中国化学品安全协会
China Chemical Safety Association

“化危为安”线上讲堂

化危为安

化危为安

化危为安

安全仪表完好性管理

主讲人：张建国

2021年5月21日

联系电话： 13323360708　　邮 箱：aqsfd_sciender@163.com

张建国

- 正高级工程师
- 全国工业过程测量和控制标准化委员会(SAC/TC124) 委员
- TŰV 莱茵功能安全高级专家和培训师(ID: #122/07)
- 霍尼韦尔亚太区安全咨询服务专家
- 中国化学品安全协会专家
- 在安全仪表领域有20余年的工程应用和安全咨询服务工作经历

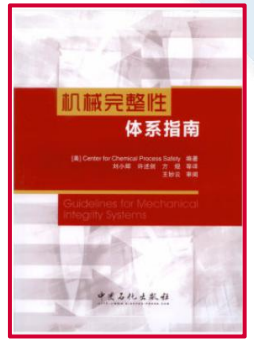
设备完好性 （机械完整性）的来历

- 1958年 美国石油协会(API) 发布 "API 510 – 压力容器检验规范 (Pressure Vessel Inspection Code, 1st Edition);
- 1990年7月 美国职业安全与健康管理局（OSHA）首次发布高危化学品的过程安全管理 (PSM)条例;

  1992年2月 PSM 最终定稿，规定了14个要素，其中：

  (11) 建立关键工艺相关设备的维护制度，包括书面规程、员工培训、适当的检查和测试，以确保持续的***机械完整性***;

  相关设备包括：***紧急停车系统（ESD - Emergency shutdown systems）***
- 2006年 化工过程安全中心（CCPS）出版 《机械完整性体系指南（GUIDELINES FOR MECHANICAL INTEGRITY SYSTEMS）》
  - ✓ ***安全仪表系统(SIS)***、关键报警和联锁...
  - ✓ 典型的MI活动包括：检查、测试和预防性维护(ITPM)；人员培训；建立相关规程; ...



设备完好性 （机械完整性）的来历

- 2017年 CCPS出版《资产完整性管理指南（GUIDELINES FOR ASSET INTEGRITY MANAGEMENT）》
- 机械完整性（MI）：为确保*重要设备*在其*整个操作年限内（the life of an operation）*适用于其预期用途而执行的系统性必要活动；
- 资产完整性管理（AIM）：确保*资产*在其*整个生命周期内（the life cycle ）*完整性的管理体系。

我国过程安全管理（PSM）的要求（1）

原国家安监总局《关于加强化工过程安全管理的指导意见》（安监总管三〔2013〕88号）列出12个要素：

- 安全生产信息管理
- 风险管理
- 装置运行安全管理
- 岗位安全教育和操作技能培训
- 试生产安全管理
- 设备完好性（完整性）

  其中指出：“七、设备完好性（完整性）- 开展安全仪表系统安全完整性等级评估。企业要在风险分析的基础上，确定安全仪表功能（SIF）及其相应的功能安全要求或安全完整性等级（SIL）。企业要按照《过程工业领域安全仪表系统的功能安全》（GB/T21109）和《石油化工安全仪表系统设计规范》的要求，设计、安装、管理和维护安全仪表系统。”
- 作业安全管理
- 承包商管理
- 变更管理
- 应急管理
- 事故和事件管理
- 持续改进化工过程安全管理工作

- SIS的完好性：1）通过设计和建造，将可靠性融入到SIS中，成为SIS 的内在品质；2）通过检验、测试、维护，以及运行状态监控，确保SIS的安全完整性得以保持，并在出现失效和性能降级时，及时成功地予以校正。

- 我国的PSM规定，是借鉴美国OSHA的PSM体系，并根据我国的国情制定的。

❑ GB/T20438-2017(IEC61508:2010)：电气/电子/可编程电子安全相关系统的功能安全

- ✓ 面向电气/电子/可编程电子仪表和系统的厂商；
- ✓ 各行业可依据该标准制定各自的行业应用标准。因此，它被称为“基本安全出版物”；
- ✓ 确定了四个安全完整性等级：SIL1、2、3、4；
- ✓ 依据该标准研发、设计、制造的系统或仪表设备，可获得权威认证机构颁发的SIL认证(SIL Claim Limit)”；
- ✓ 不过，SIL认证并非像防爆认证那样有“强制”要求；

- ✓ 对于SIL认证的仪表设备或系统，有三个重要文件：
  - ➢ **SIL证书（认证机构）；**
  - ➢ **测试/评估报告（认证机构）；**
  - ➢ **安全手册（厂商）**

用户在设计选型、安装、使用、维护等方面，要遵循安全手册。

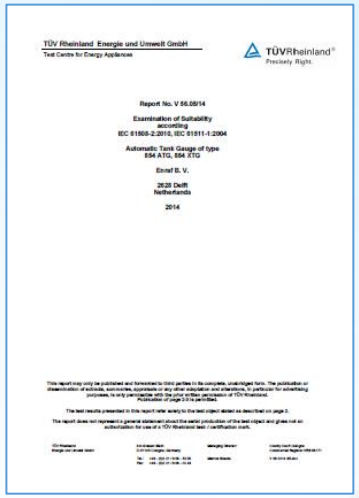
示例 - 安全手册

用于AOPS的 Honeywell Enraf Radar / Servo

TÜVRheinland®
SIL-2 approved


Certificate

No.: V 56.05/14


TÜV Rheinland Energie und Umwelt GmbH

Report No. V 56.09/14

Examination of Suitability according IEC 61508-2:2010, IEC 61511-1:2004

Automatic Tank Gauge of type 854 ATG, 854 XTG

Enraf B. V.

2628 Delft Netherlands

2014

4.3 Proof Testing

Attention!

