ISO 26262合规

解决与安全有关的E/E系统合规复杂问题

Greater China

权威认证
创享价值

Choose certainty.
Add value.

电子书

摘要

越来越多高端品牌产品召回现象的出现证明即使汽车行业领导者也无法规避功能安全问题。ISO 26262覆盖汽车安全生命周期的各个方面，包括管理、开发、生产、运行、服务与停运。汽车原始设备制造商（OEMs）及其供应商如果无法满足ISO 26262要求，则可能面临丧失竞争优势的风险。与此同时，这些制造商通常会在产品开发阶段过后考虑功能安全问题，并未将其作为设计流程一个不可分割的组成部分，常常花费数百万美元进行整改，而不是从一开始就避免问题的出现。

本电子书概述了汽车行业解决这种挑战的方法，有助于将产品责任风险降至最低，确保持续盈利。

TÜV南德意志集团

TÜV®

目录

TÜV南德意志集团专家介绍

Andreas Bärwald

TÜV南德意志集团汽车服务公司安全与电子部门业务线经理

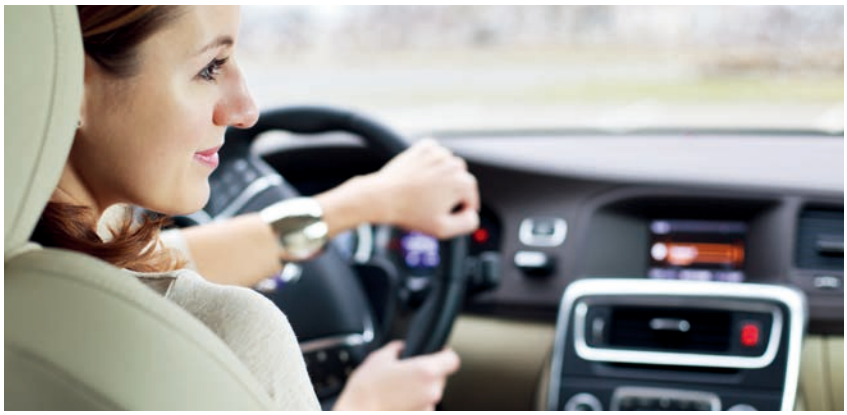
Andreas Barwald主要负责TÜV南德意志集团汽车功能安全运营，覆盖范围包括加拿大、中国、日本、韩国和美国业务部门。

作为TÜV南德意志集团认证测试实验室负责人，指定技术认证专家，Andreas带领团队为客户交付功能安全认证方案（FSCP）。确保安全专家具有一流认证资质，能够根据ISO 26262标准为公司奠定坚实基础。

Andreas于2004年首次加入TÜV南德意志集团汽车公司，担任功能安全与半导体集团经理。他拥有资深技术背景，大学期间学习计算机科学专业，加入TÜV南德意志集团前曾供职于BFI Peters——一家职业培训机构，担任IT讲师。

简介

2011年，ISO 26262标准正式发布，旨在解决与安全有关，日益普遍的电气和电子系统复杂性问题。如今，该标准已成为一项公认的先进功能安全要求。ISO 26262覆盖批量生产乘用车当中安装的各种安全相关系统，通常包括一种或多种电气和/或电子（E/E）系统。



ISO 26262是一项复杂的标准，能够帮助原始设备制造商提高产品的安全性，将产品责任的风险降至最低，保持竞争力。

ISO 26262是一项复杂的标准，能够帮助原始设备制造商提高产品的安全性，将产品责任的风险降至最低，保持竞争力。

ISO 26262框架涉及到能够确定成品当中具体安全特征的产品要求，以及降低系统故障概率的过程相关要求（但不可直接被作为产品特征）。

众多功能安全相关问题都会危及到生命，为行业带来巨大损失，汽车原始设备制造商和供应商对于这项标准的重要性毫无异议。但是，在提高汽车行业功能安全的必要性已被广泛接受的同时，很多人认为ISO 26262是一项极具挑战性的标准，鉴于其复杂性和行业内部功能安全专家资源的匮乏，ISO 26262难以阐述和执行。

