

团体标准

乘用车智能底盘域控制器硬件功能安全要求及验证

Hardware functional safety requirements and verification for passenger cars
intelligent chassis domain control unit

(报批稿)

20xx-xx-xx 发布

20xx-xx-xx 实施

中国汽车工程学会 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 底盘域控制器硬件功能安全要求	2
5.1 微控制器	2
5.2 外扩存储	3
5.3 供电	3
5.4 通信	4
5.5 输入接口	4
5.6 驱动输出	5
5.7 约束性要求	6
6 底盘域控制器硬件功能安全验证	7
6.1 一般要求	7
6.2 耐用性和鲁棒性测试	7
6.3 硬件安全要求完整性和正确性测试	7
6.4 测试用例导出方法	9
附录 A（资料性） 底盘域控制器硬件架构及接口	10
附录 B（资料性） 底盘域控制器硬件相关安全目标	11
B.1 横向控制安全目标	11
B.2 纵向控制安全目标	11
B.3 垂向控制安全目标	11
附录 C（规范性） 功能安全耐用性和鲁棒性测评	12
C.1 可靠性试验	12
C.2 电磁兼容试验	13
C.3 电性能试验	14

前言

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

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电动汽车产业技术创新战略联盟提出。

本文件由中国汽车工程学会标准化工作委员会归口。

本文件起草单位：北京经纬恒润科技股份有限公司、清华大学、中国科学院电工研究所、中国汽车工程研究院股份有限公司、北京奥特尼克科技有限公司、北京理工大学、比亚迪汽车工业有限公司、芜湖伯特利汽车安全系统股份有限公司、国汽（北京）智能网联汽车研究院有限公司、吉利汽车研究院（宁波）有限公司、中国第一汽车集团有限公司研发总院、东风汽车集团有限公司、重庆长安汽车股份有限公司、奇瑞汽车股份有限公司、长城汽车股份有限公司、舍弗勒投资（中国）有限公司、上海交通大学、辰致科技有限公司、武汉瑞立科德斯汽车电子有限责任公司、上海利氮科技有限公司、上海同驭汽车科技有限公司、北京北方车辆新技术孵化器有限公司、厦门国创中心先进电驱动技术创新中心、通标标准技术服务（天津）有限公司。

本文件主要起草人：范成建、张淑颖、张明、王政芳、莫新勇、杨正兰、谭志海、张俊智、何承坤、马瑞海、苟晋芳、王丽芳、吴艳、刘国芳、陆晓磊、唐俊、邹波、李士盈、王帅、王汉岭、施国标、吕海军、陈敏、朱琳、强玉霖、刘兴亮、周景岩、叶灿华、杨贵永、司凯中、王德平、高尚、屈新田、闫涛卫、吴珂、乔斌、肖智灵、刘佳勇、王健、杨文谦、李鑫、李栋梁、张晓亮、吴晓华、陈婧雅、吴晓东、张宇、程毅、包汉伟、苏干厅、张晓峰、舒强、彭玉钢、潘光亮、吴彦昭、林靖、王歆朔、于洪达。

乘用车智能底盘域控制器硬件功能安全要求及验证

1 范围

本文件规定了乘用车智能底盘域控制器硬件的功能安全要求及其验证方法。

本文件适用于乘用车智能底盘域控制器硬件。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19951 道路车辆 电气/电子部件对静电放电抗扰性的试验方法

GB/T 21437.2—2021 道路车辆 电气/电子部件对传导和耦合引起的电骚扰试验方法 第2部分：沿电源线的电瞬态传导发射和抗扰性

GB/T 21437.3 道路车辆 电气/电子部件对传导和耦合引起的电骚扰试验方法 第3部分：对耦合到非电源线电瞬态的抗扰性

GB/T 28046.1—2011 道路车辆 电气及电子设备的环境条件和试验 第1部分：一般规定

GB/T 28046.2—2019 道路车辆 电气及电子设备的环境条件和试验 第2部分：电气负荷

GB/T 28046.3—2011 道路车辆 电气及电子设备的环境条件和试验 第3部分：机械负荷

GB/T 28046.4—2011 道路车辆 电气及电子设备的环境条件和试验 第4部分：气候负荷

GB/T 28046.5—2013 道路车辆 电气及电子设备的环境条件和试验 第5部分：化学负荷

GB/T 33014.2 道路车辆 电气/电子部件对窄带辐射电磁能的抗扰性试验方法 第2部分：电波暗室法

GB/T 33014.4 道路车辆 电气/电子部件对窄带辐射电磁能的抗扰性试验方法 第4部分：线束激励法

GB/T 34590.1—2022 道路车辆 功能安全 第1部分：术语

GB/T 34590.5—2022 道路车辆 功能安全 第5部分：产品开发：硬件层面

GB/T 34590.7 道路车辆 功能安全 第7部分：生产、运行、服务和报废

GB/T 34590.8—2022 道路车辆 功能安全 第8部分：支持过程

GB/T 41295.3—2022 功能安全应用指南 第3部分：测试验证

3 术语和定义

GB/T 34590.1—2022 界定的以及下列术语和定义适用于本文件。

3.1

安全目标 safety goal

作为整车层面危害分析和风险评估结果的最高层面的安全要求。

[来源：GB/T 34590.1—2022，3.139]

