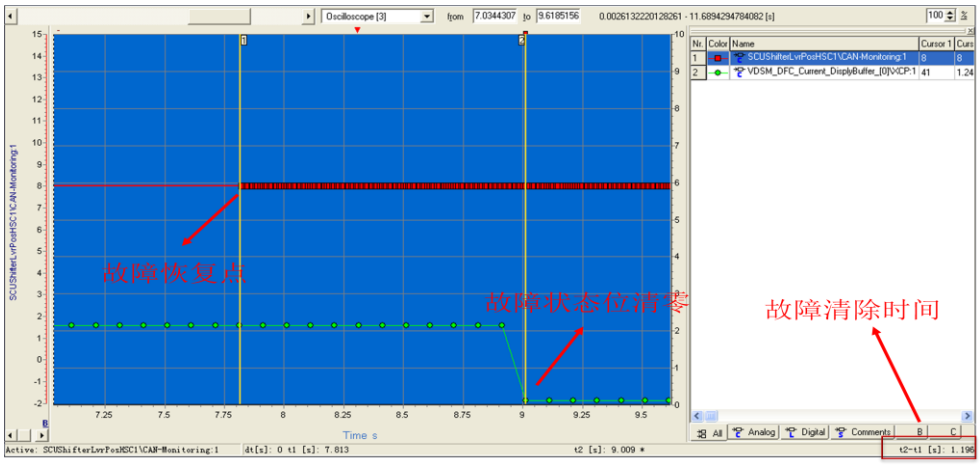

图 5.22 帧超时故障清除测试曲线

节点丢失故障确认时间测试，测试曲线如图 5.23 所示，坐标 1 为故障发生点，此时 CANoe 停止发送该节点所有帧，网络上该信号中断。坐标 2 为故障确

认点，节点丢失故障状态位置位。坐标 1 和坐标 2 之间的时间间隔符合规范要求的节点丢失故障确认时间。

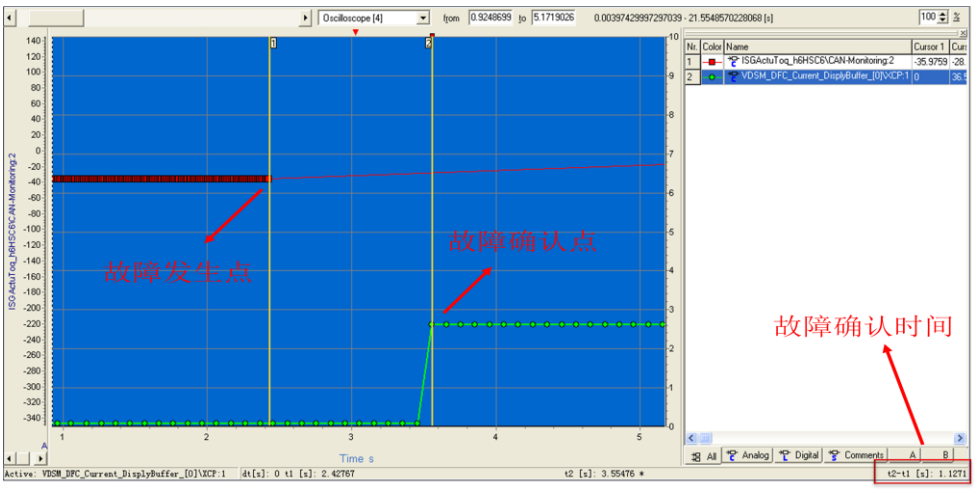

图 5.23 节点丢失故障确认测试曲线

节点丢失故障清除时间测试，测试曲线如图 5.24 所示，坐标 1 为故障恢复点，此时 CANoe 再次发送该节点的帧，网络上信号恢复。坐标 2 为故障清除点，故障状态位清零。坐标 1 和坐标 2 的时间间隔符合规范要求的节点丢失故障清除时间。

