



支持汽车安全的
最新汽车功能安全标准
“ISO 26262”

1. 前言

近年来，在汽车领域，随着自动驾驶技术的持续创新并迅速发展，越来越需要有助于在紧急情况下防患于未然的功能（功能安全）、以及将功能安全标准化的 ISO 26262 等标准。特别是在技术创新卓著的中国，ISO 26262（功能安全）已被确立为以“GB/T”开头的推荐性国家标准，ISO 26262 的第一版中文译本“GB/T 34590”已于 2017 年 10 月发布，并且已于 2018 年 5 月起开始施行。

在这种背景下，不仅汽车制造商（OEM），越来越多的汽车电子产品制造商（Tier1）也纷纷加速了功能安全支持，从全球范围来看，实现功能安全已经是必经之路。

本文将从半导体制造商的角度，在对功能安全和 ISO 26262 的关注度日益增加，并需要采取行动积极应对的背景下，介绍功能安全和 ISO 26262 是什么，以及它们如何影响最新的汽车领域。

2. 什么是功能安全？

首先，让我们重新思考一下什么是“功能安全”。

2-1. “安全”的定义

当突然被问及“请您解释一下安全是怎样的状态”时，可能很多人都难以立即作答。顺便提一下，在安全问题相关的基础导则--国际基本安全标准第一版 ISO/IEC Guide 51 中，对安全的定义是“安全 = 免于不可接受的风险”。这是一句双重否定句，可能在中文里很难立即理解，但是在英文中被描述为“Freedom from risk which is not tolerable”，可能更容易理解。但是，无论如何也很难用一句话来解释清楚“安全”到底是什么，因此我们先来解释一下安全的定义。

“安全”的反义词是“危险”。那么，“危险”是怎样的状态呢？有时会将“危险”状态称为“有风险”。通常，“风险”有大有小。因此，通过针对“危险”（即高风险）采取措施并使风险降低到能够接受范围，“危险”状态就会变为“安全”状态。换句话说，“安全”状态也可以称之为“没有不可接受的高风险的状态”。现在能够理解开头的“安全 = 免于不可接受的风险”这句话了吧。

2-2. “本质安全”与“功能安全”的比较

那么，“功能安全”是什么意思？在介绍“功能安全”时，经常引用的术语是“本质安全”。在此我们想通过与“本质安全”的比较来介绍“功能安全”。“本质安全”是一种通过消除危险原因来确保安全的方法。而“功能安全”是通过功能方面的努力将风险降低到可接受水平来确保安全的方法。

例如，以道路和铁路交叉口为例，让我们来思考一下应该采取什么措施来避免汽车和火车之间发生碰撞（图 1）。

为了消除道路和铁路交叉的危险原因，将道路和铁路分开，建立立交桥来避免碰撞的做法就是基于“本质安全”的思路。按照“本质安全”的思路，采用立交桥的做法，可以从物理上消除汽车与火车之间的碰撞。

而“功能安全”的方法则可能是通过设置铁路道口来避免碰撞。在道路与铁路的交叉处设置警报器和栏杆，在铁路上安装传感器，当传感器检测到火车接近时，警报器响起，并降下栏杆。当另外的传感器检测到火车已经通过时，警报器停止，并升起拦木机。虽然道路与铁路在物理上仍然交叉，但可通过设置铁路道口的方法将把汽车和火车相撞的风险降低到可接受的水平。这就是“功能安全”的思路。

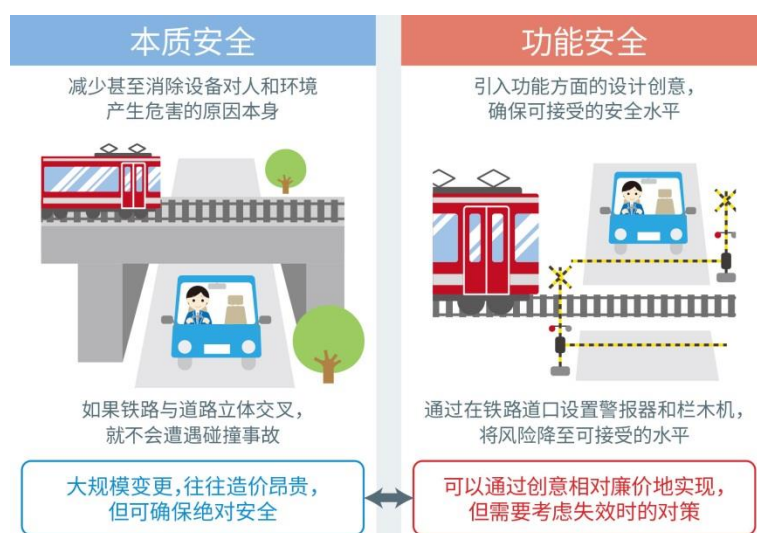


图 1. 本质安全与功能安全的思路

如前面的案例所示，“本质安全”可以确保绝对的安全性，但是通常会很昂贵。相比之下“功能安全”很多时候只要相对较低的成本就可实现，但在设计时必须考虑到当附加的功能发生故障时应如何确保安全。

