DOI:10. 19471/j. cnki. 1673-6397. 2023. 01. 011

基于 EGAS 监控概念的高压共轨柴油机控制器功能安全实现

覃艳[1,2],卫文晋[1,2],纪小娟[1,2],丛聪[1,2]

1. 内燃机可靠性国家重点实验室,山东 潍坊　261061;2. 潍柴动力股份有限公司,山东 潍坊　261061

摘要:为将汽车电子、电气系统失效的危害控制在可接受范围内,实现高压共轨柴油发动机控制器功能安全,按照 ISO 26262 的开发流程,围绕发动机控制器进行相关项分析;通过危害分析和风险评估确定安全目标预防非预期加速,其安全完整性等级为 B 级;通过功能安全概念分析确定功能安全需求为转矩监控;在技术安全概念阶段,采用 EGAS 3 级监控概念将转矩监控需求进一步细化并实现安全完整性等级的分解;设计基于 TC29x 芯片的控制器功能安全实现方案。采用 MATLAB/Simulink 搭建策略模型,进行故障注入测试。结果表明,该监控策略能有效地识别输入轴转速过高的故障,并立即做出响应,有效降低了人身伤害的风险。

关键词:ISO 26262;高压共轨柴油发动机;转矩监控;TC29x

中图分类号: U463. 6　　**文献标志码**:A　　**文章编号**:1673-6397(2023)01-0065-07

引用格式:覃艳,卫文晋,纪小娟,等. 基于 EGAS 监控概念的高压共轨柴油机控制器功能安全实现[J]. 内燃机与动力装置,2023,40(1):65-71.

QIN Yan,WEI Wenjin,JI Xiaojuan,et al. Functional safety implementation of high-pressure common rail diesel engine control unit based on EGAS monitoring concept [J]. Internal Combustion Engine & Powerplant,2023,40(1):65-71.

0　引言

安全性是汽车研发过程的关键要素之一。由于高压共轨柴油机电控系统的复杂性,各种传感器和执行器经常处于高温、强电磁干扰的恶劣工作环境中,可能出现由于控制器接收到错误信号、软件逻辑计算过程出现内存崩溃或者指令执行错误而产生违背需求的控制信号等异常情况,这些异常情况在某些场景中会对人的生命安全造成危害[1]。为提高汽车电子、电气产品功能安全,国际标准化组织(international organization for standardization,ISO)分别于 2011 年、2018 年颁布了文献[2-3]。文献[3]主要定位于汽车的电气器件、电子设备、可编程电子器件等部件,且不再仅限于文献[2]规定的质量为 3. 5 t 以下的乘用车,将卡车、公共汽车、摩托车、重型乘用车、全挂车及半挂车也纳入标准应用范围,新增摩托车危害分析和风险评估、半导体应用指南等。

近年来,越来越多的整车厂开始重视功能安全,各大芯片厂商相继为功能安全芯片推出了商业化的软件包,如英飞凌公司为 AURIX 系列单片机提供的功能安全测试库 SafeTlib,可简化开发工作,加速功能安全产品化进程[4-6]。

虽然文献[3]为道路车辆功能安全的实现提供了一套完整的流程、方法论及技术指导,但由于该标准体系庞大、复杂,难以实施落地。奥迪、宝马、戴姆勒、保时捷、大众等公司共同撰写发布了文献[7](简

收稿日期:2021-12-18

第一作者简介:覃艳(1987—),女,四川达州人,工学硕士,工程师,主要研究方向为发动机电控系统开发,E-mail: qinyan@weichai. com。

称为 EGAS 监控概念),为发动机电子控制单元(electronic control unit,ECU)等控制器的开发明确基本原则,提出开发指南。EGAS 监控概念涵盖文献[3]的相关项定义、危害分析和风险评估、功能安全概念及技术安全概念(technical safety concept,TSC),TSC 中提出的 3 级监控架构已得到广泛的认可和应用,是一种符合文献[3]要求的功能安全技术解决方案,可用于发动机控制器软、硬件的设计开发。本文中依照文献[3]的开发流程,探讨 EGAS 监控概念在高压共轨柴油发动机控制器多核芯片功能安全实现中的应用。