3.2

安全机制 safety mechanism

为了保持预期功能或者达到/保持某种安全状态，由电气/电子系统的功能/要素或者其他技术来实施的技术解决方案，以探测并减轻/容许故障、或者控制/避免失效。

[来源：GB/T 34590.1—2022，3.142]

3.3**冗余 redundancy**

除了足以实施所需功能或足以表达信息的方法外，还存在其他方法。

示例 1：重复的功能组件是冗余的一个实例，其目的是增加可用性或用于故障探测。

示例 2：对表示安全相关信息的数据增加奇偶校验位，为故障探测提供了冗余。

[来源：GB/T 34590.1—2022，3.122]

3.4**故障运行 fail operational**

功能降级模式的一种，发生违反安全目标（3.1）的故障后，功能按照标称性能运行或按照受限性能运行的功能降级模式。

3.5**汽车安全完整性等级（ASIL） Automotive Safety Integrity Level**

四个等级中的一个等级，用于定义相关项或要素需要满足的 GB/T 34590 的要求和安全措施，以避免不合理风险，其中，D 代表最高严格等级，A 代表最低严格等级。

[来源：GB/T 34590.1—2022，3.6]

4 缩略语

下列缩略语适用于本文件。

AOU：应用假设（Assumption of Use）

ASIL：汽车安全完整性等级（Automotive Safety Integrity Level）

EPB：电子驻车制动（Electronic Parking Brake）

FHTI：故障处理时间间隔（Fault Handling Time Interval）

FIT：失效率（Failure In Time）

LFM：潜伏故障度量（Latent Fault Metric）

PMHF：随机硬件失效概率度量（Probabilistic Metric for random Hardware Failure）

SGVER：车辆垂向控制安全目标（Safety Goal for Vehicle Vertical Control）

SPFM：单点故障度量（Single Point Fault Metric）

5 底盘域控制器硬件功能安全要求**5.1 微控制器**

5.1.1 当降级模式为故障运行时，底盘域控制器硬件应至少具备两路冗余的微控制器，硬件架构及接口参见附录 A。

5.1.2 微控制器应满足功能安全 ASIL D 等级。

5.1.3 微控制器故障探测和响应时间之和应小于分配给微控制器的 FHTI 要求。

注：微控制器的 FHTI 要求，根据整车企业或零部件厂商提供的底盘域控制器的 FHTI 进行分配计算。

5.1.4 微控制器安全手册中所提及的 AOU 属于应实现及验证；对于未实现或验证的安全应用假设，应给出充足的理由。

5.1.5 微控制器应具备安全机制，对中央处理器的故障进行探测，并支持用户对故障处理进行配置。

5.1.6 微控制器应具备安全机制，对时钟系统的故障进行探测，并支持用户对故障处理进行配置。

5.1.7 微控制器应具备安全机制，对存储的故障进行探测并支持用户对故障处理进行配置。

注：对硬件没有存储安全机制的情况，则由软件对安全相关的代码和数据进行故障诊断和处理（前提条件是软件安全机制对该存储故障的诊断覆盖度满足相应的 ASIL 等级需求，诊断时间间隔满足 FHTI 要求）。

5.1.8 微控制器应具备安全机制，对内部总线故障进行探测，并支持用户对故障处理进行配置。

5.1.9 除 5.1.5—5.1.8 中的硬件资源外，对于微控制器内其他安全相关的硬件资源及外设资源，底盘域控制器硬件应具备安全机制对其故障进行诊断，并支持用户对故障处理进行配置。

示例 1：由硬件进行冗余通路设计，软件对硬件冗余通路进行比较。

示例 2：硬件进行独立的故障状态采集，软件/硬件进行故障确认和故障处理。

5.1.10 底盘域控制器硬件应具备独立的微控制器故障探测电路，当微控制器发生故障且无法通过微控制器自身维持安全状态时，该独立的微控制器故障探测电路应探测到微控制器故障，且应具备独立于微控制器的故障处理模块，保证当微控制器故障时，所有功能处于安全状态，安全状态参见附录 B。