在上述“功能安全”的案例中，如果传感器损坏，那么即使火车接近时，警报器和栏杆也不会工作。这样，就会立即变为“危险”状态，因此就需要一种即使传感器损坏也不会引发危险状态的设计。例如，对传感器增加自我诊断电路，设计为如诊断出自身有问题就会降下栏杆。这样即使发生故障也会导向安全的方向，这就是“故障安全（Fail Safe）”的思路。或者需要进行“冗余设计”，比如设置双重传感器，即使一个传感器损坏，另一个传感器也会工作，在此期间可以对损坏的传感器进行修复。

顺便提一下，作为双重保险的案例，还有铁路道口警报器的红灯、汽车的前灯 / 尾灯等。这些不仅是出于外观设计的考虑，而且还有双重保险的考虑，即使一个灯灭了也能确保最低限度的安全。

2-3 如何实现功能安全

为了避免严重事故的发生，需要基于“人会犯错”、“东西会损坏”的考虑来进行制造，因而有了“功能安全”。要想实现功能安全，需要防止人受到设计对象的动作或行为的危害，而要想实现这一目标，就需要同时考虑到“系统性故障”和“随机性故障”这两方面。

“系统性故障”是指在设计时就隐含的潜在故障，通常称为“Bug(漏洞, 缺陷)”。要想防止系统性故障，就需要构建一个不会引起设计漏洞的设计流程。具体而言，需要从根据要求制定规格开始，明确每一个流程（如设计、验证、试制、评估等），并在各阶段进行评审。而且还需要管理各阶段制作的表单类文件，确保可以随时取用。

而“随机性故障”则是指制造后发生的故障。由于不能完全预防随机性故障，因此有必要设立一种安全机制，以确保即使发生这种故障也不会对人造成危害。

2-4 半导体的功能安全

随着以车载和工业设备为中心的技术创新，电子产品变得越来越困难，越来越复杂，半导体的作用也越来越大，对半导体采取功能安全措施的要求也越来越高。

通常，半导体产品是在硅电路板上形成电路、并被称为“模塑”的黑色树脂固封，因此内部是看不见的。然而，在这种小黑块中却包含着成千上万的晶体管和电阻等元件，因此，电路和模块结构等也很复杂。为了应对这些半导体产品的故障，需要从开始设计之前的规格制定阶段就纳入适当的功能安全概念。因此，半导体本身也需要同时考虑到对应系统性故障和随机性故障的“功能安

全”支持。

3. 与 ISO 26262 相关的标准

我们已经对“功能安全”的概念有所了解，下面来概述介绍本文的主题--功能安全标准“ISO 26262”。另外，请记住功能安全标准不仅仅局限于汽车领域，在其他领域也有各种功能安全标准。

3-1 主要的标准

在详细介绍“ISO 26262”标准之前，先来介绍一下主要标准。首先，“ISO”是指 International Organization for Standardization（国际标准化组织），是总部位于瑞士日内瓦的非政府机构，旨在制定并推广国际标准（IS: International Standard）。其中 ISO 9001（质量管理体系）和 ISO 14001（环境管理体系）是非常有名的标准，估计很多人可能都听说过。

其次是“IATF 16949”，汽车行业的国际质量管理体系标准。顺便提一下，IATF 标准是由国际汽车工业特别工作组制定的。“IATF 16949”是在“ISO 9001:2015”的基础上添加了汽车工业相关的必要事项，因此必须与 ISO 9001 一起使用。

“ISO 26262”是以已经存在“IATF 16949”这样的质量管理体系为前提制定的。

3-2 ISO 26262 的由来及其他功能安全标准

前面提到的 ISO 26262 是汽车电气 / 电子系统相关的“功能安全”标准，是基于 IEC 61508（也被称为功能安全的母标准）制定的（图 2）。

IEC 61508 是由 IEC（International Electrotechnical Commission: 国际电工委员会）制定的电气、电子、可编程电子系统的功能安全国际标准，对象为工厂、发电厂、机械、铁路、医疗设备、家用电器等。ISO 26262 是遵循 IEC 61508 的基本思路和框架，并根据汽车的电气 / 电子系统进行修改而成的。



图 2. 功能安全的标准体系

顺便提一下，在其他行业中也有很多基于 IEC 61508 的功能安全标准。具有代表性的标准有：流程工业（IEC 61511）、工业机械（IEC 62061）、机械类的控制系统（IEC13849）、可调速电力驱动系统（IEC61800-5-2）、家用电器（IEC 60335-1）、核能（IEC 61513）、铁路（IEC 62278）、机器人设备（ISO13482）、医疗设备（IEC 60601）、电梯（EN81）、炉用电气设备（EN50156-1）等。

