功能安全生命周期的整体分析

冯双虎 功能安全/报警管理主任工程师

摘　要: 目前，我国安全仪表系统（SIS）及其相关安全保护措施在设计、安装、操作和维护管理等生命周期各阶段，还存在危险与风险分析不足、设计选型不当、冗余容错结构不合理、缺乏明确的检验测试周期、预防性维护策略针对性不强等问题，即对 IEC61508 及 IEC61511 的理解不够全面，对整个生命周期的功能安全缺乏明显的认识。

本文旨在对 IEC61508 及 IEC61511 的应用范围及使用方法进行简单概括，使读者对 SIS 系统整个生命周期的功能安全有一个完整的认识，以指导其生命周期内的设计、安装、调试以及维护管理等各阶段的活动。

关键词：功能安全；安全完整性等级；生命周期；报警管理

引言

IEC 61511 对 SIS 系统进行了定义：用来实现一个或几个仪表安全功能的仪表系统。SIS 系统可以由传感器、逻辑解算器和最终元件的任何组合组成。

SIS 系统独立于过程控制系统（例如分散控制系统等），生产正常时处于休眠 或静止状态，一旦生产装置或设施出现可能导致安全事故的情况时，能够瞬间准确动作，使生产过程安全停止运行或自动导入预定的安全状态，必须有很高的可靠性 （即功能安全）和规范的维护管理，如果安全仪表系统失效，往往会导致严重的安全事故，近年来发达国家发生的重大化工（危险化学品）事故大都与安全仪表失效或设置不当有关。

考虑到 SIS 系统的重要性以对 SIS 系统生命周期中各阶段进行有效管理，国际及国内相关组织制定了一系列标准。

1 介绍

2000 年，国际电工委员会（International Electrotechnical Commission）发布了 IEC61508 标准《电气/电子/可编程电子安全相关系统（E/E/PES）的功能安全》，明确提出了安全相关系统的功能安全问题，即如何确保安全相关系统在危险发生时有效执行其安全功能。

2003 年发布的 IEC61511 标准《过程工业领域安全仪表系统的功能安全》则是基于 IEC61508 的框架针对过程工业中的 SIS 的细化。除此之外在 IEC61508 的基础上还延伸出了其他领域的安全仪表的相关标准，例如：核电工业领域的应用标准 IEC61513、机械领域的应用标准 IEC62061 等。其他功能安全相关的标准有德国的 DIN V 19250《控制技术测量和控制设备应考虑的基本安全原则》/DIN V VDE0801《安全相关系统中的计算机原理》、美国的 ANSI/ISA-84.01-1996《安全仪表系统在过程工业中的应用》。IEC61508-2001 及 IEC61511-2003 所对应的中国国家标准是 GB20438-2006 及 GB21109-2007。

IEC61508 及 IEC61511 提出极大的促进了功能安全的管理，虽然早已被人们所熟知，但是整体认识及细节把握上存在以下问题：

整体认识：对 IEC61508 及 IEC61511 的理解不够全面，对其应用范围认识不足，对生命周期的功能安全理解相对片面，缺乏整体的认识。

实施细节：在设计、安装、操作和维护管理等生命周期各阶段，存在危险与风险分析不足、设计选型不当、冗余容错结构不合理、缺乏明确的检验测试周期、预防性维护策略针对性不强等一系列问题。

因此，在标准的整体把握以及使用细节上仍然存在以下问题：

1、 如何清晰的界定标准的使用范围，在各阶段的活动上两者存在怎样的区别，我们又应该如何遵从；

2、 如何将各阶段的活动有机的结合起来，使不同阶段人员在原则及理念上保持一致，从而确保功能安全的准确性是亟待解决的问题。

2 应用范围及区别

IEC61511 并未对 IEC61508 中功能安全的要求做出改变，而是在此基础上进行了细化。

IEC61508 和 IEC61511 都提出了安全生命周期（Safety Lifecycle）的概念，使用生命周期框图来表示各阶段的主要活动。IEC61511 中安全生命周期的定义为：安全仪表功能实施中，从项目的概念设计阶段开始到所有安全仪表功能停止使用为止的时间段中的必要活动。也就是说，安全生命周期包括了 SIS 概念设计、安装调试、运行、测试、维护、停用等各个阶段的所有活动。

安全生命周期分为 3 个阶段：分析阶段、实现阶段和运行阶段。根据工程事件，这三个阶段活动的主题是由不同的组织机构承担的：分析阶段的主体是最终用户、专利商、设计院，甚至还包括过程危险分析（PHA、HAZOP）专业咨询机构；实现阶段的主体是设计院、

