课件2：安全仪表系统SIS安全生命周期

- 声明：本课件非本公司编制，来源于网络.

青岛劳帕安全技术咨询有限公司

核心业务

- 安全仪表系统功能评估：安全完整性等级SIL定级、验证/验算
- 过程工艺危害分析 **HAZOP**
- 培训：安全完整性等级SIL定级、验证/验算、HAZOP等培训

微信扫一扫

微信号 :**qd13184148810**

电话：13184148810

QQ:1930712371

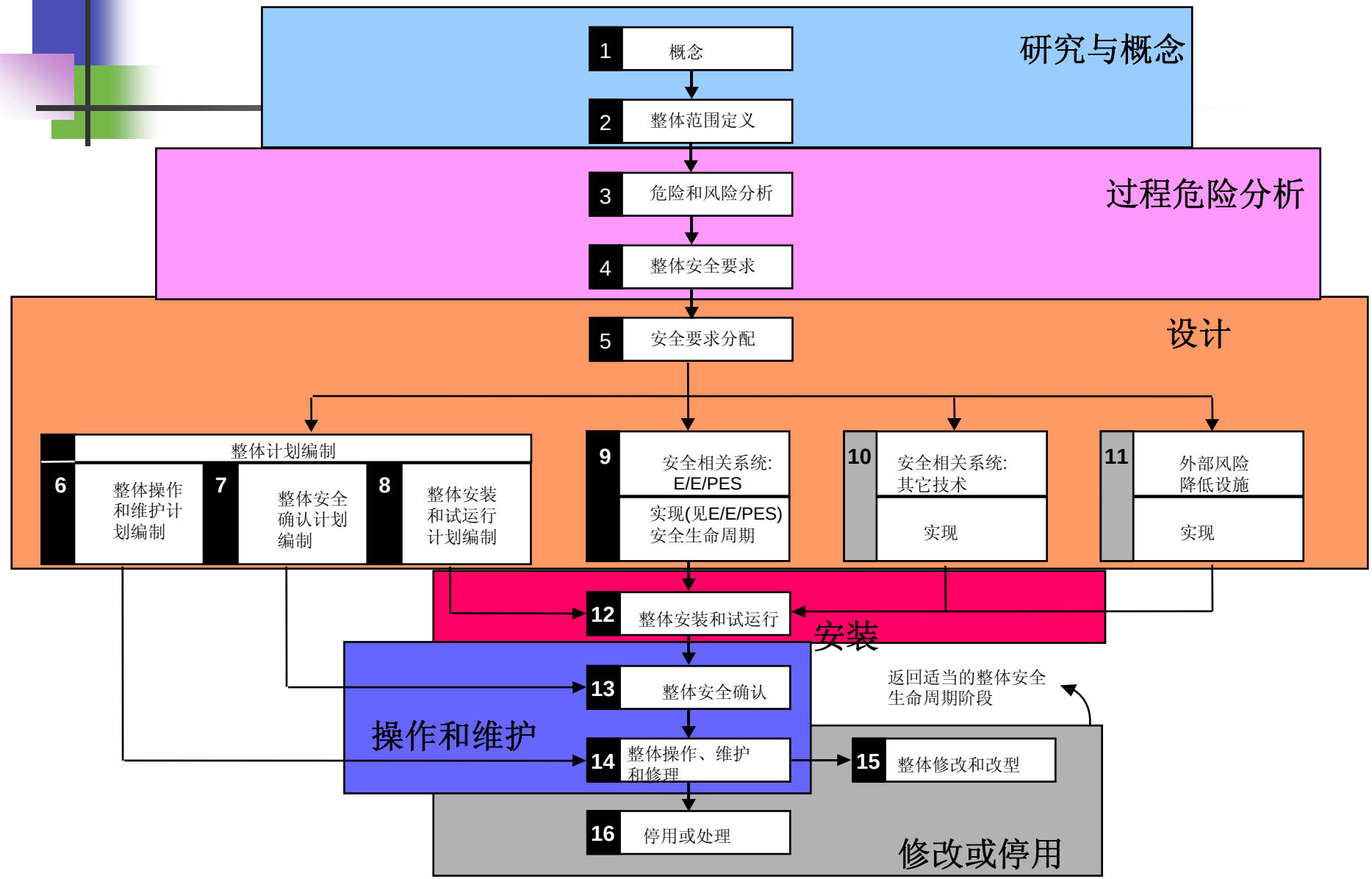
邮箱：qingdaolopa@163.com

网址：www.qingdaolopa.com

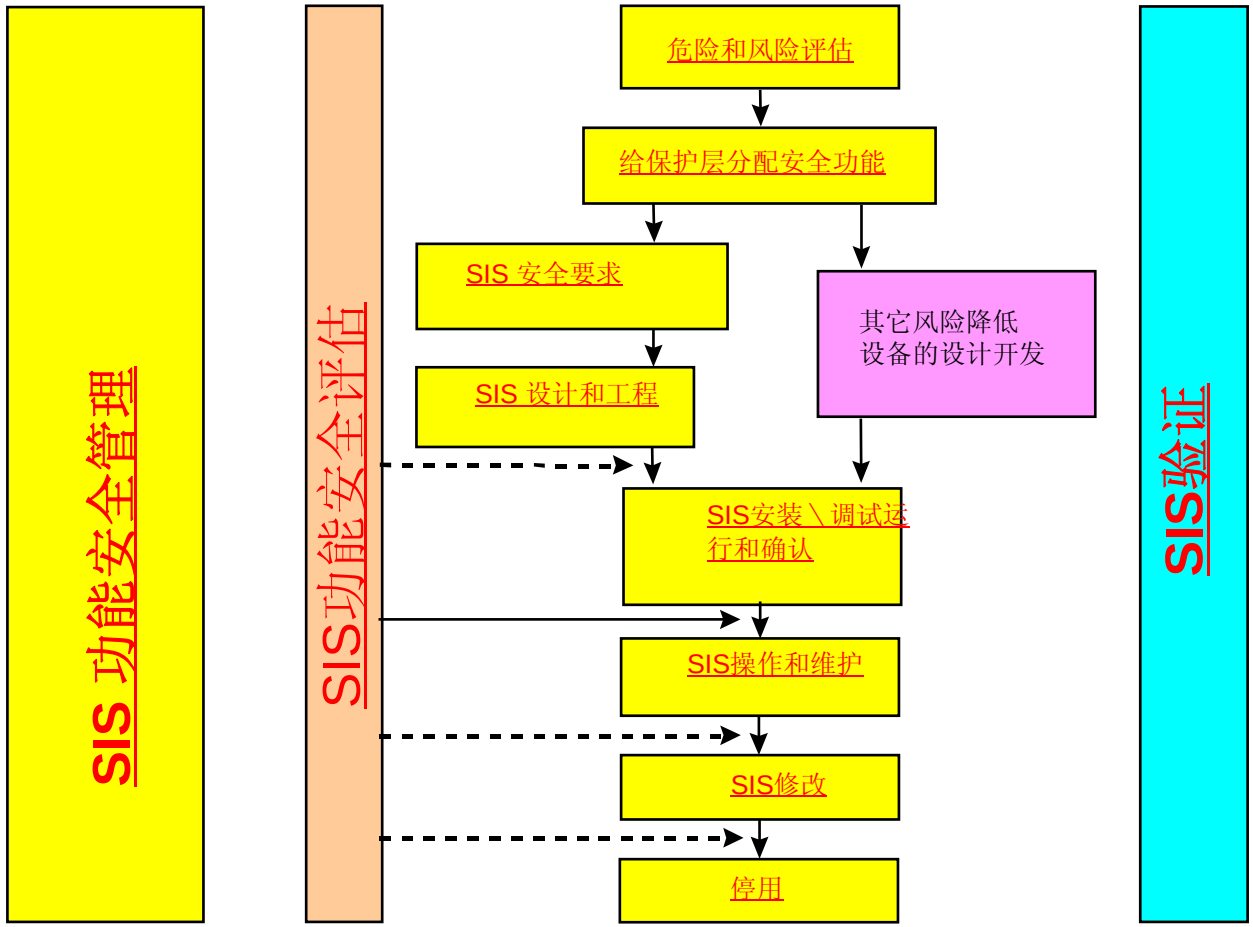
安全生命周期

安全生命周期是指从项目概念设计开始到所有的安全仪表功能停用为止时，所发生的实现安全仪表功能的必要活动。

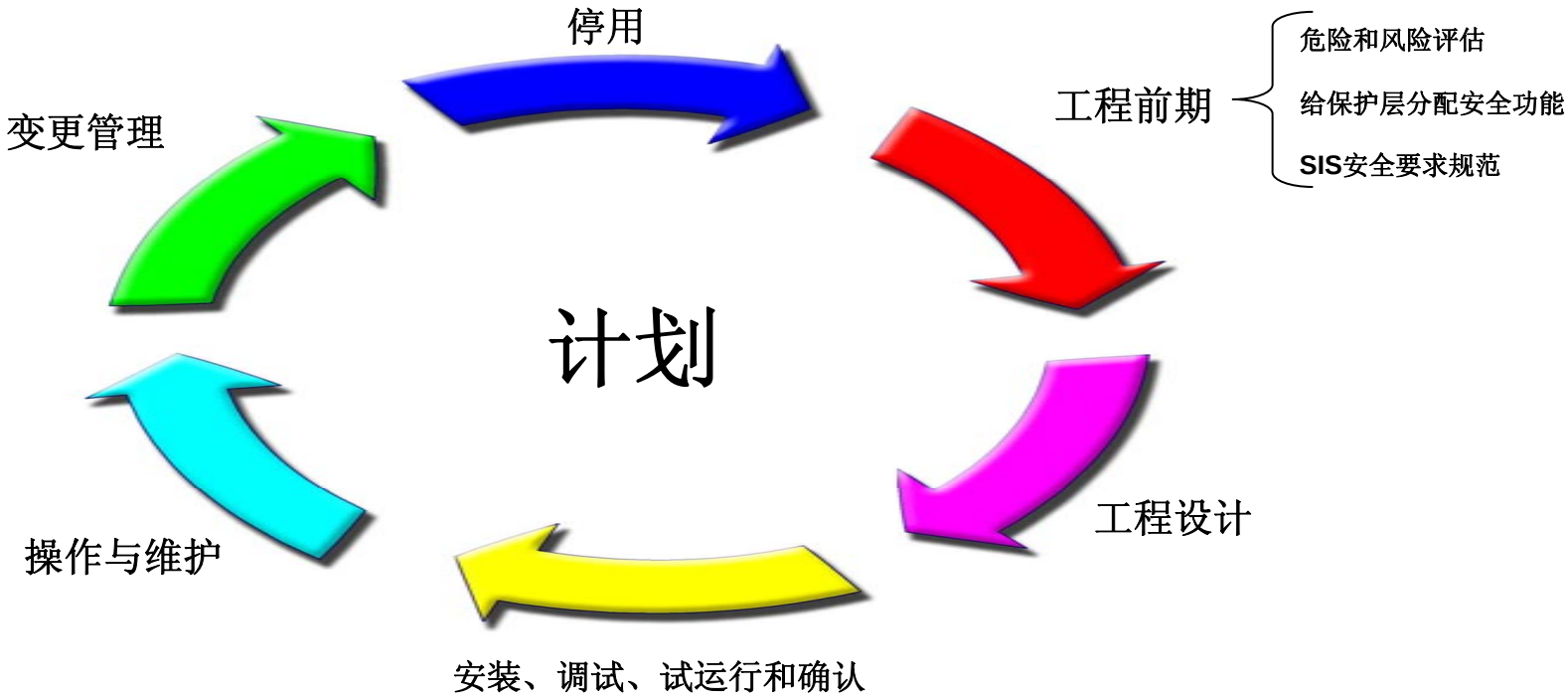
安全生命周期


研究与概念
1 概念
2 整体范围定义
过程危险分析
3 危险和风险分析
4 整体安全要求
设计
5 安全要求分配
整体计划编制
6 整体操作和维护计划编制
7 整体安全确认计划编制
8 整体安装和试运行计划编制
9 安全相关系统: E/E/PES
实现(见E/E/PES)安全生命周期
10 安全相关系统: 其它技术
实现
11 外部风险降低设施
实现
安装
12 整体安装和试运行
操作和维护
13 整体安全确认
14 整体操作、维护和修理
15 整体修改和改型
返回适当的整体安全生命周期阶段
16 停用或处理
修改或停用

安全生命周期


SIS 功能安全管理
SIS功能安全评估
危险和风险评估
给保护层分配安全功能
SIS 安全要求
其它风险降低
设备的设计开发
SIS 设计和工程
SIS安装＼调试运
行和确认
SIS操作和维护
SIS修改
停用
SIS验证

安全生命周期


停用
工程前期
危险和风险评估
给保护层分配安全功能
SIS安全要求规范
变更管理
计划
工程设计
