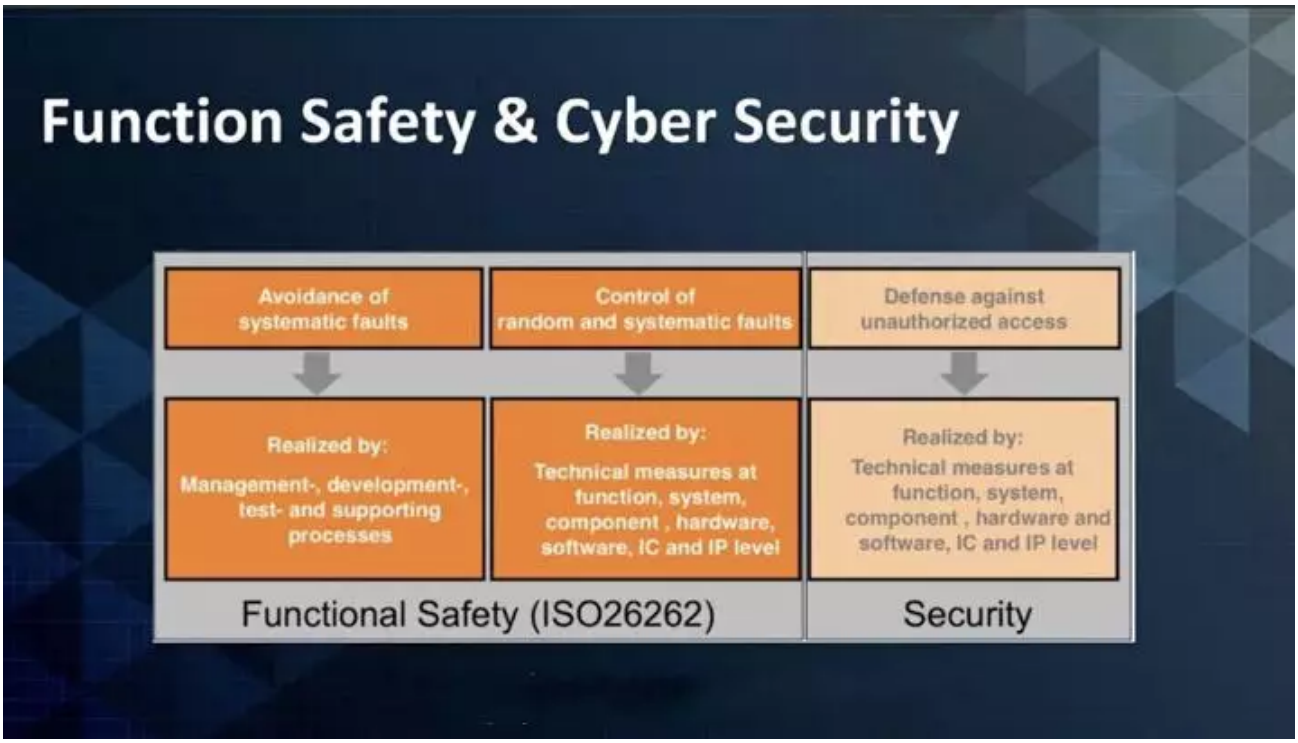
Apollo进阶课程 ③ | 开源模块讲解（中）

首先为大家介绍安全方面最基础的一个模块ISO-26262。ISO-26262是一个非常复杂、非常结构化的标准。比如说，**如果一个硬件达到了ASIL D级别的要求，那么它的故障率是10 fit（Failures In Time, in one billion device-hours of operation）**，即10亿个小时里面出一次故障。这个故障率要比windows蓝屏的概率低很多。



从英文来讲，安全有两个词：**Safety和Security**。Safety包含两个方面：系统性故障 **Systematic Faults** 和随机故障 **Random Faults 。**

系统性故障是说，我在设计汽车的时候就存在的缺陷。每次运行的时候，都一定会发现问题。软件和硬件都有可能存在系统性故障。

随机故障是由不可控的因素造成的故障，不一定会出现，比如路上颠簸了一下。一般情况下，只有硬件会出现随机故障。

而Security涉及的不是车自身的问题，而是系统被别人攻占了。以前你要攻陷一辆车，是很困难的事情，没有物理连接也没有网络连接。但是有了无人驾驶技术以后，车总是和网络相连，让车变得特别容易被攻击。