1 概念阶段

1.1 相关项定义

概念阶段是后续功能安全开发活动的基础。功能安全概念设计的第一阶段为相关项定义,该阶段应对整车层面的相关项进行定义并描述其功能,此外还需描述某相关项与驾驶员、环境及其他相关项之间的依赖和交互接口[8]。对于配有高压共轨柴油发动机的乘用车,发动机是车辆转矩的唯一来源,直接与驱动轮相连并由 ECU 控制,ECU 结合当前工况的发动机转速、共轨管压力、燃油温度等,将驾驶员的驾驶需求即加速踏板传感器信号,经过转矩计算转换为喷油量,ECU 通过喷油器的加电时间控制喷油量。除加速踏板传感器信号外,刹车、巡航控制开关、来自其他控制器的转矩请求都影响最终需求的转矩。柴油机电控系统基本框图如图 1 所示。

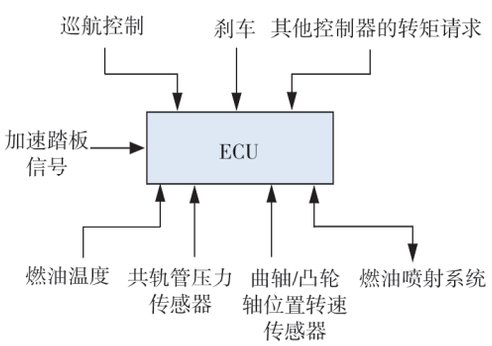

图 1 柴油机电控系统基本框图

1.2 危害分析和风险评估

相关项定义完成后,应对引起相关项故障的危害事件进行识别与分类,制定预防危害事件发生或减轻危害程度的安全目标及其安全完整性等级(automotive safety integrity level,ASIL),这一过程称为危害分析和风险评估[9]。

文献[3]将 ASIL 分为 QM、A、B、C、D 5 个等级,QM 指只需遵循标准的质量管理(quality manage)流程,无需额外的安全措施。决定 ASIL 的 3 个要素分别为严重度 S_X、暴露率 E_Y 和可控性 C_Z,其中:$X=0$、1、2、3,S_0 为无伤害,S_3 为伤害程度最严重;$Y=0$、1、2、3、4,E_0 为几乎不可能暴露于危险中,E_4 为暴露于危险的可能性极高;$Z=0$、1、2、3,C_0 为完全可控,C_3 为几乎不可控。X、Y、Z 中有一个为 0 或 $X+Y+Z<7$,则 AISL 为 QM;$X+Y+Z=7$、8、9、10 时,ASIL 分别为 A、B、C、D。对于某一安全目标,系统达到的 ASIL 等级越高,避免不合理风险的能力就越高。

基于相关项定义,采用 EGAS 监控概念分析典型驾驶情景下的系统行为及其风险,确定系统安全目标是:预防非预期加速,安全完整性等级为 ASIL B。根据安全目标,应对非预期加速行为进行检测,并在适当的故障容错时间内使车辆进入安全可控的状态。

1.3 功能安全概念

文献[3]中从概念到软件的安全需求分解过程如图 2 所示。由图 2 可知:安全目标、功能安全需求、技术安全需求、系统级安全需求及软/硬件安全需求共 5 个层级的需求共同确保安全需求的完整性、追溯性及可实现性。安全目标是最顶层的安全需求。安全目标确定后,需要在功能安全概念阶段,结合初步的系统架构设计,从安全目标提取功能安全需求并分配给相关的子系统。功能安全需求是符合安全目标的功能行为或降级的功能行为,包含相关故障的检测和控制、为达到所需的故障容错时间或减轻故障的影响而采取的系统级策略或措施。

由于非预期加速只能由转矩定义或实现过程中的故障引起,即监控驾驶转矩,或者监控车辆加速度,本文中选择对驾驶转矩进行监控[10],为此,将安全需求分配给传感器、执行器和 ECU。EGAS 监控概念中

的安全框图如图 3 所示。采用双踏板传感器设计并对其信号路径进行物理隔离,利用两路冗余的传感器信号实现可信性校验;对执行器执行状态进行实时监控;ECU 检测传感器和执行器的故障,并对基本功能进行监控。