此外，还将通过恪守安全的承诺，强化一流制造商的声誉，提高对于消费者和公司客户的吸引力。

ISO 26262共包含10个部分，提供一个整体阶段系统，用以实现制定过程管理：

ISO 26262的10个部分：

1. 词汇——覆盖标准各个组成部分的申请术语表与缩写
2. 功能安全管理——全面概述功能安全管理
3. 概念阶段——风险评估与安全概念
4. 系统层面的产品开发——系统开发安全
5. 硬件层面的产品开发——硬件开发安全
6. 软件层面的产品开发——软件开发安全
7. 生产与运行——生产开始后安全
8. 辅助过程——质保过程
9. ASIL——定向分析与安全为本分析——安全分析
10. ISO 26262指导

ISO 26262概述

总体来说，ISO 26262：

- 覆盖汽车安全方方面面（管理、开发、生产、运行、服务与停运），并且在汽车生命周期的各个阶段为必要活动提供定制化支持服务。
- 提供一种基于风险的汽车专属方法，用于判定风险类别（汽车安全完整性水平，ASILs）。
- 利用ASILs确定项目必要的安全要求，旨在确保剩余风险达到可接受水平。
- 提供确认、验证和证明方法，旨在确保达到充分且可接受的安全水平。

图1显示的是实现合规所需的多种元素图示。

虽然标准并未提出要求，但我们建议各相关方开展差距分析。差距分析主要按照标准要求，针对现有流程与产品进行评估。

通常，这一过程要求内部和独立第三方功能安全专家调查开发流程和/或技术产品或系统的关键问题。这些过程在ISO 26262当中均得到完整概述，包括文件、管理过程、技术功能和风险分析。凭借TÜV南德意志集团的多年资深经验，该过程需要经过一个多星期的研讨方可完成。

在ISO 26262安全生命周期内部阶段发现并评估风险（安全风险），确定具体安全要求，将风险降至可接受水平，同时管理、追踪安全要求。

在这些阶段当中，项目定义是首要步骤，即确定需要达到功能安全的时间，以及所需的功能安全内容。根据风险评估公认原则开展风险评估流程是实现目标的最佳方法。这种方法确定了判定产品与安全有关和与安全无关的各种措施方法。

然后针对发现的各种风险，确定安全目标。例如，如果安全气囊是安全要求项目之一，那么安全气囊意外弹出就可能成为一项潜在风险，预防这种情况的发生就是安全目标之一。

风险评估的结果被称为汽车安全完整性水平（ASIL），这是一种潜在风险测量方法，通过适当方式确定解决风险问题需要开展的活动和采取的方法。根据基于暴露概率、驾驶员的可控性以及紧急事件发生时，可能出现的严重等级等综合风险等级确定ASIL。

ASIL的确定共分四个步骤，从ASIL A（降低风险的比例最低）到ASIL D（降低风险的比例最高），ISO 26262标准根据指定ASIL详细叙述了最低要求。在开发流程最初阶段确定ASIL和风险标准是关键，然后再可能存在的风险问题方面分析安全系统功能。

