ISO 26262功能安全标准简介

发布日期: 八月 10, 2016

概览

随着各行业引进一系列产品设计和测试的标准化流程，安全保障也日益规范化。ISO 26262满足了人们对于汽车行业国际标准的需求，重点关注安全关键部件。ISO 26262基于IEC 61508 - 电气和电子(E/E)系统的通用功能安全标准。本白皮书介绍ISO 26262的关键组成以及软硬件认证。此外，本白皮书还包含ISO 26262的测试过程，以及ISO 26262合规的认证工具。

目录

1. 背景

随着汽车行业复杂性的日益提升，人们加大了开发安全合规系统的力度。例如，现代汽车使用线控系统，如油门线控。司机踩油门时，踏板中的传感器将向电子控制元件发送信号。该控制单元将分析多种因素，如引擎速度、车辆速度及踏板位置。接着，控制单元将向油门传递指令。对油门线控这类系统进行测试和验证，对汽车行业造成了挑战。ISO 26262的目标是为汽车电气和电子系统提供统一的安全标准。

ISO 26262的国际标准草案(DIS)发布于2009年6月。自发布起，ISO 26262就获得了汽车行业的支持。标准草案生效后，律师将ISO 26262视为技术巅峰，即特定时期内某种设备或流程的最高发展水平。德国法律规定，汽车生产商通常要对产品故障导致的人身伤害承担赔偿责任。技术巅峰都无法检测的故障可获得免责。[德国产品责任法(§ 823 Abs.1 BGB, § 1 ProdHaftG)]。

ISO 26262提供了通用的标准，用于衡量系统在使用时的安全性。同时，该标准还提供了通用的词汇表，用户可使用该词汇表指代系统的特定部分。这和其他安全关键应用领域保持一致：即提供一个通用的标准，让用户可以衡量系统的安全性。

2. ISO 26262的关键部分

ISO 26262采用分步系统，管理功能安全，并在系统、硬件及软件层面管理产品开发。

ISO 26262标准提供规范及推荐做法，贯穿了产品开发的全过程（从概念开发到停运）。ISO 26262详细介绍了如何为系统或组件指定可接受的风险等级，以及记录总体测试流程的方法。总而言之，ISO 26262：

- 提供汽车安全生命周期（管理、开发、生产、运行、服务、停运），并支持在各阶段中自定义必要的活动
- 提供基于风险的方法，判定汽车的风险等级（汽车安全完整性等级，简称ASIL）
- 使用ASIL指定项目的必要安全要求，以达到可接受的残余风险
- 提供验证要求和确认方法，以确保实现有效且可接受的安全性

汽车安全生命周期

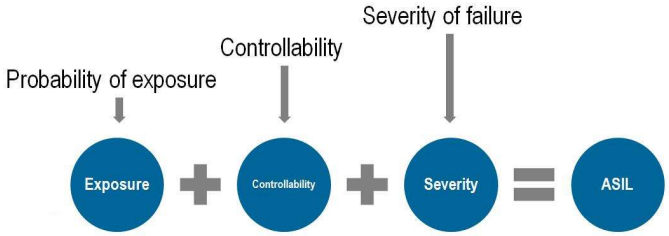
ISO 26262共有10卷，用于系列量产车，并包含针对汽车的章节。例如，ISO 26262的第7章对生产、运行、服务及停运提出了明确的安全要求。

ISO 26262汽车安全生命周期描述了整个生产生命周期。包括对安全管理员的需求、安全计划的开发以及确认方法的定义（包括安全检查、审计及评估）。这些要求用于开发电气和电子系统及元件。

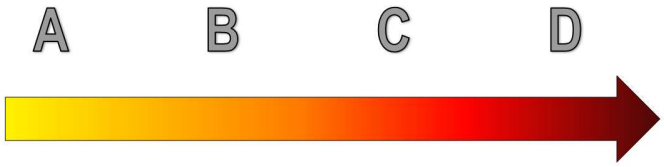
本白皮书主要介绍生命周期的开发部分。ISO 26262关于开发的部分包括定义系统、系统设计、功能安全评估以及安全验证。

汽车安全完整性等级(ASIL)

ASIL是ISO 26262标准的关键部分。ASIL是在开发过程的开始阶段确定的。用户需要根据可能的危害，分析系统的预期功能。ASIL提出这样一个问题：“如果车辆发生故障，驾驶员和相关行人会怎样？”



为了评估风险的评估，ASIL需综合考虑暴露的可能性、驾驶员的控制能力以及关键事件发生时的严重性。ASIL不处理系统所使用的技术，而只关注对驾驶员及其他行人造成的危害。



不同的安全要求分为ASIL的A、B、C、D级别，其中D级为最高安全关键流程，测试规范最为严格。ISO 26262标准根据组件的ASIL级别，分别规定了最低测试要求。这有助于确定测试时必须采取的方法。确定ASIL后，就决定了系统的安全目标。即确定了保证安全所需的系统行为。