SIS 的供货商、安装公司和最终用户；运行阶段的主体是最终用户。

尽管 IEC61508/IEC61511 生命周期框图已经明确了各阶段主要活动，但是部分内容没有重点突出，例如，新建装置与在役装置中 SIL 评估的区别及注意事项、SIL 验证计划实施等，因此使得部分读者对生命周期完整性缺少认识。基于以上两个标准，将 IEC61508 及 IEC61511 进行融合后，其生命周期框图进行重新定义如下：

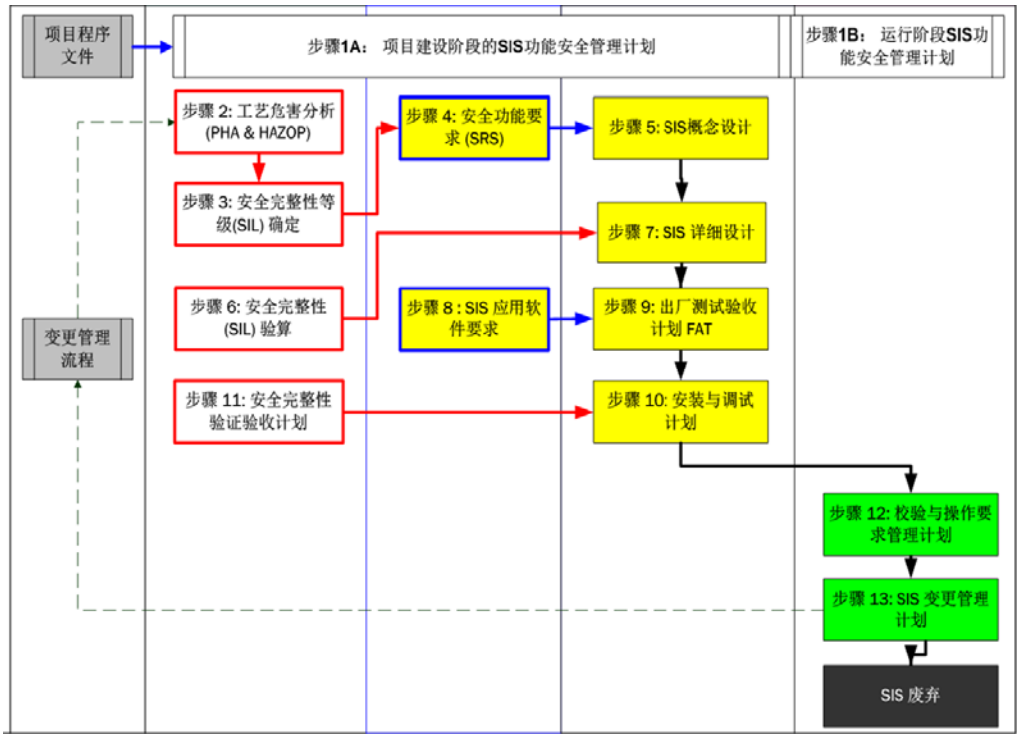


图 1

从上图可以看出各阶段的各项活动并不是孤立存在的而是互相关联，所以通过深刻了解生命周期的思想管理功能安全，才能保证 SIS 相关的各个环节都能得到有效的管理，以提高功能安全的管理水平。

小结：正确认识功能安全生命周期的各个环节，使各部分的输入输出有效衔接，可对功能安全的实施进行整体把控，从根本上提高功能安全水平。

2.1.1 应用范围

IEC61508 与 IEC61511 适用对象有所区别。如下图所示，IEC61508 主要针对设备制造商及供应商，而 IEC61511 则为设计人员、集成商及用户。所以在工程阶段，如设计、安装调试、维护及变更等阶段，IEC61511 具有更强的指导意义。

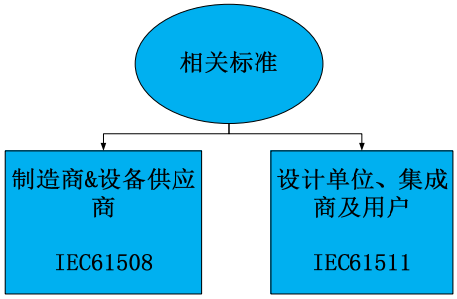


图 2

由于 IEC61508 与 IEC61511 的紧密关联性，不仅确保了不同人员在使用原则上的一致性，而且进一步提升了功能安全执行的水准。此外 IEC61511 还给出了一系列基于风险的分析方法以确定 SIS 系统的安全完整性等级，例如保护层分析方法、风险图法等。

