解说功能安全 [三]：功能安全开发思路（上）

原创 焉知 焉知自动驾驶 11月2日

收录于话题
#功能安全荟萃

17个

作者 / HYZY

出品 / 焉知

ISO 26262标准体系庞大、内容驳杂，在一开始学习这个标准时往往难以抓住核心脉络。因此本文尝试梳理ISO 26262标准体系中的功能安全开发思路，作为详细标准学习的一个引导。

首先看ISO 26262-2018中对功能安全的定义是：

"Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems."

GB/T 34590-2017中给出的对应定义为：

"不存在由电子电气系统的功能异常表现引起的危害而导致不合理的风险。"

由以上功能安全的定义，可理解功能安全的**核心思路**为：采用合适的安全措施，将因为电子电气系统功能异常表现而引起的危害控制在可容忍的风险边界。

为进一步理解上述核心思路，必须要解释清楚其中的四个关键概念：危害、风险边界、电子电气系统功能异常表现、安全措施。

一、危害

危害有很多类型，如人身伤害或者财产损失等等。功能安全里的危害（hazard）仅仅指因E/E系统的故障行为而引起的对驾驶员或者路人或周边车辆内人员（注意不仅是驾驶员）的人身危害。也就是说，功能安全开发的目的是避免伤人，而不是避免伤车。

图 1 功能安全针对的危害

二、风险边界

ISO 26262标准中使用汽车完全完整性等级（ASIL）来衡量风险的大小，随风险由高到底，ASIL等级被分为了：ASIL D、ASIL C、ASIL B、ASIL A、QM。

在上述五个等级中，质量管理QM（Quality Management）可以理解为功能安全技术体系下的"风险边界"，控制到QM风险等级的危害即为"可容忍的"。对于QM风险等级的危害，ISO 26262标准不作额外要求，符合TS 16949质量体系即可。但部分先进整车厂和零部件企业可以设定内部标准，自行定义QM风险等级中的部分危害需要采用的安全措施。

ASIL D、ASIL C、ASIL B和ASIL A四个等级均为不可容忍的风险等级，必须采取安全措施。ISO 26262标准为四个不同ASIL等级定义了不同的安全措施要求，只有采用了对应ASIL等级的安全措施，才能被认为将风险控制到了风险边界。

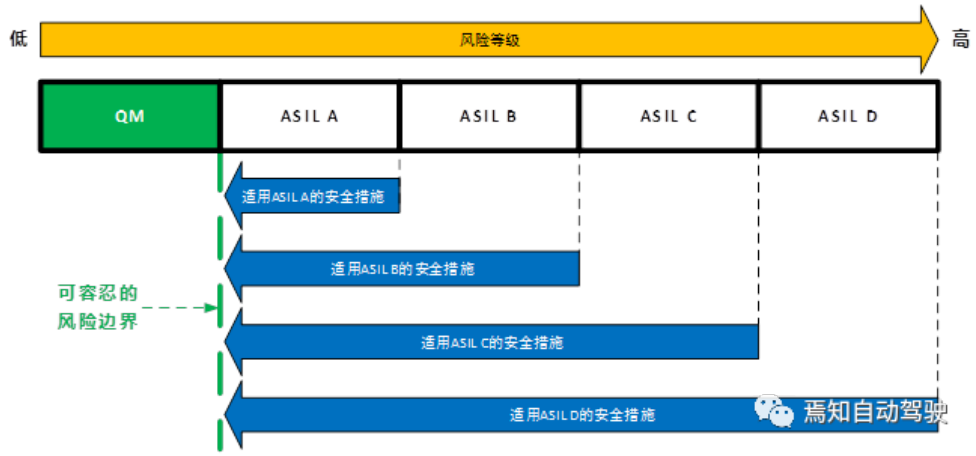

图 2 ASIL等级与风险控制

三、电子电气系统功能异常表现

1)概述

对于汽车来说，汽车操作安全中的各个方面均可能成为引发人身危害的危害源，即使将危害源限制在电子电气范畴，也会包括几种可能的危害源。而针对这些不同的危害源，就出现了功能安全、预期功能安全和信息安全等多种安全技术体系。