示例：微控制器检测到内部故障后，控制某一个或多个特定的故障指示管脚电平发生变化，该电平变化触发外部独立的微控制器故障探测电路，使得系统进入安全状态。

5.1.11 底盘域控制器硬件应保证微控制器在上下电过程中及复位状态下，所有安全相关的功能处于安全状态，安全状态参见附录 B。

5.1.12 微控制器硬件应具备存储权限管理模块，支持用户通过软件配置实现存储的免干扰设计。

示例：微控制器具备存储保护单元（MPU）。

5.2 外扩存储

5.2.1 当底盘域控制器有外扩存储模块且该模块存储了安全相关的数据，对于未依赖软件进行存储故障校验设计的情况，底盘域控制器硬件应具备安全机制，对外扩存储的故障进行探测和故障处理。

5.2.2 当底盘域控制器有外扩存储模块且该模块存储了安全相关的数据，对于未依赖软件进行存储故障校验设计的情况，底盘域控制器硬件应具备安全机制，对外扩存储与微控制器接口的故障进行探测和处理。

5.3 供电

5.3.1 底盘域控制器硬件电源接口设计应符合 C.2 及 C.3 的试验评价准则要求。

5.3.2 当降级模式为故障运行时，底盘域控制器应具备冗余的外部供电。

5.3.3 当降级模式为故障运行时，底盘域控制器应对冗余的外部供电设计独立的电源电压采集电路，并

将采集到的电压信号连接到独立的微控制器外设模块。

5.3.4 内部电源芯片应为底盘域控制器内部安全相关模块提供功能安全 ASIL D 的供电。

5.3.5 当降级模式为故障运行时，构成冗余功能的两个硬件模块应具备独立供电模块。

5.3.6 底盘域控制器硬件应具备独立于电源芯片的故障检测和处理电路，当电源芯片发生故障且无法维持正常供电功能，该独立的故障检测和处理电路应保证所有功能处于安全状态，安全状态参见附录 B。

5.4 通信

当降级模式为故障运行时，应设计冗余的通信模块，对功能安全相关的信号进行接收/发送，避免由于通信故障导致违反附录 B 的安全目标。

5.5 输入接口

5.5.1 EPB 开关采集

底盘域控制器硬件宜提供 EPB 开关采集接口电路。该接口电路应采集 EPB 开关状态或故障状态并传递到微控制器软件，支持软件进行 EPB 命令判断及故障诊断，避免由于 EPB 开关故障导致违反 B.2 的安全目标。

注：EPB 命令包括驻车、释放和空挡。

5.5.2 轮速传感器

底盘域控制器硬件宜提供轮速采集接口电路。该接口电路应采集轮速信号并传递到微控制器软件，支持软件进行轮速判断及故障诊断，避免由于轮速采集接口故障导致违反附录 B 的安全目标。

5.5.3 转向角度/位移传感器

底盘域控制器硬件宜提供转向角度/位移采集接口电路。该接口电路应采集转向角度/位移信号并传递到微控制器软件，支持软件进行转向角度/位移判断及故障诊断，避免由于角度/位移传感器采集接口故障导致违反 B.1 的安全目标。

5.5.4 方向盘转角传感器

底盘域控制器硬件宜提供方向盘转角采集接口电路，该接口电路应采集方向盘转角信号并传递到微控制器软件，支持软件进行方向盘转角判断及故障诊断，避免由于方向盘转角采集接口故障导致违反 B.1 的安全目标。

5.5.5 驾驶员手力扭矩传感器

底盘域控制器硬件宜提供扭矩传感器的驾驶员手力扭矩采集接口电路。该接口电路应采集驾驶员手力矩信号并传递到微控制器软件，支持软件进行驾驶手力扭矩判断及故障诊断，避免由于驾驶员手力扭矩采集接口故障导致违反 B.1 的安全目标。

5.5.6 车身高度传感器

底盘域控制器硬件宜提供车身高度采集接口电路。该接口电路应采集车身高度信号并传递到微控制器软件，支持软件进行车身高度判断及故障诊断，避免由于车身高度传感器采集接口故障导致违反 B.3 的安全目标。

5.5.7 制动踏板采集

底盘域控制器硬件宜提供制动踏板采集接口电路。该接口电路应采集驾驶员制动踏板请求并传递到微控制器软件，支持软件进行制动踏板开度判断及故障诊断，避免由于制动踏板采集接口故障导致违反 B.2 的安全目标。

5.5.8 加速踏板采集

底盘域控制器硬件宜提供加速踏板采集接口电路。该接口电路应采集到驾驶员加速踏板请求并传递到微控制器软件，支持软件进行加速踏板开度采集及故障诊断，避免由于加速踏板采集接口故障导致违反 B.2 的安全目标。