操作与维护
安装、调试、试运行和确认

安全生命周期目的

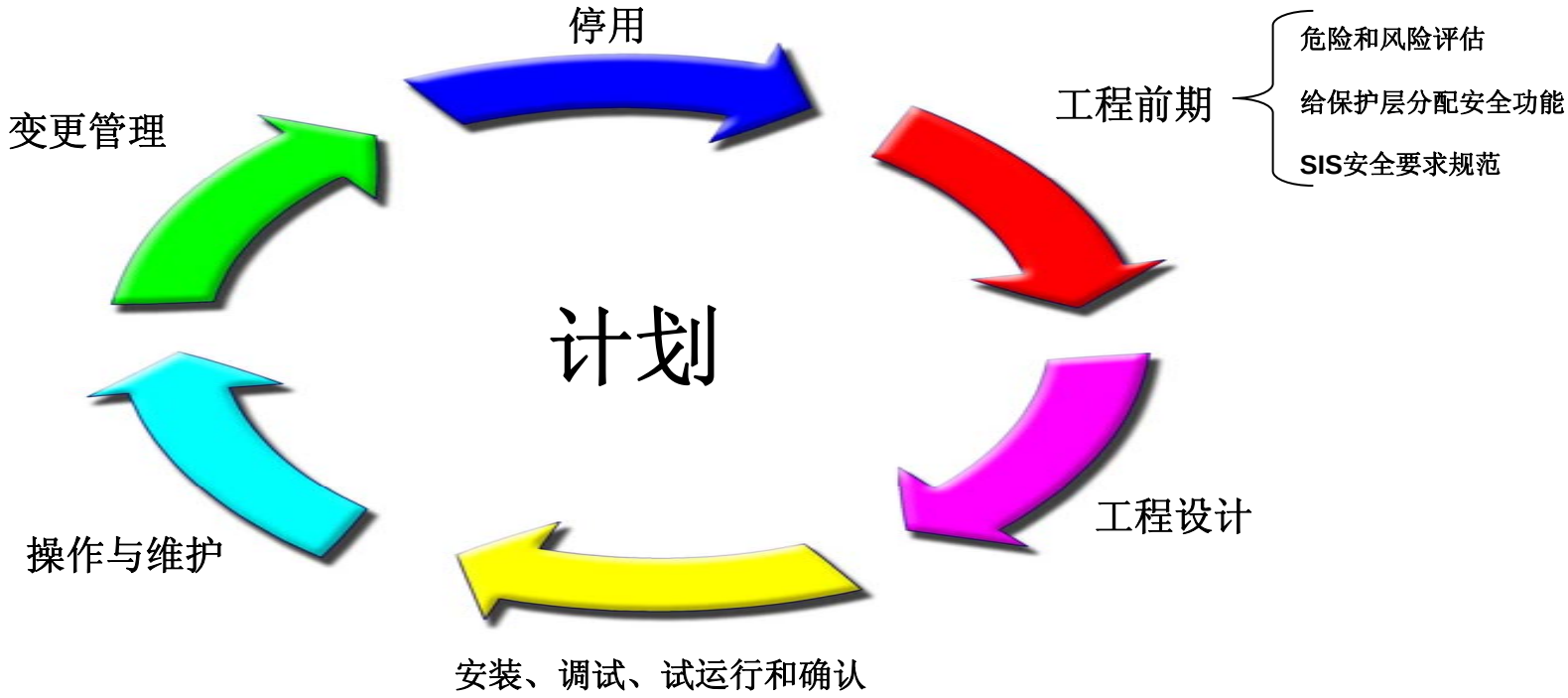
目的

- 定义和确定安全生命周期活动的各个阶段及要求；
- 组织安全生命周期内的技术活动；
- 确保有（或拟订有）适当的计划，以确保安全仪表系统能满足安全要求。

安全生命周期要求

要求

- 在编制安全计划过程中，应定义一个结合了本标准要求的安全生命周期。



要求

- 应根据它的输入、输出和验证活动来定义安全生命周期的每个阶段。(见下表)

安全生命周期阶段或活动		目的	要求所在章或条	输入	输出
图8方框号	标题				
1	危险和风险评估	确定过程及相关设备的危险和危险事件、导致危险事件后果、与危险事件相关的过程风险、风险降低和要达到必要的风险降低所需要的安全功能要求	8	过程设计、布局、人员配备安排、安全目标	危险、要求的安全功能和相关风险降低的描述

要求

- 应编制安全生命周期所有阶段的安全计划，定义准则、技术、措施和程序，以：
  - 保证过程的所有相关模式都能达到SIS安全要求；这包括功能和安全完整性两方面的要求；
  - 保证安全仪表系统正确安装和调试运行；
  - 保证安装后仪表安全功能的安全完整性；
  - 在操作（如检验测试、失效分析）过程中保持安全完整性；
  - 在安全仪表系统的维护活动期间管理过程危险。

1. 危险和风险评估

目　的

目的（1/2）

- 确定过程及其相关设备的危险和危险事件；
- 确定导致危险事件的事件序列；
- 确定与危险事件相关的过程风险；
- 确定风险降低的任何要求；
- 确定达到必要的风险降低所要求的安全功能；
- 确定每个安全功能是否是安全仪表功能（见第9章）。

目的（2/2）

注1：本章的对象是过程工程师、危险和风险专家、安全管理人员及仪表工程师。的目的是认识多学科方法确定安全仪表功能的典型要求。

注2：在合理可执行的情况下，应把过程设计成固有安全的。如果做不到，设计中就需要增加如机械保护系统和安全仪表系统这样的风险降低方法。这些系统可单独工作，也可相互组合。