其中功能安全针对的危害源就是"电子电气系统功能异常表现"，具体来说，包括两种类型：系统性失效和随机硬件失效。

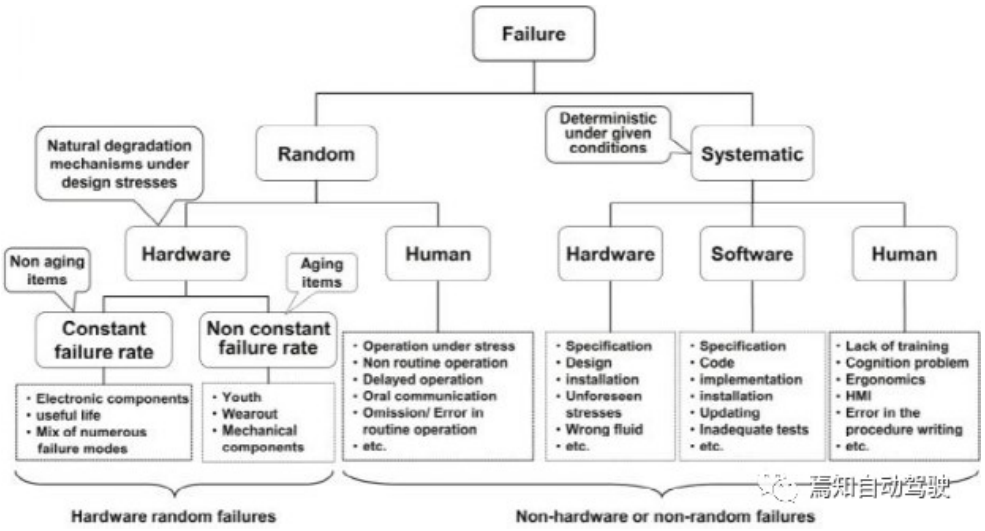

图 3 失效类型

2)系统性失效

系统性失效（systematic failure）指以确定的方式与某个原因相关的失效，只有对设计或生产流程、操作规程、文档或其它相关因素进行变更后才可能排除这种失效。即系统性失效可理解为因设计考虑不足造成的产品功能失效。

造成系统性失效的原因可能包括：

- 系统架构设计错误

  –系统易触发或不能避免安全危害保障；

  –不能足够地检测和防护安全危害。

- 零部件功能设计和制造错误

  –硬件设计偏离环境、边界条件和寿命要求；

  –软件设计中的架构错误以及逻辑或数据处理错误。

- 生产装配和维修中的错误
- 可预料到的客户操作错误、滥用或非正常使用（非恶意使用）

  –例如，误触某功能键、插座错位、同时踩刹车和油门、玩弄开关等。

3)随机硬件失效

随机硬件失效（random hardware failure）指在硬件要素的生命周期中，非预期发生并服从概率分布的失效。即随机硬件失效可理解为因器件本身的设计寿命到了（如：器件退化或老化）造成的产品功能失效。

随机硬件失效可以认为是硬件的可靠性问题，其深层原因是由物理原因导致的，比如腐蚀、热应力、老化等。因为这些原因的随机特性，导致硬件在何时发生失效时无法预测的，但是会遵循某种概率分布（比如指数分布）。随机硬件失效的概率分布可以从测试和历史数据中得到。

下图4为通用的“浴盆曲线”，表示出了硬件的失效概率分布。

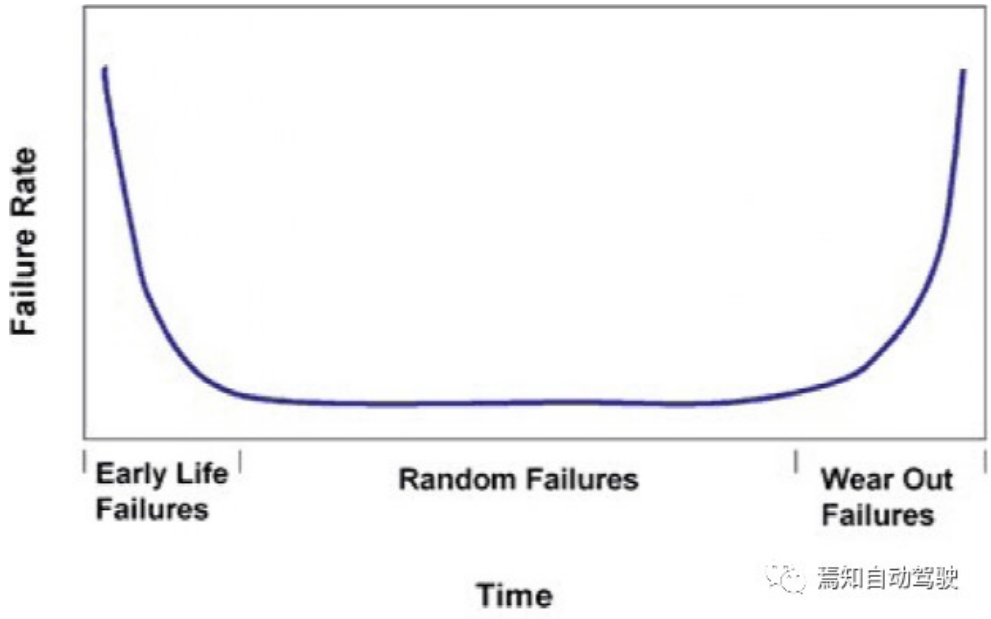

图 4 可靠性“浴盆曲线”

收录于话题 #功能安全荟萃·17个

上一篇　　下一篇