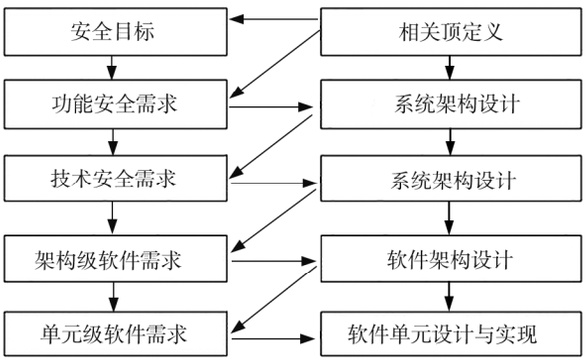

图 2　控制器安全需求分解(软件)

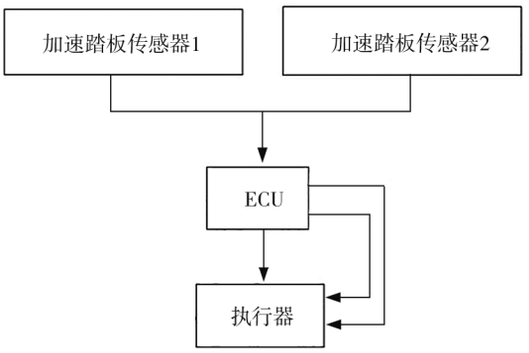

图 3　控制器安全框图

1.4　技术安全概念

技术安全概念阶段将功能安全需求细化为具体的技术安全需求,即安全机制,并基于具体的系统架构实现对技术安全需求的软硬件分配[10]。

ASIL 自上而下继承,若不对其进行分解,传感器、执行器、ECU 都要按照 ASIL B 来开发。与基本功能相比,安全机制规模更小、复杂度更低,ASIL 等级的分解有利于降低开发难度。ASIL 分解应遵循免干扰的原则(freedom from interference,FFI),安全机制与基本功能应相互独立,确保不存在共因失效;另外,ASIL 的分解使得不同 ASIL 的功能并存于 ECU 中,应确保不存在级联失效,即基本功能和 ECU 硬件的错误不影响安全机制。加入转矩监控这一安全机制后,安全机制和基本功能构成冗余设计,共同满足安全目标,因此,“预防非预期加速”这一安全目标等级 ASIL B 可分解为两部分:原转矩计算策略按照 QM 开发,记为 QM(B);转矩监控策略按照 ASIL B 开发,记为 ASIL B(B)。

将冗余的安全机制分配给足够独立的系统,是满足 FFI 要求的效率最高的分配方式。EGAS 提出 3 级监控概念,将不同 ASIL 的功能分解到 3 个不同的软、硬件层级:Level2 对 Level1 进行监控,确保 Level1 的基本功能正常;Level3 对 Level2 的监控确保 Level2 的监控功能正常,另外,Level3 还监控芯片级的硬件故障并提供独立的故障响应。

至此,概念阶段的活动都得以有效实施,高压共轨柴油机 ECU 的 3 级功能安全架构得以确定:相关项定义识别出高压共轨柴油机控制器的功能安全相关因素及其边界;危害分析与风险评估得出了最顶层的安全需求,即安全目标——预防非预期加速(ASIL B);功能安全概念由安全目标派生出转矩监控需求——对功能安全相关的核心控制功能转矩计算进行监控;在技术安全概念阶段,转矩监控需求进一步细化并通过 ASIL 的分解来降低开发成本,提高需求的可实现性。转矩监控需求派生并细化自安全目标,因此,实现了转矩监控需求,就实现了整个 ECU 的安全目标。

2　高压共轨柴油机控制器转矩监控设计

2.1　基于 TC29x 的 EGAS 3 级监控概念

英飞凌的 AURIX 系列 32 位单片机专用于满足汽车行业对 ECU 功能安全的要求。TC29x 单片机共 3 个 Tricore 内核,其中,主芯片 CPU1 带锁步核,且单片机自带的硬件安全机制可以检测不同的单点故障,极大减少工作量[6]。