应该指出的是，虽然 ISO 26262 旨在实现功能安全，但它并不是法律。因此，不遵守 ISO 26262 标准并不违法。但是，汽车制造商不会购买不符合标准的产品。汽车制造商通过根据 ISO 26262 设计电气 / 电子系统来证明能够确保汽车的安全。而且，设计应确保即使发生了电气 / 电子系统故障，也不会造成人身（不仅包括驾驶员和乘客，还包括行人等）伤害。

3-3 如何满足 ISO 26262 标准？

要想满足 ISO 26262 标准，就需要从“流程支持”和“产品支持”这两方面来对应。这种标准中所说的“流程”是指包括输入、处理、输出在内的整个流程，“流程支持”是指在包括开发步骤在内的整个开发流程中进行对应。要求通过完善公司内部规定和开发标准等，来建立开发时所需的文件和评审等开发流程。“产品支持”是指在产品功能方面的对应，在设计的产品中设置一种安全机制，能够在产品的哪里发生了故障时检测出该故障，并进行某种处理，从而避免危险。

接下来再稍微具体一些思考一下流程支持和产品支持。

前面介绍过，从“人会犯错”的角度看，设计时隐含的潜在故障（=即 Bug，缺陷，漏洞）是系统性故障，作为避免这种系统性故障的对策，就需要流程支持。要想在设计时不存在潜在缺陷，应规定开发时所需的文件和评审等，并将其作为文档保留以用作证据。所有的软件故障都是系统性故障。

另外，前面也介绍过，从“东西会损坏”的角度看，将市场（或工厂）发生的故障归为随机性故障（或随机性硬件故障），作为应对这种随机性故障的对策，就需要产品支持。在设计时需要考虑各种余量以避免产品损坏。从功能安全的角度出发，要求即使发生故障也不会造成人身伤害。因此，需要设立一种安全机制，以确保能够检测出故障并针对不同的故障做出适当的处理。在设计初期的规格探讨阶段，需要研究并探讨每种功能可能会发生的故障，以及针对该故障应该设立什么样的安全机制。产品支持是指为了对应随机性故障从而增加安全机制。

3-4 设计者的产品责任

可能您没有听说过“产品责任（Product Liability）”吧。产品责任是指由于产品的缺陷，造成了人身伤害或财产损失，甚至危及人的生命安全时，应该由产品的生产者承担赔偿责任。设计者需要证明自己设计的产品不存在设计缺陷（即 Bug），因此设计者需要保留设计依据和设计时的假设等各种证据，因此应对产品责任也可以被视为流程支持的一部分。

4. ISO 26262 的详细介绍

ISO 26262 于 2011 年 11 月发布第一版，于 2018 年 12 月发布修订后的第二版。在第一版中，涉及的对象是 3,500kg 以下的量产乘用车；在第二版中，对象范围扩大至卡车、公共汽车及两轮机动车。在这里将围绕第二版中修订的内容来详细介绍 ISO 26262 的细节（图 3）。



图 3. ISO 26262 概览

4-1 卡车 & 公共汽车（T&B）的增加

在第二版中的第一个主要变化是受该标准约束的对象车辆。在第一版中的对象车辆是 3,500kg 以下的量产乘用车，但第二版中超出了该框架，对象车辆扩大到了卡车、公共汽车及两轮机动车。实际上，在制定第一版时，也曾经计划包括卡车和公共汽车等对象，但是由于相关的研究需要花费很多时间，于是暂时限定为 3,500kg 以下的车辆。通常，卡车多由汽车制造商来制造基础车辆（驾驶室、引擎、底盘零件部分等），由车身制造商（Body Builder）来制造车身部分（集装箱、翻斗、搅拌筒等）。由于可能会发生根据 ISO 26262 设计和制造的基础车辆上组装了没有根据 ISO 26262 设计和制造的车身部分等情况，因此似乎需要很长时间来讨论该如何应对这类情况。另外，图 3 的 Part 1 的术语集中，也增加了卡车和公共汽车（T&B）用的术语和缩写。

4-2 两轮机动车的增加

如图 3 所示，通过“Part 12”新增了两轮机动车相关的规定。在这里规定的对象是“除 ISO 3833 中定义的轻便摩托车之外的两轮机动车或无载荷时重量低于 800kg 的三轮机动车”。轻便摩托车是指最高时速低于 50km/h 的 50cc 以下的两轮车。虽然日本的机动自行车（带马达的自行车）的法定速度是 30km/h，但设计速度为 60km/h 左右，因此不属于轻便摩托车范畴。为了便于理解，下面将 Part 12 的对象两轮机动车进行了分类：