2.1.2 软硬件开发

尽管 IEC61508 及 IEC61511 都对生命周期中各阶段的活动提出了具体要求，但由于 IEC61511 着重于流程工业的安全仪表系统，针对各阶段活动，其输入输出也更加详细。下图为在软硬件开发过程中，应如何遵从标准要求。

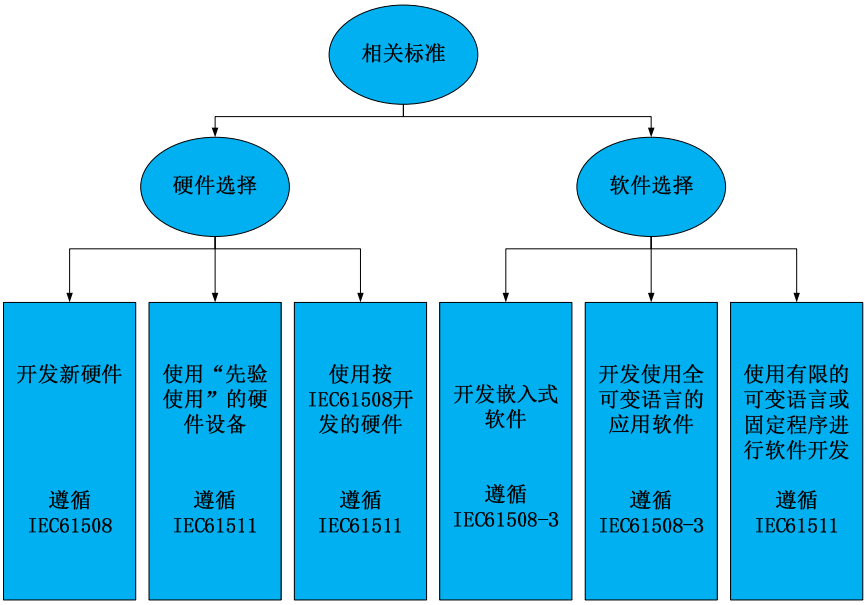


图 3

2.1.3 安全功能分配

IEC61508 与 IEC61511 均提出了功能安全的概念，但是 IEC6508 仅提供了安全功能分配的目的及各项要求（例如，考虑必要的风险降低及安全完整性要求等）并没有给出指导方法，IEC61511-3 则针对安全完整性等级给出了具体实施方法（例如，安全矩阵法、风险图及保护层分析等）及并对典型案例进行了分析。

IEC61508 中功能安全的定义为：与受控设备及受控设备控制系统相关的总体安全的一部分；取决于 E/E/PE 安全相关系统和其他风险降低措施的正确运作。在 IEC61511 中，功能安全的定义为：与工艺过程和基本过程控制系统（Basic Process Control System，BPCS）相关的总体安全的一部分；取决于 SIS 和其他保护层机能的正确运作。由此可见，两个标准均表示为安全相关系统执行安全功能的能力，在核心观点上是一致的，即功能安全是 SIS 设计和运行管理的核心问题之一。

根据 IEC61508 的定义，安全功能 SIF 是由 E/E/PE 安全相关系统或其他风险降低措施实现的，用于针对特定危险事件使受控设备（Equipment Under Control）达到或保持安全状态的功能。

在功能安全的基础上 IEC61511 进一步提出了仪表功能安全的概念。IEC61511 对安全仪表功能的定义为：由 SIS 执行的，具有特定安全完整性等级（Safety Integrity Level，SIL）的安全功能，用于应对特定的危险事件，达到或保持过程的安全状态。并明确了化工过程工业中的 SIS 的范围：紧急停车系统（Emergency Shut-Down System，ESD）、火气系统（Fire and Gas System，FGS）、燃烧器管理系统（Burner Management System，BMS），及高完整性压力保护系统（High Integrity Pressure Protection System，HIPPS）等。SIS 的使

用目的在于必要时可通过执行安全功能，将化工过程的风险降低到可接受的水平。在此基础上提出了风险的概念。

风险是针对一个特定危险事件发生频率和后果的综合度量，风险的削减并不局限于 SIS，其削减过程如下。

- 初始风险：工艺过程中特定危害性事件的风险，确认工艺风险时不考虑其他安全保护因素的影响，如 BPCS 及相关的人为因素；
- 可接受风险（工艺安全目标等级）：基于当前的社会价值特定环境下的可以被接受的风险；
- 剩余风险：危害性事件在考虑所有保护层之后的风险。