基于 TC29x 的高压共轨柴油机 ECU 转矩监控设计 EGAS 3 级监控概念如图 4 所示。

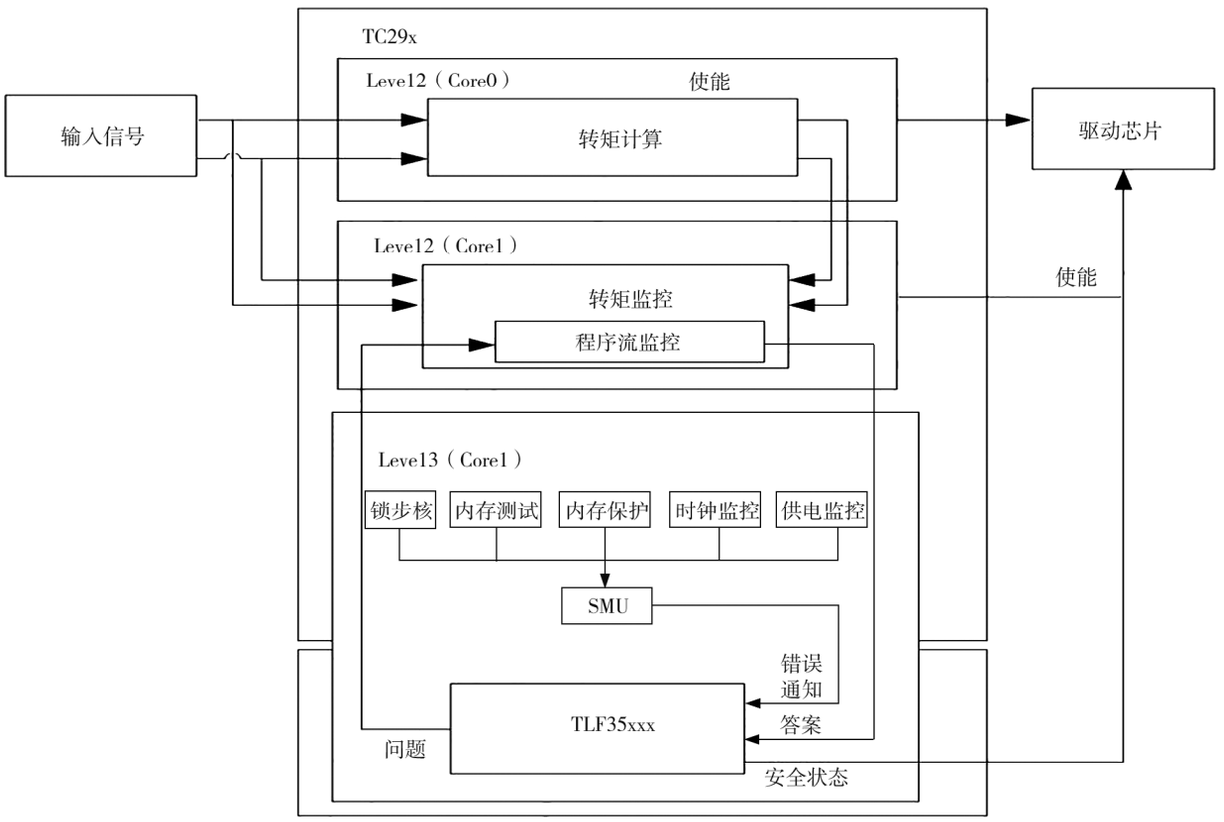

图 4 基于 TC29x 的柴油机控制器 EGAS 3 级转矩监控概念

2.2 功能级

Level1 实现基本功能[QM(B)],称为功能级,位于主芯片 CPU0 上,包含需求转矩的实现、传感器信号的诊断和校验、传感器故障反应等发动机控制功能。

对与安全相关的传感器信号进行诊断和信号范围校验是最基本的要求。对轨压信号进行信号范围校验及梯度诊断,若检测到故障则使用设定值作为当前轨压信号的替代值跛行回家。而对双路踏板传感器信号,应分别对其进行信号范围校验,当其中一路信号范围超上、下限时,采用另一路信号跛行回家;当两路信号的差值超限时,取两路信号中的最小值跛行回家;当已使用其中一路信号跛行回家而之后该路信号也检测到超上、下限故障时,发动机进入怠速工况,检测到传感器供电故障也会触发发动机进入怠速工况。

