基于功能安全硬件指标的转向系统方案

李　兵，张小乐，罗　毅
（联创汽车电子有限公司，上海　201206）

摘　要：根据功能安全标准，不同的汽车安全完整性等级（ASIL）对应不同的硬件指标要求。通过对硬件指标和诊断覆盖率的分析，提出了可以满足功能安全硬件指标要求的转向系统控制器方案。该方案包括扭矩传感器、电机位置传感器、电机电流传感器、微控制器等部件，并对系统硬件指标的符合性进行了分析验证。

关键词：转向系统；功能安全；诊断覆盖率；硬件指标
中图分类号：U 463.4　　**文献标志码**：A　　**文章编号**：1673-6540(2021)04-0099-05
doi：10.12177/emca.2020.222

Steering System Scheme Based on Functional Safety Hardware Metrics

LI Bing，　*ZHANG Xiaole*，　*LUO Yi*
（DIAS Automotive Electronic Systems Co.，Ltd.，Shanghai 201206，China）

Abstract：According to functional safety standards，different automotive safety integration levels（ASIL）correspond to different hardware metrics. Through the analysis of hardware metrics and diagnostic coverage，a steering system controller scheme that meets the requirements of functional safety hardware metrics is proposed. The program includes torque sensors，motor position sensors，motor current sensors，micro controllers，etc. The conformity of the system hardware metrics is analyzed and verified.

Key words：steering system；functional safety；diagnostic coverage；hardware metric

0　引　言

随着汽车技术的发展，车载电子电气系统越来越多，功能越来越复杂。为了确保车辆电子电气系统的安全性，ISO 组织于 2011 年发布了 ISO 26262-2011 标准，用于指导车辆电子电气系统的功能安全开发，2018 年发布了 ISO 26262-2018 的第二版[1]，对标准进行了完善，同时该标准也适用于摩托车和商用车以及半导体的开发。中国也于 2017 年正式发布了关于汽车功能安全的标准 GB/T 34590-2017[2]，汽车电子电气系统的功能安全开发越来越受到重视。

功能安全标准中将失效分为系统性失效和随机硬件失效。根据功能安全等级，对系统性失效提出了不同的要求，对随机硬件失效也提出了不同的硬件架构度量指标。目前中国国内对功能安全标准的研究[3]以及转向系统功能安全分析有部分成果[4-5]，对商用车、线控转向系统的安全设计也有研究[1,6]，但对如何满足功能安全标准中硬件指标相关文献较少。为此，本文对如何满足功能安全标准的硬件指标进行了相关分析，并通过分析计算验证系统满足功能安全的硬件指标。

1　转向系统功能安全等级和硬件指标要求

根据功能安全标准，要确定电子电气系统的功能安全等级和功能安全目标，需要完成系统的相关项定义，定义需包括系统的功能、接口、环境

收稿日期：2020-12-09；收到修改稿日期：2021-01-18
作者简介：李　兵（1982—），男，硕士，工程师，研究方向电动转向系统功能安全开发。
张小乐（1981—），男，硕士，研究方向为电动转向系统及其控制。
罗　毅（1978—），男，研究方向为电动转向系统控制开发。

条件、法规要求和已知的可能危害等。电动助力转向(EPS)系统通常使用无刷电机或有刷电机提供转向助力,本文以无刷电机 EPS 系统为例进行分析。典型无刷 EPS 系统示意图如图 1 所示。