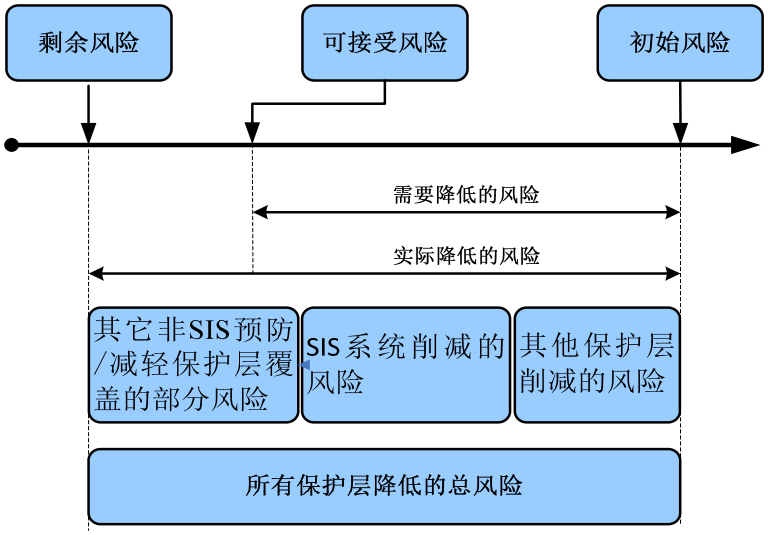


图 4

安全功能的作用在于降低风险。然而无限制的降低风险是不现实的。在实践中，人们往往是按照 ALARP（As Low As Reasonably Practicable）的原则，将风险降低到可接受的程度，保证受控设备或过程处于足够安全的状态。因此，要确保安全功能的合理有效，就需要对受控对象进行准确充分的危险辨识和风险分析。随后基于可接受风险的标准确定风险降低的要求。在确定了必要的风险降低要求之后，如其他保护层无法提供足够的风险削减，则需要 SIS 能够正确地降低风险，这就引出了 SIS 的另一个概念，即功能安全完整性等级（Safety Instrument Level, SIL）。SIL 是 IEC61508 和 IEC61511 中提出的一个重要概念。IEC61511 中安全完整性（Safety Integrity）的定义为：在所有规定条件下，一定时间内，SIS 圆满地执行所要求的安全仪表功能的平均可能性。

由于不同的行业或工艺流程对安全仪表系统的需求概率不同，因此 IEC61508/IEC61511 均引入了操作模式的概念。IEC61508 中，定义了三种操作模式：连续模式、高要求模式以及低要求模式。IEC 61511 没有提及高要求模式。对于应用于不同的操作模式下的 SIS 系统，其可靠性指标也是不一样的。

低要求模式：在这种模式下，安全相关系统的操作频率不大于每年一次或者不大于两倍的检验测试频率。

高要求模式或连续模式：在这种模式下，安全相关系统的操作频率大于每年一次或者大于两倍的检验测试频率。

然而新版的 IEC61508-2010 及 LOPA 国标中均将检验测试频率的限制去掉，仅将一年作为不同模式的分割点。EXIDA 认为仅将一年作为不同模式的分割点缺乏必要的依据，例如，某种操作模式的需求间隔为 10 个月，而其最长的检验测试间隔仅为 1 个月，仍然可以作为低要求操作模式。考虑到测试间隔及诊断间隔对安全仪表系统可靠性的影响，因此 EXIDA 将安全仪表系统的可靠性与以上两个参数关联起来，并通过测试间隔与需求间隔的比值来区分高要求与低要求模式，具体对应关系见下表如下表所示：

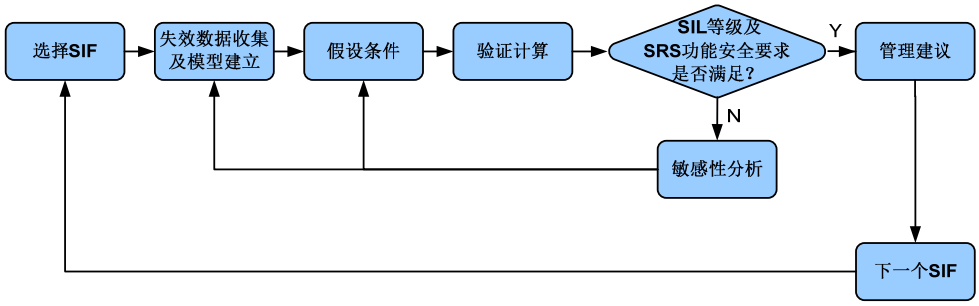
表 1

需求模式	需求间隔与 自动诊断间隔	需求间隔与 测试间隔	可靠性指标
连续模式	DI <= ATI	DI <= PTI	PFH
高要求模式	DI >> ATI	DI <= PTI	PFH
低要求模式	DI >> ATI	DI >> PTI	PFD_{avg}