To make sure that the safety rated loops remains SIL compliant a proof test has to be performed once per 5 years.

Points of attention:

- It is strongly recommended not to open the 854 ATG/XTG level gauge for proof testing unless test results or other findings demand internal maintenance and/or repair.
- For the purpose of this procedure it is assumed that the Service Engineer performs the proof test:
  - preferably from the control system, using available diagnostic tools,
  - as an alternative at the gauge, using a Portable Enraf Terminal (PET).

❑ GB/T21109-2007(IEC61511: 2003)：过程工业领域安全仪表系统的功能安全

- ✓ 新版IEC61511:2016，GB/T21109还没有完成升版；
- ✓ 它是GB/T20438体系下过程工业SIS的应用标准；它的条款和相应规定，只针对SIL1、2、3；
- ✓ 关于SIS仪表设备选型规定：
  - 选择仪表设备用于SIS并具有特定的SIL，应符合IEC 61508 硬件/软件的SIL认证；以及/或者关于“以往使用”的要求，视情况而定。
  - 所选设备的适用性应始终在操作环境的背景下考虑。
- ✓ 该标准围绕两个概念建立了一套“性能化”的方法论：
  - ➢ SIL；
  - ➢ 安全生命周期(SLC)：为SIS工程和应用建立工作流程和质量体系；
- ✓ 该标准只规定了应该做什么，而没有规定如何做；
- ✓ 并非传统的”YES/NO“标准，

  因此在安全措施设置、SIF的仪表选型和配置上可以有很多选项，需要通过HAZOP/LOPA等确定SIL要求，并对最终是否达到目标SIL要求进行验证计算。

- IEC61511:2016 术语3.2.51 - 以往使用（Prior Use）

基于以往在类似操作环境下的操作经验，用户对设备是否适合在SIS中使用、是否能够满足所需的功能和安全完整性要求进行的书面评估

✓ 为了证明SIS设备符合基于早先使用的条件，用户应该将该设备在类似操作环境中已经取得了令人满意的性能等相关证据形成书面文档。了解设备在操作环境中的行为表现并有高度的确定性是必要的，即计划的设计、检查、测试、维护和操作实践是足够的。

✓ “经使用证明”是制造商基于其仪表设备设计基础(例如温度极限、振动极限、腐蚀极限、期望的维护支持)进行的论证证明。“以往使用”涉及在过程工业领域的应用中，在特定操作环境下设备实际安装的性能表现，这通常与制造商的设计基础有所不同。

GB/T 20438.4—2017/IEC 61508-4:2010

3.8.18

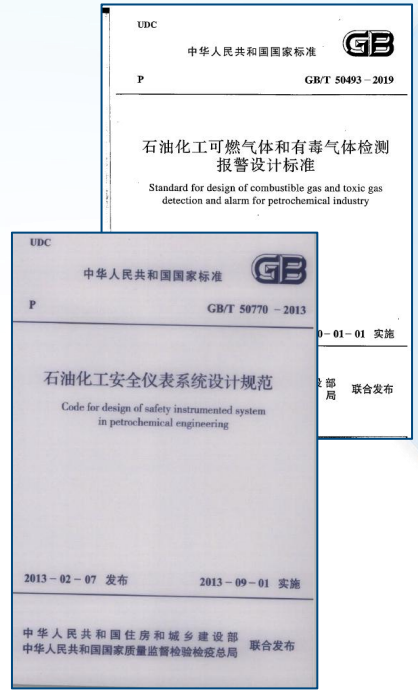
经使用证明　proven in use

针对一个组件的特定配置，基于对其运行经验的分析，证明危险的系统性故障的可能性足够低，使得每个使用该组件的安全功能达到其要求的安全完整性等级。

- **GB/T 50770-2013：石油化工安全仪表系统设计规范**
  - ✓ 目前，该标准主编单位正组织对其进行升版；
- **GB/T 50493-2019：石油化工可燃气体和有毒气体检测报警设计标准**
- **…**
- **公认的、一般可接受的良好工程实践 (RAGAGEP)**

  根据已建立的规范、标准、出版的技术报告、推荐的实践指南、或者类似的指导文件， 形成工程、操作、或维护活动的基础。

  - ✓ 不包含政府的法规；
- **（企业的）内部工程实践**
  - ✓ 企业多年积累的、行之有效的、好的经验。



SIS的功能安全管理

- 对于企业的SIS操作和维护，标准规定的功能安全管理主要有几个方面：

- ✓ **硬件配置/软件组态（Configuration）管理；**
- ✓ **文档管理**（文档是企业的长期资产）；
- ✓ **变更管理 （MOC)；**
- ✓ **人员能力管理**（包括对人员能力的保鲜、更新，以及持续评估）；
- ✓ **功能安全评估（FSA – Functional Safety Assessment）：**基于证据的调查，以判定由一个或多个保护层所实现的功能安全。
- ✓ **功能安全审核 (Audit)：**对于按计划安排的功能安全要求是否有效地执行、并满意地达到规定的目的，进行系统性地独立检查。

- 在SIS的现场操作和维护阶段，要将**评估**和**审核**结合起来，周期性开展A&A活动，确保SIS的功能安全管理水平的持续改进。

- SIL/PFDavg/RRF之间的关系

安全完整性等级	“要求”时失效的平均概率（PFDavg）	风险降低因数（RRF）
SIL 4	1E-04 to 1E-05	10,000 to 100,000
SIL 3	1E-03 to 1E-04	1,000 to 10,000
SIL 2	1E-02 to 1E-03	100 to 1,000
SIL 1	1E-01 to 1E-02	10 to 100

$$PFDavg = \frac{1}{RRF}$$

PFDavg = f (λ, TI, MTTR, β, ……)