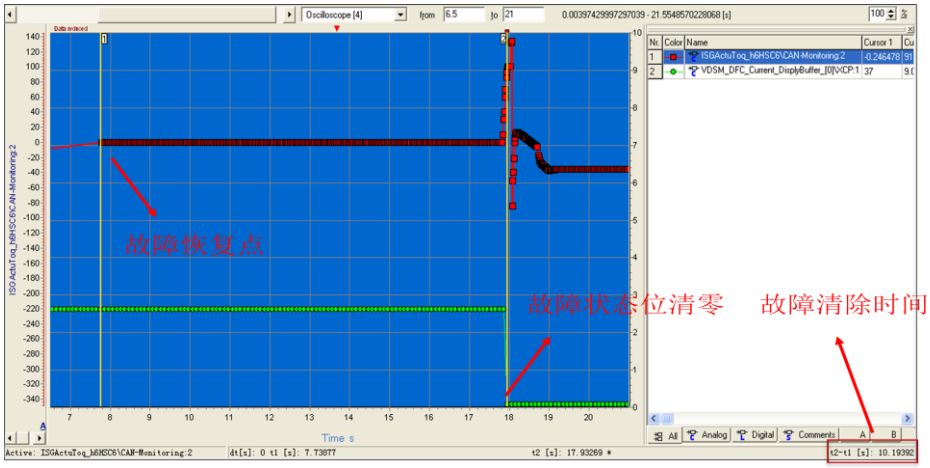

图 5.24 节点丢失故障清除测试曲线

BUS OFF 故障确认时间测试，测试曲线如图 5.25 所示，在控制器重连五次后，BUS OFF 故障确认，即 BUS OFF 故障状态位置 1。

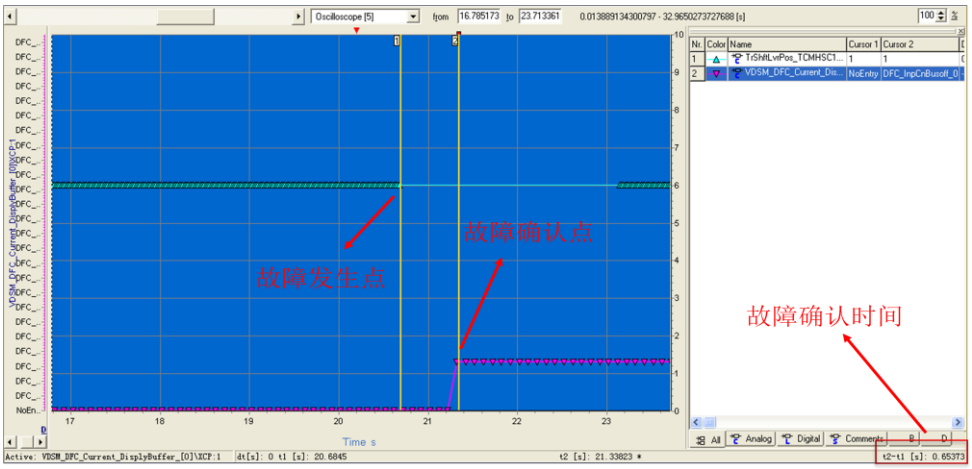

图 5.25 BUS OFF 故障确认测试曲线

BUS OFF 故障清除时间测试，测试曲线如图 5.26 所示，坐标 1 所示位置为故障实际恢复点，该时刻设备停止干扰，故中断信号恢复。坐标 2 所示位置为故障清除点，即故障状态位状态清零。坐标 1 和坐标 2 之间的时间间隔符合规范要求的 BUS OFF 故障清除时间。

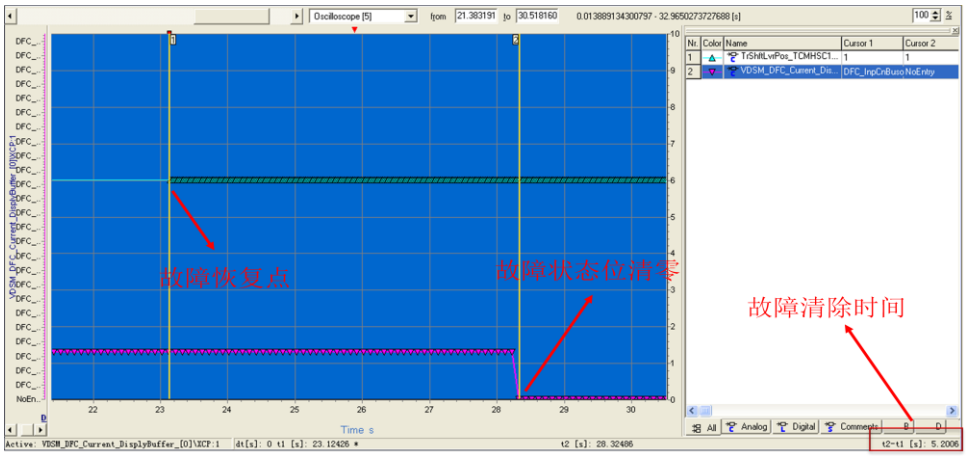

图 5.26 BUS OFF 故障清除测试曲线

Check Sum 故障确认时间测试，测试曲线如图 5.27 所示，坐标 1 为故障发生点，此时 Check Sum 机制失效。坐标 2 为故障确认点，Check Sum 故障状态位置位。坐标 1 和坐标 2 的时间间隔符合规范要求的 Check Sum 故障确认时间。