来自其他控制器的转矩请求通常通过 CAN 线传输,应加入循环冗余校验码校验进行数据保护,同时,ECU 也应对解析后的信号进行可信性校验。

2.3 功能监控级

Level2 为功能监控级[ASIL B(B)],位于主芯片 CPU1 上,对 Level1 的转矩计算进行监控并在故障状况下触发系统反应。转矩监控策略如图 5 所示。Level1 转矩计算使用的输入信号也是 Level2 的输入,进行需求转矩冗余计算,计算结果与实际的发动机转矩进行比较。实际发动机转矩采用测量所得的喷油提前角、喷油器加电时间、喷油次数,结合轨压、发动机转速反向计算得到。若两者不同,触发独立于 Level1 的故障反应。如果 Level2 无法触发独立的故障反应,则触发 Level1 的故障反应并对 Level1 的故障反应进行监控,例如监控发动机转速是否降至合理范围等。

除转矩监控外,Level2 还应对 Level1 计算的喷油相关输出参数进行监控,包括喷油提前角、喷油缸号及最大喷油次数,当有参数不在有效范围之内时,说明 Level1 发生了故障。

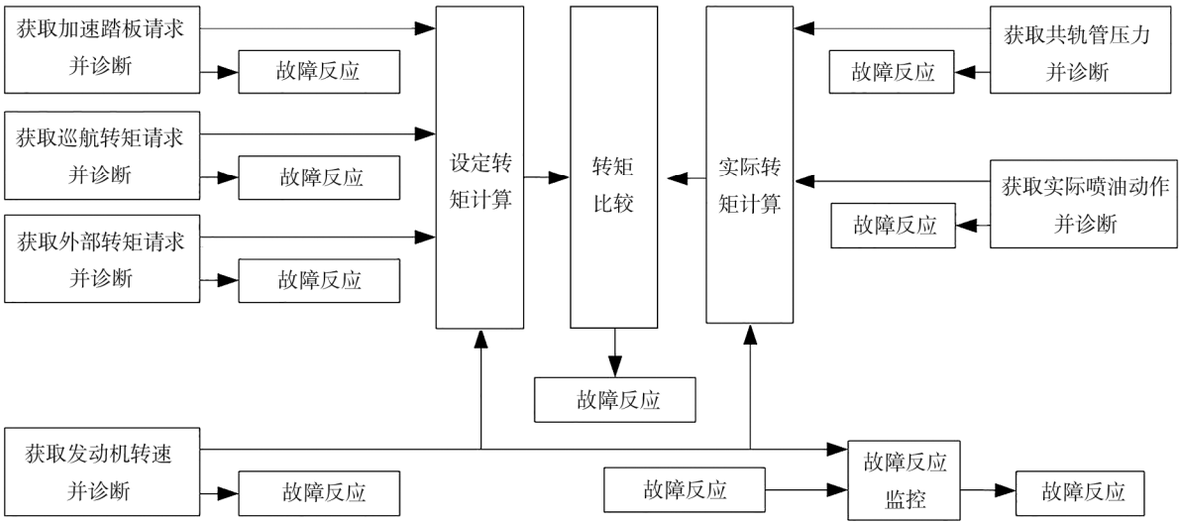

图 5　Level2 转矩监控策略

当前主流高压共轨柴油机 ECU 大多采用智能电磁阀驱动芯片来驱动喷油器:主芯片控制喷油触发信号,驱动芯片根据配置参数调制驱动电流并通过串行外围设备接口(serial peripheral interface,SPI) 向主芯片实时报告诊断信息。Level1 应对诊断信息进行处理,Level2 应测量喷油器的实际加电时间并与 Level1 设定值进行比较,防止 Level1 中存放喷油驱动参数的随机存取存储器(random access memory,RAM)发生位翻转等错误,或者参数向驱动芯片传递过程中发生 SPI 传输错误而导致喷油实际执行与设定出现偏差。

2.4　控制器监控级

Level3 为控制器监控级(ASIL B(B)),位于主芯片 CPU1 和监控芯片上,监控芯片独立于主芯片,通过与主芯片的问答通信测试控制器程序执行的正确性,发生错误以后,触发独立于主控制器的监控系统反应。

为检测单点故障,主芯片 TC29x 需要激活并配置锁步核、内存测试、内存保护等功能[4]。

1)锁步核功能。根据 EGAS 监控概念,锁步核功能可替代指令集测试,对于带有锁步核功能的主芯片 CPU1,校验核在物理上与主核独立,较主核延迟 2 个时钟周期且与主核执行完全相同的指令,通过比较两核的输出检查软件错误或其他瞬时错误。