六个主要的参数：

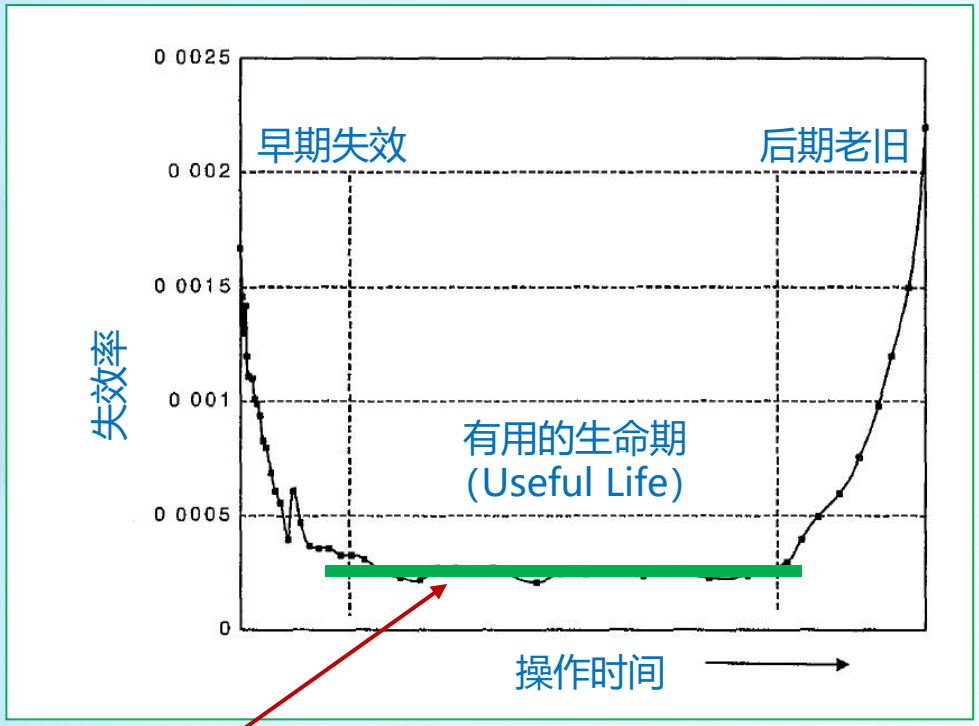
- 失效率（λ）；
- 表决形式（MooN）；
- 诊断覆盖率（DC）；
- 检验测试（Proof Test）的时间间隔（TI）；
- 平均恢复时间（MTTR）；
- 公共原因失效（β）；

- 什么是“**要求（Demand）**”？

需要SIS系统即刻采取相应动作的工艺状态（或事件），以便取得或保持工艺过程的安全状态。

例如：工艺参数达到HH（高高）或 LL(低低) 设定值。

❑ 浴盆曲线 – 可靠性分析最基础模型



失效率（λ）近似为常量

- “**早期失效**”来源，包括仪表设备出厂时的内在品质不合格，以及运输、仓储、安装、调试等环节造成的内在品质降低；
- “**有用的生命期**”代表仪表设备**正常品质**对应的使用年限。在这一段时间内，如果使用、维护得当，会有稳定的安全性能；
- “**后期老旧**”状态，仪表设备的安全性能会明显地下降，即失效率随时间不断增大。如若经评估认为可以继续使用，一是要改变维护策略，更加精心地维护；二是PFDavg验证计算已经没有意义。

诊断的组态及响应示例

- 一台智能压力变送器，正常输出信号：4～20mA，用于高高（HH）压力关断；变送器内部失效时，可组态为偏置到< 3.6mA或者> 21.5mA。如何选择?

✓ 选项1： 基于“故障安全”原则，组态为偏置到 > 21.5mA，并在逻辑控制器的程序上给出报警，那么该失效分类为：可检测的安全失效（λ_{SD}）；

优点：安全性高； **缺点**：误停车率高（牺牲可用性换取安全性）

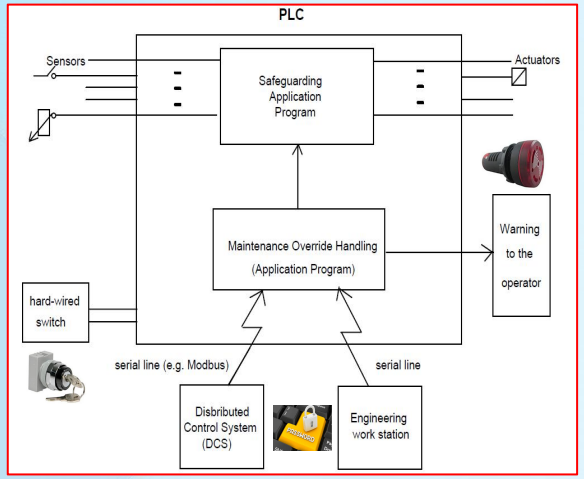
✓ 选项2： 在满足SIL的前提下，组态为偏置到 < 3.6mA ，并在逻辑控制器的程序上给出报警，由于**此时该变送器已完全丧失了安全功能**，因此该失效分类为：可检测的危险失效（λ_{DD}）；