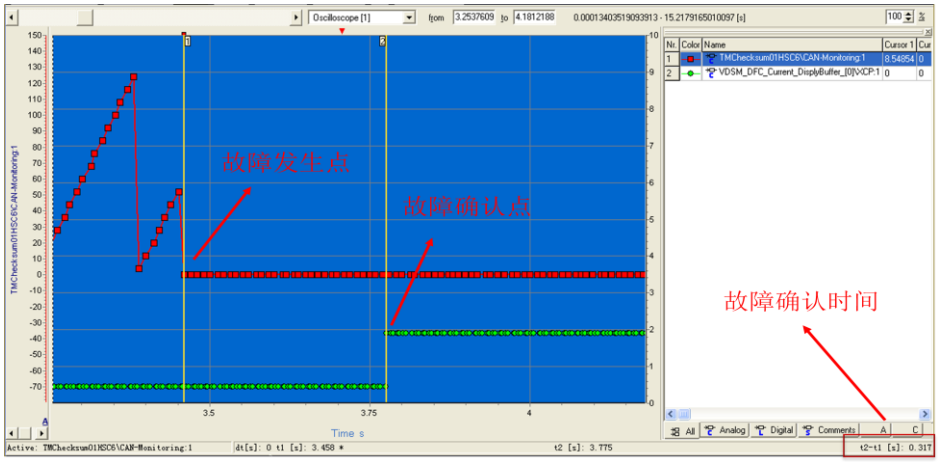

图 5.27 Check Sum 故障确认测试曲线

Check Sum 故障清除时间测试，测试曲线如图 5.28 所示，坐标 1 所示位置为故障实际恢复点，该时刻设备停止干扰，故 Check Sum 机制恢复。坐标 2 所示位置为故障清除点，即故障状态位状态清零。坐标 1 和坐标 2 之间的时间间隔符合规范要求的 Check Sum 故障清除时间。

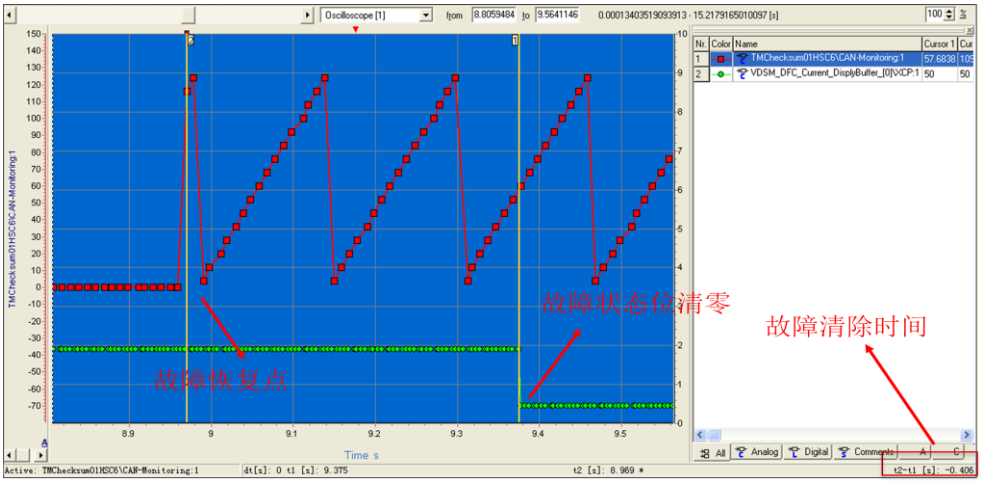

图 5.28 Check Sum 故障清除测试曲线

Rolling Counter 故障确认时间测试，测试曲线如图 5.29 所示，坐标 1 为故障发生点，此时 Rolling Counter 机制失效。坐标 2 为故障确认点，Rolling Counter 故障状态位置位。坐标 1 和坐标 2 的时间间隔符合规范要求的 Rolling Counter 故障确认时间。