注3：图9示出了过程工厂中典型的风险降低方法（没有层次分别）。

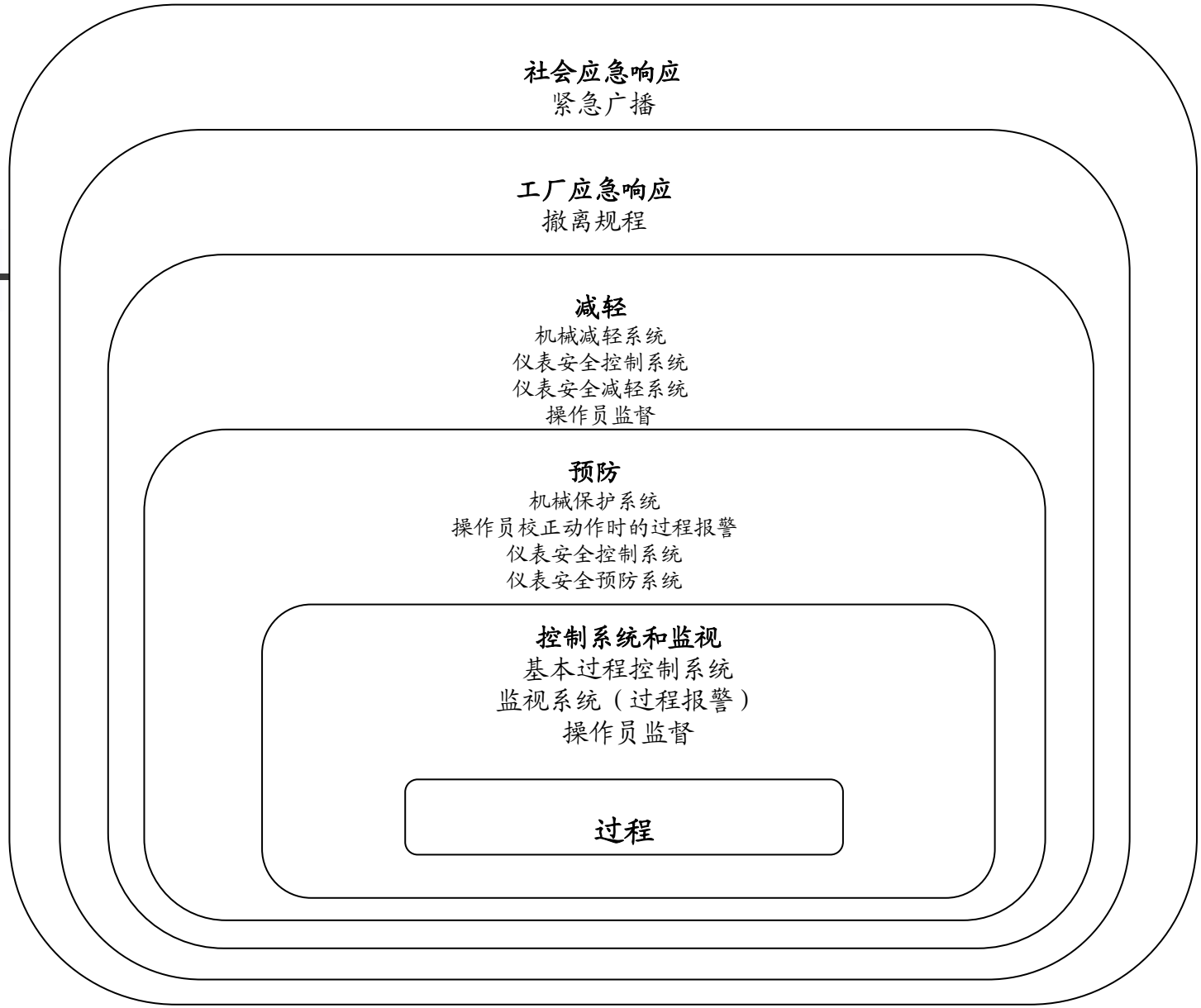


图9 过程工厂中常见的典型风险降低方法

要　求

要求

- 对过程及其相关设备（如BPCS）应进行一次危险和风险评估。其结果应是：
  — 已识别的每个危险事件及其起因（包括人为错误）的描述；
  — 事件的后果和可能性描述；
  — 工况考虑，如正常运行、起动、停机、维护、过程扰乱、紧急停机；
  — 为达到要求的安全性需增加的风险降低要求；
  — 关于为降低或消除危险和风险所采取的措施的信息的描述或引用；
  — 在风险分析中对可能的要求率和设备失效率等所作的假设,以及对操作约束或人为干预的可信度的详细描述；
  — 在考虑到安全层之间、安全层和BPCS（Basic process control system）之间由共同原因失效引起有效保护潜在降低的情况下（见注1），分配给各保护层的安全功能（见第9章）；
  — 用作安全仪表功能的安全功能的确定（见第9章）。

要求

注1：在确定安全完整性要求时，需考虑产生要求的系统和被设计用来响应这些要求的保护系统之间共同原因的影响。例如，控制系统失效提出了（保护）要求，保护系统中使用的设备同控制系统中使用的设备类似或相同。在这种情况下，当一个共同原因使保护系统中的类似设备变得无效时，控制系统中设备的一次失效产生的（保护）要求可能就得不到有效地响应。因为在最初确定危险和分析风险的过程中，保护系统的设计未必就已完成，在这样早的一个阶段中还不可能辨别出共同原因问题。在这种情况下，只要完成了安全仪表系统和其他保护层的设计，就有必要重新考虑安全完整性要求和安全仪表功能要求。在确定过程和保护层整体设计是否满足要求时，需要考虑共同原因失效。

注2：在GB/T 21109.3中示出了用于确立安全仪表系统所要求的SIL的例子。

要求

- 对保护层提出要求的BPCS的危险失效率(不遵循GB/T 21109)不应被假设小于10^{-5}/h。
- 应记录危险和风险评估，使以上各项之间的关系清楚和可追溯。

注1：上述要求并不强制风险和风险降低目标一定要赋数值。也可以使用绘图法（见GB/T 21109.3）。

注2：必要的风险降低的程度根据应用与国家法规要求的不同而有所不同。一个为多个国家所接受的原则是：采取额外的风险降低措施，直到花费的成本同取得的风险降低变得不成比例为止。

应用要求

应用要求

- 只能根据任务的结果来规定危险和风险评估的要求。这意味着组织可以使用它认为有效的任何技术，只要该项技术能得到安全功能及其相关性能水平的清楚描述。
- 危险和风险评估应确定和涉及在所有合理的可预见的情况下（包括故障工况和合理的可预见的误用）发生的危险和危险事件。

应用要求

- 就过程领域的一个典型工程项目而言，需要在基本过程设计的初期就执行预先的危险和风险评估。

  注：在此阶段假设通过固有安全原理以及好的工程实践的应用，已把危险消除掉了或者已把危险降低到了合理可行的程度（在GB/T 21109的范围内不包含这种降低危险的活动）。
- 对SIS而言，这种预先的危险和风险评估是很重要的，因为确立、设计和实现一个SIS是复杂的任务，需要占用相当长的时间。
- 及早了解这个工作的另一理由是在完成过程和仪表图之前需要系统结构方面的信息。

应用要求

- 进行一次最终的危险和风险评估。

注：一般只要完成了过程流程图和提供了所有的原始过程数据，启动预先危险和风险评估的信息就足够了。应该认识到当进行详细设计时，可能引入附加危险。因此，一旦完成了过程和仪表图，还有必要进行一次最终的危险和风险评估。

一般这个最终的分析使用一个正式的和全文档化的规程，如危险和可操作性研究（HAZOP）。应证实所设计的安全层足以保证工厂的安全。

在该最终分析期间，需考虑安全系统的失效是否会导致任何新的危险或者请求。如果在此阶段确定有任何新的危险，则有必要定义新的安全功能。另一较可能产生的结果是查明了可导致在初始阶段已识别危险的附加事件。于是需考虑是否需要对初始分析所确定的安全功能及其性能要求进行修订。

应用要求

- 在考虑更复杂的设计或是新的过程设计的情况下，有必要采用一种更结构化的方法（例如IEC 60300-3-9：1995）。

  注1：用来确定危险的方法取决于正在考虑的应用，对有些简单的过程来说，在对一种标准设计（如海上钻井平台）具有广泛操作经验的情况下，使用工业上编制的检查列表（例如ISO 10418和API RP 14C中的安全分析检查表）可能是足够的。

  注2：ISO 17776中给出了有关选择合适技术的其他信息。

应用要求

- 当考虑特定失效事件的后果时，应分析所有可能的结果，及对结果产生影响的失效事件的频率。在风险分析中应忽略或去除不可靠的结果。

  例：使管道或压力容器承受超过设计的压力不一定会产生灾难性的污染损失。在许多情况下，设备都经过超过设计的压力试验，惟一可能导致火灾的后果是可燃物质的泄漏。在评价后果时，需咨询负责工厂机械完整性的人员。它们不但需要考虑原始试验压力还要考虑包括腐蚀允许量在内的原始设计以及腐蚀管理程序是否到位。在后果是基于这些假设的情况下，清楚地讲明这个问题是很重要的，这样就能把相关的规程结合到安全管理系统中。

应用要求

- 当考虑后果时，另外一个问题是许多人可能会受到某种特殊危险的影响。

  注：许多情况下，操作和维护人员只是偶尔在危险区域出现，在预测后果时应考虑到这一点。在使用这种统计方法时应注意并非对所有的情况它都有效，比如只是在起动期间才发生危险以及人员经常出现在危险区的情况。还应考虑到由于在事件的发生过程中要对征兆进行调查，所以在危险事件附近出现的人数还可能增加。

应用要求

- 当对SIS的潜在要求源进行评估时，评估应包括以下情况：
  — 起动
  — 连续操作
  — 停机
  — 维修错误
  — 手动干预（如手动控制器）
  — 供应的中断（如空气、冷却水、氮、动力、蒸汽、加热保温层等）。

应用要求

- 当考虑要求频率时，在某些复杂情况下，可能有必要进行一次故障树分析。仅在因多个事件的同时失效而产生严重后果的情况下（例如，未为所有泄压的最坏情况设计减压收集器），这经常是必要的。
  - 应对什么时候应把操作员错误包含在可能引起的危险事件，以及这种事件发生的频率的事件清单中做出判断。例：如果操作员动作需经允许规程或者开锁设施（为防止偶然动作而配备的）才能执行，那么通常就可排除操作员错误。
  - 还需注意的情况是在什么场合，由于操作员动作降低要求频率是可信任的。这种信任会受到人为因素（比如需要多快地采取动作）和涉及任务的复杂程度的限制。

应用要求

- 在操作员对报警采取动作以及所声明的风险降低因子大于10的情况下，则需要根据GB/T 21109.1设计整个系统。承担安全功能的系统包括检测危险工况的传感器、报警显示、人工响应以及操作员用来消除任何危险的设备。
- 声明的风险降低因子不大于10的情况无需遵从GB/T 21109，这时应仔细考虑人为因素问题。由于报警而降低风险的任何声明必须得到三个方面的支持：对该报警必要响应的文档化描述，足以供操作员采取正确动作的时间，保证操作员采取预防动作的培训。