优点：可用性高； **缺点**：安全性低（如果PFDavg计算满足SIL要求，该选择可接受）

IEC61511:2016 – 检测到故障时对系统行为的设计和管理要求

当在SIS中的危险故障被检测出来时，应采取补偿措施以保持安全操作。如果无法维持安全操作，则应采取特定的动作，以达到或保持工艺过程的安全状态。

当SIS中的任何故障是通过报警引起操作员注意时，应对该报警进行适当的检验测试和变更管理。

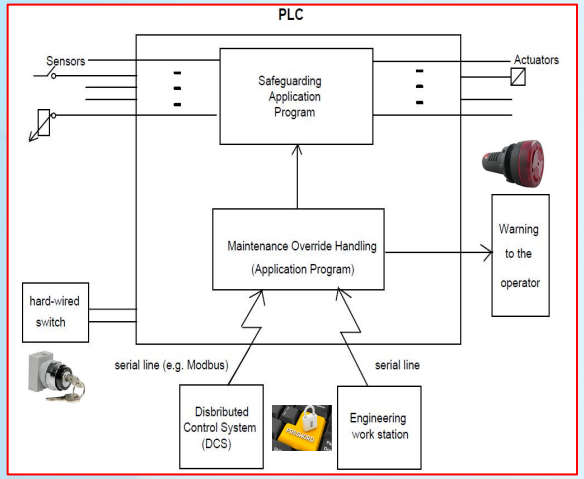


- **旁路**（bypass）- 阻止全部或部分SIS功能被执行的措施；
- **补偿措施**（compensating measure）- 在已知SIS性能下降的任何维护或工艺流程操作期间，临时实施的、计划好的、并且是形成书面文档的风险管理方法；
- **平均恢复时间**（MTTR - mean time to restoration）：预计的SIF功能恢复时间；

  MTTR包括：检测到失效的时间、开始维修前准备工作时间（包括：备件准备、作业工单审批、工艺准备）维修的实际使用时间、重新投用的时间。
- **最大允许的维修时间**（MPRT - maximum permitted repair time）：在检测到故障后，工艺允许修复的最大持续时间；

  注：它是工艺采取对等的补偿措施给出的最大时间窗口，

  MTTR ＜ MPRT;



- 旁路操作应有相应的操作规程、补偿措施；要提供必要的信息告知操作员处于旁路状态，以及如何操作、旁路的时间限制等。
- 只有经过危险分析，确认补偿措施有效，并提供足够的风险降低能力后，才能允许SIS在旁路期间保持连续操作。
- 所有旁路的状态应记录在旁路日志（log)中。所有旁路需要授权并进行显示。
- SIS逻辑控制器对I/O的”强制（Force)“，不应作为应用程序、操作规程和维护的一部分。不得在控制器处于在线状态下，对I/O进行”强制“操作。
- 维护/工程师站（接口）不得用作操作接口。

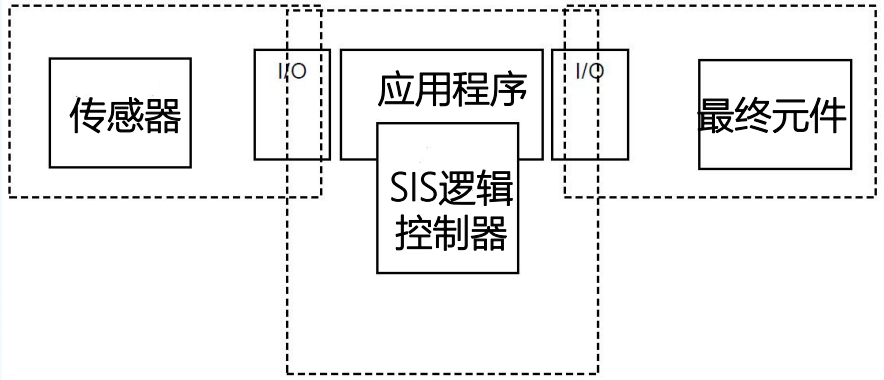
关于检验测试（Proof Test）

- **检验测试** - 为检测SIS中隐含的危险失效而进行的**周期性测试（时间间隔TI）**，如有必要，通过维修使系统恢复到“如新”状态，或者尽可能接近这种状态。（IEC61511-1:2016 术语3.2.56）

- **检验测试覆盖率** （C_{PT}）– 通过检验测试能够检测出的失效所占百分比。全面彻底的检验测试应该使检验测试覆盖率达到100%。（ISA-TR84.00.03-2012术语）

- 不论设定的SIL多少，检验测试都要力求全面彻底，达到“**完好如新**”状态。

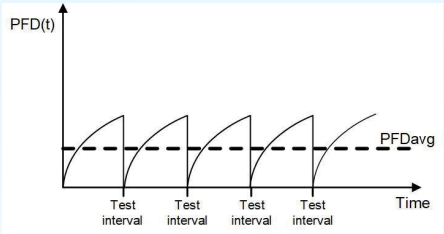
- 检验测试经常按照仪表/子系统**分段**进行，但在**开车前的现场验收（SAT）**时，应考虑对整个SIF进行一次“**端到端**”测试，确保SIF的整体功能性。



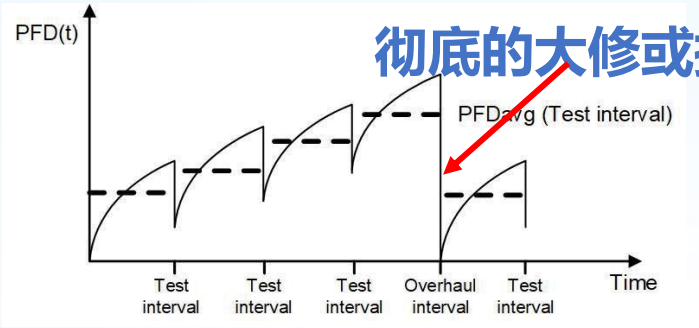
SIF分段测试要确保段间重叠

关于检验测试（Proof Test）

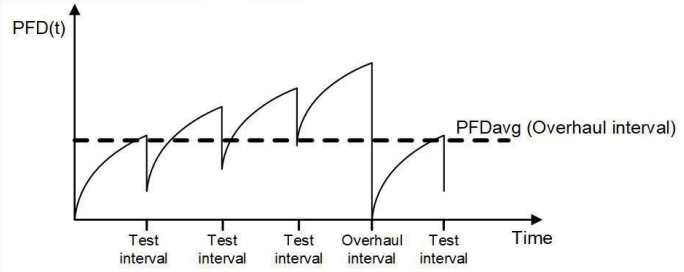
- 应在设计阶段考虑检验测试间隔时间（TI）、旁路等维护需要（即可维护性）；
- 依据厂商资料、借鉴工业数据库中提供的失效模式，并通过FMEDA确定检验测试的规程以及覆盖率；
- 可以利用装置非计划停车机会，对SIS阀门等进行测试；
- 在SIS仪表设备处于”老旧“状态（参见浴盆曲线）时，要适时调整维护策略（例如，缩短TI）；
- 不能按期进行检验测试时，应有必要的审批程序并进行影响分析；