在ISO 26262安全生命周期内部阶段发现并评估风险（安全风险），确定具体安全要求，将风险降至可接受水平，同时管理、追踪安全要求。

图1：ISO 2626结构概述

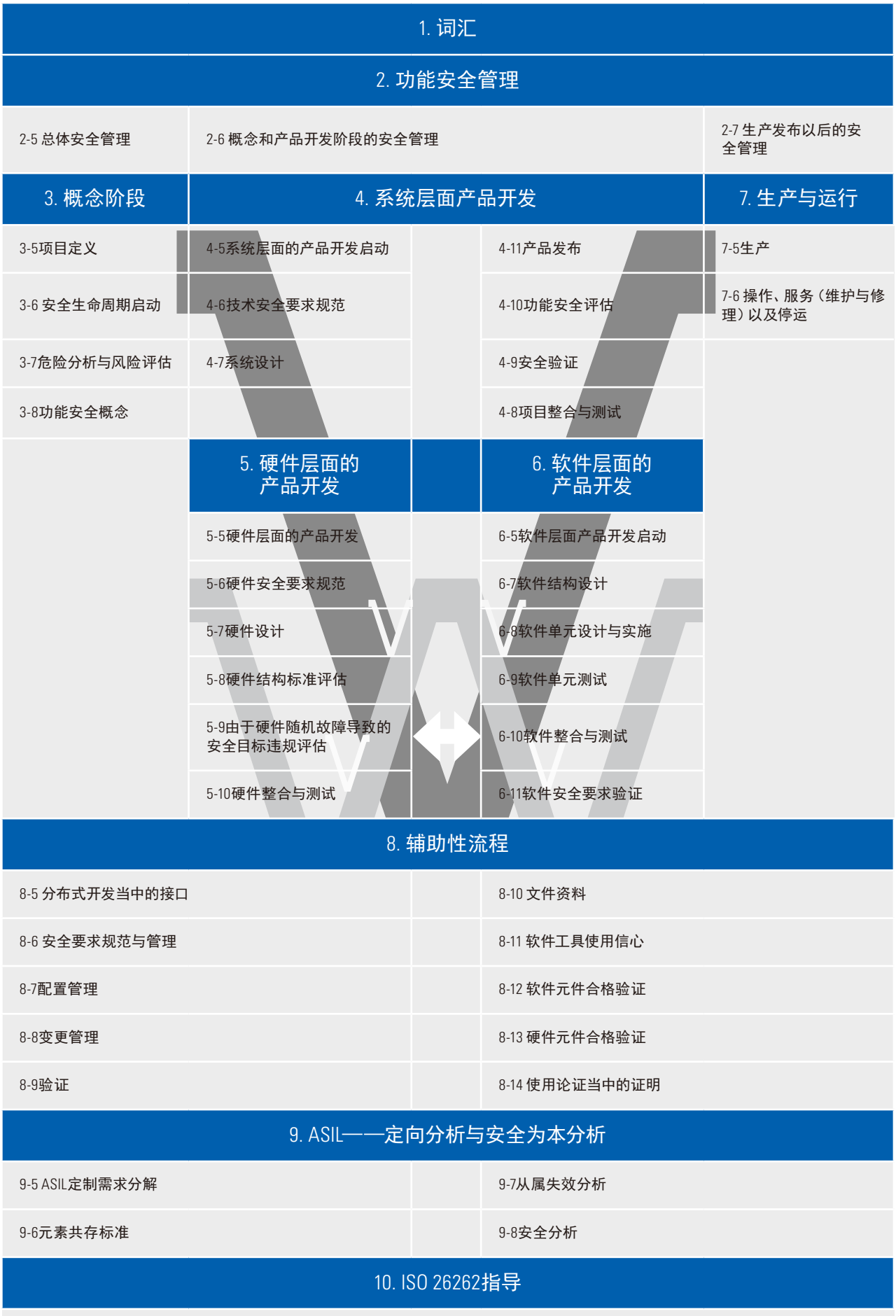
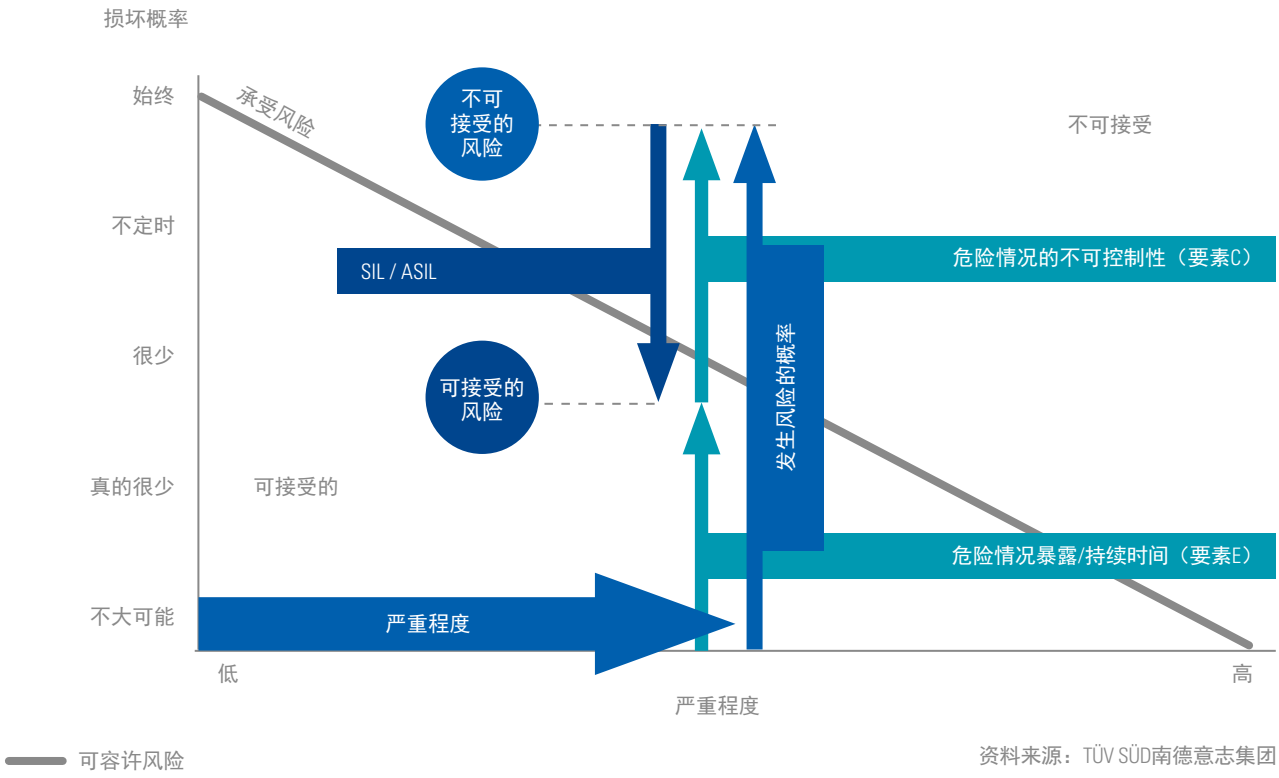