5.6 驱动输出

5.6.1 EPB 电机驱动输出

5.6.1.1 底盘域控制器宜提供 EPB 电机驱动输出模块。该驱动输出模块应满足 5.6.1.2—5.6.1.9 的要求。

5.6.1.2 底盘域控制器硬件应具备独立于 EPB 驱动电路的安全机制进行 EPB 驱动电路故障探测和处理，应在 FHTI 时间内导入安全状态，安全状态 B.2。

5.6.1.3 底盘域控制器硬件应具备 EPB 电机电流采集模块，将采集到的电流信号传递到微控制器。

5.6.1.4 底盘域控制器硬件应具备 EPB 电机电压采集电路，将采集到的电压信号传递到微控制器。

5.6.1.5 底盘域控制器硬件应具备 EPB 电机输出状态反馈电路，能够支持软件区分 EPB 电机的动作和不动作状态，并将采集到的输出状态传递到微控制器。

5.6.1.6 底盘域控制器硬件应具备独立于 EPB 电机驱动电路的故障关断路径，当 EPB 电机驱动电路故障时，底盘域控制器硬件应通过该独立的故障关断路径控制电机停止运动。

5.6.1.7 左右卡钳的 EPB 电机驱动电路应具备各自的输出状态反馈电路。

5.6.1.8 EPB 电机驱动电路应与输出状态反馈电路独立。

5.6.1.9 EPB 电机驱动功能电路应与 EPB 故障关断模块独立。

5.6.2 空气弹簧高度电磁阀驱动输出

5.6.2.1 底盘域控制器宜提供空气弹簧高度电磁阀驱动输出模块。该驱动输出模块应满足 5.6.2.2—5.6.2.6 的要求。

5.6.2.2 底盘域控制器硬件应具备独立于空气弹簧高度电磁阀驱动电路的安全机制，进行该驱动电路故障探测和处理，应在 FHTI 时间内导入安全状态，安全状态参见 B.3。

5.6.2.3 底盘域控制器硬件应具备空气弹簧高度调节电磁阀输出状态反馈电路，能够支持软件区分电磁阀的动作和不动作状态，并将采集到的输出状态传递到微控制器。

5.6.2.4 底盘域控制器硬件应具备独立于空气弹簧高度电磁阀驱动电路的故障关断路径，当空气弹簧高度电磁阀驱动电路故障时，该故障关断路径应关闭电磁阀。

5.6.2.5 空气弹簧高度电磁阀驱动电路应与输出状态反馈电路独立。

5.6.2.6 空气弹簧高度电磁阀驱动电路应与空气弹簧高度电磁阀故障关断路径独立。

5.6.3 空气弹簧进气电磁阀驱动输出安全要求

5.6.3.1 底盘域控制器宜提供空气弹簧进气电磁阀驱动输出模块。该驱动输出模块应满足 5.6.3.2—5.6.3.6 的要求。

5.6.3.2 底盘域控制器硬件应具备独立于空气弹簧进气电磁阀驱动电路的安全机制，进行该驱动电路故障探测和处理，应在 FHTI 时间内导入安全状态，安全状态参见 B.3。

5.6.3.3 底盘域控制器硬件应具备空气弹簧进气电磁阀输出状态反馈电路，能够支持软件区分电磁阀的动作和不动作状态，并将采集到的输出状态传递到微控制器。

5.6.3.4 底盘域控制器硬件应具备独立于空气弹簧进气电磁阀驱动电路的故障关断路径，当空气弹簧进气电磁阀驱动电路故障时，硬件应关闭电磁阀。

5.6.3.5 空气弹簧进气电磁阀驱动电路应与输出状态反馈电路独立。

5.6.3.6 空气弹簧进气电磁阀驱动电路应与空气弹簧进气电磁阀故障关断路径独立。

5.6.4 空气弹簧排气电磁阀驱动输出安全要求

5.6.4.1 底盘域控制器宜提供空气弹簧排气电磁阀驱动输出模块。该驱动输出模块应满足 5.6.4.2—5.6.4.6 的要求。

5.6.4.2 底盘域控制器硬件应具备独立于空气弹簧排气电磁阀驱动电路的安全机制，进行该电磁阀驱动电路故障探测和处理，应在 FHTI 时间内导入安全状态，安全状态参见 B.3。