2)内存测试功能。EGAS 监控概念要求在每个驾驶循环发动机起动前对整个只读存储器(read-only memory,ROM)进行一次校验,而对 Level2 和 Level3 相关的 ROM 和 RAM 进行周期性循环校验;TC29x 的存储器测试模块配置内存测试功能,自带的错误检测和纠正模块能自动纠正 1 位的错误并检测 2 位的错误。

3)内存保护功能。由于不同 ASIL 的软件模块并存于 ECU 中,为实现 FFI,为 QM 和 ASIL B 软件模块划分不同的内存空间,并通过内存保护单元进行配置,使不同 ASIL 的软件模块对各内存空间具备不同的访问权限,QM 软件模块无法改变 ASIL B 软件模块的代码和数据,而 ASIL B 模块可访问 QM 模块,实现不同 ASIL 的软件模块的协同工作,降低故障级联的概率。

4)时钟监控功能。时钟监控的目的是检测并通知时钟异常,TC29x 的时钟控制模块最多可监控 6 个时钟源。

5)供电监控功能。单片机内部不同功能模块的供电电压源不同,TC29x 的电源控制模块提供对外部 5 V、内部 3.3 V、内部 1.3 V 供电等的过压和欠压监控,供电监控与时钟监控都是为了避免出现共因失效。

单片机所支持的监控功能将检测到的错误传输给错误收集和处理模块 SMU,SMU 模块将错误通知

ERR 信号发送给外部监控芯片,外部监控芯片触发独立于主芯片的故障反应,从而实现外部监控芯片对主芯片的监控。监控芯片采用功能安全电源芯片 TLF35xxx,除可实现对芯片自身供电输入、供电输出(单片机供电、通讯专用供电、2 路 5 V 传感器供电)的过压、欠压、对地短路故障监控外,内嵌的窗口狗和功能狗可实现对主芯片的实时监控和程序流监控(AUTOSAR 中称之为逻辑监控)。

窗口狗将时间窗口分为开启(open window,OW)和关闭(closed window,CW)2 个阶段,CW 内不允许喂狗,喂狗必须在 OW 结束前;喂狗使 OW 结束,CW 开启;若在 OW 内无喂狗或在 CW 内喂狗,则窗口狗错误计数器会加 2,并开启一个新的 OW;当错误计数器大于 0 时,正确的喂狗会使计数器减 1。窗口狗不仅可以检测实时任务是否超时,还可检测任务执行间隔是否过快或过慢。

功能狗即问答通信。TLF35xxx 向主芯片提出一个 4 位的问题,同时启动一个从 0 开始计数的心跳计数器,主芯片的答案应包含 4 个响应,根据获得的问题编号和响应编号采用伪随机算法实时计算所得,于心跳周期结束(EGAS 认为不能超过 80 ms)前按顺序将 4 个响应回复给 TLF35xxx,即最后一个响应复位心跳计数器。响应错误或心跳计数器超时,则功能狗错误计数器加 2。Level3 对 Level2 的监控程序进行监控,确保程序按照正确的时序执行,监控结果作为答案的一部分回复给监控芯片,出现问题后监控芯片可发起独立于主芯片的故障反应。

ERR 信号、窗口狗和功能狗错误都会触发监控芯片的安全状态控制功能,TLF35xxx 的安全状态信号 SS1/SS2 拉低,与其关联的安全相关驱动随之关闭,以保护系统。

基于 EGAS 监控概念的高压共轨柴油机控制器功能安全监控为包含功能级、功能监控级和控制器监控级在内的 3 级安全架构,其每层级均涉及到硬件设计(包含芯片选型)和软件逻辑,软硬件共同配合满足需求。该安全架构合理精巧,具有较高的学习和应用价值,其中硬件-Level3(控制器监控级)可作为独立于环境的安全要素应用于其他场景中,如电机驱动控制器等。

依照文献[3]描述的各环节过程来评估产品的功能安全完善程度,评估交付产品的技术水平和工程化能力。采用 MATLAB/Simulink 搭建策略模型,进行故障注入测试,验证系统设计、软件设计与硬件设计有效性。测试结果表明,该监控策略能有效地识别输入轴转速过高的故障,并在故障发生时立即做出响应,有效降低了人身伤害的风险。