图2：危险分析方法



资料来源：TÜV SÜD南德意志集团

接下来需要确保既定安全要求符合设计预期，要将重要硬件故障纳入到考虑范围当中，预防系统故障问题出现。另外，还应根据相应的ASIL规定，借助适当的流程和方法，落实明确了安全要求的既定安全目标。

通过确定功能安全概念实现上述目标，在技术安全概念与安全设计（或安全架构）当中详述技术方面内容，制定硬件与软件安全要求。以安全气囊为例，可以确定一种安全架构，制止安全气囊意外充气，同时，在车辆事故当中保护驾驶员的人身安全。

与此同时，还要制定一种方案，弥补一致性缺口。例如，发生短路时，安全相关电子系统的硬件布局图极易出现故障，因此，计划当中应概述布局图（设计图）变更方法，预防故障出现。此外，还应描述设计技术修订方法，其他系统和所需辅助文件必须实现安全交互过渡。这将确保各项活动得到正确记录，如果出现问题，可在后期进行重新评估。此外，即使没有更改布局或概念的必要，也需要予以记录。尽早采取这些措施具有决定性的关键作用，后期变更成本高昂且十分耗时。

另外，证实系统满足指定ASIL也是一个十分关键的步骤。可借助专家，通过内部或具有专业资质的第三方开展适当的测试与分析工作，完成验证，确定安全功能平均故障间隔时间。

很多贯彻执行过ISO 26262标准的人都能够理解获得外部评估与认证的

价值和重要性。在认证的最终阶段，一般需要从独立评估机构处获得技术报告或证明，作为符合最新标准的证明。例如，TÜV南德意志集团根据客户方文件资料和现场评估提供测试服务。针对系统、硬件、软件和工具进行评估，总结编制技术报告。作为市场领导型汽车制造商的供应商而言，这点至关重要，法国、德国、日本、韩国和美国通常只接受具有良好声誉的第三方提供的报告或证明。

员工能力

ISO 26262确定了合规所需的复杂“功能性”步骤，首先必须确保工作人员了解ISO 26262与您的产品之间的关联，以及为满足合规要求，进行变更的方法。这些可以通过培训现有员工、聘请功能安全专家或将工程外包给独立第三方的方式实现。

