汽车功能安全系列知识分享（一）：ISO26262 的发展历程

近年来，电动汽车（EV）以及汽车辅助驾驶以及无人驾驶（AV）已成为汽车行业发展的大趋势，并呈现加速发展之势。而汽车作为复杂的系统，需要在各种工况之下在使用寿命期间达到很高的安全标准。目前，诸如转向失控、制动失灵等自动/辅助驾驶事故，电池自燃等各种新型安全事故亦层出不穷。汽车功能安全因而愈发重要，并且已经随着自动驾驶技术以及电动汽车的发展和普及，迅速成为与自动驾驶等新技术同等重要的技术热点，已经成为自动驾驶和电动汽车量产投放市场决定性的一环。

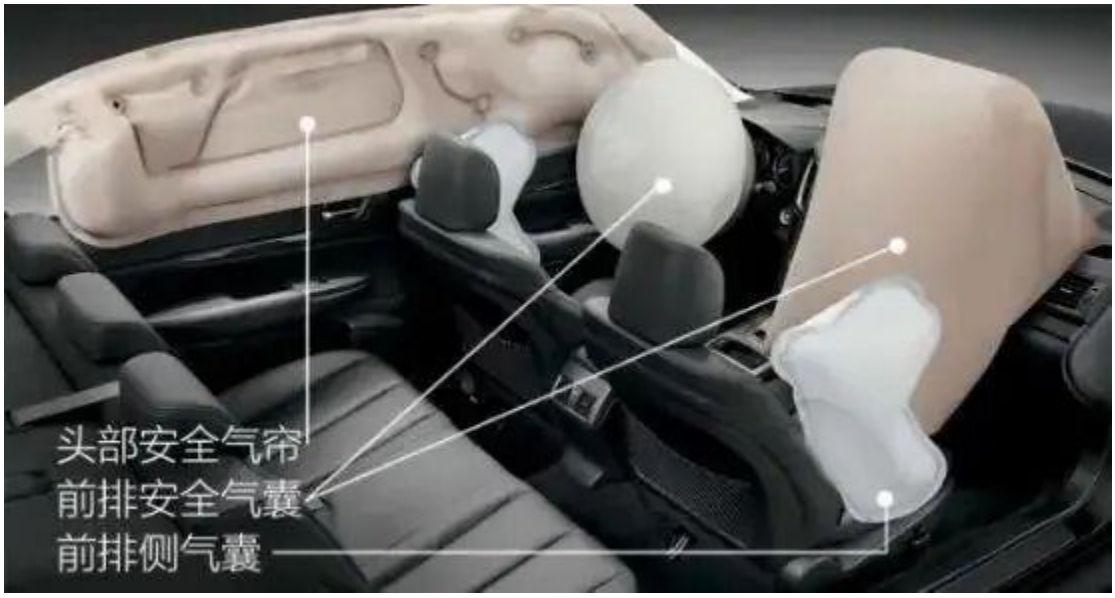
汽车出现功能安全问题，相关设计人员将承担法律责任

在欧美，汽车的功能安全已经是超过二十年的老话题了。欧洲的相关法律是《通用产品安全指令 2001/95/EC》（GPSD）。正如数字所示，这是一条相当古老的法律。法律简单地规定："产品开发者有责任以符合最先进开发原则的方式开发安全产品。"最先进的技术仅仅是尊重公认的最佳实践。迄今为止，这方面的相关标准是 IEC 61508。现在， ISO 26262 出现并取代了汽车特定应用（小于 3.5 吨的车辆）的这一解释，2018 版又涵盖了卡车、公共汽车与摩托车。德国 VDA 明确将最佳实践定义为 IEC-61508 和 ISO 26262。

相关法律自颁布以来一直有效。唯一改变的是解释。ISO 26262 自 2009 年以 DIS 格式发布。从那时起，它已成为公共领域的知识，世界上任何律师都可以使用它来解释公认的最佳实践。由于它取代了 IEC 61508，因此没有宽限期。如果你不应用它，你需要证明你在没有它的情况下履行了最新标准。如果出现安全问题，他们会以故意的无知或鲁莽的行为起诉你。这意味着对公司处以巨额罚款，对工程师和安全负责人处以个人法律责任，甚至监禁。