- 轻便摩托车、电动自行车：非对象
- 日本的机动自行车、两轮机动车、低于 800kg 的三轮车：对象
- 800kg 以上的三轮车和四轮以上的车辆：非对象（这些不属于 Part 12 的范畴，而是原有 Part 中的约束对象）

4-3 半导体指南

通过“Part 11”新增了半导体指南。Part 11 仅仅是一个指南，因此这部分中没有必要条件和工作成果相关的内容，但提出了在进行半导体设计时应该如何理解 Part 5（硬件设计）和 Part 6（软件设计）中规定的内容。在第一版中，对于半导体设计时应该如何应对的规定是比较模糊的，但在第二版中则给出了很多示例，可以说，按照 ISO 26262 进行半导体设计变得更加容易了。

4-4 目的细化

比较 ISO 26262 标准的第一版和第二版可以看出，第二版中对目的项目的描述显著增加。这

是为了通过增加具体案例等，来使各部分的目的变得更容易理解。由于不仅仅局限于必要条件项目，还可以通过其他手法来确保安全性，因此详细描述了应该遵守的原理。

4-5 备注和案例的增加

增加了很多备注和案例，以使必要条件和推荐的说明更加容易理解。

5. 关于获得认证

前面介绍了 ISO 26262 的概要和一些细节，那么怎样才能获得 ISO 26262 的认证呢。在本节中，我们将介绍该认证的获得方法和 ROHM 的活动。

5-1 通过第三方认证机构获得认证

要取得上述 ISO 26262 的认证，通常的做法是接受以 TÜV Rheinland、TÜV SUD、SGS TÜV、DNV-GL、TÜV Saarland 等为代表的第三方认证机构的审查，并取得认证。TÜV (=Technischer Überwachungs-Verein) 是获得德国技术监督协会批准的、进行审查和认证的民间审查机构。对于是否已确立了符合 ISO 26262 标准的流程（公司内部规定、开发标准、程序书等）进行审查和认证。

5-2 也可以自我认证

只要能说明是按照 ISO 26262 标准执行的，未必一定要通过第三方认证机构获取认证。即使没有获得认证，只要能够证明是按照标准中规定的必要条件组成的工作成果，并且是按照标准进行的开发，也没有问题，但要理解标准中的含义并付诸实践，需要非常大的工作量，要想证明满足了所有的要求，可能是一项艰巨的任务。因此，比起向每个客户一一证明遵行标准的内容，还不如接受第三方认证机构审查并获得认证，以此来表明符合标准的做法效率更高。

5-3 ROHM 已经取得了流程认证

ROHM 从 2015 年开始构建 ISO 26262 的流程，约在 2 年半后的 2018 年 3 月，通过德国第三方认证机构 TÜV Rheinland 获得了 ISO 26262 的流程认证（图 4）。换句话说，ROHM 的 ISO 26262 流程已经被认定为是符合 ISO 26262 标准的流程。一般通常的做法是根据顾问等外援的建议来构建流程，但 ROHM 不止于此，还举办了多场研讨会来学些和了解该标准，以调整方向，建立符合标准的流程。



图 4. ROHM 的 ISO 26262 流程认证书

5-4 功能安全工程师（FSE）和功能安全经理（FSM）

ROHM 拥有 24 名获得 TÜV Rheinland 认证的功能安全工程师 (Functional Safety Engineer)，3 名获得更高资格认证的功能安全经理 (Functional Safety Manager)（截至 2020 年 2 月）。功能安全工程师归属于开发车载 IC 的部门，在按照 ISO 26262 流程推进开发时，以及在接到客户的 FIT、FMEDA 委托时，作为功能安全负责人履行职责。另外，功能安全经理归属于独立于 IC 开发的部门，以确保标准要求的独立性的形式，执行评审确认、功能安全审查、功能安全评估等确认证实措施。

6. 支持功能安全的车载应用的电路配置示例

最后，介绍一下在最近的车载应用中，半导体是如何为构建功能安全做贡献的，同时介绍一下 ROHM 的行动和解决方案。

6-1. 针对最近的车载应用的安全设计

说到车内的显示装置，除了车速里程表、转速表、水温表、燃油表、各种指示器等仪器仪表外，当然还有导航系统等。此外，近年来，仪表盘已经逐渐开始采用 LCD（液晶显示），后视镜和内后视镜采用电子镜的车辆也多起来了（图 5）。



图 5. 车辆的显示装置示例

这些显示装置具有向驾驶员传递各种信息的重要作用，因此如果显示装置发生故障导致无法显示、出现黑屏的话，就会给驾驶员带来麻烦。但是，对于仪表盘和电子镜来说，比起黑屏，错误显示可能更危险。