应用要求

- 倘若下列条件成立，降低对SIS的要求率就能把一个报警系统用作一种风险降低的方法：
  - 当失控将导致对SIF的一次要求时，用于报警系统的传感器不用作控制目的；
  - 用于报警系统的传感器不用作SIS的组成部分；
  - 已经考虑到关于风险降低的限制，这种风险降低可被声明用于BPCS和共同原因问题。

应用要求

- GB/T 21109.3给出了可用来确定安全仪表系统的SIL的技术示例，还包含在选择用于某个特定应用的方法时需考虑哪些问题的指南。
- 当确定是否需要风险降低时，需要具有一些过程安全和环境目标。它们专用于特定的现场或操作公司，并且可同未使用附加安全功能的风险水平进行比较。

应用要求

- 在确定需要风险降低之后，有必要考虑需要执行什么样的功能以使过程返回到某个安全状态。理论上，可以用通用术语描述这些功能而无需涉及某个特殊技术。

  例如在过压保护的情况中，可把功能描述成防止压力上升超过某个规定值。

  无论是一个安全阀或是一个安全仪表系统都能执行此功能。当如上描述功能时，则可在生命周期的下一阶段（给保护层分配仪表安全功能）来决定所使用的技术类型的选择。实际上，根据所选的系统类型，功能要求是不相同的；在某些情况下，此阶段和下一阶段可结合起来。

应用要求

- 总之，危险和风险分析应考虑：
  — 每个已确定的危险事件和导致该危险事件的事件序列；
  — 与每个危险事件相关联的事件序列的后果和可能性；可定量或定性表示它们；
  — 每个危险事件的必要的风险降低；
  — 为降低或消除危险和风险而采取的措施；
  — 在分析风险过程中所作的假定，包括估计的要求率和设备的失效率；应详细说明操作约束或人为干预取得的任何信任；
  — 在每个SIS生命周期阶段（如验证和确认活动）对与安全相关系统有关的关键信息的引用。

应用要求

- 构成危险和风险分析组成成分的信息和结果都应文档化。
- 当已经做出了决定并且可用的信息变得更精确时，可能有必要在整个SIS安全生命周期的各个阶段反复进行危险和风险评估。

应用要求

- 在过程工业中，在许多应用中需考虑要求的一个重要理由是BPCS失效。传感器、阀或控制系统都可能引起BPCS失效。
- 在过程工业中使用的控制系统有时具有冗余处理器，传感器和阀一般没有冗余。当给BPCS分配一个失效率时，需要知道失效率有一个重要限制。

GB/T 21109.1对与某个特殊危险有关的危险失效率作了限制，即除非系统的实现符合该标准的要求，能声明的危险失效率只能到每小时10^{-5}。这种限制的理由是如果声明的危险失效率较低，它应是在GB/T 21109.1表4的失效率范围之内。此限制保证了不满足GB/T 21109.1要求的系统不会有高的置信度水平。

2.给保护层分配安全功能

目　的

目的

- 给保护层分配安全功能；
- 确定要求的安全仪表功能；
- 确定每个安全仪表功能相关的安全完整性等级。

注：在分配过程中应考虑其他工业标准或规程。

分配过程要求

分配过程要求

- 分配过程应导出以下结果：

  — 给专用来预防、控制或减轻来自过程及其相关设备危险的保护层分配安全功能；

  — 给安全仪表功能分配风险降低目标。

  注：法规要求或其他工业法规可确定分配过程中的优先权。

- 通过考虑安全仪表功能提供的风险降低要求，可推导出该功能要求的安全完整性等级。

  注：相关指南见GB/T 21109.3。

分配过程要求

- 在要求模式下操作的每个安全仪表功能所需要的SIL，应根据表3或表4来规定。当使用表4时，既不能用检验测试间隔也不能用要求率来确定安全完整性等级。
- 在连续操作模式下操作的每个安全仪表功能所需要的SIL，应根据表4来规定。

表3 安全完整性水平：要求时的失效概率

要求操作模式		
安全完整性等级（SIL）	要求时的目标平均失效概率	目标风险降低
4	≥10-5～<10-4	>10000～≤100000
3	≥10-4～<10-3	>1000～≤10000
2	≥10-3～<10-2	>100～≤1000
1	≥10-2～<10-1	>10～≤100

分配过程要求 分配过程应用要求 SIL定义

表4 安全完整性等级：SIF的危险失效频率

连续操作模式	
安全完整性等级（SIL）	执行仪表安全功能的目标危险失效频率（每小时）
4	$\geqslant 10^{-9} \sim < 10^{-8}$
3	$\geqslant 10^{-8} \sim < 10^{-7}$
2	$\geqslant 10^{-7} \sim < 10^{-6}$
1	$\geqslant 10^{-6} \sim < 10^{-5}$

危险和风险评估的应用要求 分配过程要求 分配过程应用要求 SIL定义

分配过程要求

注1：另外的说明见3.2.43。

注2：安全完整性等级用数值定义以便为替代设计和解决方案的比较提供一个客观目标。然而应该认识到，在当前的知识状况条件下，许多失效的系统原因还只能进行定性评估。

注3：对于连续模式下的一个安全仪表功能所要求的每小时的危险失效频率，是通过把在连续模式下操作的安全仪表功能失效所产生的风险（用危险失效率表示），连同在考虑到其他保护层的贡献时导致同一风险的其他设备的失效率一并考虑来确定的。

注4：能用几个较低安全完整性等级的系统来满足一个较高等级功能的需要（如使用一个SIL 2和一个SIL 1的系统共同满足一个SIL 3功能的需要）。

分配过程应用要求

分配过程应用要求

- 本条的要求是商定将使用的安全层和分配仪表安全功能的性能目标。实际上，在许多情况下，只有在使用固有的安全设计或其他技术系统存在问题的场合，才将安全功能分配给安全仪表系统。
- 这类问题的例子包括对燃烧容量的限制或者针对放热反应的保护。使用基于仪表的系统而不是像安全阀这类更传统方案的任何决定，都需要有坚实的理由来支持，而这种理由要经受得住制定规章制度的权威机构的质询。

分配过程应用要求

- 如上所述，危险和风险评估与分配可能同时进行；在某些情况下，分配可以在危险和风险评估前进行。
- 决定给安全层分配安全功能通常应根据用户组织发现是切实可行的依据做出。还应考虑已确定的良好的行业惯例。然后在假定其他安全层是可信任的情况下，对安全仪表系统做出判定。

  例如，在已安装安全阀，并且它们是根据工业法规设计和安装的情况下，判定它们本身是否达到足够的风险降低。在安全阀的大小和性能还不完全满足应用，或者禁止将气体释放到大气中的情况下，安全仪表系统仅用于限制压力。

分配过程应用要求

- 在把一个安全功能分配给一个仪表安全功能时，需考虑应用是以要求模式还是以连续模式操作。
  - 过程领域中的大多数应用在要求不是很频繁的情况下都使用要求操作模式。在这类情况中，GB/T 21109.1的表3是常用的合适量值。

分配过程应用要求

— 有些应用要求很频繁（例如要求率每年大于1），这类应用更适合当作连续模式，因为危险失效概率主要是由SIS的失效率决定的。在这些情况下，宜使用GB/T 21109.1表4中的适当量值。失效导致即时危险，在连续模式中是很少见的。如果对于控制系统的所有失效模式而言，保护系统不能满足要求，燃烧器或汽轮机速度控制就可采用连续模式应用。

分配过程应用要求

- GB/T 21109.1的表3中SIL是通过PFDavg来定义的。而目标PFDavg是通过要求的风险降低来确定的。要求的风险降低能通过对没有SIS时的过程风险同允许风险进行比较来确定的。它能够通过GB/T 21109.3中的技术按照定量或定性的原则来确定。

分配过程应用要求

- GB/T 21109.1的表4用执行SIF的危险失效目标频率来定义SIL。可通过SIS的允许失效率并考虑特定应用中失效的后果来确定SIL。
- 当使用GB/T 21109.1的表4来确定要求的SIL时，目标会基于安全仪表系统的危险失效频率。在使用GB/T 21109.1的表4时，使用检验测试间隔或要求率把危险失效频率转换成要求时的危险失效概率是不正确的。尽管单位看起来是一样的，但这会导致GB/T 21109.1的表4的不恰当转换，并可能导致安全功能的SIL要求的不规范。

分配过程应用要求

- 要求时的平均失效概率目标或者每小时的危险失效频率目标适用于仪表安全功能，并不适用于单个部件或子系统。一个部件或子系统（如传感器、逻辑解算器和最终元件）除了它被用于某个特定SIF之外，不能给它指派一个SIL。但它具有独立的最大SIL能力的申明。
- 危险和风险评估和分配过程的输出，应该是安全系统所执行功能的一个清晰的描述，包括潜在的安全仪表系统及其所有仪表安全功能的安全完整性等级要求（连同操作模式——连续或要求）。它构成了SIS安全要求规范的基础。应清楚地描述确保能维持安全所需要执行的功能。

分配过程应用要求

- 在此实现阶段，不必规定传感器和阀门的架构的细节。决定采用什么样的架构比较复杂，特定系统是否要求2oo3传感器和1oo2阀取决于许多因素。

分配过程应用要求

- 需要完全了解GB/T 21109.1中表3和表4的含意。特别是，单个仪表安全功能可以声明的PFDavg限制到10^{-5}，这相当于10^{5}的风险降低（SIL 4）。可靠性分析指出由于硬件随机失效的PFDavg小于10^{-5}是可以达到的，但GB/T 21109.1认为系统失效和共同模式失效会限制实际可能达到的性能。强烈推荐在风险分析显示出需要高的风险降低的情况下，应注意到过程领域中要达到SIL 4的仪表安全功能是困难的。解决办法是使用几个较低完整性的独立SIS。