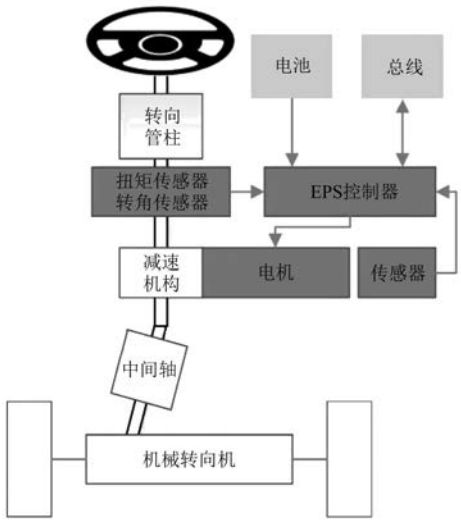

图 1　典型无刷 EPS 系统示意图

EPS 系统的主要功能是控制电机提供助力,辅助驾驶员进行转向操作。EPS 控制器根据转向扭矩传感器和转角传感器的信号以及车辆总线信号,计算出目标电机指令,然后根据电机位置传感器和电流传感器的信号控制无刷电机提供目标输出。根据危害分析和风险评估方法,由严重度 S 暴露度 E 和可控度 C 3 个评分可得到 EPS 系统的整车危害,进而得到汽车安全完整性等级(ASIL)和功能安全目标,文献[1,3]均提到了对 EPS 系统的功能安全分析。根据文献[3],EPS 功能安全等级和功能安全目标如表 1 所示。

表 1　EPS 功能安全等级和功能安全目标[3]

序号	整车危害	ASIL 等级	功能安全目标
1	非预期的车辆侧向运动	D	车辆非预期的侧向运动应满足非预期侧向运动度量
2	非预期的失去侧向运动控制	D	应确保驾驶员对车辆侧向运动的控制能力,相应转向盘手力应满足非预期失去转向控制度量
3	转向沉重	QM-A	转向手力满足转向沉重度量
4	非预期的失去驾驶辅助功能	QM	驾驶辅助功能关闭时影响驾驶员发出功能关闭警示

对于功能安全目标 1 和 2,EPS 系统的安全状态可定义为关闭电机输出,此时转向系统恢复机械转向,驾驶员仍可通过方向盘正常驾驶车辆,保证车辆安全。对于功能安全目标 3 和 4,功能安全等级为 QM 或 ASIL A,EPS 系统的安全状态也可以为关闭电机输出,保证机械转向能力。

上述 EPS 功能安全等级包括 ASIL D ASIL A 和 QM,按照功能安全标准[2] ASIL D 等级对应的硬件指标要求:单点故障度量(SPFM)>99%,潜伏故障度量(LFM)>90%,随机硬件失效概率度量(PMHF)<10 硬件失效率(FIT)。QM 和 ASIL A 无硬件指标要求。

2　硬件指标的计算方法

功能安全标准 ISO 26262－2018 和 GB/T 34590－2017 中定义了硬件指标的具体计算方法和过程,文献[7]中也对实践中如何进行功能安全硬件指标的计算提出了部分建议。

根据功能安全标准需使用失效模式、影响及其诊断分析 FMEDA 和定量故障树分析(FTA)方法对硬件指标进行计算,计算过程简言之就是对系统中所有安全相关的元器件进行失效率 FIT 的计算,通过对诊断覆盖率和故障类型进行分析,可以得到不同类型故障的 FIT 数值,最后将结果进行汇总就可以得到系统的 SPFM、LFM、PMHF。

根据文献[7],对于 ASIL D 目标的单点故障需要选取覆盖率高的诊断机制,即诊断覆盖率达到 99%,这样通常可满足系统整体单点故障度量>99%的要求。在此基础上对于潜伏故障也尽可能进行诊断,通常也可满足系统 LFM>90%的要求。选取高诊断覆盖率的单点故障安全机制和潜伏故障安全机制同样有助于系统满足 PMHF 的要求。

3　转向系统设计方案

图 2 是一种满足 ASIL D 功能安全等级的 EPS 系统设计方案。包括扭矩和转角传感器、CAN 通信、电源等外部接口,控制器内部有微控制器、电源芯片、驱动芯片和驱动桥,以及相分离驱动和相分离电路,还有执行器三相无刷电机以及电机位置传感器和电流传感器。以下对各部件满足功能安全要求的设计方案进行简单说明。