如果出现黑屏，驾驶员会立即注意到问题，但在驾驶过程中驾驶员不会一直凝视仪表盘和电子镜，因此一旦发生显示卡顿、延迟显示等情况，驾驶员可能不会意识到发生了故障。如果车速里程表显示发生卡顿，且显示的速度比实际速度低的话，那么驾驶员就可能注意不到超速。另外，如果电子镜的显示滞后于实际状态，当其他车辆已经从后方接近了，但车上的电子镜却没有显示时，后果会怎样呢？如果真的发生这种故障，驾驶员可能会在改变车道时无法注意到后方车辆，从而引发事故。仪表盘和电子镜的设计必须要避免这类故障的发生。但是，虽说是“不发生故障的设计”，只要是电子设备，就如前面所介绍的，都有可能因某种问题而损坏。

那么，怎样的设计才算好呢？可以通过一些设计，让驾驶员能够注意到故障情况，例如，始终监测显示的数据，当显示卡顿时，或当发生错误显示时，也像发生黑屏和异常时一样，能够显示错误警告画面。如上所述，即使发生故障也不会引发事故的设计，也就是针对“功能安全”的设计是非常必要的。

6-2 仪表盘、电子镜的电路配置

让我们来具体看一下在进行这样的设计时，实际的仪表盘和电子镜的电路配置是怎样的。

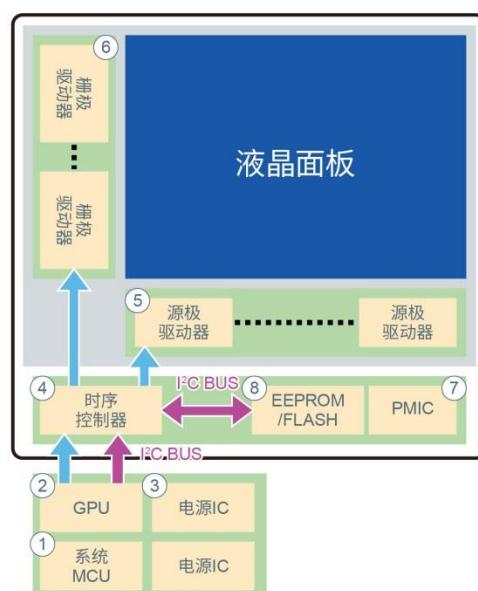


图 6. 显示装置的电路配置示例

图 6 是车辆显示装置的电路配置示例。下面将按图中的编号来介绍它们各自的功能。

- ① 系统 MCU (Micro Control Unit) 负责控制整个系统。它相当于系统的大脑，负责整个系统的处理。
- ② GPU (Graphics Processing Unit) 负责显示、相当于显示的大脑的部分。相对于 CPU (Central Processing Unit) 作为电脑的大脑，擅长整个计算机的处理，这里的 GPU 是专门用于图形处理的 IC。
- ③ 电源 IC 负责供给整个系统所需的电源。
- ④ 时序控制器负责把来自 GPU 的图像数据发送到显示液晶面板的源极驱动器，并根据其显示结果来控制栅极驱动器。
- ⑤ 源极驱动器根据液晶面板的显示所需的图像数据，调整源极放大器电路的电流，并决定一个像素的亮度。
- ⑥ 栅极驱动器根据源极驱动器的显示数据逐行显示。
- ⑦ 面板用 PMIC (Panel Power Management IC) 用来生成显示液晶面板所需的电压。
- ⑧ EEPROM / FLASH 用来存储时序控制器的初始设置数据、查找表、指示器的图像等，并可在 GPU 发来的图像上覆写显示指示器的图像。

6-3 ROHM 的液晶面板芯片组

在图 6 的应用中，如果时序控制器控制两个驱动器，把来自 GPU 的图像数据直接显示在液晶面板上的话，一旦发生显示异常，将无法做任何操作，会直接导致事故发生。

针对这种问题，ROHM 的车载用时序控制器，能够监测来自 GPU 的图像数据，当发生数据异常或输入信号异常时，使之显示黑屏，或通知微控制器使之显示错误警告画面等，从而让驾驶员注意到异常，成功地解决了该问题。

而且，ROHM 的液晶面板用芯片组，拥有控制各液晶驱动器的时序控制器：BU90AL210 / BU90AL211 / BU90AD410、驱动液晶面板的源极驱动器和栅极驱动器：ML9882 / ML9873 / ML9872、多功能电源 IC：BM81810MUV、进行图像视频校正的伽玛校正 IC：BD81849MUV，可从整体上确保液晶面板的功能安全（图 7）。