分配过程应用要求

- 根据GB/T 21109.1的9.2.4的注4：

  为了达到较高的风险降低水平（如大于103），可以使用多个SIS。当使用多个SIS来达到较高的风险降低时，重要的是每个SIS应能独立地执行安全功能，并且各SIS之间应有足够的独立性。

  例如，把一个SIL 2的压力检测回路同一个SIL 1的液位检测回路组合起来，以达到具有103风险降低要求的过压安全功能也许并不可取；因为液位传感器检测到一个高液位之前，压力容器就可能已经超过了它的压力限值。

分配过程应用要求

- 另外，在使用多个SIS时，还应考虑共同原因失效。此外，还要满足GB/T 21109.1中定义的所有其他要求，包括表5中定义的最低故障裕度要求。

举例

- 为了说明怎样组合所使用的多个SIS来达到较高的风险降低水平，考虑下例：
- 一个由2oo3变送器组、一个2oo3逻辑解算器和一个1oo2最终元件组构成的一个具有PFDavg为3.05×10^{-4}的SIS。该SIS达到的风险降低大约为3.3×10^{3}。
- 假定使用两个这样的系统来产生一个10×10^{6}（$3.3\times10^{3}\times3.3\times10^{3}$）的风险降低是不正确的。共同原因因素（如使用相同的技术、根据同样的功能规范设计两个系统）、人为因素（如编程、安装、维护）和外部因素（如腐蚀、堵塞、空气管道的冻结、闪电）都将限制系统提高。还有必要考虑两个系统间任何共享的部件。

举例

- 一种较可行的解决办法是使用尽可能多样性的部件（为了最小化潜在的共同原因问题）的一个非冗余第二系统。
- 例如，考虑包含仅一个开关、继电器逻辑和仅一个最终元件的系统，该系统具有一个7.7×10^{-3}的PFDavg。此系统达到的风险降低大约为1.3×10^{2}。
- 把基于软件的SIS和单纯继电器型SIS组合起来，可得到的总体理论风险降低为4.3×10^{5}($3.3\times10^{3}\times1.3\times10^{2}$)。如上所述，尽管在理论上性能的组合似乎是可能的（因为无论哪个SIS都能使过程单元停机），但同样不得不考虑共同原因因素，并且由于这些因素使之可达到的风险降低要稍微低一点。

安全完整性等级4的附加要求

安全完整性等级4的附加要求

- 分配给安全仪表系统安全仪表功能的安全完整性等级不能高于4。在过程工业中要求某一个安全仪表功能的安全完整性等级为4的应用是罕见的。因为在合理的情况下，要在整个安全生命周期中达到和保持这样高的性能等级是困难的，所以应避免这种应用。在规定这种系统的情况下，要求在整个安全生命周期的所有方面都具备高等级的能力。

  如果分析结果是指派给一个安全仪表功能的安全完整性等级为4，则应考虑改变过程设计使过程变得更固有安全或者增加附加保护层。这些增强措施也许能降低安全仪表功能的安全完整性等级要求。

安全完整性等级4的附加要求

- 只有在满足下面的准则a)或者b) + c)时才允许安全仪表功能的安全完整性等级为4：

  a) 已由适当的分析方法和测试明显表明满足目标安全完整性失效量；

  b) 已具有对被用作安全仪表功能组成部分的部件的广泛的操作经验；

  注：这种经验应是在相似的环境中取得的，并且至少那些部件已用于相当复杂等级的系统中。

  c) 安全仪表功能组成部分所包含部件的硬件失效数据已经足够多，从而可为要声明的硬件安全完整性目标失效量提供足够的置信度。

  注：数据应是在相应的环境、应用和复杂程度下取得的。

对作为一个保护层的基本过程控制系统的要求

对作为一个保护层的基本过程控制系统的要求

- 基本过程控制系统也可作为一个保护层。如图9所示。
- 一个用作保护层的的BPCS风险降低因子（它并不符合本标准或GB/T 20438－2006）应小于10。

  注：当考虑一个BPCS降低风险的信任度有多大时，应考虑到这样一个事实，即BPCS的一部分也可以是一个事件的起源。
- 如果要求BPCS的风险降低因子大于10，则应按本标准的要求进行设计。

应用要求

对作为一个保护层的基本过程控制系统的要求

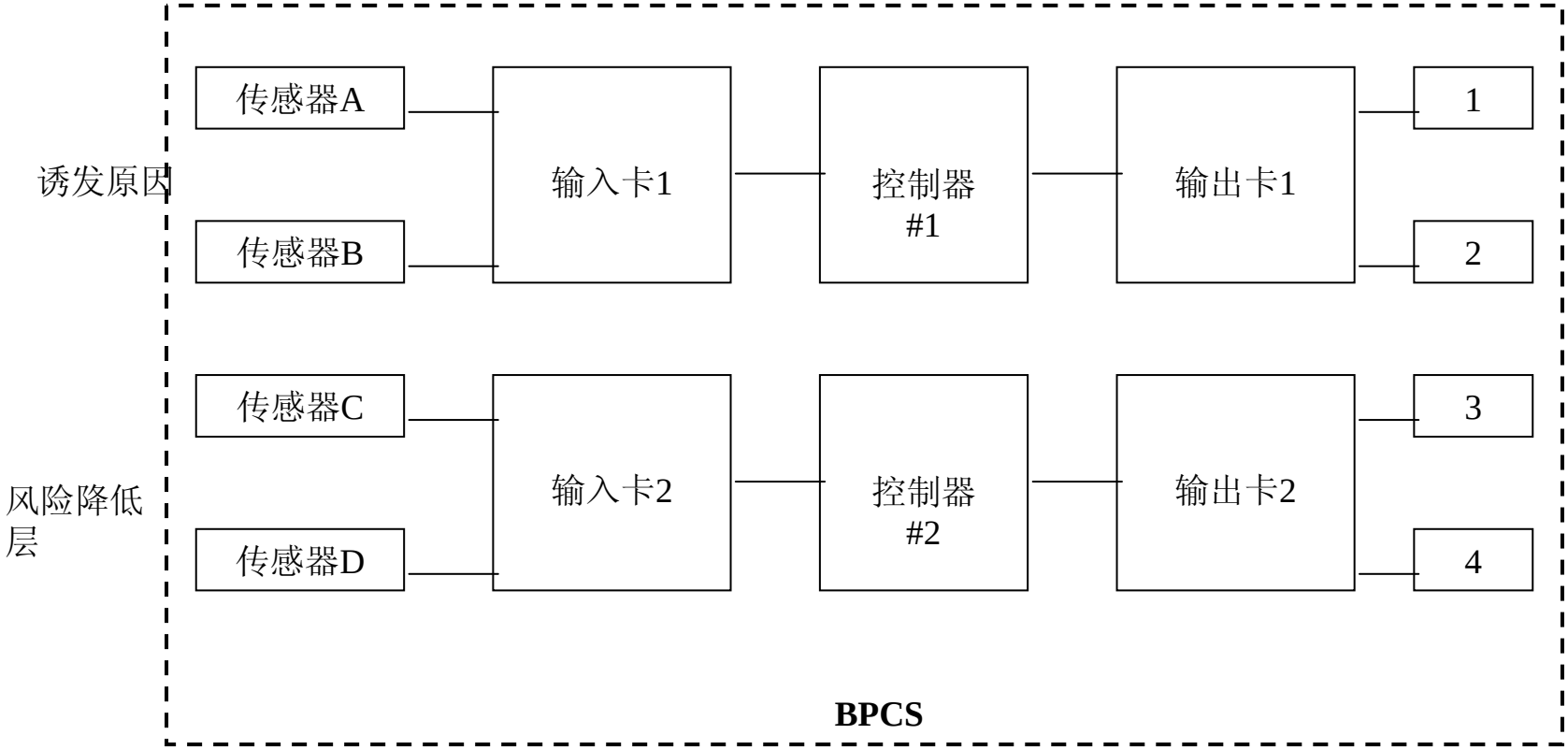
- 基本过程控制系统也可视为是一个遵从某些条件的保护层。如果在BPCS中，以降低过程风险为目的的功能得到实现，针对预定要降低的确定的风险，也可给BPCS分配一个风险降低。

对作为一个保护层的基本过程控制系统的要求

- 不需遵从GB/T 21109.1，仪表型系统就可声明低于10的风险降低。这使得BPCS可用于某些风险降低，而无需按GB/T 21109.1的要求实现该系统。
- 应通过考虑BPCS的完整性（由可靠性分析或者性能数据确定）和用于配置、修改、操作和维护的规程表证明所作的任何声明都是合理的。
- 当在BPCS中给功能分配风险降低时，保证提供访问保密和更改管理是重要的。能声明的一个BPCS功能的风险降低也可由BPCS功能和诱发原因之间的独立程度来确定。

图2说明了BPCS功能和诱发原因之间的独立性。

图2 BPCS功能和诱发原因的独立性说明



举例

- 考虑一个流量控制回路是诱发原因的情况。此诱发原因包括一个流量变送器、一个控制器和一个控制阀。为了给BPCS中的一个压力控制回路分配风险降低，压力变送器应连接到一个独立的控制器，调节一个独立的最终元件（例如到燃烧系统的排气阀）。

防止共同原因失效、共同模式失效和相关失效的要求

防止共同原因失效、共同模式失效和相关失效的要求

- 应对保护层的设计进行评估，以确保保护层之间、保护层同BPCS之间共同原因失效、共同模式失效和相关失效的可能性同保护层的整体安全完整性要求相比足够低。这种评估可以是定性的也可以是定量的。