ISO-26262是一个行业规范而不是一个例法，只覆盖Safety，不覆盖Security。但我们在做无人驾驶的时候，必须考虑security。

通过ISO-26262的认证是一个特别慎重的流程。

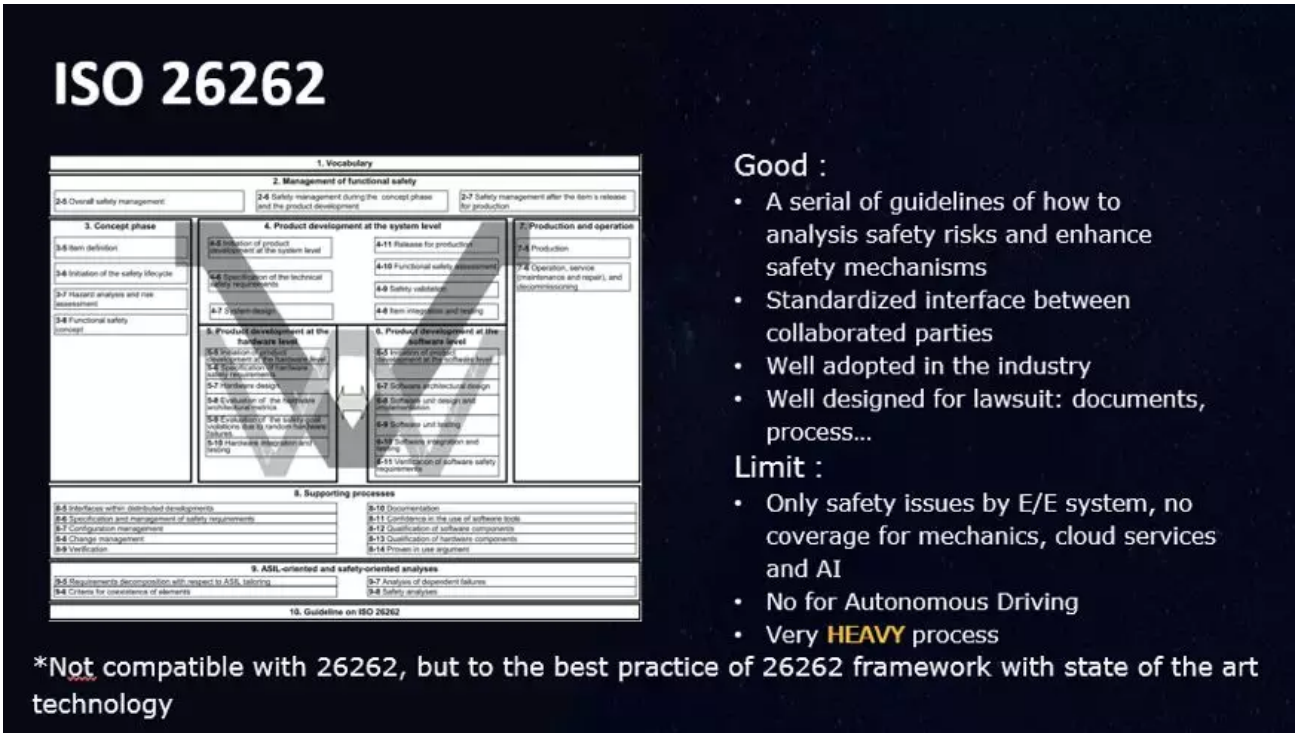
首先你需要明确车具备哪些功能以及这些功能由哪些零部件完成。其次，需要考虑对于车的每个功能是否会出现故障，一旦出现问题是什么级别的问题。

有两种问题，例如做车的加速系统：一种问题是车在人没有意识的情况下加速了。另一种是，需要车加速的时候它没有加速。我们需要把这些问题放到具体的情景中去考虑，最严重的问题是哪一种。对于判断一个问题是否严重，ISO-26262给了三个判断标准：**Exposure、Controllable、Separately。**

> **Separately**是指车和人分离，出事故后有多少概率会造成人员伤亡。
>
> **Exposure**是指这件事情是否常见。
>
> **Controllable**是指车出现了问题，驾驶员是否有机会接管。

ISO-26262的认证过程是一个“V型”。首先要看是什么开发环境，其次要分析问题的等级是怎么样的。如果是一个很高的等级需要判断这个问题出现的概率有多大。然后考虑这个问题具体要怎么解决。也就是先做High Level层级的，再到Function层级，然后到Technique层级。

Technique层级涉及软件和硬件。软件硬件确保了安全性后，再返回往上去做验证。对于ISO-26262更高级别的要求，它会要求有很多Redundant system。如果现行的系统坏了，下面还有一套系统。如果出现问题，另外这个系统具备使它停下来的机制。