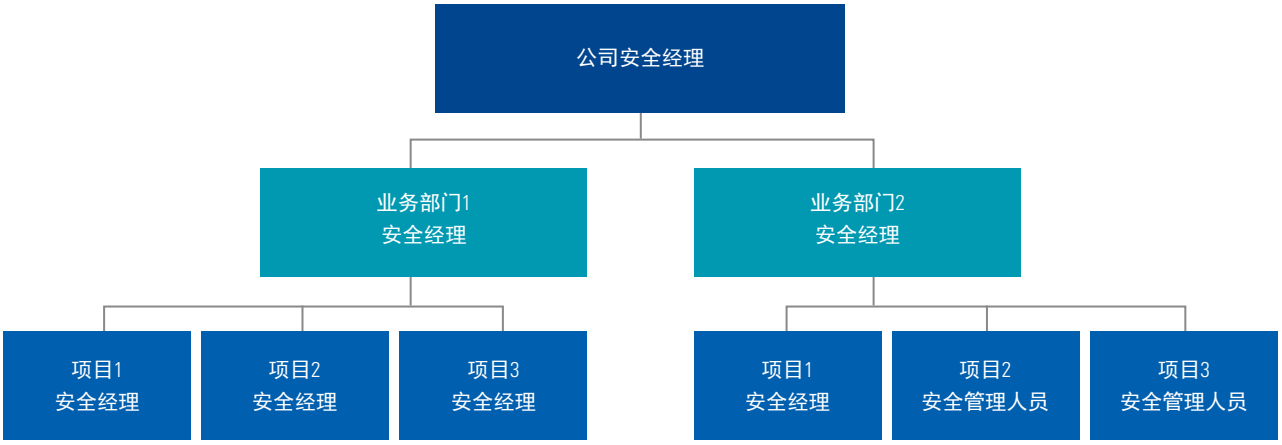
相关人员必须透彻理解ISO 26262内容、10个部分所需的文件资料以及标准当中存在的关键问题，其重要性不言而喻。

在大型机构当中，通常设有三个主要职位，为组织内部的功能安全管理提供支持帮助：

1. 公司安全经理
2. 业务部门安全经理
3. 项目安全经理——标准当中唯一要求设立的职位

职务等级显示在图3当中。

图3：成功实现功能安全管理的三种关键职务



资料来源：TÜV SÜD南德意志集团

相关人员必须透彻理解ISO 26262内容、10个部分所需的文件资料以及标准当中存在的关键问题，其重要性不言而喻。

公司安全经理是组织安全文化的监管负责人，负责确保全体员工、公司管理团队和外部服务供应商之间进行持续有效交流。此外，还负责进一步拓展并提高业务范围内的功能安全，确保公司具体指导方针和员工培训随合规变更而及时更新。

与此同时，还需要促进定期开展部门审计工作，确保遵守公司在功能安全方面制定的规范。各个不同业务部门的安全经理会定期召开例会。

业务部门安全经理并非标准范围内的指定职务，但在大型机构内部比较常见。他们是业务单元内部的核心联系点，主要负责所有与功能安全有关的问题和基本数据维护，确保员工得到适当充分培训。

项目安全经理的职位最为重要，也是标准唯一要求设立的职位。项目安全经理与业务部门安全经理合作，协调具体功能安全项目工作。项目安全经理通常负责制定并维护项目安全计划，开展评估工作，采取适当措施避免系统故障问题出现，贯彻执行验证和确认方法。同时负责协调内外部对口资源（业务单元、供应商、客户等）。

打造功能安全文化

想要实现功能安全，只是了解ISO 26262要求是远远不够的。必须培养出一种公司文化，让各个级别员工与公司同呼吸、共命运。

功能安全是质量管理的一种拓展，只有全体员工都遵守高标准方可发挥有益作用。例如，如果100名工程师当中只有一名同事参与发展过程，那么就有可能错过活动的开展，或采取错误方法工作，这种情况会引发安全问题。

为了帮助原始设备制造商和供应商在企业内部同样营造这种文化，必须部署适当的管理流程，严格执行安全规定。

功能安全是质量管理的一种拓展，只有全体员工都遵守高标准方可发挥有益作用。

实际执行

TÜV南德意志集团的功能安全小组的成立已有30多年，他们在全球范围内与原始设备制造商和汽车供应商合作，其中包括：

GAIO团队在TÜV南德意志集团的支持与帮助下，成功获得ISO 26262认证。

东芝集团*

东芝集团开发并制造多种汽车零部件产品，包括汽车、逆变器、电池、微型计算机、高级驾驶员辅助系统及其相关软件。2012年3月，借助TÜV南德意志集团服务，东芝集团获得最高标准的ISO 26262软件开发流程认证。如今，该流程能够根据最高汽车安全完整性水平（ASIL D）辅助产品开发。