  注：相关失效的定义见3.2.12。

- 评估应考虑下列因素：

  — 保护层之间的独立性；

  — 保护层之间的多样性；

  — 不同保护层之间的物理分离；

  — 保护层之间、保护层同BPCS之间的共同原因失效（例如，在SIS中安全阀堵塞可能会产生与传感器堵塞相同的问题）。

应用要求

防止共同原因失效、共同模式失效和相关失效的要求

- 在早期阶段应考虑的一个重要问题是在每层中的各冗余部分之间（例如同一压力容器上的2个安全阀之间）、各安全层之间或者各安全层和BPCS之间是否存在任何共同原因失效。

  一个基本过程控制系统测量的失效可能引起对安全仪表系统提出一次要求，以及在安全仪表系统中使用一个具有同样特点的设备的情况就是它的一个例子。

防止共同原因失效、共同模式失效和相关失效的要求

- 在这种情况下，有必要确定是否存在使两台设备同时失效的可信的失效模式。在判明是一个共同原因失效的情况下，则可采取以下动作：

  a）可通过改变安全仪表系统或者基本过程控制系统的设计来减少共同原因。降低共同原因失效的可能性的两种有效方法是设计的多样化和物理分离。这是通常优先选用的方法。

  b）当确定总的风险降低是否足够时应考虑共同原因事件的可能性。这要求对由要求原因以及保护系统失效构成的故障树进行一次分析。在这种故障树上可以表示出共同原因失效并通过适当的建模方法量化对整个风险的影响。

防止共同原因失效、共同模式失效和相关失效的要求

- BPCS和SIS共享的任何传感器或者执行机构都很可能引入共同原因失效，而解决装置的这种共享的方法应如本条中所述。

防止共同原因失效、共同模式失效和相关失效的要求

- 当对共同原因失效、共同模式失效和相关失效的可能性执行一次评估时，应使用下面所列的考虑。评估的范围、形式和深度取决于预期功能的安全完整性等级。对安全完整性水平为3或者更高的情况而言，共同原因、共同模式和相关失效的影响也许是决定性的。应考虑：

  — 各保护层之间的独立性：应进行一次失效模式影响分析，以便确立单一事件是否能引起不止一个保护层失效或者BPCS和一个保护层同时失效。分析的深度和严密性取决于风险。

防止共同原因失效、共同模式失效和相关失效的要求

— 各保护层之间的多样性：目标应是各保护层和BPCS之间的多样性，但并不一定总是能作到。例如过压保护，在这种情况中，BPCS压力控制回路的一次失效将导致一次要求。BPCS和SIS都需要测量压力，并对提供的合适设备有一个限制。使用从不同生产厂购买的设备也许能达到某些多样性，但如果使用同类型的连接方式把SIS和BPCS传感器连接到过程，则多样性也许很有限。

— 不同保护层之间物理分离：物理分离可以降低由物理原因引起的共同原因失效的影响。根据比如精确性和响应时间这样的功能需要，BPCS和SIS的测量连接位置应有最大物理间隔。

3. SIS安全要求

目　的

目的

- 为了达到要求的安全功能，根据要求的仪表安全功能及其相关的安全完整性规定每个SIS的要求。

一 般 要 求

一般要求

- 安全要求应从仪表安全功能分配和在安全计划编制过程中确定的那些要求中推导出来。

  注：SIS要求应以下述方法表达和构建：

  — 清楚、精确、可验证、可维护和可行；

  — 易于被在生命周期任何阶段有可能使用这些信息的人理解。

一般应用要求

- SIS安全要求规范可以是单独一个文档，也可以是包含规程、图纸或公司标准惯例的几个文档的一个集合。可由危险和风险评估组和/或工程项目组本身拟订这些要求。

--详见SIS设计和工程

4. SIS设计和工程

SIS设计和工程

（一）目的
（二）一般要求
（三）检测故障时的系统行为要求
（四）硬件故障裕度要求
（五）选择部件和子系统的要求
（六）现场装置
（七）接口
（八）维护或测试设计要求
（九）SIF的失效概率

5. SIS安装、调试运行和确认

目的

集成和测试SIS；根据要求的仪表安全功能和要求的安全完整性，确认SIS在各方面都满足安全要求。

SIS安装和调试运行

目　的

目的

- 根据规范和图纸安装安全仪表系统；
- 调试安全仪表系统以便为最终的系统确认做好准备。

要　求

要求

- 安装和调试运行计划编制应定义安装和调试运行所需的所有活动。计划编制应提供：

  — 安装和调试运行活动；

  — 安装和调试运行所使用的规程、措施和技术；

  — 何时进行这些活动；

  — 负责这些活动的人员、部门和组织。

  在合适的情况下，可把安装和调试运行计划编制整合到整个工程项目计划编制中。
- 应按设计和安装计划正确安装安全仪表系统的所有部件（见14.2.1）。

要求

- 应根据计划编制调试运行安全仪表系统，以用于最终的系统确认。调试运行活动应包括（但不限于）证实：

  — 已正确接地；

  — 已正确接通电源并可供电；

  — 已停止搬运并已拆除包装材料；

  — 无物理损伤；

  — 已正确校准好所有的仪表；

  — 所有现场装置都可供使用；

  — 逻辑解算器和输入/输出可供使用；

  — 到其他系统和外设的接口可供使用。

要求

- 应产生SIS调试运行的相应记录，说明测试结果以及在设计阶段所确定的目的和准则是否得以满足，如果调试运行中出现失败，则应记录失败的原因。
- 对实际上并不依据设计信息进行安装的情况，应由有资格的人员对其差异进行评价，并确定可能对安全产生的影响。如已确定这种差异对安全没有影响，则应把设计信息更新为“竣工（as-built）”状况，如果这种差异对安全有负面影响，则应修改安装来满足设计要求。

要求

应用要求

- 应按设计和安装计划安装SIS。项目组应正确审查SIS与设计的任何偏离，以确保仍能满足所有的设计要求。在正确安装SIS之后，应对SIS进行充分地调试运行，并启动确认活动。
- 尽管GB/T 21109.1已把调试运行作为一个单独的阶段进行了论述，但要认识到应用、项目组经验以及项目需求可能要求调试分几个阶段来完成。

SIS安全确认

目　的

目的

通过审查和测试来确认安装和调试好的安全仪表系统及相关的安全仪表功能达到了安全要求规范中所声明的那些要求。

注：有时也把这称为一种现场验收测试（SAT）。

-详见SIS设计和工程

6. SIS操作和维护

目　的

目的

- 保证在操作和维护过程中能保持所要求的每个安全仪表功能的SIL；
- 操作和维护SIS使之能保持设计的功能安全。

要　求

要求

- 应编制安全仪表系统的操作和维护计划。此计划应提供：
  — 例行的和异常的操作活动；
  — 检验测试活动、预防性维护和故障维修活动；
  — 操作和维护使用的规程、措施和技术；
  — 遵从操作和维护规程的验证；
  — 何时进行这些活动；
  — 负责这些活动的人员、部门和组织。

要求

- 应根据相关的安全计划编制制定操作和维护规程，此规程应提供：
  — 为保持“同设计一样的”SIS的功能安全所需执行的例行动作，例如遵从由SIL确定所定义的检验测试间隔；
  — 在维护或操作期间，为防止一个危险事件的不安全状态和/或减小事件后果需要采取的动作和约束（例如，为了测试或维护一个系统，何时需对它进行旁路，以及需实现何种附加缓解步骤）；
  — 需保留的系统失效以及对SIS的要求率的信息；
  — 显示对SIS进行审核和测试的结果需保持的信息；

要求

— 当SIS发生故障或失效时应遵从的维护规程，它包括：

- 故障诊断和修理规程；
- 重新确认规程；
- 维护报告要求；
- 跟踪维护性能的规程。

注：应考虑：

- 报告失效的规程；
- 分析系统失效的规程。

— 保证在正常维护活动期间使用的测试设备已被正确校准和维护。

要求

- 应根据相关规程进行操作和维护。
- 应就操作员所在领域内的SIS功能和操作对它们进行培训。这样的培训应保证它们能了解：
  - SIS怎样工作（脱扣点及SIS因此所采取的动作）；
  - SIS能预防的危险；
  - 所有旁路开关的操作以及在什么样的情况下才应使用这些旁路
  - 任何手动停机开关的操作和手动起动活动以及何时才应启动这些手动开关；

    注：也许还应包括“系统复位”和“系统重新起动”。
  - 对任何诊断报警的启动的预期行为（例如当启动任何SIS报警，从而指示SIS存在某种问题时，应采取什么样的动作）。

要求

- 应按要求培训维护人员，使得SIS（硬件和软件）的功能特性能维持它的目标完整性。
- 应分析预计的和实际的SIS行为之间的差异，必要时应作修改以保持要求的安全，这包括监视：
  — 紧随对系统提出要求后所采取的动作；
  — 在例行测试或者实际要求过程中作为SIS组成部分的设备所产生的失效；
  — 提出要求的原因；
  — 伪脱扣的原因。

注：分析预期行为和实际行为之间的所有差异是十分重要的。它不应同在正常运行中所遇到的监视要求相混淆。

要求

- 操作和维护规程可能需要修订，有必要时应在修订后进行：
  — 功能安全审核；
  — SIS测试。

要求

- 应编写每个SIF的书面检验测试规程，以便揭露诊断未检测到的危险失效。这些书面的测试规程应描述需要执行的每个步骤并应包括：

  — 每个传感器和最终元件的正确操作；

  — 正确的逻辑动作；

  — 正确的报警和指示。

注：下面的方法可用来确定需被测试的未检测到的失效：

- 故障树检查；
- 失效模式和影响分析；
- 以可靠性为核心的维护。

检验测试和检查

检验测试

检验测试

- 应使用一个书面的规程（见16.2.8）进行定期的检验测试以便揭露未检测到的故障，这种故障会阻碍SIS按安全要求规范操作。
- 应测试包括传感器、逻辑解算器和最终元件（如停机阀和电机）在内的整个SIS。
- 检验测试频率应同使用PFDavg计算所决定的一样。