3 结语

以工程项目为基础,探讨 EGAS 监控概念在高压共轨柴油发动机控制器多核芯片功能安全实现中的应用。针对避免输入轴转速过高的“预防非预期加速”安全目标,采用 3 级监控方法,通过危害分析和风险评估确定安全目标预防非预期加速,其安全完整性等级为 ASIL B;经过功能安全概念分析确定功能安全需求为转矩监控;在技术安全概念阶段,采用 EGAS 3 级监控概念将转矩监控需求进一步细化并实现 ASIL 等级的分解;设计基于 TC29x 芯片的实现控制器功能安全实现方案。该设计解决了系统复杂化带来的由电气、电子系统故障导致的风险越来越高这一问题,提高了电控系统的安全性和可靠性。

随着汽车行业智能驾驶技术的爆炸式发展,人们发现危害通常源自复杂系统和场景导致的非预期安全问题,因此在功能安全之外又出现了预期功能安全,另外,智能驾驶带来的信息安全问题也日益凸显。功能安全、预期功能安全与信息安全不是相互独立的,三者融合必然会成为新的趋势,整车厂和供应商需要建立起一套完整的安全体系,才能提供给用户安全可靠的产品。

参考文献:

[1]荣芬,吴晓东,许敏. 基于 ISO 标准的道路车辆线控转向系统的功能安全概念设计[J]. 汽车安全与节能学报,2018,9(3):250-257.

[2]International Organization for Standardization. Road vehicles: Functional safety:ISO 26262—2011[S]. Geneva, Switzerland: ISO, 2011.

[3]International Organization for Standardization. Road vehicles: Functional safety: ISO 26262—2018[S]. 2nd ed. Geneva, Switzerland: ISO, 2018.

[4]王俊明,周宏伟. 基于 ISO 26262 的车道保持辅助的功能安全概念设计[J]. 重庆交通大学学报(自然科学版),2019,38(3): 135-142.

[5]MISHRA A, BAUMEISTER M. MCU 实现汽车功能安全合规性[J]. 电子产品世界,2013,20(3):22-24.

[6]Infineon Technologies AG. User's Manual of TC29x B-step 32-bit Single-chip Microcontroller[M]. V1. 2. Munich, Germany: Infineon Technologies AG, 2014.

[7]EGAS Workgroup. Standardized EGAS Monitoring Concept for Gasoline and Diesel Engine Control Units[S]. Version 6. 0. Frankfurt, Germany: EGAS Workgroup, 2015.

[8]董涛,朱元,吴志红,等. 基于 AURIX SafeTlib 的功能安全软件实现[J]. 信息通信,2017,177(9):57-59.

[9]刘法旺,李艳文. 自动驾驶系统功能安全与预期功能安全研究[J]. 工业技术创新,2021,8(3):62-68.

[10]吴静波,卢耀真,李明明,等. 基于 ISO 26262 的新能源汽车转矩监控策略研究[J]. 现代电子技术,2021,44(11): 87-92.

[11]李俊杰. EM-CVT 的功能安全性分析与控制软件实现[D]. 重庆:重庆理工大学,2020.

Functional safety implementation of high-pressure common rail diesel engine control unit based on EGAS monitoring concept

QIN Yan[1,2], WEI Wenjin[1,2], JI Xiaojuan[1,2], CONG Cong[1,2]

1. State Key Laboratory of Internal Combustion Engine Reliability, Weifang 261061, China;

2. Weichai Power Co., Ltd., Weifang 261061, China

Abstract: In order to control the hazard of failure of automobile electronic and electrical systems within an acceptable range, the realization of functional safety of high-pressure common rail diesel engine controller is studied. According to the development process of ISO 26262, relevant items are analyzed around the engine controller; through hazard analysis and risk assessment, the safety objective is determined to prevent unexpected acceleration, and its safety integrity level (ASIL) is B. Through functional safety concept analysis, it is determined that the functional safety requirement is torque monitoring. In the technical safety concept stage, the torque monitoring requirements are further refined and the ASIL level is decomposed by using the EGAS three-level monitoring concept. A safe implementation scheme of controller function based on TC29x chip is designed. MATLAB/Simulink is used to build the strategy model for fault injection test. The results show that the monitoring strategy can effectively identify the fault of high input shaft speed and respond immediately, effectively reducing the risk of personal injury.

Keywords: ISO 26262; high-pressure common rail diesel engine; torque monitoring; TC29x

(责任编辑:郎伟锋)