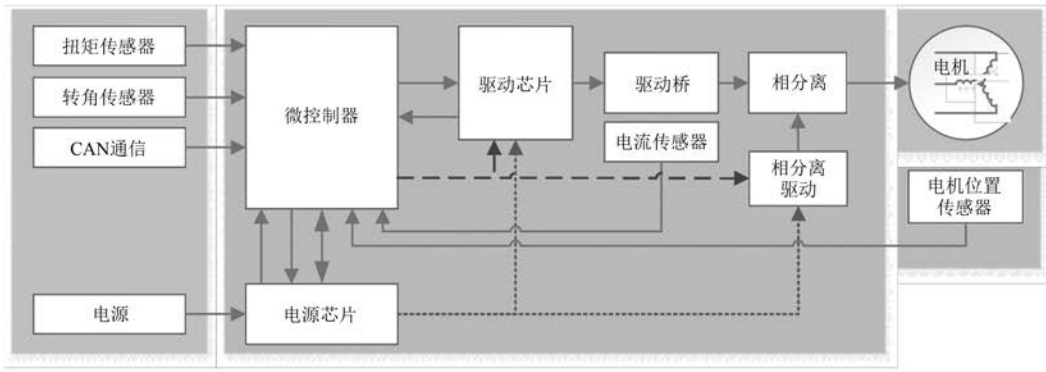

图 2　EPS 系统设计方案

3.1　安全路径

如前所述,EPS 系统的功能安全最高等级是 ASIL D,安全状态是关闭电机助力,使系统进入安全状态的方式称为安全路径。

在图 2 的 EPS 系统中设计有 2 条安全路径。其中,虚线标注的即为安全路径。一条安全路径通过微控制器关闭电机驱动电路并使能相分离电路,使电机输出关闭。另一条由带看门狗功能的电源芯片实现,当微控制器无法正确运行时,看门狗电路可以发现该故障并通过电路关闭电机驱动电路并使能相分离电路,使电机输出关闭。

2 条安全路径的设计可以保证发生任意故障时,系统均可以进入安全状态。同时,方案中需保证系统断电及初始化时安全路径处于关闭状态。

3.2　扭矩传感器

由 EPS 基本工作原理可知,扭矩传感器信号如出错可能直接违反功能安全目标 1,因此该传感器与该功能安全目标的实现密切相关,由第 2 节可知,对于该部件需选择诊断覆盖率达到 99% 的安全机制。

表 2　传感器安全机制诊断覆盖率[2]

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率
通过在线监控进行失效探测	D.2.1.1	低
测试模式	D.2.6.1	高
输入比对/表决(1oo2、2oo3 或者更好的冗余)	D. 2. 6. 5	高
传感器有效范围	D.2.10.1	低
传感器相关性	D.2.10.2	高
传感器合理性检查	D.2.10.3	中

根据 GB/T 34590 标准第五部分附录 D(表 2),对于传感器选择 D.2.6.1,D.2.6.5,D.2.10.2 等安全机制可以实现高诊断覆盖率,即 99%。在该 EPS 系统中,对于扭矩传感器选择两通道的设计方案,即 D.2.6.5,可满足扭矩传感器的高诊断覆盖率要求。

该 EPS 系统中扭矩传感器信号如图 3 所示。2 个通道的信号斜率相反,差异化的设计方案可以降低共因失效概率。

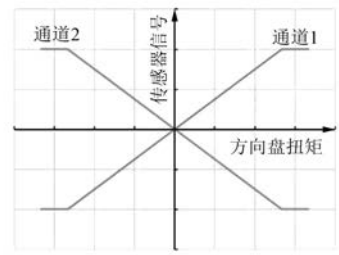

图 3　扭矩传感器信号示意图

3.3　微控制器

微控制器是 EPS 系统的核心器件,对于微控制器的处理单元、存储器、片上通信等均需要考虑可能的失效模式和对应的安全机制。本文 EPS 系统的微控制器选用成熟芯片供应商提供的满足 ASIL D 等级的微控制器,包含锁步核、ECC 存储、内部通信保护及时钟监控、电源监控等多种安全机制以及 SMU 故障处理模块。通过选用 ASIL D 的芯片来满足对于微控制器高诊断覆盖率的要求。