其中：DI（demand interval）为需求时间间隔，ATI（auto diagnostic interval）为自动诊断时间间隔，PTI（Proof test interval）为测试时间间隔。

2.1.4 安全完整性等级（SIL）验算

在 IEC61508/IEC61511 的生命周期图中均没有将安全完整性等级的验算部分清晰的表示出，从而导致对本标准不熟悉或认知不足的人员忽略了 SIL 验算的重要性。EXIDA 对此部分进行了介绍，其流程图如下所示。



图表 5

SIL 验算的主要基于 SIL 定级分析成果及安全功能规格书（SRS），根据各个 SIF 回路表决机制、公因失效（β）以及检验测试周期及覆盖率等相关因素，对各 SIF 回路的 PFDavg（要求时的平均失效概率）进行计算，并考虑各 SIF 回路的硬件结构约束特性，来考察 SIF 回路能否达到 IEC 61508/ IEC 61511 中对应 SIL 等级的可靠性要求。

对硬件结构约束的要求，IEC61508 与 IEC61511 有所不同，如下表所示：

IEC 61508 中规定了安全功能所声明的最高安全完整性等级，该安全功能使用了一个考虑了硬件故障裕度和安全失效分数的子系统。满足下列条件，其部件被要求达到安全功能的一个子系统可视为 A 类：

1）所有组成部件的失效模式都被很好地定义；

2）故障状况下子系统的行为能够完全确定；

3）通过现场经验获得充足而可靠的数据，可显示出满足所声明的检测到的和未检测到的危险失效的失效率。

典型 A 类设备：开关、气动增压器、执行器、阀门、继电器，或由电阻、电容放大器

等构成的简单电子模块，A 类系统的结构约束要求见**表格 2**。硬件安全完整性：A 类安全相关子系统的结构约束（IEC 61508）

表格 2 硬件安全完整性：A类安全相关子系统的结构约束（IEC 61508）

安全失效分数（SFF）	硬件故障裕度（HFT）		
	0	1	2
<60%	SIL1	SIL2	SIL3
60%~<90%	SIL2	SIL3	SIL4
90%~<99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

B 类子系统：

满足下列条件，其部件被要求达到安全功能的一个子系统可视为 B 类：

1）至少一个组成部件的失效模式未被很好地定义；或

2）故障状况下子系统的行为不能完全确定；或

3）通过现场经验获得的数据不够充分、可靠，不足以显示出满足所声明的检测到的和未检测到的危险失效的失效率。

典型 B 类子系统：基于微处理器的设备，或具有复杂自定义逻辑的设备，复杂系统和元件的行为比较难以确定，例如压力变送器、逻辑控制器等，很难得到其所有组件的失效模式及后果。这类元件及系统均属于 B 类系统，B 类安全相关子系统的结构约束见**表格 3**

表格 3 硬件安全完整性：B类安全相关子系统的结构约束（IEC 61508）

安全失效分数（SFF）	硬件故障裕度		
	0	1	2
<60%	不允许	SIL1	SIL2
60%~<90%	SIL1	SIL2	SIL3
90%~<99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

例如：某 B 类子系统的 SFF 为 92%，SIL2 对应的故障裕度要求为 0，则 1oo1 结构即可满足要求。

为减少 SIF 设计的潜在缺陷，IEC61511 定义了最低的硬件故障裕度要求。这些潜在缺陷可能是由于 SIS 系统设计中假设条件变化，或部件与子系统故障率的不确定性所导致的。

值得注意的是，硬件故障裕度表示对部件或子系统冗余的最低要求。根据不同的应用，可能要求不同的部件失效率、检验测试间隔及硬件冗余以满足对 SIF 的 SIL 要求。**表格 4** 及 **表格 5** 给出了对 PE 逻辑解算器的硬件故障裕度要求。

