解说功能安全 [二]：智能网联汽车的“安全三剑客”

原创 焉知汽车 焉知自动驾驶 11月1日

收录于话题
#功能安全荟萃

17个

作者 / HYZY
出品 / 焉知

01

“安全三剑客”

功能安全、预期功能安全和信息安全均属于汽车操作安全的一个部分（见《解说功能安全[一]：汽车操作安全体系下的功能安全》），同时这三项安全技术也一起并成为智能网联汽车操作安全性的“安全三剑客”。

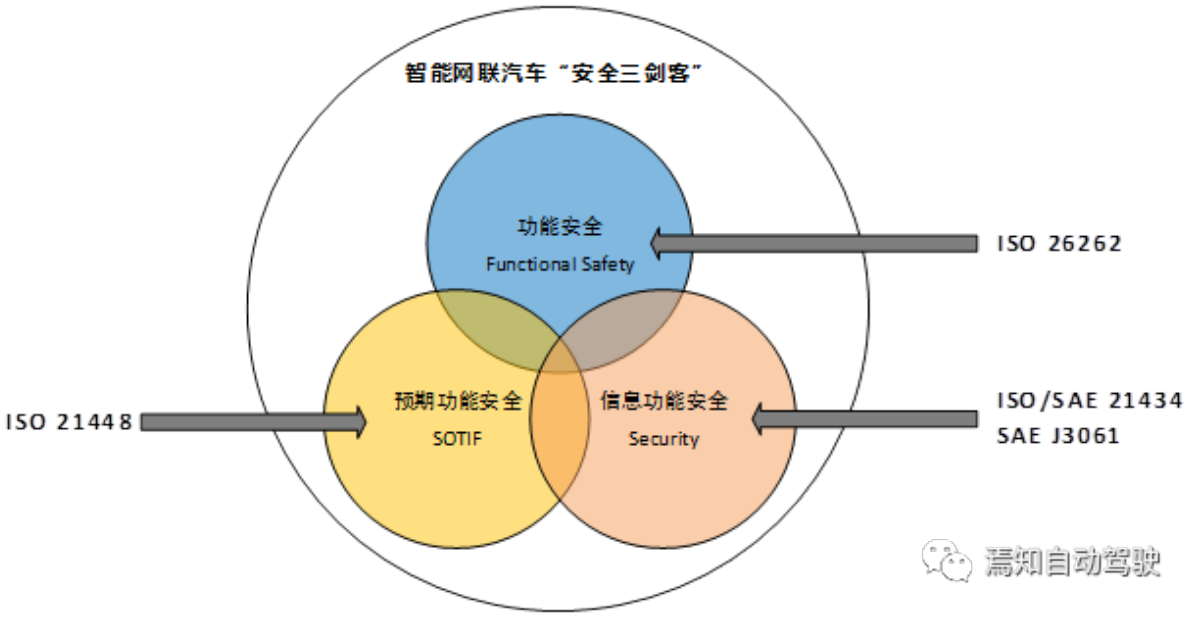

图 1 智能网联汽车操作安全性“三驾马车”

三项安全技术的适用范围及对应的技术标准见下表1。

表 1 三项安全技术适用范围及对应技术标准

危害源头	危害事件原因	应用标准
系统自身	E/E 系统失效	ISO 26262
	无论有或没有合理可预见的误用，存在性能限制场景感知不足	ISO 21448
	合理可预见的误用，不正确的 HMI（例如用户混淆、过使用）	ISO 21448 ISO 26262 European statement of principal on the design of human-machine-interface
	由系统技术导致的危害	针对性标准
外部因素	成功利用车辆安全漏洞进行攻击	ISO 21434 / SAE J3061
	来自主动型基础设施和/或 V2V 通讯、外部装置及云服务的影响	ISO 20077* ISO 26262
	来自车辆周边环境的影响（其它道路使用者、被动型基础设施、环境条件：天气、电磁环境）	ISO 21448 ISO 26262