注：SIS的不同部分可能要求不同的测试间隔，例如，逻辑解算器的测试间隔可能与传感器或最终元件的不同。

检验测试

- 应以一种安全和及时的方式修复检验测试过程中发现的任何缺陷。
- 应以某些定期的间隔（由用户确定），根据各种因素，包括：历史测试数据、工厂经验、硬件降级和软件可靠性等，重新评价测试频率。
- 应用逻辑的任何改变都需要进行全面检验测试。只有在进行过适当的复审，以及对改变的部分进行测试以保证能正确地实现改变时才允许有例外。

检验测试的应用要求

检验测试的应用要求

- 为了达到安全要求规范中规定的要求时的平均失效概率，应选择检验测试间隔。
- 检验测试频率应符合应用厂商的建议和良好工程惯例；如果根据以往操作经验认为有必要，也可以使用更高的测试频率。

检验测试的应用要求

- 有许多策略可用于选择SIF的检验测试间隔。

  例如，有些用户选择尽可能长的检验测试间隔，以使维护成本最低和使测试的潜在影响最小。在这种情况下，SIS设计可能在装备上包括更多的冗余、增加的诊断覆盖率和鲁棒部件。在设计完成之后，则可对设计进行一次计算，从而确定能达到SIF定义的SIL性能的最大测试间隔。这种设计理念的负面影响会导致工厂中的每个系统都有不同的测试间隔，并可能要求更严格的适应性跟踪。这种设计理念也可能鼓励设计性能趋向性能曲线的下端（例如对SIL 1的系统，PFDavg=10^{-1}；对SIL 2的系统，PFDavg=10^{-2}）。

检验测试的应用要求

其他用户可能希望根据已定义的检验测试间隔进行标准化，并以同样的测试间隔对厂商的所有系统进行测试。例如，它们可能希望每年测试每个SIF，从而它们就可以相应地设计每个SIS。在开始设计之前，预选一个检验测试间隔，用户就可预选能满足大多数应用要求的SIL的结构、部件和诊断覆盖率。通过把这种设计定义在公司标准中，可以降低大多数应用的设计工程成本。在这种情况下，应对SIS进行一次计算，以确保使用预选的检验测试间隔可以满足所要求的SIL性能。

检验测试的应用要求

- 在选择一个检验测试间隔时，应对要求模式系统的要求率、每个被测部件的失效率、整个系统性能要求进行考虑。

  注：在考验终端脱扣元件不可行的情况下，编写的规程应包含：

  a）在单元停机期间测试最终元件；

  b）在在线测试期间，尽可能通过考验输出（例如输出脱扣继电器、关停电磁阀、阀门部分行程）来测试SIS。

  c）在计算SIF的PFDavg时，应考虑最终元件测试周期的任何限制。

检　查

检查

- 应对每个SIS进行定期目视检查，以保证不存在未经授权的修改和可观察到的缺损（如缺螺栓或仪表罩、固定架生锈、线断开、管道破裂、加热保温层破损、绝缘缺失）。

检查的应用要求

- 如GB/T 21109.1中所述，检查SIS不同于检验测试。尽管检验测试可确保SIS运转正常，但都需要通过目测来确认安装的机械完整性。
- 通常是在检验测试的同时进行检查，但在需要时也可更频繁地进行检查。

检验测试和检查文档

检验测试和检查文档

- 用户应保存可证实检验测试和检查已按要求完成的记录，这些记录至少应包括以下信息：

  a)执行的测试和检查的说明；

  b)测试和检查的日期；

  c)执行测试和检查的人员姓名：

  d)被测系统的序列号或者别的惟一标识符（如回路号、工位号、设备号和SIF号）；

  e)测试和检查的结果（如“发现as-found”和“听任as-left”状况）。

检验测试和检查文档应用要求

- 对已发现问题的记录进行的检验测试和检查得出的结果进行归档是重要的。关于这些结果要保存多久没有特别要求，不过为了能复查以往结果，以便查看部件是否存在失效历史，通常应保存足够长的时间。

例如，当一个传感器使一次检验测试失败时，良好惯例是审查以往检验测试的结果，以便查看在前几次测试中该传感器是否也曾使类似的一次检验测试失败过。如果历史表明重复的失效，则应考虑使用不同类型的传感器重新设计SIS。

7. SIS修改

目　的

目的

- 在对任何安全仪表系统进行修改之前应正确编制修改计划并对修改进行复审和批准；
- 保证不管SIS作何改变都能保持所要求的SIS安全完整性。

注：应对BPCS、其他设备、过程和操作条件的修改进行复审，以确定它们的这种修改是否会对SIS的要求特性和频率造成影响。应进一步考虑有不利影响的那些修改，以确定风险降低水平是否依然足够。

要 求

要求

- 在对安全仪表系统进行修改之前，授权和控制更改的规程应到位。
- 规程应包括确定和请求要作的工作的简明方法，以及可能会受到影响的危险。
- 应进行一次分析，以确定所建议的修改结果对功能安全的影响。当分析显示所建议的修改将影响安全时，则应返回安全生命周期的第一个受修改影响的阶段。
- 未经正式授权不得开始修改活动。

要求

- 对SIS的所有更改都应保留相应的信息。这些信息包括：
  — 修改或更改的描述；
  — 更改的理由；
  — 可能会受影响的已确定的危险；
  — 修改活动对SIS的影响的分析；
  — 更改要求的所有批准；
  — 验证所有更改已正确实现，以及SIS按要求执行所使用的测试；
  — 相应的配置历史；
  — 验证所有更改不会对未修改的SIS组成部分产生不利影响所使用的测试。

要求

- 应由经过适当培训的合格人员来执行修改。包括所有受影响的和适当的人员被通知变更，并应就更改对它们进行培训。

8. SIS停用

目　的

目的

- 保证任何安全仪表系统在停用之前要对它进行一次正确的复审，并应得到必要的授权；
- 保证在停用活动过程中保持要求的安全仪表功能继续运行

要　求

要求

- 在执行一个安全仪表系统的任何停用之前，授权和控制更改的规程应到位。
- 规程应包括确定和请求要作的工作的简明方法，以及可能会受到影响的危险。
- 应分析由于所建议的停用活动结果对功能安全的影响。评估应包括危险和风险评估的更新，该更新应足以确定其后应重新执行的安全生命周期各阶段的深度和广度。评估还应考虑：

  — 在执行停用活动过程中的功能安全；

  — 停用某个安全仪表系统对相邻的操作单元和设施服务的影响。

要求

- 在编制安全计划来重新启用GB/T 21109.1的相关要求（包括重新验证和重新确认）的过程中，应使用影响分析的结果。
- 未经正式授权不得开始停用活动。

9. SIS验证

目　的

目的

- 通过复审、分析和/或测试，来证明要求的输出能满足在验证计划编制确定的安全生活周期的适当阶段（图8）定义的要求。

要　求

要求

- 验证计划编制应定义安全生命周期的适当阶段（图8）要求的所有活动。验证计划应提供以下各项以符合本标准：
  — 验证活动；
  — 验证所使用的程序、措施或技术，包括生成执行和解决方案建议；
  — 何时进行这些活动；
  — 负责这些活动的人员、部门和组织，包括它们的独立水平
  — 确定要验证的项目；
  — 确定验证依据的信息；
  — 如何处理不一致性；
  — 工具和支持分析。

要求

- 应根据验证计划进行验证。
- 验证过程的结果应可用。

注1：验证过程中所使用的技术、措施及独立水平的选择依赖于一系列因素，包括复杂程度、设计的新颖性、技术的新颖性和要求的安全完整性等级等。

注2：验证活动的例子包括设计复审、工具和技术（包括软件验证工具和CAD工具）的使用。

应用要求

应用要求

- GB/T 21109.1已考虑各个组织将有它们自己的验证规程，并且并不总是要求以同样的方式执行这些规程。换句话说，本条的目的是在事先就计划好所有的验证活动，连同任何会被使用的规程、措施和技术。
- 提供验证结果是重要的，这样可以证明在安全生命周期的各个阶段都已进行了有效的验证。

10. SIS功能安全评估

目　的

目的

- 对SIS所达到的功能安全进行调查并作出判断

要　求

要求

- 通过对安全仪表系统实现的功能安全和安全完整性做出判断，来定义和执行功能安全评估的规程。规程应要求指定包括特定安装所需的技术人员、应用和操作专家在内的评估小组。
- 评估组的成员至少应包括一位非工程项目设计组成员的高级资质人员。

注1：当评估组很大时，应考虑在组内包含多个与项目组无关的高级资质人员。

注2：在编制功能安全评估计划时，应考虑：

— 功能安全评估的范围；

要求

— 参加功能安全评估的人员；
— 功能安全评估组的技能、职责和权限；
— 作为功能安全评估活动的结果所产生的信息；
— 评估所涉及的任何其他安全团体的身份；
— 为完成功能安全评估活动所要求的资源；
— 评估组的独立水平；
— 修改后重新确认功能安全评估的方法。

要求

- 在安全计划编制过程中，应确定执行功能安全评估活动的安全生命周期阶段。

注1：当确定新的危险时，进行修改后和在操作间歇时，可能需要进行附加的功能安全评估活动。

要求

注2：在以下阶段，应考虑执行功能安全评估活动（见图8）：

— 阶段1：在已执行危险和风险评估、已确定要求的保护层和已制定安全要求规范之后；

— 阶段2：在设计好安全仪表系统之后；

— 阶段3：在完成安全仪表系统安装、预调试和最终确认，以及制定好操作和维护规程之后；

— 阶段4：在取得操作和维护经验之后；

— 阶段5：在对安全仪表系统进行修改之后和停用之前。

要求

注3：功能安全评估活动的次数、规模和范围依赖于特定的情况。其决策因素大约包括：

— 项目规模；
— 复杂程度；
— 安全完整性等级；
— 项目持续时间；
— 失效事件的后果；
— 设计特征的标准化程度；
— 安全规章制度的要求；
— 相似设计的以往经验。