通过ISO 26262认证，东芝集团能够持续推进汽车系统业务拓展，提供满足最高国际安全标准的安全可靠产品。

*包括东芝集团半导体与存储产品公司以及东芝集团社会基础设施系统公司。

松下电器公司

TÜV南德意志集团同样帮助松下电器公司的开发流程获得ISO 26262认证。如今，其汽车设备与设备软件开发过程备受认可，能够达到最高汽车安全完整性水平（ASIL D）。

TÜV南德意志集团认证证明松下电器公司的软件开发过程满足安全要求。帮助公司制造更加安全的产品，有助于创建一种安全无忧、环保、便捷舒适的汽车社会。

GAIO科技有限公司

GAIO是亚太地区首家获得ISO 26262嵌入式软件验证工具认证的公司。一般而言，ISO 26262要求用户根据工具置信度（TCL），针对采用的各项工具制备开发工具资质报告。但是，TÜV南德意志集团授予GAIO的工具认证能够满足要求最为严格的工具置信度（TCL3）。因此，GAIO的最终用户无需自行开展工具资质认证。

结论

ISO 26262极其复杂，但对于原始设备制造商和供应商而言却是必不可少的，因为该标准有助于改善产品的安全性能，将责任风险降至最低。ISO 26262不仅有助于确保车辆、系统和元件的安全性，还能提高一流原始设备制造商与供应商的声誉，提高产品吸引力，保持竞争优势。

TÜV南德意志集团汽车功能安全专家网络遍布全球各地，这些专家具有资深行业经验，能够为ISO 26262活动提供实时支持。作为备受国际认可的ISO 26262测试机构，TÜV南德意志集团是全球功能安全领导专业权威之一，参与ISO 26262标准的制定。我们在整个汽车价值链当中提供复杂完善的知识服务、功能安全评估、测试、认证以及培训服务。

访问以下网页，了解更多TÜV南德意志集团的汽车行业解决方案：

www.tuv-sud.cn

权威认证　创享价值

TÜV南德意志集团是一家优质、安全和可持续发展的专业测试、检验、审核、认证，培训和知识服务解决方案提供商。我们在世界各地超过800个地方设立了办事处，因此在欧洲、美洲、中东、亚洲和非洲均享有认证资格。通过为我们的客户提供客观的解决方案，我们为企业、消费者和环境都增添了有形价值。

* 上述部分服务可能由于当地法规的原因而无法在您的地区提供。欢迎您与我们联系咨询。

我们在大中华区的分公司及办事处：

上海	Tel.:+86 21 6141 0123	台州	Tel.:+86 576 8966 1886	青岛	Tel.:+86 532 8503 0106	厦门	Tel.:+86 592 7706 188
上海测试中心	Tel.:+86 21 6037 6300	苏州	Tel.:+86 512 6809 5318	大连	Tel.:+86 411 8230 4203	东莞	Tel.:+86 769 2168 7092
上海工业材料实验室	Tel.:+86 21 6014 9880	成都	Tel.:+86 28 8952 0656	沈阳	Tel.:+86 24 6223 3726	泉州	Tel.:+86 595 2281 3681
无锡	Tel.:+86 510 8820 3737	杭州	Tel.:+86 571 8111 0758	长春	Tel.:+86 431 8462 9833	长沙	Tel.:+86 731 8458 5815
宁波	Tel.:+86 574 2786 6658	常州	Tel.:+86 519 8123 9872	香港	Tel.:+852 2776 1323	柳州	Tel.:+86 158 0772 5319
永康	Tel.:+86 579 8711 7995	重庆	Tel.:+86 23 8980 9513	香港元朗办事处	Tel.:+852 2443 3774	台北	Tel.:+886 2 2898 6818
南京	Tel.:+86 25 8779 0058	北京	Tel.:+86 10 6590 6186	深圳	Tel.:+86 755 8828 6998	台中	Tel.:+886 4 2287 0566
合肥	Tel.:+86 551 6537 8730	天津	Tel.:+86 22 8319 2258	广州	Tel.:+86 20 3832 0668		