完美的检验测试（C_{PT} =100%）



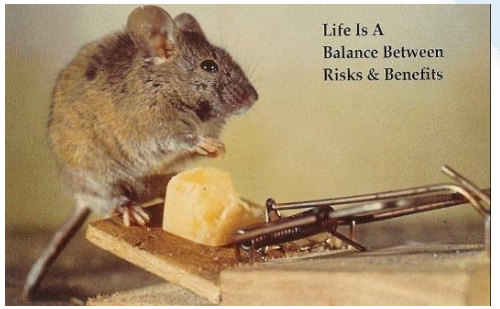
不完美的检验测试（C_{PT} ＜ 100%）



不完美的检验测试对PFDavg的影响

STR（误停车率）/ MTTF^{SP} （平均无误停车时间）

- 在满足安全性（SIL）要求的同时，SIF设计还必须实现足够的工艺过程可用性；
- 过程可用性除了影响生产，误停车后再次开车也间接影响安全；
- SIS的功能安全标准没有给出关于过程可用性的STR/MTTF^{SP}量化指标；
- STR/MTTF^{SP}在SIS仪表设备是在良好的安装和维护前提下、基于“安全失效率”等参数计算得出。
  - ✓ 对于高过程可用性要求的场合，MTTF^{SP}应该不低于50年；
  - ✓ 作为一般规则，MTTF^{SP}应是大检修时间间隔的5～10倍。例如，大检修安排是4年一次，MTTF^{SP} 应处在20～40年范围内。