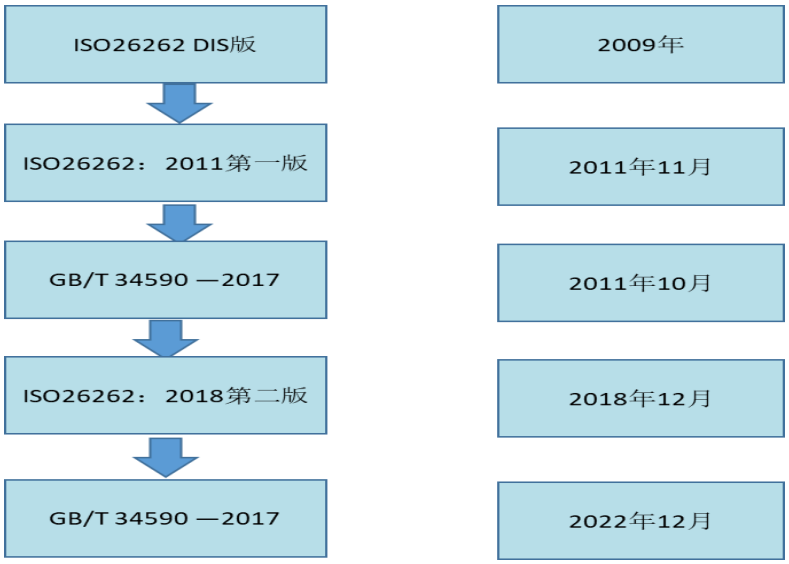
汽车安全责任典型案例

在德国，曾经发生过这么一个具体案例：车辆即使切断开关处于关闭位置，乘客侧安全气囊仍被激活，在低速正面碰撞中，乘客侧安全气囊展开，导致乘客座椅上的一名婴儿死亡。调查发现，切断开关读取正确，但数据在存储在 EEPROM 再从 EEPROM 读取过程中发生错误，这是一个软件错误。负责的软件工程师曾多次出庭，并被起诉犯有过失杀人罪、无期徒刑。这意味着有犯罪记录。本案中的软件设计工程师虽然最终被宣判无罪，但他的任期被终止，犯罪记录仍然被保持，这会严重影响其职业生涯。事实上，即使该工程师不来自起诉发生的国家，如果最终产品在该市场销售，无论其居住地在哪里，工程师都可能在该国承担责任。



ISO26262 的发展历程

由于 IEC 61508 是一个通用标准，对汽车电子电器有些方面不是特别适用，汽车电子电器的快速发展给 IEC 61508 标准带来了很大的挑战，因此非常有必要在汽车行业形成特定的标准，ISO26262 应运而生。ISO26262 标准经历了如下发展历程：

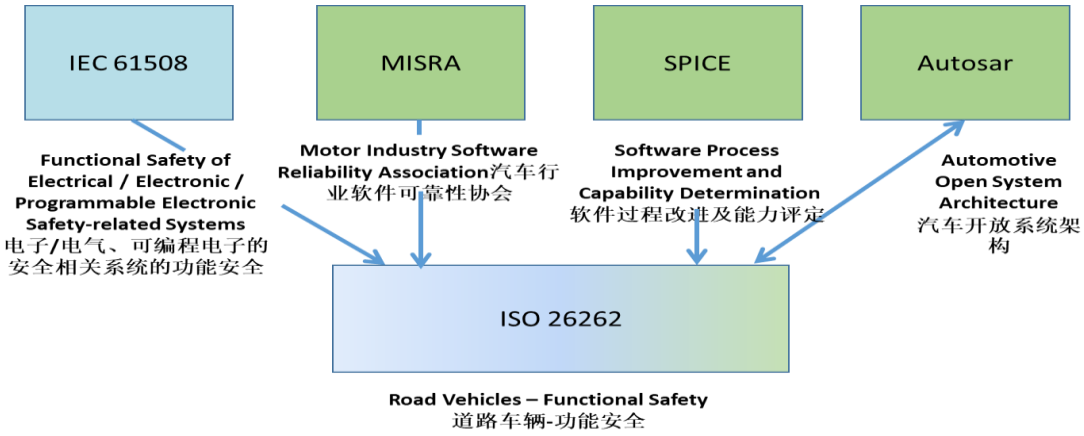


ISO26262 第一版的适用范围仅适用于重量不超过 3.5t 的乘用车，在第二版中，则扩展到卡车、公共汽车和摩托车，使其在汽车行业有着更广泛的应用。

ISO26262 的相关标准

ISO26262 是在 IEC61508 标准上派生出来的，并融合了 ASPICE、AUTOSAR 等要求。主要

定位在汽车行业中特定的电气器件、电子设备、可编程电子器件等专门用于汽车领域的部件，旨在提高汽车电子、电气产品功能安全的国际标准。



未完待续，更多精彩内容敬请关注