超越 ISO 和 ASIL 标准的车辆安全性：以太网网络组件如何提高自动驾驶汽车的安全性

Steffen Lorenz，Jochen Schyma
汽车以太网解决方案
NXP Semiconductors Germany GmbH
德国汉堡/慕尼黑
steffen.lorenz@nxp.com

Claude R. Gauthier，博士
汽车以太网解决方案
恩智浦半导体公司
美国圣何塞
claude.gauthier@nxp.com

摘要

全自动驾驶汽车的蓬勃发展从许多方面改变了行业现状，尤其是在车辆安全性方面。如今，安全目标通过端到端“概念”实现，而驾驶员则是最后一道防线。但是，一旦计算机掌握了控制权，通信路径的可用性对于允许发生故障后继续运行的系统至关重要。因此，车辆安全性要求将功能安全性与可靠性相结合。

在这种情况下，以太网 IC 的作用也在发生变化。尽管当前的汽车网络通常未对这些连接 IC 提出安全要求，但是 IC 供应商已开始看到对具有一定安全要求和 ASIL 等级产品的需求日益增加。除了查看市场营销数据和勾选特性列表，还需要更多的信息来比较内置安全功能的价值。

本文将介绍网络 IC 中功能安全的系统环境和示例，并对网络最终将如何支持故障预防进行展望。最后，本文将提供 ISO 26262 实现方法的背景知识。

I. 引言

汽车行业正追随三大趋势：自动驾驶、电气化和面向服务、用户定义的HMI。所有这些趋势都加速向车辆分布式E/E架构过渡。这种过渡，加上即将出现的具有完全或部分自动驾驶功能的新兴汽车，对车载网络的功能安全要求产生了影响。

ISO 26262[1]从总体上定义了将E/E系统故障引起的固有风险降至可接受水平的开发步骤。根据潜在严重性、遭遇故障情况的可能性以及系统发生故障时的可控性，会为每个系统分配一个汽车安全完整性等级(ASIL)，从A（最低）到D（最高）。系统的不同部件将继承使用这些安全要求。本文将重点讨论单独使用的安全元件的开发，这通常用于标准IC的开发。

II. 单独使用的安全元件

ISO 26262中描述的流程是一种自上而下的方法，将继承使用从系统级至子部件的安全要求。作为例外，定义了一个“单独使用的安全元件”(SEooC)开发流程。IC通常作为SEooC进行开发，因为其开发要比实际系统的开发早很多，而且通常不是专门针对一款特定车辆。在IC的开发过程中，需要对未来环境做出假设。假设的环境也会针对此SEooC开发定义ASIL。

在安全相关系统中使用 SEooC 时，系统集成商必须根据实际环境的安全要求（即特定功能的开发）来验证 SEooC 开发假设（参见图 1）。只有满足了所有假设，SEooC 的 ASIL 才有效。例如，SEooC 开发可能已针对某些内部故障模式假设了一个外部安全措施。在实际系统中，必须可以提供该措施。因此，如果不了解使用环境，IC 的 ASIL 分级就没有用。