表格 4 PE逻辑解算器的最低硬件故障裕度（IEC-61511）

SIL	最低硬件故障裕度（HFT）		
	<60%	60%~90%	＞90%

1	1	0	0
2	2	1	0
3	3	2	1
4	应用特殊要求		

当使用的装置符合所有下列各项时，**表格 5** 中规定的除 PE 逻辑解算器外所有子系统（如传感器、最终元件和非 PE 逻辑解算器）的最低硬件故障裕度可减少 1：

根据以往使用的情况，合理选择硬件（先验使用）；

只允许调整过程参数：如测量范围、上限或下限失效指示；

过程参数的调整有严格的管理要求及措施，如：跳线、密码；

SIL 要求小于 SIL4。

表格 5 PE逻辑解算器的最低硬件故障裕度（IEC-61511）

SIL	最低硬件故障裕度（HFT）
1	0
2	1
3	2
4	应用特殊要求

目前国内的 SIL 验算仅停留在对硬件随机失效的计算上，没有综合考虑系统性失效及软件失效的影响，对在系统性失效进行验算时应重点考虑公因失效（例如，分离/隔离、复杂性设计、多样性及冗余配置等）的影响。对软件失效的分析应遵从 IEC61508-3 中的要求，如设计和编码标准、动态分析与测试、功能及黑盒测试等。

对 PFD_{avg} 的确认上，缺少对 MTTF（误动作停车概率）的考虑。频繁的误动作跳车不但影响生产，而且跳车后重启往往会引起新的安全风险。

针对新建装置，可通过对安全仪表回路（SIF）验算及敏感性分析，在设计阶段有效的指导了各 SIF 回路的硬件冗余配置、关键元器件的选型等，并对日后运行阶段测试覆盖率、检测周期等日常检维修策略提供了指导性的建议。

对在役装置，还应考虑工艺改造、安全仪表系统的变更以及检维修策略的变更等因素，其实际工艺风险也可能发生变化，因此，应当在运行期间，在检修时对 SIS 系统进行再验证。再验证工作应与在役装置的 HAZOP 工作相结合，除了对回路 PFD_{avg}、硬件结构约束进行审查之外，特别重要的是针对各个 SIF 回路的校验测试周期、测试方法与结果进行验证。以确保 SIS 系统在整个生命周期内符合完整性要求。

2.1.5 操作维护

目前国内在检维修策略的制定上缺乏预防性措施，尤其在检测测试周期及测试覆盖率的确定上缺乏依据。通过制定合理的检验测试周期及覆盖率可增加 SIF 回路的 SIL 可靠性。近年来，在线检测的措施有所增加，如阀门的 PVST 功能。通过阀门部分行程测试（PVST）可对阀门的部分危险失效进行周期性的检测，从而在整体上减少了检测测试的周期。通过进一步分析得出，通过增加 PVST 可以带来以下优势：

- 提高检验测试周期，提高 SIL 等级
- 提供有预测性的维护数据
- 延长阀门全行程测试（FST）周期

- 优化硬件结构约束
- 减少不必要的旁路设置
- 可在线进行检验测试，同时满足安全需求

3 总结及展望

通过上述分析，我们认识到对生命周期各阶段是紧密相关的，因此对功能安全的生命周期进行综合分析具有非常重要的意义。

国家安全生产监督总局在2014年11月发布的116号文“加强化工安全仪表系统管理的指导意见”中对新建装置及在役装置设计建立安全仪表系统的相关要求中也提到，报警管理（Alarm Management）、火灾报警及可燃气检测系统（Fire and Gas Detection System，FGS）的可靠性及布局合理性分析等方面的分析应参照安全仪表功能进行管理和检验测试。

目前我们国内市场上的与功能安全相关的软件仅为单一功能的分析或计算软件，日后对软件的需求为将各阶段活动进行有效衔接（例如，HAZOP→SIL定级→SRS→SIL验算等）并考虑报警管理、火气系统（FGS）的综合管理软件。

因此，未来应将重点放在 SIS 系统生命周期完整性的管理上，对仪表的可靠性进行综合性的分析也愈发重要。

参考文献：

[1] IEC 61508，Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems

[2] IEC 61511，Functional Safety-Safety Instrumented Systems for the Process Industry Sector

[3] GB/T 20438-2006 电气/电子/可编程电子安全相关系统的功能安全

[4] GB/T 21109-2007 过程工业领域安全仪表系统的功能安全

[5] EXIDA：safety equipment reliability data handbook V1 sensor

[6] EXIDA：safety equipment reliability data handbook V2 logic solver interface module

[7] EXIDA：safety equipment reliability data handbook V3