5.6.4.3 底盘域控制器硬件应具备空气弹簧排气电磁阀输出状态反馈电路，能够支持软件区分电磁阀的动作和不动作状态，并将采集到的输出状态传递到微控制器。

5.6.4.4 底盘域控制器硬件应具备独立于空气弹簧排气电磁阀驱动电路的故障关断路径，当微控制器故障/域控制器内部供电故障/电磁阀驱动电路故障时，硬件应关闭电磁阀。

5.6.4.5 空气弹簧排气电磁阀驱动电路应与输出状态反馈电路独立。

5.6.4.6 空气弹簧排气电磁阀驱动电路应与空气弹簧排气电磁阀故障关断路径独立。

5.7 约束性要求

5.7.1 底盘域控制器硬件部分如有 ASIL 等级分解，应进行独立性分析。

5.7.2 应对支撑故障运行的冗余资源进行独立性分析。

5.7.3 应对安全机制和被诊断的硬件模块进行独立性分析。

5.7.4 底盘域控制器硬件应支持安全机制自检。

5.7.5 底盘域控制器硬件设计中，对于符合 GB/T 34590 要求的芯片，硬件设计应实现芯片安全手册中对硬件的应用假设。对于未实现/未验证的安全应用假设，应给出充足的理由。

5.7.6 底盘域控制器硬件设计所选用的硬件元器件，应符合 GB/T 34590.8—2022 中 13.4 的要求。

5.7.7 底盘域控制器的硬件元器件/模块设计应满足外部环境和运行应力的要求。

5.7.8 底盘域控制器应进行硬件指标计算，如无特殊规定，目标值要求应符合表 1 的规定。

表 1 底盘域控制器硬件指标目标值要求

ASIL 等级	SPFM	LFM	PMHF (FIT)
ASIL B	90%	60%	100 ^a
ASIL C	97%	80%	100 ^a
ASIL D	99%	90%	10 ^a
^a 整车企业或零部件厂商根据实际相关项的系统复杂度，定义底盘域控制器的 PMHF 要求。			

5.7.9 底盘域控制器硬件开发和验证流程应满足 GB/T 34590.5 的要求。

5.7.10 底盘域控制器的生产、运行、服务、报废流程应满足 GB/T 34590.7 的要求。

6 底盘域控制器硬件功能安全验证

6.1 一般要求

6.1.1 应按照 GB/T 34590.5—2022 中 6.4.9 和 7.4.4 对 5.1—5.7 中的硬件安全要求及设计进行验证。

6.1.2 硬件功能安全验证测试，应包含在环境和运行应力作用下的耐用性和鲁棒性测试，以及硬件安全要求完整性和正确性的测试。硬件功能安全验证测试的输入材料应包含硬件需求定义、硬件原理图、软硬件接口定义等。

6.2 耐用性和鲁棒性测试

底盘域控制器采用可靠性试验、电磁兼容试验、电性能试验进行耐用性和鲁棒性测试，验证底盘域控制器硬件满足 5.1—5.6 中的设计要求，测试方法及评价准则符合附录 C。