**注：ISO 20077 道路车辆 – 延伸车辆（ExVe）方法。*

02 功能安全和信息安全

1)功能安全和信息安全的联系

来自车辆外部的信息安全威胁同样可能会造成人身危害，因此可以将信息安全威胁纳入功能安全的危害源头进行协同分析。

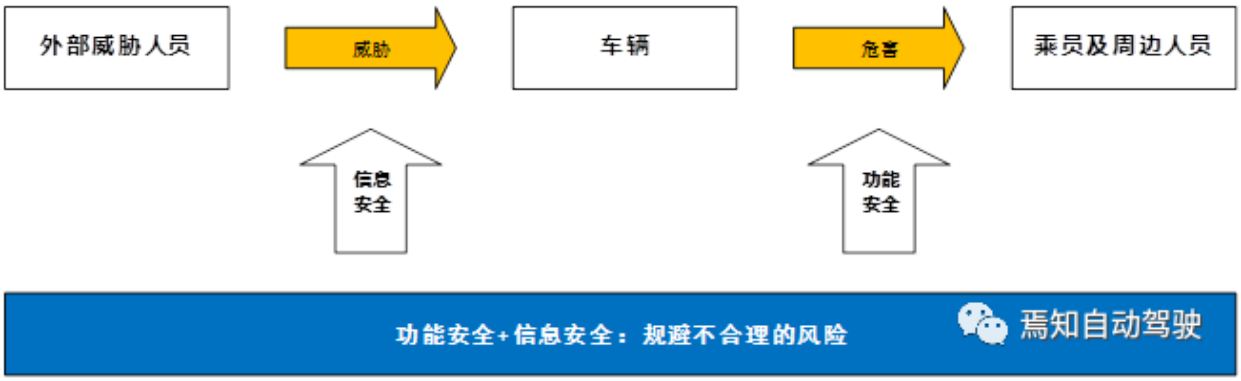

图 2 功能安全和信息安全的关系

下图3展示了在车道偏离系统上，功能安全和信息安全协同作用的示例。

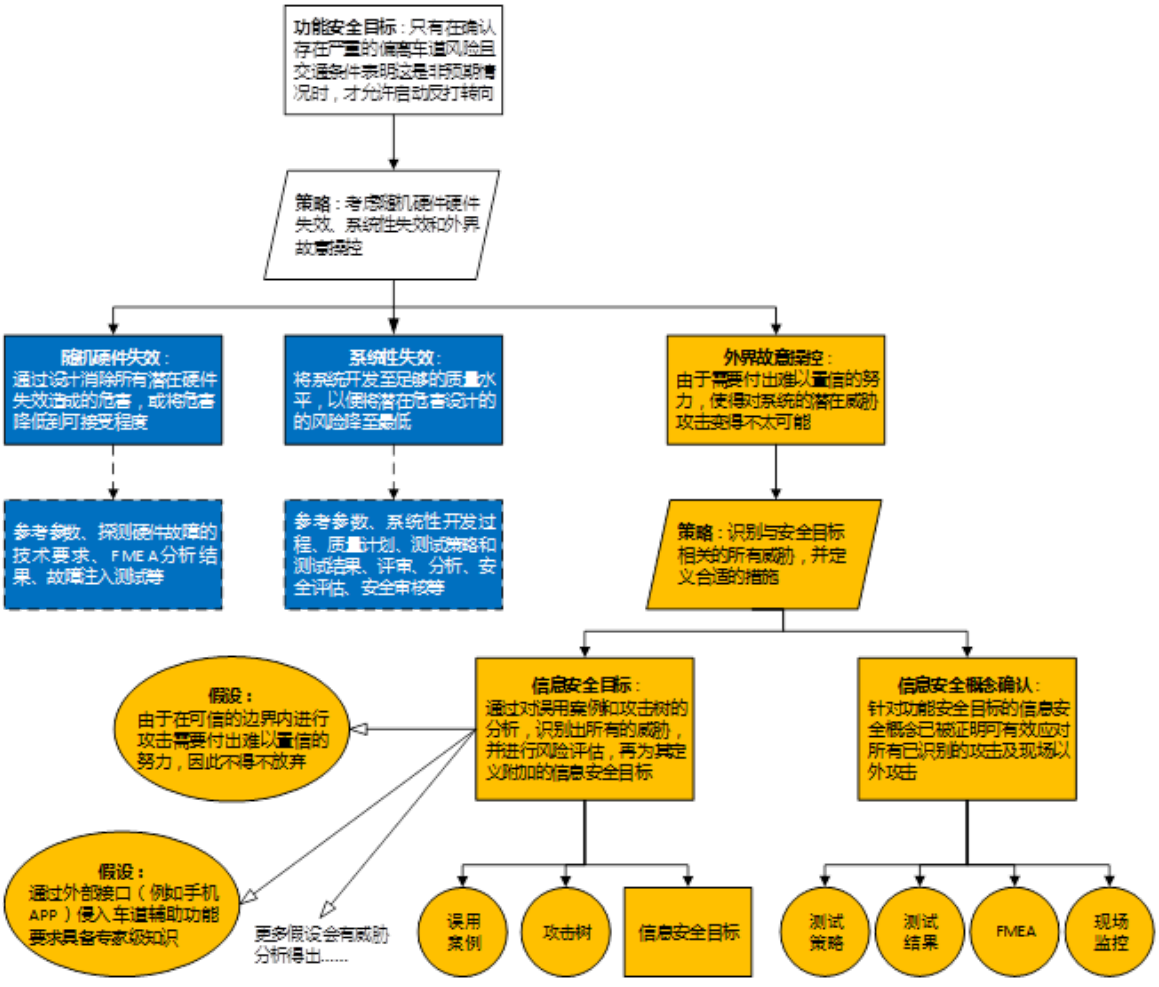

图 3 车道偏离系统功能安全和信息安全协同作用示例

2)功能安全和信息安全的交互要求

为明确功能安全和信息安全之间的关系，ISO 26262-2018版本中新增了要在功能安全和信息安全之建立交互的要求。

A.功能安全管理中的交互要求

- 信息安全活动的计划及里程碑，应考虑与功能安全活动计划之间的相关性，例如软件开发、工具选取、编程语言和指南；
- 协调信息安全和功能安全的现场监控活动，包括事件报告、跟踪和解决，以便将与人身安全相关的信息安全事件传达给功能安全。

B.概念阶段的交互要求

- 将信息安全威胁视为功能安全的危害源进行分析，以支持危害分析及风险评估和安全目标的完整；
- 功能安全可以提供危害和相关风险信息，以支持信息安全识别威胁；
- 需分析E/E系统受到攻击时采用的信息安全应对策略和措施，对功能安全目标及功能安全概念的影响。

C.产品开发阶段的交互要求

- 需分析E/E系统受到攻击时采用的信息安全应对策略和措施，对技术安全概念及系统设计的影响；
- 信息安全软件和硬件的设计考虑，需满足软件及硬件的功能安全需求及设计约束，例如独立性；
- 功能安全可以提供与安全措施设计与实施相关的信息，以便传达可能与信息安全相关的功能安全约束；
- 应协调功能安全和信息安全的分析活动，以发现信息安全对功能安全的潜在影响。安全分析还可以考虑信息安全策略及措施的影响；
- 为解决系统性失效而定义的信息安全措施，需确认对功能安全的潜在影响，例如，开发功能安全与信息安全共享的安全措施所需要的方法。

D.生产和运行阶段的交互要求