例如，让我们以雨刷系统为例。安全分析将确定丧失雨刷功能会对驾驶员的视线造成何种影响。ASIL指导如何选择适当的方法，以达到一定程度的产品完整性。本指南旨在补充目前的安全做法。目前，汽车制造采用高安全标准，ISO 26262旨在规范行业内的特定做法。

3. 硬件组件认证

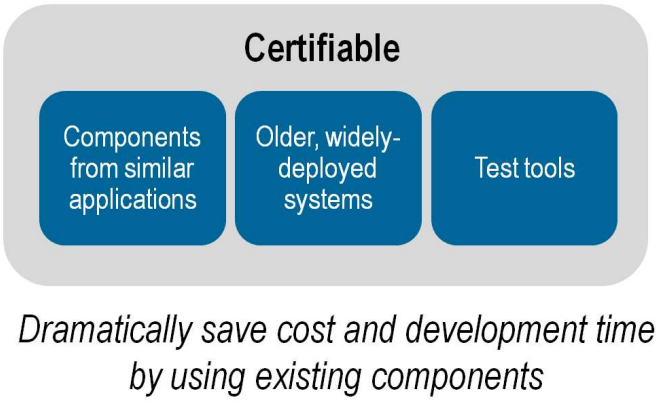
硬件认证有两个主要目的：展示部件如何适应整体系统，并评估故障模式。基础硬件组件可通过标准资格评估，但更复杂的部件要求通过ASIL分解及测试进行评估。硬件组件的认证通常是在一系列环境和操作条件下进行测试。接着，使用多种定量方法分析测试结果，并写入资格报告，附带测试程序、假设及输入标准。

4. 软件组件认证

认证软件组件包括：确定功能要求、资源使用以及预测在故障和过载情况下的软件行为。在实际应用的开发阶段使用认证的软件可大幅简化该过程。认证的软件组件通常是优秀的产品，可在项目中复用，包含库、操作系统、数据库及驱动软件。

为了认证软件组件，标准要求在正常操作条件下进行测试，并在系统中插入故障，以判定其如何应对非正常输入。设计阶段将分析并处理软件错误，如运行时和数据错误。

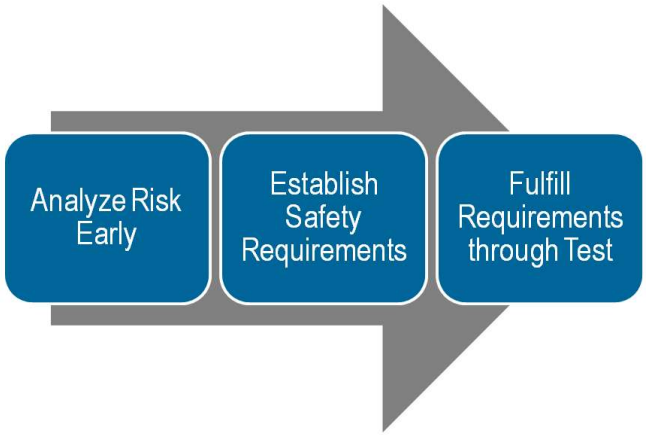
5. “在实践中证明”的证据



硬件及软件组件可通过“在实践中证明”的证据，证明其符合ISO 26262要求。若组件已在其他实际应用中无故障运行，则可适用该条款。ISO 26262也适用于在实践中得到证明的早期系统。很多情况下，若某种系统已经在几百万辆汽车上得到验证，则没有必要重新检验其是否符合标准。例如，目前制造的汽车中，很多系统是按照ISO 26262发布前的高级别安全标准制造的。实际应用过程中，这些安全关键部件运行良好。从更早期汽车就保持不变的可靠系统仍然符合ISO 26262认证。类似实际应用中的认证组件，和获得广泛部署的早期实际应用一起，极大地降低了总体系统复杂度。

6. 应用于现有流程

执行类似于ISO 26262这样的新标准的主要挑战之一是将其应用于现有流程。对于新标准，需要使用试验项目展示如何实现该标准，及其对现有流程的影响。目前的结果表明，ISO 26262符合业内现有的安全理念。各公司已经开始重视在开发阶段评估风险并进行危害分析，以及在各流程中进行测试。



计划执行ISO 26262的公司需要理解，目的是在开发过程的早期阶段分析风险、确立适当的安全要求，并通过开发中的测试最终达到这些要求。

7. 测试工具认证

测试是ISO 26262开发过程中的关键部分。安全关键系统必须合理应对测试场景，并在面对各种人为及环境输入时保持在指定的安全范围内。使用高质量测试系统可提高产品性能、提升质量及可靠性，并降低返修率。据估计，相比于在实际应用中，在生产中发现的错误导致的故障花费将降低10倍；而若在设计环节发现错误，则又比生产中降低10倍的花费。通过发现错误并收集数据，可改进设计或流程。测试为您的组织创造了价值。通过技术创新和最佳实践方法推动流程创新，可大幅提升效率，降低花费。人们容易忽略工具，只考虑系统的设计。但实际上，工具对终端用户的安全十分重要。