底盘域控制器耐用性和鲁棒性测试方法应满足 GB/T 34590.5—2022 中 10.4.6 的要求。

6.3 硬件安全要求完整性和正确性测试

6.3.1 功能测试

6.3.1.1 功能测试一般要求

在正常室内没有增加额外的环境应力下，应采用功能测试方法验证底盘域控制器硬件满足 5.1—5.6 中的设计要求。

6.3.1.2 微控制器功能测试

测试方法：在底盘域控制器定义的电源电压范围内，测试微控制器的电源质量、上下电过程中功能安全相关的引脚状态、微控制器晶体、微控制器安全假设中硬件实现的部分。

评价准则：微控制器功能满足 5.1 硬件设计要求。

6.3.1.3 外扩存储功能测试

测试方法：使底盘域控制器正常运行，测试外扩存储的电源质量、外扩存储与微控制器之间的接口波形特性及读写操作。

评价准则：外扩存储功能满足 5.2 硬件设计要求。

6.3.1.4 供电相关功能测试

测试方法：在底盘域控制器定义的电源电压范围内调节电源电压，测试底盘域控制器硬件功能及电源相关的休眠唤醒功能。测试底盘域控制器内部安全相关的芯片的供电质量。

评价准则：底盘域在定义的电源电压范围内，硬件功能满足设计要求。内部安全相关芯片的供电满足 5.3 设计要求。

6.3.1.5 通信功能测试

测试方法：对通信硬件模块进行测试，含供电质量、通信模块与微控制器之间的交互接口及收发工况、外部接口电平特性。

评价准则：通信模块功能满足 5.4 设计要求。

6.3.1.6 输入接口功能测试

测试方法：将实际的外部传感器或与实际传感器特性相符的外部信号与底盘域控制器连接，监控软件判断的信号结果。

评价准则：输入接口模块满足 5.5 设计要求。

6.3.1.7 驱动输出功能测试

测试方法：将实际的外部负载与底盘域控制器连接，软件控制负载按照所定义的工况工作，监控负载的工作状态及软件读取的电压/电流反馈信号。

评价准则：驱动输出模块满足 5.6 设计要求。

6.3.2 故障注入测试

6.3.2.1 故障注入测试一般要求

底盘域控制器应采用故障注入测试方法，模拟硬件元器件/模块的失效，验证 5.1—5.6 中底盘域控制器硬件资源安全机制的有效性。不同类型硬件元器件/模块的故障注入方式，参考 GB/T 41295.3—2022 中 9.6。

6.3.2.2 冗余安全机制故障注入测试

测试方法：对微控制器、供电模块、通信模块等冗余设计进行测试，模拟冗余硬件模块中的一个模块失效，在底盘域控制器正常运行时注入该失效，对冗余模块中另一个模块的功能和性能进行监控。

评价准则：冗余设计的两个模块中，一个模块失效后，另一个模块仍能满足设计需求。

6.3.2.3 微控制器故障注入测试

测试方法：模拟微控制器内部某一单点失效使其触发微控制器故障探测，当底盘域控制器正常运行时注入该失效，对 5.1.10 中微控制器故障探测电路及故障处理模块进行监控。

评价准则：微控制器故障时底盘域控制器能够进入安全状态，安全状态参见附录 B。

6.3.2.4 输入接口故障注入测试

测试方法：模拟与 5.5 中实际硬件接口功能相符的失效，当底盘域控制器正常运行时注入该失效，对软件判断结果进行监控。

评价准则：软件可以对故障做出正确判断。

6.3.2.5 输出驱动故障注入测试

测试方法：模拟与 5.6 中实际硬件输出功能相符的失效，当底盘域控制器正常运行时注入该失效，对软件判断结果进行监控，同时对输出驱动状态进行检测。

评价准则：软件可以对故障做出正确判断，故障后输出驱动状态满足安全状态的要求，安全状态参见附录 B。

6.4 测试用例导出方法

底盘域控制器硬件测试用例应按照 GB/T 34590.5—2022 中 10.4.4 的要求导出。

附录 A
(资料性)
底盘域控制器硬件架构及接口

底盘域控制器硬件接口及横向、纵向、垂向控制功能的执行器控制资源分布示意图 A. 1。

注 1：实际产品开发过程中，横向、纵向、垂向控制功能相关的各传感器及执行器驱动模块的分布，由整车企业或零部件厂商根据整车架构进行确定。

注 2：实际产品开发过程中，横向、纵向、垂向控制功能相关的各传感器接口的实现方式以及各执行器的驱动实现方式，由整车厂或零部件厂商结合实际情况进行确定。

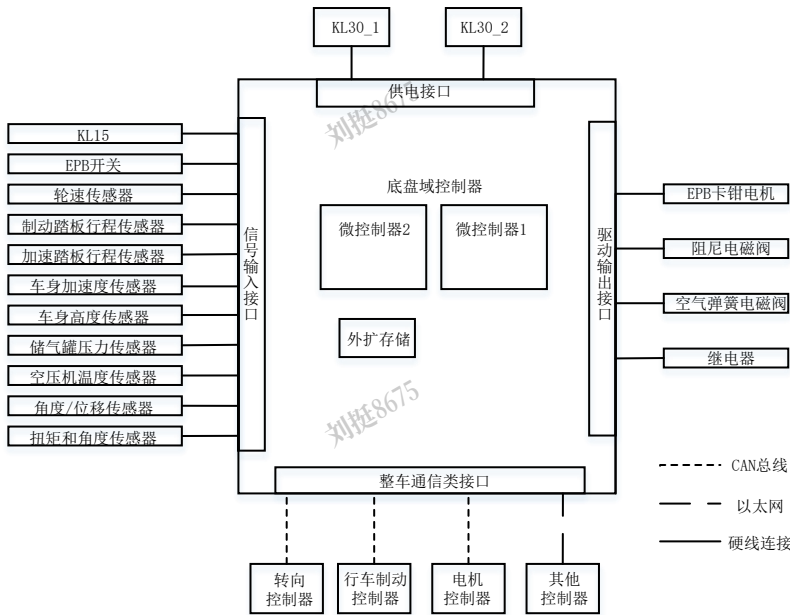


图 A. 1 底盘域控制器对外接口示意图

附 录 B
(资料性)