电压异常或微控制器损坏时微控制器自身无法保证其输出的安全,需要外部电压监控电路和外部看门狗电路对微控制器进行监控。

3.4 电源芯片和看门狗

为了保证系统满足功能安全要求,除了微控制器内部各安全机制之外,还需要对微控制器的供电采用适当的安全机制,同时需要通过看门狗功能对微控制器的程序运行进行监控。

对于微控制器的供电,可选用带输出电压监控(安全机制 D.2.8.2,表 3)的电源芯片;对于程序运行监控,可选用对程序序列的时间和逻辑监控的组合(安全机制 D.2.9.4,表 4)。本文 EPS 系统选择了带看门狗和电源监控的电源芯片,同时该芯片具备安全路径功能,在上述安全机制检测到相应故障时,可直接关闭电机输出,保证系统进入安全状态。

表 3 电源安全机制诊断覆盖率[2]

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率
电压或电流控制(输入)	D.2.8.1	低
电压或者电流控制(输出)	D.2.8.2	高

表 4 程序序列安全机制诊断覆盖率[2]

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率
具有独立时间基准,无时间窗口的看门狗	D.2.9.1	低
具有独立时间基准和时间窗口的看门狗	D.2.9.2	中
程序序列的逻辑监控	D.2.9.3	中
对程序序列的时间和逻辑监控的组合	D.2.9.4	高
基于时间的程序序列的时间和逻辑联合监控	D.2.9.5	高

3.5 电机驱动电路

电机是 EPS 系统中的执行器,根据 GB/T 34590 标准第五部分附录 D(表 5),对于执行器选择 D.2.6.1 测试模式,D.2.11.1 监控(即一致性测试)可以实现高的诊断覆盖率(即 99%)。在本 EPS 系统中,对于电机驱动电路采用了监控电机实际电流的设计方案,即 D.2.11.1,该方案可以满足对执行器的高诊断覆盖率的要求。

表 5 执行器安全机制诊断覆盖率[2]

安全机制/措施	参见技术概览	可实现的典型诊断覆盖率
通过在线监控进行失效探测	D.2.1.1	低
测试模式	D.2.6.1	高
监控(即一致性控制)	D.2.11.1	高

3.6 电机电流传感器

根据 EPS 基本工作原理可知,电流传感器如出错也会直接违反功能安全目标 1,因此对于该部件也需选择诊断覆盖率达到 99% 的安全机制。图 4 所示为电流示意图,选择三相/三路电流采样的设计方案,根据基尔霍夫第一定律,电机三相电流之和始终为零,该安全机制也属于功能安全标准中的 D.2.6.5。该方案可以满足对电流传感器高诊断覆盖率的要求,例如可以诊断出单个电流采样值卡滞或漂移等故障。如出现电机对壳体漏电流等非电流传感器故障,通过三相电流和也可以判断系统出现异常,使系统进入安全状态。

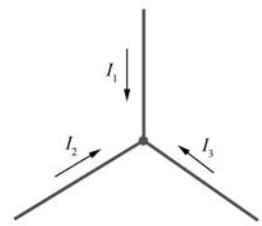

图 4 电流示意图

3.7 电机位置传感器

对于采用三相无刷电机的 EPS 系统,电机位置传感器若出错也会直接违反功能安全目标 1 和功能安全目标 2,因此该部件也需选择诊断覆盖率达到 99% 的安全机制。本文 EPS 系统中,电机位置传感器也选择了两通道设计方案,即 D.2.6.5。图 5 为本文设计方案中电机位置传感器信号示意图。通道 1 为直接角度信号,通道 2 传感器为磁阻传感器,在电机轴处有磁钢,磁钢旋转产生的磁场方向变化会使该传感器输出 sin 和 cos 两路信号,两路信号满足三角函数关系,通过

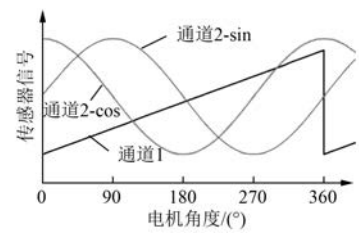

图 5 电机位置传感器信号示意图

对两路信号的比值 sin/cos 进行反正切计算也可以得到电机角度,同时 2 个通道差异化的设计方案也可以降低共因失效概率。该方案可以满足对电机位置传感器高诊断覆盖率的要求。