ISO 26262承认，使用广泛应用的软件工具可简化或自动化开发电子、电气及软件元素（提供安全相关功能）开发所需的步骤及任务。介绍工具认证过程的细节前，需要定义一个工具认证的重要部分：工具置信水平。

工具置信水平

通过工具的输入和输出，可开发典型（或参考）用例。分析用例便可确定工具置信水平，简称TCL。TCL和ASIL决定软件工具要求的认证水平。确定置信水平，需要评估一下两种因素：

- 软件工具出故障的可能性，以及错误输出对开发中的安全相关项目或元素会造成何种危害
- 在输出中预防或检测该错误的可能性

工具置信水平分为TCL1、TCL2、TCL3和TCL4，其中TCL4为最高置信水平，TCL1为最低置信水平。

工具认证过程

在ISO 26262中，认证工具有诸多要求。例如，必须已经确定了ASIL。工具必须包含用户手册、独特的标识及版本号、功能描述、安装过程以及环境（仅举几例）。ISO 2626要求以下认证材料：

- 软件工具认证计划
- 软件工具文档
- 软件工具分类分析
- 软件工具认证报告

软件工具认证计划

软件工具认证计划(STQP)是在安全相关项目开发生命周期的早期创建的。它主要关注两个方面：计划软件工具的认证，以及能证明该工具符合所需置信水平的用例。

STQP必须包含的项目有：软件工具独特的标识及版本号、用例、环境、描述、用户手册以及确定好的ASIL。

软件工具分类分析

软件工具分类分析(STCA)的主要目的是确定工具置信水平。确定TCL有两个主要因素。第一个因素是**工具影响**(TI)。第二个因素是**工具错误检测**(TD)。根据这两个因素，选择合适的TCL。

工具影响分为TI1和TI2。当故障软件工具不可能违反安全要求时，可选择TI1。其他情况则选择TI2。

例如，假设某工具在执行特定软件功能时，会在文档中产生错误字符。这仅仅是一个小错误，并不违反测试时的安全要求。该错误造成的是TI1类别的工具影响。若工具造成的错误以任何形式改变了系统行为，则选择TI2。

工具错误检测分为TD1、TD2和TD3。TD1代表对工具检测错误的能力有高度的置信，而TD3则代表很低的置信水平，即只能随机检测出错误。

例如，假设某工具用于检测设计模型的错误。该工具对模型执行静态分析。当静态分析良好时，该工具不能检测模型中的所有可能违规行为。还有一点值得注意的是，这并不一定意味着该模型是错误的，而仅仅表明需要额外的测试。该例是一种中等程度的置信水平，即TD2。

		工具错误检测		
		TD1	TD2	TD3
工具影响	TI1	TCL1	TCL1	TCL1

TI2	TCL1	TCL2	TCL3

根据所需置信水平，一旦确定了工具影响(TI)和工具错误检测(TD)，就确定了TCL的级别。多个用例可能导致不同的TCL。出现这种情况时，请使用最高级别的TCL。对每个软件工具，用户需进行工具分类。

软件工具文档

为确保正确使用软件工具，必须提供多种信息。

- 功能描述
- 安装过程描述
- 用户手册
- 操作环境
- 异常状态下的预期行为

软件工具认证报告

软件工具认证报告包含结论以及完成认证且满足要求的证据。任何验证期间产生的故障或错误输出都需在此进行分析和记录。

从实践中提升的置信

从实践中提升置信是工具认证的一个重要方面。若能证明某工具已经符合认证要求，就无需进一步的认证。这将大幅降低开发过程中的花费及时间成本。然而，在开发该项目前，认证要求必须在每个安全相关项目或元素上得到证明。为达到该要求，该工具必须证明：

- 曾经为了相同的目的，在类似的用例中使用
- 该工具的规范保持不变
- 未在曾经开发的安全相关项目中违反安全要求

例如，假设工具A用于验证汽车X的ECU（引擎控制单元）。若测试工具A未违反任何安全要求，且保持不变，那么它就可用于检测汽车Y的ECU，只要汽车Y的ECU用途与汽车X的ECU使用方法类似。

8. 下一步

欲知NI测试工具如何用于测试安全相关项目，请参考 NI测试安全兼容系统最佳实践 (http://zone.ni.com/devzone/cda/tut/p/id/13671)。该白皮书包含诸如模型回路测试和硬件回路测试等技术，贯穿整个开发过程。此外，该白皮书还讨论了组件重用的优势及效率提升。

其他资源

NI测试安全兼容系统最佳实践 (http://zone.ni.com/devzone/cda/tut/p/id/13671)

观看ISO 26262认证的介绍视频 (http://zone.ni.com/wv/app/doc/p/id/wv-3077)