底盘域控制器硬件相关安全目标

B.1 横向控制安全目标

底盘域控制器相关的横向控制安全目标参考 GB 17675—2021 中 B.2.5.1。

B.2 纵向控制安全目标

底盘域控制器相关的纵向控制安全目标参考 GB 21670—2025 中 A.2.3.1 和 GB/T 43254—2023 中 6.2。

B.3 垂向控制安全目标

底盘域控制器硬件垂向控制安全目标见表 B.1。

表 B.1 底盘域控制器垂向控制安全目标列表

编号	安全目标	ASIL 等级	安全状态
SGVER_001	避免悬架高度非预期调节，导致车辆失稳	ASIL B	停止悬架高度调节，并提醒驾驶员
SGVER_002	避免悬架高度调节时，四轮高度调节不一致，导致行车过程车辆失稳	ASIL B	停止悬架高度调节，并提醒驾驶员
SGVER_003	避免悬架高度调节方向与预期方向相反，导致车辆失稳	ASIL B	停止悬架高度调节，并提醒驾驶员

附 录 C
(规范性)
功能安全耐用性和鲁棒性测评

C.1 可靠性试验

C.1.1 随机振动试验

试验方法：按 GB/T 28046.3—2011 中 4.1.2.4 进行试验。

评价准则：

- a) 底盘域控制器在试验过程中及试验后，无明显的物理失效（裂纹等）。
- b) 底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.1.2 机械冲击试验

试验方法：按 GB/T 28046.3—2011 中 4.2.2 进行试验。

评价准则：

- a) 底盘域控制器在试验过程中及试验后，无明显的物理失效（裂纹等）。
- b) 底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.1.3 自由跌落试验

试验方法：按 GB/T 28046.3—2011 中 4.3 进行试验。

评价准则：

- a) 底盘域控制器在试验过程中，可以有明显的损坏但不能存在隐性损伤。
- b) 底盘域控制器在试验后，所有功能应自动恢复正常。

C.1.4 低温试验—贮存试验

试验方法：按 GB/T 28046.4—2011 中 5.1.1.1 进行试验。

评价准则：底盘域控制器在试验后，所有功能应自动恢复正常。

C.1.5 低温试验—运行试验

试验方法：按 GB/T 28046.4—2011 中 5.1.1.2 进行试验。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.1.6 高温试验—贮存试验

试验方法：按 GB/T 28046.4—2011 中 5.1.2.1 进行试验。

评价准则：底盘域控制器在试验后，所有功能应自动恢复正常。

C.1.7 高温试验—运行试验

试验方法：按 GB/T 28046.4—2011 中 5.1.2.2 进行试验。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.1.8 温度循环试验

试验方法：按 GB/T 28046.4—2011 中 5.3.1 进行试验。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.1.9 温度冲击试验

试验方法：按 GB/T 28046.4—2011 中 5.3.2 进行试验。

评价准则：底盘域控制器在试验后，所有功能应自动恢复正常。

C.1.10 湿热循环试验

试验方法：按 GB/T 28046.4—2011 中 5.6.2.3 进行试验。

评价准则：底盘域控制器在按 GB/T 28046.1—2011 中 5.3 工作模式 3.2 进行试验时，所有功能应符合设计要求。

C.1.11 高温高湿试验

试验方法：按 GB/T 28046.4—2011 中 5.7 进行试验。

评价准则：底盘域控制器在按 GB/T 28046.1—2011 中 5.3 工作模式 3.2 进行试验时，所有功能应符合设计要求。

C.1.12 防水防尘试验

试验方法：按 GB/T 28046.4—2011 中 7 进行试验。

评价准则：

- a) 底盘域控制器在防水试验后，所有功能应自动恢复正常。
- b) 底盘域控制器在防尘试验中及试验后，所有功能应符合设计要求。

C.1.13 化学负荷试验

试验方法：按 GB/T 28046.5—2013 中 4 进行试验。

评价准则：底盘域控制器在试验后，所有功能应自动恢复正常。

C.1.14 高温寿命试验

试验方法：按 GB/T 28046.4—2011 中 5.1.2 进行试验，试验持续时间按 GB/T 28046.1—2011 中附录 B 要求计算。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.2 电磁兼容试验

C.2.1 线束激励法试验

试验方法：按 GB/T 33014.4 进行试验。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.2.2 辐射抗扰度—ALSE 法试验

试验方法：按 GB/T 33014.2 进行试验。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.2.3 电源线瞬态传导抗扰度试验

试验方法：按 GB/T 21437.2—2021 中 4.4 进行试验。

评价准则：

- a) 试验脉冲为 1/2b 的试验评价准则如下：

- 1) 底盘域控制器在试验过程中, 允许一个或多个功能失效。
- 2) 底盘域控制器在试验后, 所有功能应自动恢复正常。
- b) 试验脉冲为 2a/3a/3b 的试验评价准则: 底盘域控制器在试验过程中及试验后, 所有功能应符合设计要求。