产品名称	功能	HD720 (1280×720)		FHD级 (1920×720)		FHD1080 (1920×1080)		3K级 (2880×1080)	
		产品名称	个	产品名称	个	产品名称	个	产品名称	个
时序控制器	各液晶驱动器控制	BU90AL211	1	BU90AL211	1	BU90AL210	1	BU90AL211/BU90AD410	1
源极驱动器	液晶面板驱动	ML9882 (1440ch)	3	ML9882 (1440ch)	4	ML9882 (1440ch)	4	ML9882 (1440ch)	6
栅极驱动器	液晶面板驱动	ML9873 (960ch)	1	ML9873 (960ch)	1	ML9872 (540ch)	2	ML9872 (540ch)	2
PMIC	多功能电源IC	BM81810MUV	1	BM81810MUV	1	BM81810MUV	1	BM81810MUV	1
伽玛校正IC	图像视频校正	BD81849MUV	1	BD81849MUV	1	BD81849MUV	1	BD81849MUV	1

图 7. 功能安全芯片组产品示例

如图 8 所示，该液晶面板芯片组可检测出各种故障，具有与车辆显示装置所要求的安全性相对应的功能。

组成芯片组的每个 IC，都有相互检测可能会出现的故障模式的功能，除了前述的时序控制器功能外，还可以随时确认并反馈源极驱动器和栅极驱动器的损坏、剥落、以及输入液晶的信号等信息。所组成的芯片组可完善检测出面板的异常。在车速表和后视镜采用液晶面板时，通过导入功能安全，有助于预防所担心的重大事故。

面板用的 PMIC 中搭载了丰富的功能：始终监测是否能够正常提供液晶面板显示所需的电压，当发生电压异常时，自动关闭电源的功能，另外内置双重寄存器用以在异常检出时，实行自动刷新使之从异常中恢复。因此还可防止噪声干扰等意外的影响，具有非常高的可靠性。

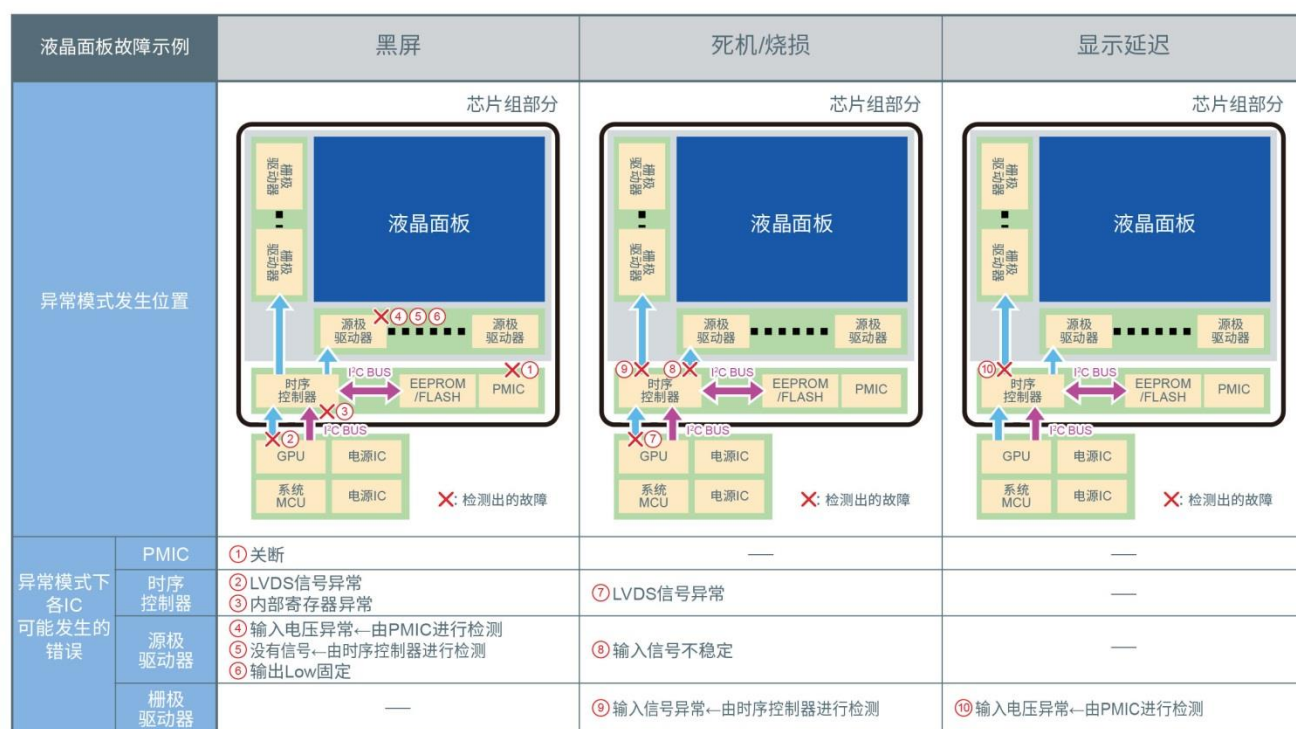


图 8. 可检测出的故障示例

6-4 普通 ECU 内部的电源电路配置

下面将另一个话题。在汽车 ECU（Electronic Control Unit）中，通常需要多个电源。要求分别提供适合 MCU（也有内核和 I/O 需要独立电源的情况）、传感器、电机驱动器、CAN（Controller Area Network：车内使用的串行通信协议）等的电压和电流。在车内，电源 IC 通过 12V 电池生成所需电压/电流的电源。这些电源既可以由多个电源 IC 构成，也可以由多通道 PMIC（Power Management IC）构成，在车载 ECU 的情况下，该电源发生异常时可能会引发事故（图 9）。