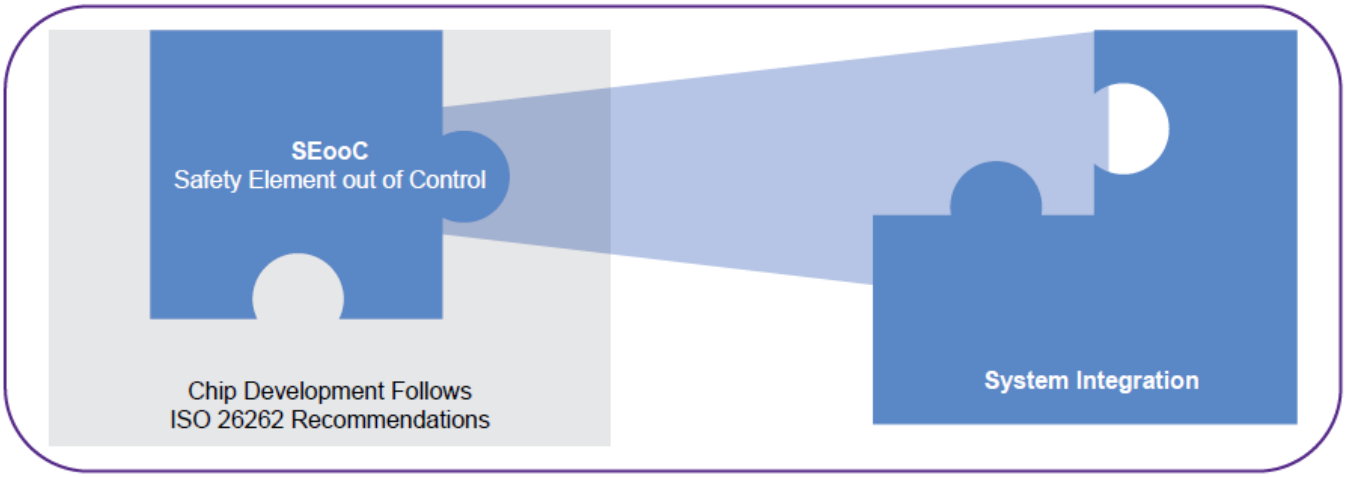


图 1：SEooC 的整合

III. 机器人车辆中的功能安全

通常，有几种功能安全措施可以涵盖所有类型的故障，并且在端到端保护系统中都会提供这些功能。这些安全措施可以检测数据是否受损、发送过迟、多次发送，甚至丢失。简而言之，当今的车载网络相对而言是安全的。我们几乎可以说，我们当前的工作已经完成。

原因在于不久的将来。尽管如此，让我们从目前常见的方法开始。让我们假设汽车使用传感器数据来实现驾驶辅助系统，例如自动距离控制。端到端保护确保了数据的正确性，如果网络损坏，系统会检测到不再能提供有效的传感器数据。系统将被关闭，驾驶员将收到通知，以接管全部控制权。车辆保持运行。

现在假设自动驾驶汽车面临同样的情况。没有驾驶员可以接管；因此，系统必须让车辆停止行驶（见图 2）。没有驾驶员，或者至少没有一个能立即做出反应的驾驶员，将导致安全状态直接影响车辆服务的可用性。