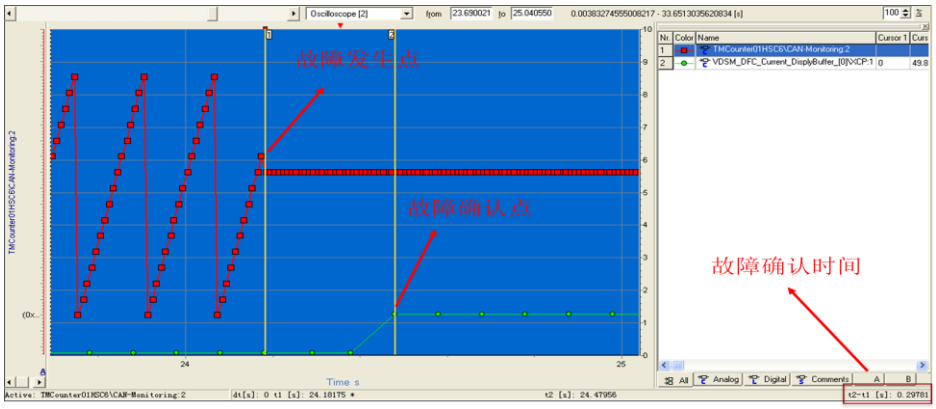

图 5.29 Rolling Counter 故障确认测试曲线

Rolling Counter 故障清除时间测试，测试曲线如图 5.30 所示，坐标 1 所示位置为故障实际恢复点，该时刻设备停止干扰，故 Rolling Counter 机制恢复。坐标 2 所示位置为故障清除点，即故障状态位状态清零。坐标 1 和坐标 2 之间的时间间隔符合规范要求的 Rolling Counter 故障清除时间。

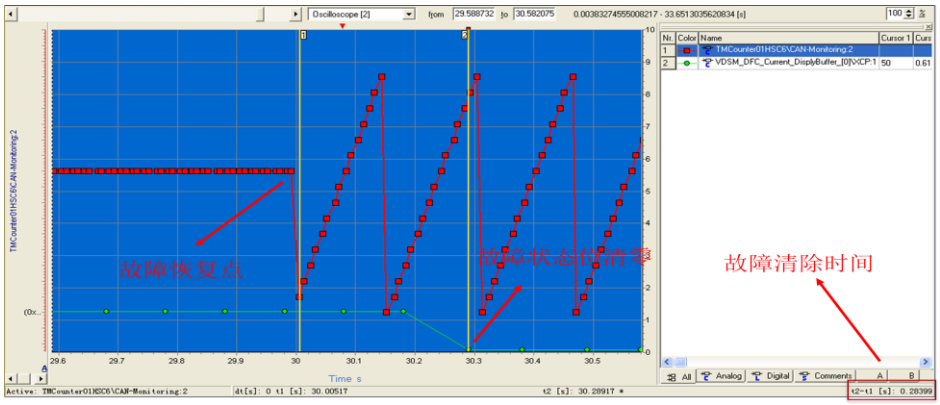

图 5.30 Rolling Counter 故障清除测试曲线

5.5 本章小结

通过本章的计算分析可出：

1、为了满足单点故障度量目标值，需要增加诊断覆盖率高的安全机制，特别是对于失效率高的部件；

2、为了满足潜在故障度量目标值，需要增加对安全机制失效的探测，以降低双点潜在失效；

3、一个满足单点故障度量目标值和潜在故障度量目标值的硬件设计不一定能满足随机硬件失效概率度量目标值，反之亦然；

4、测试验证表明电控单元违反安全目标的单点和潜在双点故障都可以被探测或感知；

第 6 章 结论与展望

6.1 结论

本文的研究工作探讨了功能安全的研究方法，介绍了机电复合传动控制系统的工作原理。通过计算给出了硬件架构度量—单点故障度量和潜在故障度量以及作为硬件架构度量补充的随机硬件失效概率度量等三个度量值，通过对比各自的度量目标值定量的评估出硬件设计是否满足 ASIL 的目标以及改进的方法和途径。最后通过硬件在环测试设备，对硬件设计及其安全机制进行了验证。以上分析方法都结合了实际的工程开发，对功能安全研究提供了有益的补充。

从研究过程中可以得出以下结论：

1、车用机电复合传动控制系统和扭矩相关的功能均为安全相关的功能，需要：a、满足安全目标“避免因为非预期车辆加减速导致剧烈碰撞”；b、满足 ASIL 等级为 C；c、满足安全状态“输出扭矩为 0，发出故障灯、警示灯点亮请求”；