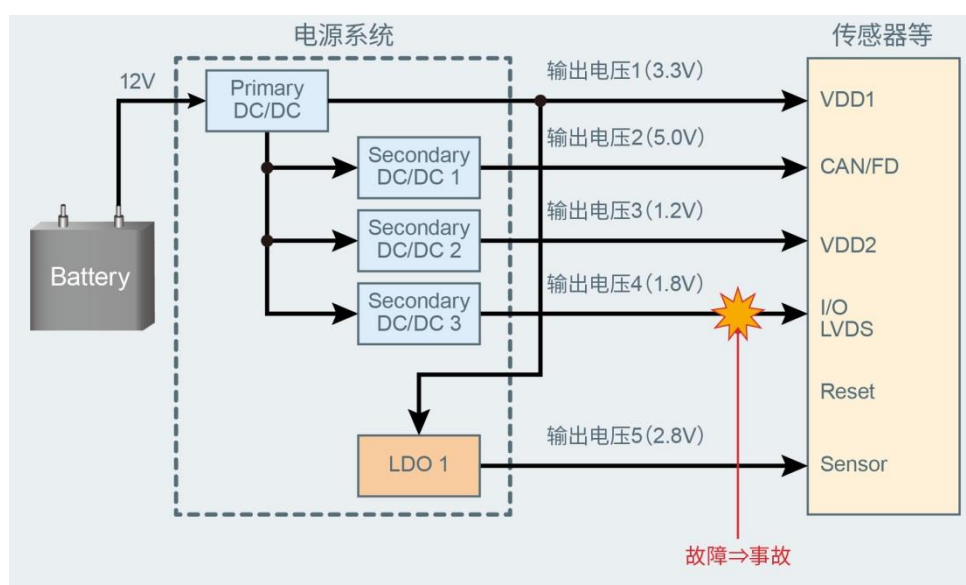


图 9. 电源配置示例

所以，需要能够监控 ECU 内的多个电源、并在发生异常时根据所异常进行避免事故的处理，电源监控 IC 就发挥着这个作用。电源监控 IC 会监控这些电压，并在发生异常时通知 MCU，提示其进行处理。

如上所述，车载应用要实现“功能安全”，不仅需要主功能，还需要“安全机制”，即能够监控主功能是否正常，当发生异常时，能够根据每种功能进行处理，保护人员（包括驾驶员、乘客以及行人）安全的功能。此外，还需要能够确认这些“安全机制”是否在正常运行的“自我诊断功能”。

6-5 ROHM 的电源监控 IC

针对这一问题，ROHM 通过在独立的电源监控 IC 中内置各种监控功能和自我诊断功能，实现了可以轻松为现有电源增加功能安全性，并且已经实现量产的一款电源监控 IC，即可以监控多个电源的电源监控 IC“BD39040MUF”。另外，具有更高检测精度的“BD39042MUF”也正在开发中（图 10）。

产品名称	构成	检测级别	检测精度	封装	供应情况
BD39040MUF	4ch Power Good + Watchdog Timer	±10%	±3%	VQFN16FV3030	量产中
BD39042MUF	4ch Power Good + Watchdog Timer	±6%	±1.4%	VQFN16FV3030	开发中

图 10. ROHM 的电源监控 IC 产品示例

这款“BD39040MUF”，除了电源电压 VDD 的监控（RESET）功能外，还可以同时监控 4 通道的电源，并可分别独立检测电源的异常（欠压/过压）。还配有窗口型看门狗定时器（WDT），可检测出 ECU 内部 MCU 的异常。另外，还具有支持 ECU 的功能安全所需的以下功能：内置多重基准电压来进行相互监控功能、WDT 的时钟振荡器监控功能、启动时诊断 IC 内部的检测功能是否正常工作的自我诊断功能（图 11）。