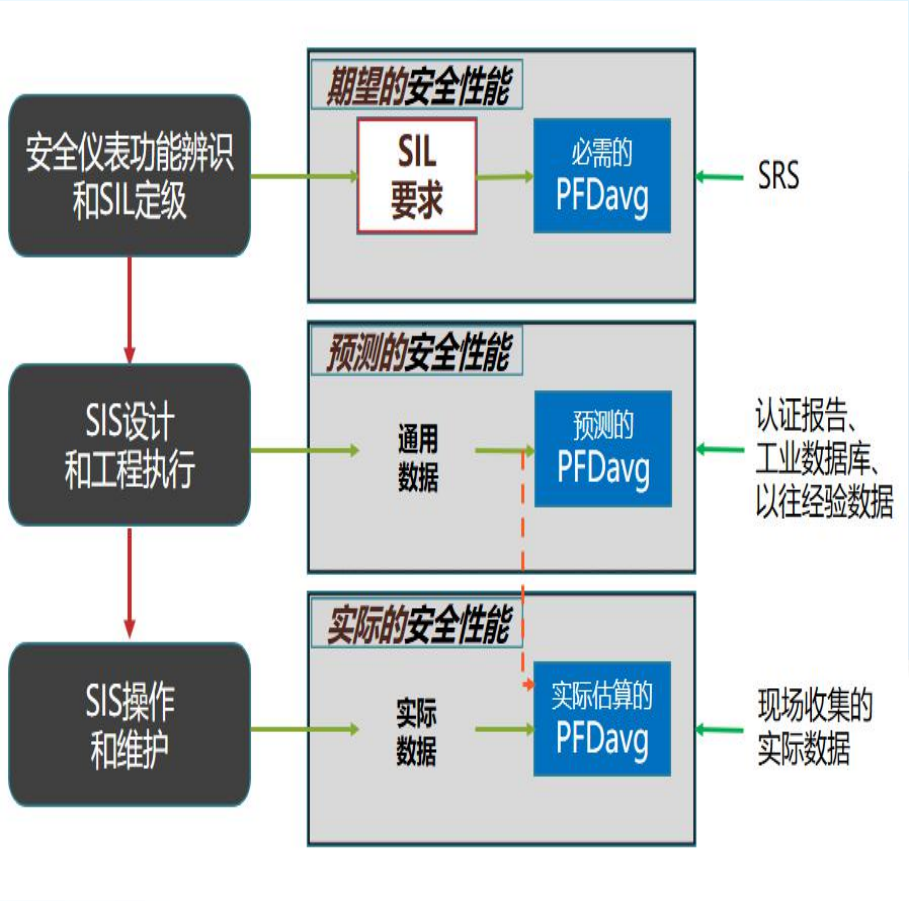


- 对于在役SIS的安全性能验证，最好的数据是实际积累的可靠性数据

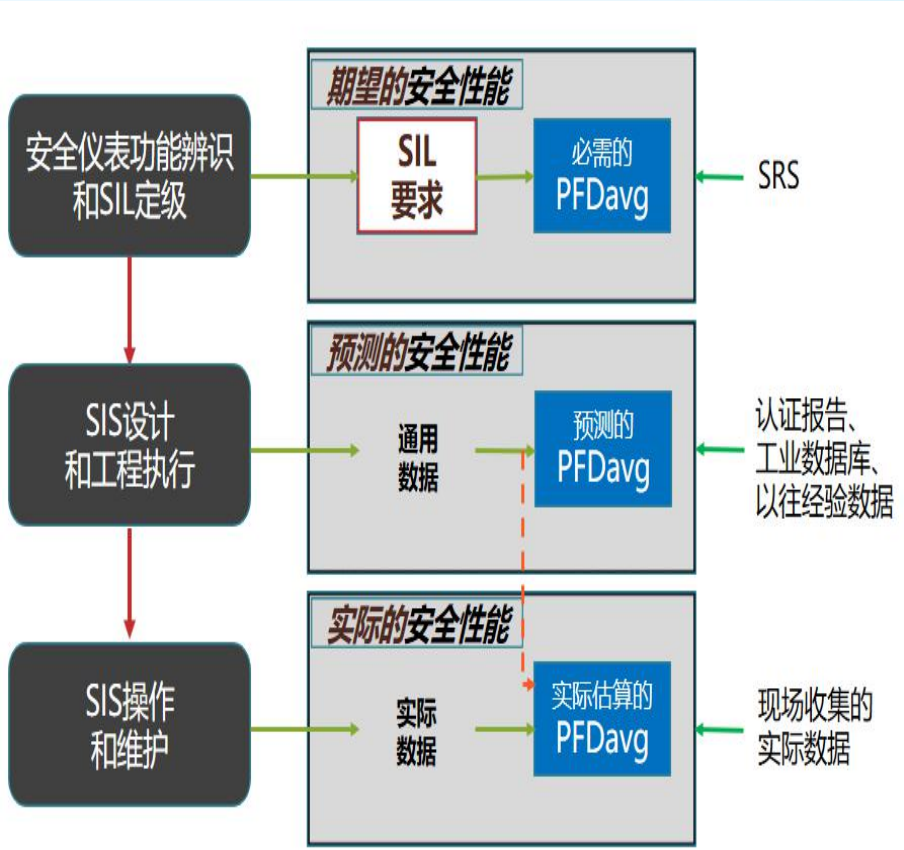
✓ 116号文“三、（七）……要加强安全仪表系统相关设备故障管理（包括设备失效、联锁动作、误动作情况等）和分析处理，逐步建立相关设备失效数据库。要规范安全仪表系统相关设备选用，建立安全仪表设备准入和评审制度以及变更审批制度，……”；

✓ GB/T21109(IEC61511-1:2016) 规定：

- 要制定规程，收集与“要求率”和SIS可靠性参数有关的数据（条款16.2.2）；
- 监视并评估SIS的可靠性参数是否符合设计时的假设（条款5.2.5.3）；



- 对于在役SIS的安全性能验证，最好的数据是实际积累的可靠性数据
  - 要有有效的适当证据，（表明仪表）设备可适用于SIS（条款11.5.3.1）
  - “以往使用（Prior Use）”评估涉及书面收集设备在类似操作环境下的性能信息（条款11.5.3.1注释3）
  - 在量化随机失效影响时采用的可靠性数据，应该可信、可追溯、文档化、对其合理性进行了适当评判，并且基于来自在类似操作环境下应用的、同类设备的现场反馈（条款11.9.3）



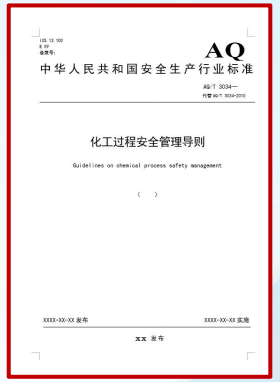
- 这些规定都表明，有必要建立适当的机制，跟踪SIS的实际性能。

通过对第一手数据和资料的评估，SIS仪表设备选型从目前高度依赖所谓“**SIL认证**”，逐步向基于“**以往使用**”规则、**建立准入和评审制度**过渡。

我国过程安全管理（PSM）的要求（2）

- 目前正在制定的AQ/T 3034—XXXX 《化工过程安全管理导则》，代替AQ/T 3034-2010《化工企业工艺安全管理实施导则》，给出了20个要素：

- **安全领导力**
- **全员安全生产责任制**
- **安全文化建设**
- 安全生产信息管理
- **安全生产合规性要求**
- **化工装置（设施）安全规划与设计**
- 安全教育、培训和能力建设
- 风险管理
- 装置原始开车安全
- 安全操作
- 设备完好性管理
- **安全仪表管理**
- **重大危险源安全管理**
- 高风险作业安全管理
- 承包商安全管理
- 变更管理
- 应急准备与响应
- 安全事故事件管理
- **本质更安全**
- 要素审核（安全生产绩效考核）与持续改进


AQ
中华人民共和国安全生产行业标准
化工过程安全管理导则
Guidelines on chemical process safety management

- PSM体系更加完善，体现我国安全管理理念的进步；
- 将管理体系、技术体系、人员能力等有机结合；
- 着眼全生命周期管理，通过持续改进实现生产过程的本质更安全；
- 将“***安全仪表***”从“***设备完好性***”中剥离出来，单独成为一个要素，体现了国家安全监管对“安全仪表“的重视；
- “安全仪表“涵盖的范围比单纯的”安全仪表系统（SIS)”更宽泛，比如“安全控制、报警、联锁（SCAI）”；