C.2.4 信号线瞬态耦合抗扰度试验

试验方法: 按 GB/T 21437.3 进行试验。

评价准则: 底盘域控制器在试验过程中及试验后, 所有功能应符合设计要求。

C.2.5 静电抗扰度试验

试验方法: 按 GB/T 19951 进行试验。

评价准则:

- a) 下电模式下, 底盘域控制器在试验后, 所有功能应符合设计要求。
- b) 上电模式下, 试验电压绝对值范围在 8kV 至 15kV 时, 满足如下要求:
 - 1) 底盘域控制器在试验过程中, 允许一个或多个功能失效。
 - 2) 底盘域控制器在试验后, 所有功能应自动恢复正常。
- c) 上电模式下, 试验电压绝对值范围在小于 8kV 时, 底盘域控制器在试验过程中及试验后, 所有功能应符合设计要求。

C.3 电性能试验

C.3.1 直流供电电压范围试验

试验方法: 按 GB/T 28046.2—2019 中 4.2 进行试验。

评价准则: 底盘域控制器在有效电压范围内进行试验时, 所有功能应符合设计要求。

C.3.2 过电压—在 $T_{max}-20^{\circ}\text{C}$ 下试验

试验方法: 按 GB/T 28046.2—2019 中 4.3.1.1 进行试验。

评价准则: 底盘域控制器在试验后, 所有功能应自动恢复正常。

C.3.3 过电压—在常温下试验

试验方法: 按 GB/T 28046.2—2019 中 4.3.1.2 进行试验。

评价准则: 底盘域控制器在试验后, 所有功能应自动恢复正常。

C.3.4 叠加交流电压试验

试验方法: 按 GB/T 28046.2—2019 中 4.4 进行试验。

评价准则: 底盘域控制器在试验过程中及试验后, 所有功能应符合设计要求。

C.3.5 供电电压缓降和缓升试验

试验方法: 按 GB/T 28046.2—2019 中 4.5 进行试验。

评价准则:

- a) 底盘域控制器在有效电压范围内进行试验时, 所有功能应符合设计要求。
- b) 底盘域控制器在有效电压范围外进行试验, 试验后, 所有功能应自动恢复正常。

C.3.6 供电电压瞬时下降试验

试验方法：按 GB/T 28046.2—2019 中 4.6.1 进行试验。

评价准则：

- a) 底盘域控制器在试验中，存储器功能应正常，其他功能允许一个或多个参数超出范围。
- b) 底盘域控制器在试验后，所有功能应自动恢复正常。

C.3.7 复位性能试验

试验方法：按 GB/T 28046.2—2019 中 4.6.2 进行试验。

评价准则：底盘域控制器在试验中，允许输入输出全部功能有功能偏差，恢复正常工作电压后，所有功能应符合设计要求。

C.3.8 启动特性试验

试验方法：按 GB/T 28046.2—2019 中 4.6.3 进行试验。

评价准则：底盘域控制器在试验中及试验后，所有功能应符合设计要求。

C.3.9 抛负载试验

试验方法：按 GB/T 28046.2—2019 中 4.6.4 进行试验。

评价准则：底盘域控制器在试验后，所有功能应自动恢复正常。

C.3.10 反向电压试验

试验方法：按 GB/T 28046.2—2019 中 4.7 进行试验。

评价准则：底盘域控制器在试验后，恢复正常的连接后，所有功能应符合设计要求。

C.3.11 参考接地和供电偏移试验

试验方法：按 GB/T 28046.2—2019 中 4.8 进行试验。

评价准则：底盘域控制器在试验过程中及试验后，所有功能应符合设计要求。

C.3.12 单线断开试验

试验方法：按 GB/T 28046.2—2019 中 4.9.1 进行试验。

评价准则：底盘域控制器在试验后，所有功能应符合设计要求。

C.3.13 多线断开试验

试验方法：按 GB/T 28046.2—2019 中 4.9.2 进行试验。

评价准则：底盘域控制器在试验后，所有功能应符合设计要求。

C.3.14 短路保护试验

试验方法：按 GB/T 28046.2—2019 中 4.10 进行试验。

评价准则：底盘域控制器在试验后，所有功能应符合设计要求。

参考文献

- [1] GB 17675—2021 汽车转向系 基本要求
 - [2] GB 21670—2025 乘用车制动系统技术要求及试验方法
 - [3] GB/T 43254—2023 电动汽车用驱动电机系统功能安全要求及试验方法
-