ISO-26262优点与缺陷

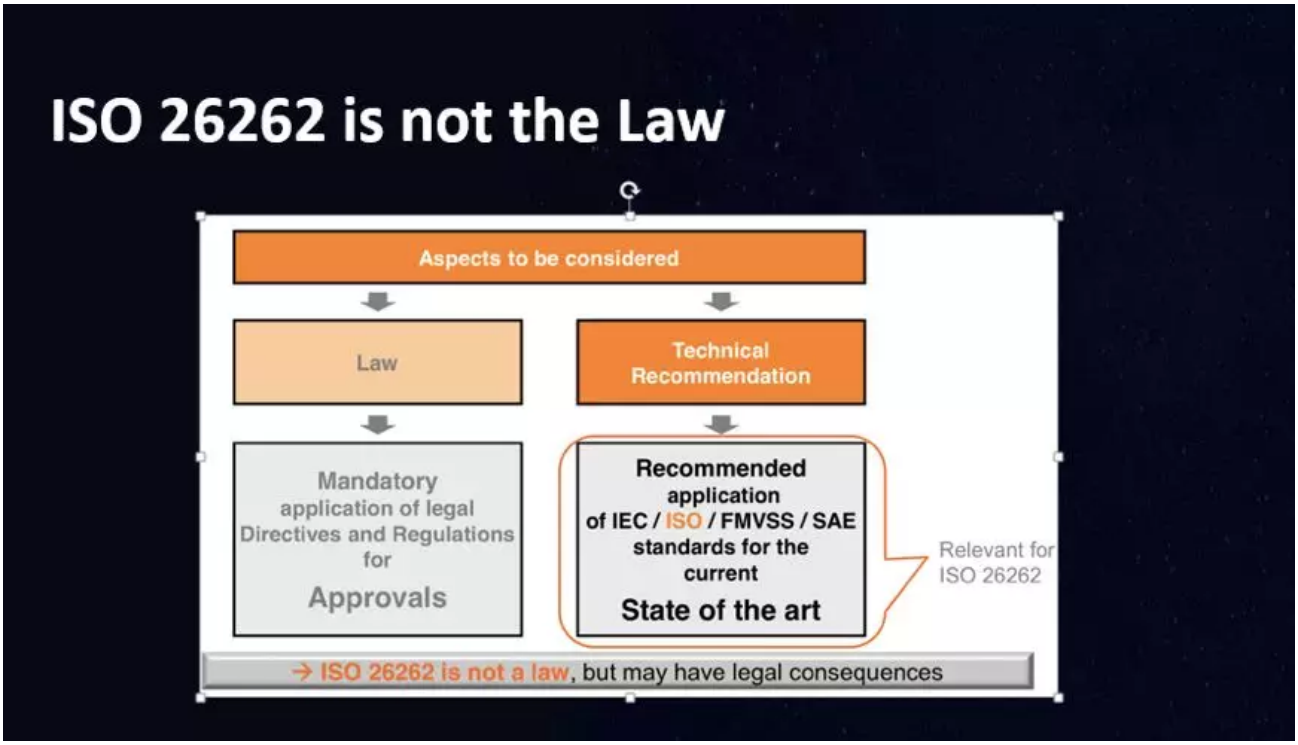
ISO-26262代表了汽车行业在安全方面可以做到的极限，在汽车行业有很高的威望。

首先，它是对技术的一个引导。毋庸置疑它会使车更加安全。其次，它有很高的商业附加值。通过这个认证最多的车是德系车，德系车价格远高于同行。第三，它涉及法律中权责的问题。

汽车行业是一个复杂的行业。车厂要把汽车组装起来，需要对供应商提各种各样的要求。一旦汽车出现了安全问题，供应硬件零件如果符合安全要求，车厂就要承担责任。而汽车的召回一般都是十亿美金这个量级的。所以这个认证它虽然不是法律，但它在打官司的时候特别有用。

但ISO-26262也有缺点。它的认证过程很繁杂（Very Heavy Process），不符合敏捷开发的需求。ISO-26262一定是每一层的文档都准备完毕，才可以做下一层。

我们做一个APP可能以月计迭代都算慢的，但是做车可能需要十年的规划，我们现在开的车可能就是他们十年前规划出来的。


ISO 26262 is not the Law
Aspects to be considered
Law
Technical Recommendation
Mandatory application of legal Directives and Regulations for
Approvals
Recommended application of IEC / ISO / FMVSS / SAE standards for the current
State of the art
Relevant for ISO 26262
→ ISO 26262 is not a law, but may have legal consequences

END