2、技术安全需求规范起到上承功能安全需求下启技术安全概念的重要作用，每一个技术安全需求都必须：a、满足安全目标；b、匹配其对应的 ASIL 等级；c、技术上是可行的；d、成本是可接受的；

3、每一个实施安全相关功能的部件都有违反安全目标的失效模式，这些失效模式都需要相应的安全机制防止单点故障，一个部件可能对应多个安全机制，对安全机制的失效分析可以应对双点故障的潜伏；

4、单点故障度量和潜在故障度量适用于评估硬件架构设计满足 ASIL 等级的状态。随机硬件失效概率度量作为硬件架构度量的补充，适用于评估随机硬件失效的残余风险；

5、硬件在环测试可以验证硬件安全机制的有效性，测试用例的设计直接决定了功能安全验证的完整性；

6.2 展望

本文的研究虽然取得了初步的成功，尚有许多有待进一步深入研究的工作：概念阶段开发功能安全分析；软件开发功能安全分析；ASIL 的分解方法；

相信随着对功能安全开发的深入研究，会不断补充完善现有的研究成果。

致谢

在本文即将完成之际，首先衷心感谢我的导师钟再敏教授！感谢您从开题到中期报告，以及在论文的撰写过程中给予的悉心指导和帮助，您严谨的治学精神、渊博的学识、丰富的工程经验让我在论文的写作过程中不断进步和积累。在此，请接受我对您的真挚感谢！

衷心的感谢张剑锋博士！在上汽的这几年的工作和论文撰写过程中，我从您那里学到了很多知识，感谢您的无私帮助和支持！您在专业和学术上的指导令我受益良多，您宽厚坦诚的为人处事态度成为我生活中的榜样。

感谢工作中给予我巨大帮助的同事—周宇星、冷宏祥、蒋新华。感谢捷能公司的所有同事。感谢我的家人对我的支持！

当近一年的艰辛凝聚成今天的成果，高兴之余，不禁感慨颇多。还记得刚开始着手论文撰写时的迷茫，跨过重重障碍时的喜悦，让我再次深刻体会了“千里之行，始于足下”的道理。

再次感谢和祝福所有帮助我关心我的人！

2016 年 1 月

参考文献

[1] 陈清泉. 现代电动汽车技术[M]. 北京:北京理工大学出版社, 2002

[2] Heinz-Jakob Neusser,Hanno Jelden,Kai Buhring.The Powertrain of the Jetta Hybrid from Volkswagen[J].MTZ Worldwide January 2013 Volume 74,Issue 1

[3] Zeraoulia,Benbouzid M,Diallo M.Electric Moror Drive Delection Issue for HEV Propulsion Systems:Acomparatiove Study[J].IEEE Transactions on Vehicular Technology, 2006,55(6):1756

[4] 朱军. 新能源汽车动力系统控制原理及应用[M]. 上海:上海科学技术出版社, 2013

[5] 钟再敏，王心坚，陈辛波. 有效改善换挡动力中断的车用有源传动装置[J]. 同济大学学报（自然科学版），2011 年 3 月第 39 卷第 3 期

[6] 黄贤广, 何洪文. 混合动力车辆动力耦合装置特性研究[J]. 上海汽车, 2008 年第 4 期

[7] 文凯, 夏珩, 裴锋. 基于 ISO26262 的电动四驱混合动力系统功能安全概念设计[J]. 机电工程技术, 2012 年第 41 卷第 12 期

[8] 沈延, 张剑锋, 冷宏祥. 纯电动汽车安全系统设计. 上海汽车, 2012（06）:7-10

[9] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 1: Vocabulary.Geneva IEC,2011

[10] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 3: Concept phase.Geneva IEC,2011

[11] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 4: Product development at the system level.Geneva IEC,2011

[12] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 5: Product development at the hardware level.Geneva IEC,2011

[13] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 6: Product development at the software level.Geneva IEC,2011

[14] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 8: Supporting processes.Geneva IEC,2011

[15] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses.Geneva IEC,2011

[16] ISO/DIS 26262.Road Vehicles-Functional Safety[S] -Part 10: Guideline.Geneva IEC,2012

[17] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 1:General requirements

[18] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 7:Overview of techniques and measures

[19] Seo-Hyun Jeon. Automotive Hardware Development According to ISO 26262. Feb. 13~16,2011 ICACT 2011

[20] Yung-Chang Chang. Assessing Automotive Functional Safety Microprocessor with ISO 26262 Hardware Requirements. 2014 IEEE