- 为了响应信息安全事件而需要进行设计变更，变更方案（信息安全事件解决策略）需考虑对功能安全的影响。

功能安全和预期功能安全

1)预期功能安全的概念

随着智能网联汽车技术的发展，人们发现并不是所有的车辆安全问题都源于系统错误和失效，而是很多时候来源于环境影响或系统本身的功能/性能不足。例如，自动驾驶系统即使不发生故障，也可能因为神经网络黑盒输出等因素的不确定性导致功能的偏离，进而造成交通伤害。

这类非故障情况下，因系统功能不满足预期而导致的安全风险就是预期功能安全要解决的问题。具体来说预期功能安全提供了开发智能驾驶车辆功能的方法和规则，包括：

- 提供智能驾驶系统架构的基本概念方法；
- 评估有别于ISO 26262的智能驾驶功能的风险；
- 提供标准方法，确认智能驾驶场景和测试结果的可靠性；
- 提供测试，验证智能驾驶安全防护的真实可行性；
- 提供基础标准条例，用于认可发布智能驾驶功能投产。

2)功能安全和预期功能安全的关系

功能安全和预期功能安全的对比见下表2，功能安全用于解决电子电气失效对人造成的危害，而预期功能安全用于解决系统非故障原因对人造成的危害。ISO 26262标准中对电子电气系统的标称功能及性能没有要求，预期功能安全的存在弥补了这部分遗憾。

表 2 功能安全和预期功能安全的对比

对比项	功能安全	预期功能安全
采用标准	ISO 26262	ISO/PAS 21448
出错原因	电子电气功能随机出错或系统出错	不够完善的障碍物检测功能； 避开障碍物的功能不可靠； 没有全面设计针对误操作或滥用的措施
出错危害	比如，无故加速失控	比如，没有避开障碍体
安全措施	防范随机和系统性出错	防范功能定义的缺陷或非完整性； 制定完整的防范误操作或滥用引起的功能失误

04

“安全三剑客”的融合趋势

融合“安全三剑客”是未来智能网联汽车安全技术的一个重要趋势，并且行业已在这个方向上进行了一定的探索（例如百度发布的《自动驾驶安全第一白皮书》），相信未来会我们会看到更多的行业实践。

收录于话题 #功能安全荟萃·17个

上一篇

解说功能安全 [三]：功能安全开发思路（上）

下一篇

解说功能安全 [一]：汽车操作安全体系下的功能安全