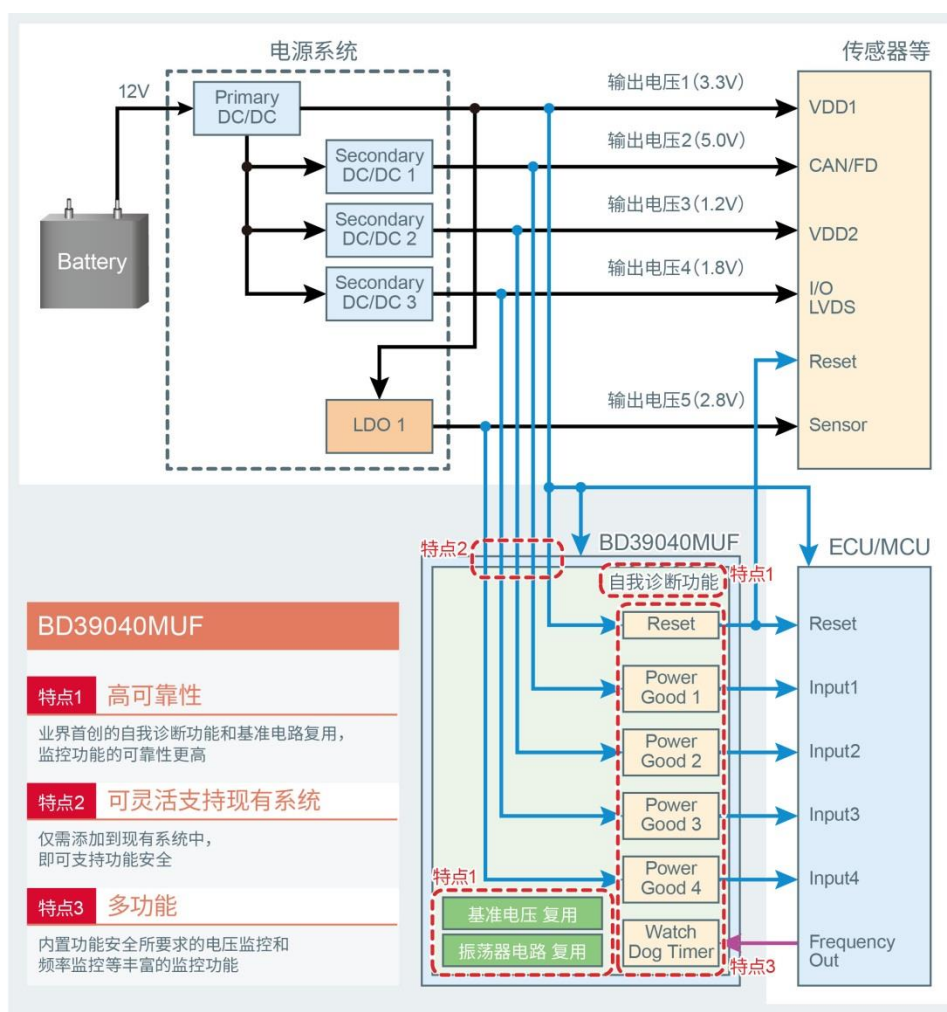


图 11. ROHM 的电源监控 IC“BD39040MUF”框图

仅需在现有系统中添加电源监控 IC，既可以利用很小的空间实现功能安全所要求的电源监控功能。ROHM 的电源监控 IC，非常有助于简化功能安全系统设计。

7. 后记

我们花了很长时间来谈论功能安全和 ISO 26262，如果您能够学到一点并且满意，我们将感到非常高兴。

ROHM 将面向汽车领域继续开发众多高品质、高可靠性的产品，也会继续提供类似此次介绍的解决方案，助力实现汽车的安心与安全。未来，ROHM 将通过加强符合 ISO 26262 标准的产品开发，为汽车文化的进一步发展贡献力量。

This document is intended to introduce ROHM' s products (hereinafter "Products"). Any ROHM Products should be used in conjunction with the latest specifications and data sheet thereof. Please contact the sales office of ROHM or visit ROHM' s web site. The information contained in this document is provided on an "as is" basis. ROHM shall not be in any way responsible or liable for any damages, expenses or losses incurred by you or third parties resulting from inaccuracy, error or use of such information. All information specified herein including but not limited to the typical functions of and examples of application circuits for the Products is for reference only. ROHM does not warrant that foregoing information will not infringe any intellectual property rights or any other rights of any third party regarding such information. ROHM shall bear no responsibility whatsoever for any dispute arising from the use of such technical information. ROHM does not grant you, explicitly or implicitly, any license to use or exercise intellectual property or other rights held by ROHM and other parties. If you intend to export or ship overseas any Products or technology specified herein that may be controlled under the Foreign Exchange and Foreign Trade Act and other applicable export regulations, you will be required to obtain a license or permit under the acts and regulations. The content specified in this document is current as of March, 2020 and subject to change without any prior notice.

ROHM Co., Ltd.

2323 Owen Street,
Santa Clara, CA 95054 U.S.A
TEL : +1-408-720-1900
www.rohm.com