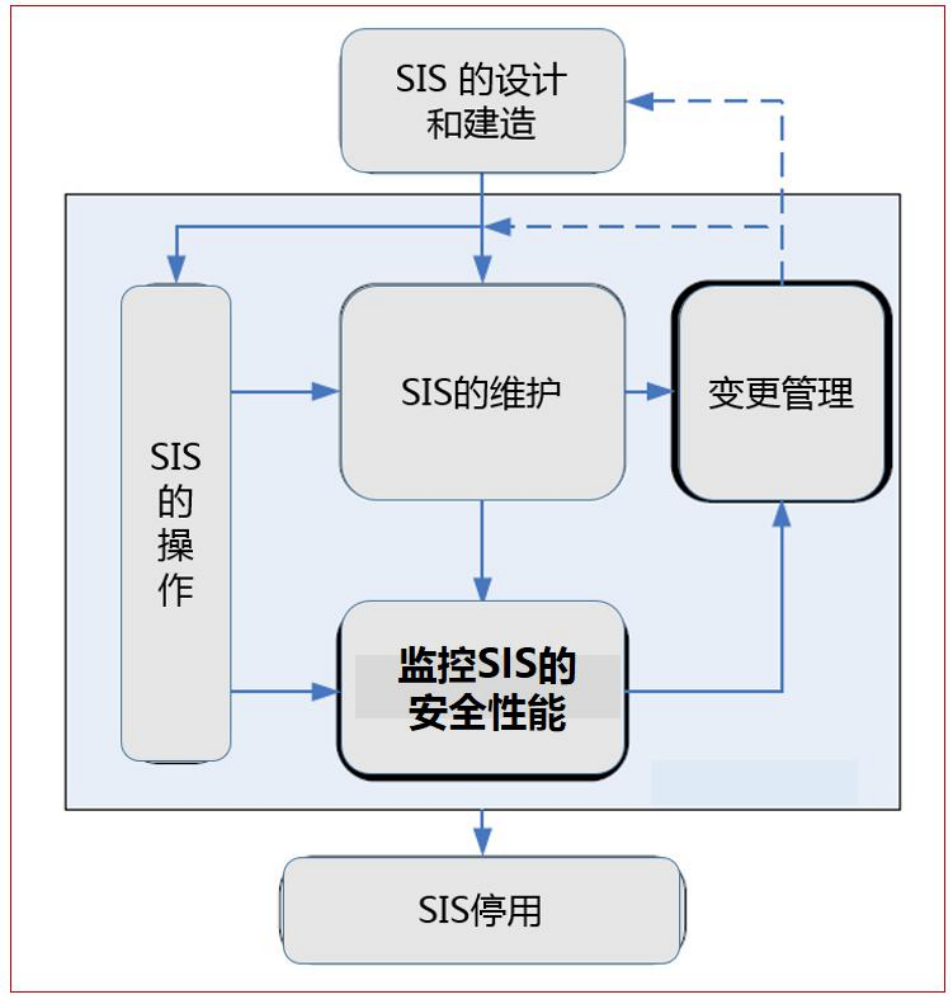
- **确认**（Validation）– 在SIS安装调试完成之后，通过文档审查、现场查验、 整体测试等一系列活动，项目工程各方和最终用户共同“见证”并确认最终交付的SIS完全符合了SRS，并为装置投产准备就绪，所有权从项目方向业主方移交，也称为“现场验收测试（SAT）”，以前也称为“开车前验收测试（PSAT）”。从本质上，它标志着SIS项目合同项下工程阶段的结束；

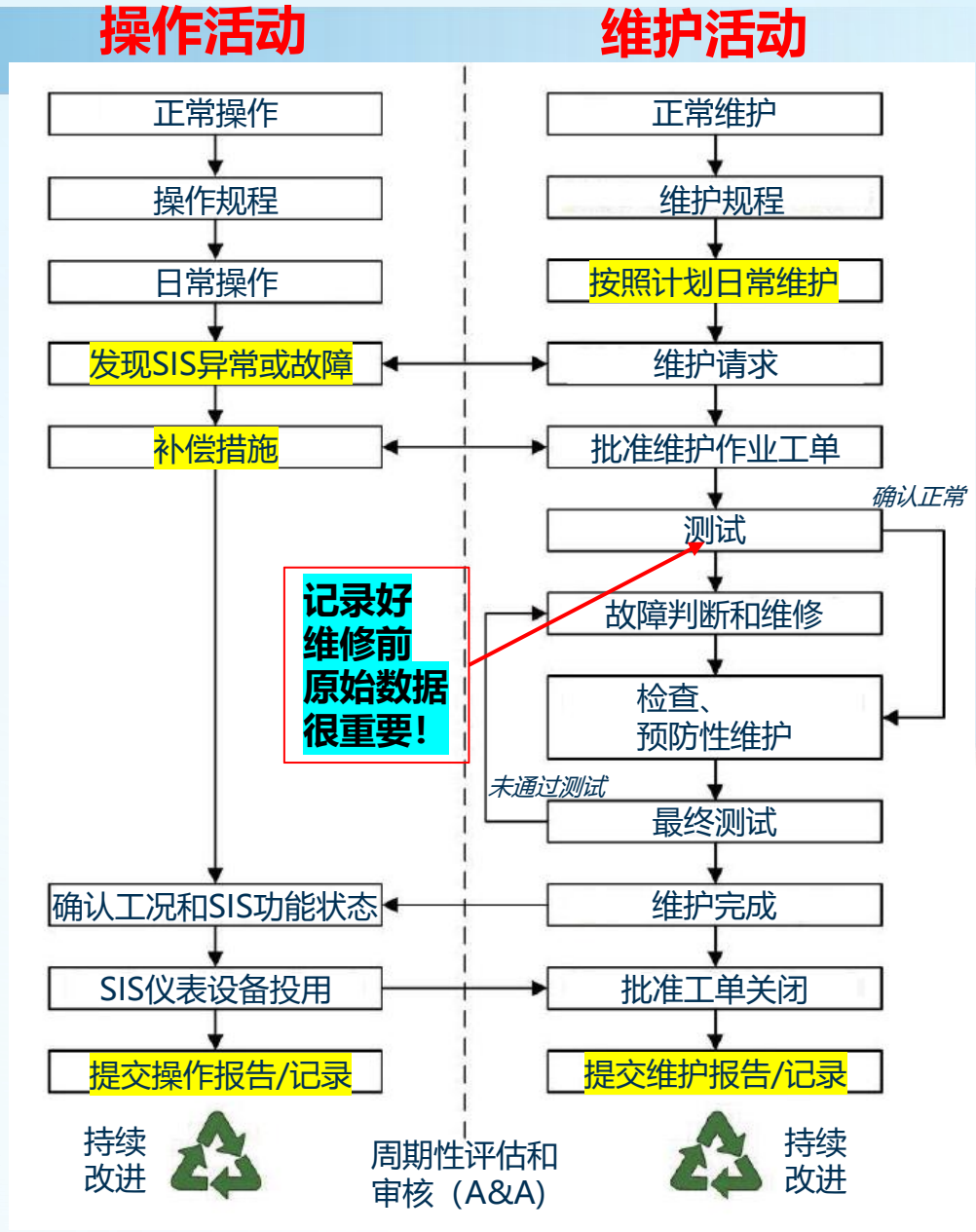
- SAT期间的测试活动是首次“检验测试”；SAT过程中积累的文档（包括调试记录、校验记录）将成为未来SIS操作和维护的基准点。