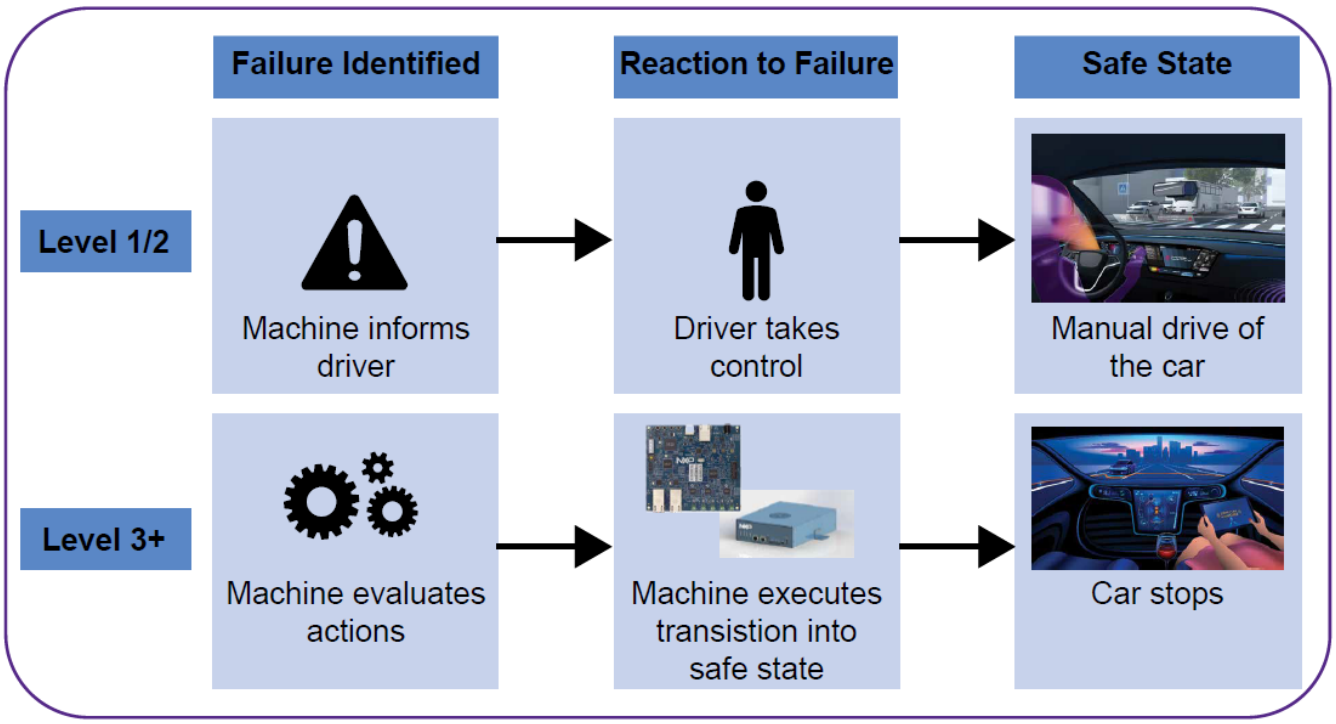
IV. 网络IC如何保持车辆行驶

我们用非黑即白的方式描述了这种情况，有很多情况不会直接导致汽车停下来。尽管如此，还是值得仔细研究一下，了解在网络 IC 上采取措施来提高车辆服务可用性将如何改善汽车性能。

可以在以下几方面通过确保车内通信服务的可用性来提高车辆服务可用性：

- 预防故障
- 预测故障
- 应对故障

通信可用性取决于信号路径中的组件可靠性。它从开发过程中的正确流程开始（包括组织中的安全文化），并以制造过程中的实际汽车质量措施结束（例如基于鉴定数据和返修的技术筛选）。这些措施的相互作用确保将故障率降到最低。在测试过程中已经筛选去除了故障概率较高的薄弱器件。这可降低现场故障概率，并会使系统进入安全状态。



1

图 2：系统对故障的应对取决于自动驾驶等级

另一个方面是故障的可预测性。从纯功能安全的角度来看，这方面并不相关，因为 ISO 26262 流程侧重于检测故障并可靠地过渡到安全状态。停驶的汽车更安全。但是，考虑到可用性，在故障实际发生之前花一些精力来检测故障很有意义。当温度升高时，可以关闭系统不必要的部件，但重要部件仍保持活动状态。对于以太网而言，可以将某些信息娱乐连接关断，只保持骨干通信畅通。一个示例是以太网 PHY 的信号质量指示符，可用它来检测因环境条件而导致的物理信道质量下降。

最后，有一些故障发生时没有事先通知。这种情况无法完全防止。在许多情况下，这将由系统级别的端到端检测功能来应对；因此，在较低级别添加检测功能既不会增加诊断的覆盖面，也不会提高系统的安全性。然而，可以从另一个方面来解释为什么在发生故障的地方进行检测很有意义。越靠近故障源进行检测，系统对此故障做出反应并防止对整个系统造成影响的可能性就越大。带 ECC 保护存储器的以太网交换机能够纠正错误的内存单元，因此即使发生故障，仍能正确传输数据。网络可能会使用 IEEE 802.1CB[2] 以太网流复制/消除功能来构建冗余通道，以提高在电缆或连接器发生故障情况下的可用性，尽管就功能安全而言它并非完全冗余的。

V. 结论

网络组件（特别是以太网 IC）的功能安全开发很有意义，但是有必要对数据手册中的简明 ASILx 额定值提出质疑。只有了解环境详情，才能判断安全措施的价值。

成熟的开发过程和高制造质量是保持同等高水平的安全性并提高未来汽车服务可用性的基础。预防、预测和应对故障场景的正确措施构成了面向高度可靠的未来汽车网络的完整方案。

参考资料

1 ISO 26262:2018，路面车辆——功能安全，第 2 版。

2 IEEE 802.1CB:2017，适用于局域网和城域网的 IEEE 标准——提升可靠性的帧复制和消除