3.8 系统方案总结

综上所述,所提 EPS 系统各个与安全目标相关部件均选择了高诊断覆盖率,通过标准中 FMEDA 和定量 FTA 方法对硬件指标进行计算和分析,可得校核结果如表 6 所示。

表 6 硬件指标校核结果

功能安全目标	ASIL 等级	SPFM/%	LFM/%	PMHF
车辆应满足非预期侧向运动度量	D	99.55	98.70	7.11FIT
应满足非预期失去转向控制度量	D	99.73	98.69	5.77FIT

可以看出,本文 EPS 的系统方案满足 2 个 ASIL D 功能安全目标的 SPFM、LFM 和 PMHF 指标,另外 2 个功能安全目标等级为 QM 和 ASIL A,这 2 个目标无硬件指标要求。综上,所提 EPS 系统满足功能安全标准规定的随机硬件失效的硬件指标度量。

4 结　语

汽车电子电气系统越来越复杂,按照功能安全标准对控制器进行开发来保证车辆安全也越来越重要。本文介绍了汽车转向系统的功能安全目标和功能安全等级,以及功能安全标准中硬件指标的基本要求和计算方法。重点分析了转向控制器中各个硬件部件对功能安全目标的影响以及安全机制的选择,通过对所有相关部件的安全设计可以保证控制器系统满足功能安全硬件指标。

本文主要探讨了针对随机硬件失效的安全机制,对于系统性失效,功能安全标准中主要通过开发流程和分析评审验证等来避免;另外针对部分系统性失效也可以采用 E-Gas 3 层架构或其他安全机制来监控,保证系统安全[8]。

该 EPS 系统方案属于 Fail Silent 系统,发生失效后的安全状态是关闭转向电机输出。随着高等级自动驾驶的开发,转向系统需要实现 Fail Operational 的要求,在无人驾驶中即使发生失效后仍能提供转向功能。Fail Operational 对转向系统提出了更高的要求,需要在本文 Fail Silent 系统的基础上对转向系统进行冗余设计,从而保证自动驾驶中的整车安全[9]。

【参 考 文 献】

[1] 徐闯,谭雁清. 基于 ISO26262 的商用车电动助力转向功能安全设计[J]. 汽车零部件,2018(6):34.

[2] 全国汽车标准化技术委员会. 道路车辆功能安全:GB/T 34590-2017[S]. 2017.

[3] 付越,李波,尚世亮,等. 乘用车转向系统功能安全标准研究[J]. 中国汽车,2019(8):43.

[4] 吴炜,黄迪,陈迹,等. 电动助力转向系统(EPS)的功能安全相关分析初探[C]//2015 中国汽车工程学会年会论文集,2015.

[5] 黄晓玫,魏慧琴. 基于 ISO 标准的 EPS 系统的功能安全分析[C]//中国计算机用户协会网络应用分会 2019 年第二十三届网络新技术与应用年会,2019.

[6] 荣芩,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.

[7] 罗来军,李兵. 功能安全硬件指标计算的实践[J]. 传动技术,2019,33(2):37.

[8] 伍理勋,陈建明,陈磊,等. 电动汽车电机驱动控制器功能安全架构研究[J]. 控制与信息技术,2018(3):1.

[9] 胡伟,林成杰,吴虎强. 自动驾驶汽车下电动助力转向发展研究[J]. 汽车零部件,2019(1):81.

(上接第 82 页)

[9] 罗德荣,贺锐智,黄守道,等. 单定子双转子盘式对转永磁同步电机动态滑模控制[J]. 电工技术学报,2019,34(9):1806.

[10] DENG W, ZUO S. Axial force and vibroacoustic analysis of external-rotor axial-flux motors[J]. IEEE Transactions on Industrial Electronics, 2018, 65(3): 2018.

[11] 唐任远. 现代永磁电机理论与设计[M]. 北京:机械工业出版社,1997.