要求

- 至少应执行一次功能安全评估。执行功能安全评估以确保能正确控制过程及其相关设备引起的危险。最低限度应在已被发现的危险成为现行之前（即阶段3）执行一次评估。在已被发现的危险成为现行之前评估组应证实：

  — 已执行危险和风险评估（见8.1）；

  — 已实现和解决由危险和风险评估提出的适用于安全仪表系统的建议；

  — 已到位并已正确执行项目设计更改规程；

  — 已解决由先前的功能安全评估提出的建议；

要求

— 根据安全要求规范设计、构造和安装安全仪表系统，已确认和解决任何差异；
— 与安全仪表系统有关的安全、操作、维护和紧急规程都已到位；
— 安全仪表系统确认计划编制是合适的并已完成确认活动
— 人员培训已完成，有关安全仪表系统的相应信息已提供给维护和操作人员；
— 实现进一步功能安全评估的计划或策略已经就位。

要求

- 当开发和生产工具被用于任何安全生命周期活动时，这些工具本身应进行功能安全评估。

  注1：对这些工具的评估程度，取决于他们对所应达到的安全的影响。

  注2：开发和生产工具包括例如：仿真和建模工具、测量设备、维护活动中使用的设备和配置管理工具。

  注3：工具的功能安全评估包括（但不限于）：校准标准、操作历史和缺陷列表的可追溯性。

要求

- 应提供功能安全评估的结果以及通过该评估提出的建议。
- 在必要时，所有相关信息都应能提供给功能安全评估组。

应用要求

应用要求

- 良好的功能安全评估（FSA）惯例应考虑以下属性：
  - 对每个功能安全评估（FSA）都应拟制一个计划，这个计划应根据评估范围、评估人员、评估人员的能力以及评估将产生的信息来编排；
  - FSA应考虑到公司外部或者内部的标准、指南、规程或编程习惯（codes of practice）范围内所包含的标准和作法。FSA计划应定义对于特定的评估/系统/应用领域应评估些什么；

应用要求

— 在不同的系统开发过程，功能安全评估的频次可能改变，但至少在系统面临潜在危险之前应进行一次FSA。有些公司也可能在构建/安装阶段之前进行一次评估，以防止在生命周期的较后阶段出现高成本的返工；

— 在定义FSA频次和严密性时应考虑以下系统属性：

- 复杂程度；
- 安全重要性；
- 类似系统以往的经验；
- 设计特征的标准化；

应用要求

— 在评估之前应提供足够的设计、安装、验证和确认活动的证据。足够证据的可用性本身可能是一个评估准则。证据应代表系统设计或安装的当前/认可状态；

— 评估者的独立性一定要合适；

— 评估者应具有适合于所评估系统的技术和应用领域的经验和知识；

— 在整个生命周期和对所有系统而言，实现FSA的方案都应保持系统性和一致性。FSA是一种主观的活动，为了尽可能多的消除主观性，可以使用检查列表来定义一个组织可接受活动的详细指南。

应用要求

- FSA产生的记录应是完整的。并且在生命周期下一阶段开始之前，评估结论应同负责SIS功能安全管理人员的意见一致。

应用要求

- 为了增强评估的客观性，需要独立于项目组的评估人员。需要高级（例如经验、等级、职位）评估人员，以保证它们所关心的问题能被适时的关注和涉及。进一步建议，对于某些大型项目组或评估组，可能有必要拥有多个独立于初始项目组的高级人员。
- 根据公司组织结构和公司内部的专家意见，也许不得不通过外部组织来满足对独立评估人员的要求。

  相反地，对于熟练进行风险评估及安全仪表系统应用的内部组织的公司可使用它们本身的资源来满足独立组织的要求，当然这样的内部组织应独立于负责项目的那些组织并在管理和其他资源方面是同负责项目的那些组织分开的。

应用要求

- 评估量与工程项目的规模和复杂程度有关。在同一时间可以对不同阶段的结果进行评估。在正在运行的工厂中改变不大的情况下尤其可能。
- 在某些地区，在阶段3进行的功能安全评估常被称为起动前的安全复审（Pre-Startup-Safety-Review（PSSR））。
- 评估组应能得到它们执行评估所需要的任何信息。这包括从设计阶段一直到安装、调试运行和确认阶段所作的危险和风险评估得到的信息。

11. SIS 功能安全管理

目的

目标是确定为满足功能安全目的所必需的管理活动

本章的目的在于达到和保持安全仪表系统的功能安全，并且不同于为达到工程场所安全所需的通用健康和安全措施

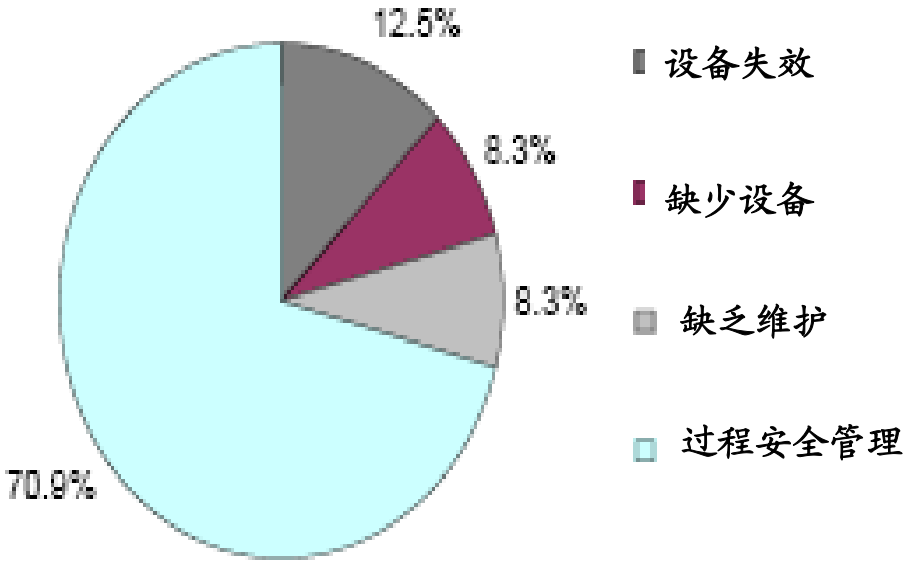
一般要求

- 应确定实现安全的政策和策略；
- 确定评价达到安全的方法，并在组织范围内进行交流。
- 安全管理系统应适当，以确保在使用安全仪表系统的场合下，它们能够把过程置于和/或保持在安全状态下。

功能安全管理

绝大部分导致爆炸的原因是不适当的 SMP

一项更详细的分析显示，SMP不适当的原因是由于：缺少培训，缺少管理监督，以及进行的过程不够充分



[HSE97: 健康与安全管理局，特别研究报告139/1997，《燃气装置中的爆炸》第6.2节 英国 1997

责任确定与告知

- 应确定负责执行和复审每个安全生命周期阶段的人员、部门、组织或其他单位，并告知它们各自应负责的职责（包括相关的、发证的管理当局或安全法规团体）。

人员能力要求

- 涉及安全生命周期活动的人员、部门或组织应能胜任执行它们所负责的活动。
- 人员的工程知识，培训情况和经验应该至少涉及以下几项：

  a）适合过程应用的工程知识、培训和经验；
  b）适合所使用应用技术的工程知识、培训和经验（如电气、电子或可编程电子）；
  c）适合所使用传感器和最终元件的工程知识、培训和经验；
  d）安全工程知识（如过程安全分析）；
  e）法律和安全法规要求的知识；
  f）适合其在安全生命周期中担当的角色的足够管理和领导技能；
  g）对事件潜在后果的理解；
  h）仪表安全功能的安全完整性等级；
  i）应用和技术的新颖性和复杂性。

风险评价和风险管理

- 应确定危险、评价风险和确定必要的风险降低。
- 从经济角度来看，它可能也有助于考虑潜在的资金损失。

计划编制

- 应编制安全计划以确定要求执行的活动以及负责执行这些活动的人员、部门、组织或其他单位。在整个安全生命周期当中，必要时应重新编制安全计划。
- 安全计划编制可集成在：
  - 质量计划中名为“安全计划”的段；或
  - 名为“安全计划”的单独文档；或
  - 包含公司规程或作业指导书的几个文档。

执行和监视

- 应执行规程以确保即时跟踪和有关安全仪表系统的建议满意解决，这些建议来源于：
  - a）危险分析和风险评估；
  - b）评估和审核活动；
  - c）验证活动；
  - d）确认活动；
  - e）事件后的和事故后的活动。

功能安全管理

- 任何给全权负责安全生命周期一个或几个阶段的组织提供产品或服务的供应商，应按该组织的规定提供产品或服务，并应有质量管理系统。为了建立恰当的质量管理系统，这些规程应设置到位。

评价安全仪表系统性能的规程

- 为了根据安全要求来评价安全仪表系统的性能，应执行下列方面的规程：
  - 确定和预防可能危及安全的系统失效；
  - 评估安全仪表系统的危险失效率是否符合设计中的假定值；
  - 1：通过检验测试、诊断或要求时操作失效可以揭示危险失效。
  - 2：应考虑规程来确定当失效率大于设计中的假定值时应采取的必要校正动作。
  - 在实际操作中，评估对仪表安全功能的要求率，以验证在确定完整性等级要求时进行风险评估所做的假设。

青岛劳帕安全技术咨询有限公司

核心业务

- 安全仪表系统功能评估：安全完整性等级SIL定级、验证/验算
- 过程工艺危害分析 **HAZOP**
- 培训：安全完整性等级SIL定级、验证/验算、HAZOP等培训

微信扫一扫

微信号 :**qd13184148810**

电话：13184148810

QQ:1930712371

邮箱：qingdaolopa@163.com

网址：www.qingdaolopa.com