功能安全 IEC 61508 标准新旧版的对比

IEC61508 是国际通用的功能安全基础标准，其核心内容即为功能安全产品的系统、硬件、软件设计做出详尽的要求，以使其能够按满足功能安全的方式进行设计和开发。它为电气/电子/可编程电子安全相关系统建立一个通用的方案，并促进各个应用部门标准的开发。是安全相关系统的总的通用标准，对安全相关系统具有重大意义和重要地位，各个领域的安全相关系统都必须遵循这个标准。

新版 IEC 61508-2010 标准不仅与时俱进地更新了几乎所有技术相关的内容，也总结了近年的技术发展和应用经验基础，依据功能安全技术的理念发展趋势，从系统性能力、硬件/软件安全完整性要求、功能安全管理方面提出了若干新的要求，由此，引起了 IEC 61508 标准衍生而出的各领域功能安全应用标准的逐步更新。IEC 61508 标准的更新，对于 SIS 制造商、集成商和用户来说，如何使产品的设计、集成和使用尽可能地满足新版标准成为一个关键问题。当然，满足新标准的产品将具有更高的质量和技术优势，也由于体现了更接近实际的功能安全理念而为用户创造了更多的价值。

在新版 ICE61508-2010 中，定义了 **SC（systematic capability）**的概念，即系统性能力。用于表征一个组件的系统性安全完整性是否符合指定 SIL 的要求。SC 等级也分为 4 个级别：SC1~SC4，对应于 SIL 的四个等级。也就是说，一个组件具有 SC N 等级，就表示其系统性安全完整性满足 SIL N 等级。它表示，SIL 并非只与系统冗余程度和 SFF 有关。当使用两个或多个具有较低 SIL 的组件来实现更高的 SIL 时，就必须考虑组合后的系统是否具有足够的 SC 等级。此外，对于已有使用经验的组件，新版 IEC 61508-2010 标准还允许通过提供这些组件满足规定的“使用中证实（Proven-in-use）”的证据，来证实组件具有一定级别的 SC 等级。SC 概念的提出，为用户如何真正实现所需的 SIL 提供了更好的思路，也对制造商和集成商的功能安全设计提出了更苛刻的要求。要想达到要求的 SIL，产品制造商必须在设计开发过程中严格遵守标准。

旧版标准中，与 SFF 和 PFD/PFH 计算直接相关的随机硬件失效被分为危险失效和安全失效，其中，安全失效包含了所有不会导致 SIS 拒动的失效。而新版标准中，**安全失效**被重新定义为只会导致 SIS 误动的失效。对于其他既不会导致 SIS 拒动、也不会导致 SIS 误动的失效，根据其是否执行安全功能而分为无关失效和无影响失效，且此两类失效不参与到 DC、SFF、PFD/PFH 的计算中。

在进行软件安全完整性评定时，与 SIS 设计相关的软件包括系统软件和软件工具两大类，而不包括应用场合相关的应用软件。新版 IEC 61508-2010 中，**着重强调了这些软件工具对于实现安全的重要性**。对于在线的软件工具，必须与安全相关的嵌入式软件相同对待。而对于离线的软件工具，根据其对安全产品的影响程度不同分为 T1、T2、T3 三类。进一步提高了对 SIS 系统软件及外部支持软件工具的要求，对避免系统性失效更为有效。

从功能安全管理方面，新版 IEC 61508-2010 标准最大的变化体现在对**安全生命周期的**

变化。新版标准将旧标准中的 E/E/PES 实现阶段分为了 E/E/PES 安全需求规范和 E/E/PES 实现两个阶段。用于明确区分用户提出的 E/E/PES 安全需求规范和产品设计者提出的 E/E/PES 设计需求规范。

在**安全手册**的规定方面，新版 IEC 61508-2010 标准特别增加了 E/E/PES 和软件的规定作为规范性要求，要求制造商必须提供详尽的安全手册，以便在产品集成和使用中实现功能安全。