[21] 王春喜. 功能安全标准及应用研究[J]. 山东大学学报(工学版), 2005 年第 6 期

[22] 刘佳熙，郭辉，李君. 汽车电子电气系统的功能安全标准 ISO 26262[J]. 上海汽车，2011 年第 10 期

[23] 仲子平. 汽车自动变速器的电子控制及其发展趋势[J]. 现代机械, 2005 年第 3 期
[24] A Smith,N Bucknor,H Yang.Contorls Development for Cluth-Assisted Engine Starts in a Parallel Hybrid Electric Vehicle.SAE 2011 -01-0870,2011
[25] 刘秋铮. AMT 离合器自适应控制策略及执行器系统开发[D]. 吉林大学, 2006
[26] 秦玉伟, 皇甫国庆, 肖令禄. 汽车传感器的应用以及发展趋势[J]. 传感器世界, 2008 年第 7 期
[27] 麻友良, 丁卫东. 汽车电器与电子控制系统[M]. 机械工业出版社, 2003
[28] Horst Schubotz. Experience with ISO WD 26262 in Automotive Safety Projects[J]. SAE 2008-01-0126,2008
[29] GB/T18384. 1-2001. 电动汽车 安全要求 第 1 部分：车载储能装置[S]. 北京：中国标准出版社, 2001
[30] GB/T18384. 2-2001. 电动汽车 安全要求 第 2 部分：功能安全和故障防护[S]. 北京：中国标准出版社, 2001
[31] GB/T18384. 3-2001. 电动汽车 安全要求 第 3 部分：人员触电防护[S]. 北京：中国标准出版社, 2001
[32] GB/T18387-2013. 电动汽车的电磁场发射强度的限值和测量方法. 北京：中国标准出版社, 2013
[33] 李增辉. FMEA 及 FTA 在汽车产品开发中的应用研究[D]. 合肥工业大学, 2006
[34] 李研强, 李杨, 王知学. 汽车电子系统可能失效原因分析与对策[J]. 山东科学, 2011 年第 2 期
[35] 李朝青. 单片机原理及接口技术[M]. 北京:北京航空航天大学出版社, 1999
[36] 魏学哲, 戴海峰, 孙泽昌. 汽车嵌入式系统开发方法. 体系架构和流程. 同济大学学报, 2012（07）：1064-1070
[37] ISO. ISO11898-1-2003. Road vehicles-Controller area network(CAN)-Part1:Data link layer and physical signaling. ISO Standards,2003
[38] ISO. ISO11898-2-2003. Road vehicles-Controller area network(CAN)-Part2:High-speed medium access unit. ISO Standards,2003
[39] 赵春明, 乔旭彤, 马宁等. 基于 CAN 总线的电动汽车分布式控制系统的故障诊断研究. 车辆与动力技术, 2005 年第 2 期
[40] 杨栩楠. 功能安全与微控制器自诊断技术的研究[D]. 北京交通大学, 2010
[41] 郑伟, 李艳文. 汽车集成安全系统硬件架构功能安全概念设计. 汽车科技, 2014 年第 6 期
[42] 常达, 肖子渊. 汽车离合器控制系统故障诊断的研究[J]. 北京汽车, 2001 年第 6 期
[43] Potential Failure Mode & Effects Analysis,Chrysler LLC,Ford Motor Company,General Motors Corporation,Jun. 2008
[44] 张英武, 袁国顺. 微处理器故障注入工具与故障敏感度分析[J]. 半导体技术, 2008 年第 7 期
[45] 孙俊朝, 王建莹, 杨孝宗. 故障注入方法与工具的研究现状. 宇航学报, 2001（4）：99-104
[46] 杨国青, 历蒋. 基于 ISO26262 功能安全标准的汽车电子系统测试方法. 电子产品世界, 2013. 4
[47] 张鹏, 张君鸿, 张琳等. 混合动力汽车故障诊断功能开发. 上海：上海汽车, 2011

个人简历、在读期间发表的学术论文与研究成果

个人简历：

严洪江，男，1975 年 11 月生.

1999 年 7 月毕业于东南大学 测控技术与仪器专业 获学士学位.

2012 年 3 月入同济大学读在职硕士研究生.

专利：

[1] 严洪江,冷宏祥,张剑锋,俞开元,倪季平.集成板式抗电磁干扰器件及其制备方法.发明.2012 年受理.上海捷能汽车技术有限公司.

待发表论文：

[1] 严洪江.基于功能安全的加速踏板位置传感器硬件设计分析.上海汽车