- **开车前安全审查**（Pre-Startup Safety Review，PSSR） - CCPS -
  工艺装置开车前的评估，用于确认能够按照设计要求操作，有充分明确的安全、操作、维护、以及紧急响应规程，已经进行了适当的危险分析，任何的变更修改都遵循了相应的管理程序，其中遗留问题得以解决，推荐的改进方案得到了落实，相关人员的培训已经完成。

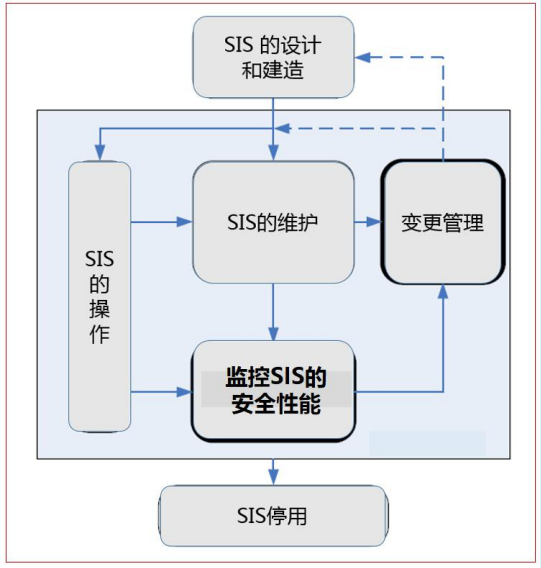
- PSSR是安全监管要求，也是SIS的功能安全评估（FSA）活动；
  ✓ 例如，安监总管三〔2013〕88号所要求的、建设项目试生产前的“三查四定”是其应有内容。

SIS的现场操作和维护





SIS的操作规程



- 操作规程，又称为标准操作规程（SOP - Standard Operating Procedures），SIS的操作规程涉及复位、操作/维护旁路、紧急停车按钮（ESD）、对报警的响应等方面，包括：
  - ✓ 正常操作，
  - ✓ 开车，
  - ✓ 停车，
  - ✓ 仪表维护、测试，
  - ✓ 仪表维护准备，
  - ✓ 工艺设备旁路或停止使用
- 规程应定义在每种操作模式下操作人员如何与SIS交互动作。 应描述控制、报警、画面，以及指示信息，确保操作员理解正在显示的信息以及对异常和紧急工况应做出的期望响应。
- 操作规程应提供以下信息：
  - ✓ 由SIS预防的危险事件，
  - ✓ SIF构成描述，
  - ✓ 关断设定值和SIF动作，
  - ✓ 如何正确使用旁路和复位，包括所需的工艺状态，
  - ✓ 对SIS报警和关断如何响应，
  - ✓ 何时以及如何执行手动停车，
  - ✓ 检测到故障时的操作规定，包括维持安全操作必需的补偿措施。

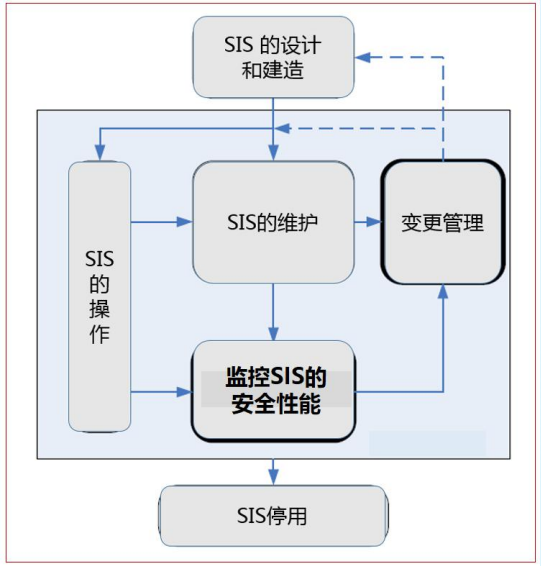
- 制定计划、并按照计划完成**预防性(Preventive)维护**活动；
  - ✓ 前瞻性地进行维护，检测和纠正初始故障和降级状态；也称为“计划性维护”、“主动性维护”，或者“固定时间维护”；

- 制定计划、并按照计划完成**预测性(Predictive)维护**活动：
  - ✓ 基于”性能状态“的维护；
  - ✓ 对诊断出的降级状态或故障进行响应；
  - ✓ 日常巡检，尽可能早地发现初始失效（征兆）和降级状态；在装置停车或旁路状态下，根据需要进行“介入”检查；
  - ✓ 校验/标定检查；
  - ✓ 检验测试；
  - ✓ 监测并管理仪表设备的“老旧”状态；

- 制定计划、并按照计划完成**被动性(Reactive)维护**；
  - ✓ 纠正性(Corrective)，“运行到失效（即不坏不修）”。对于SIS，由于很多危险失效是“隐性的”，待到发现可能为时已晚，因此，要加强预防和预测性维护，尽量避免被动性维护。

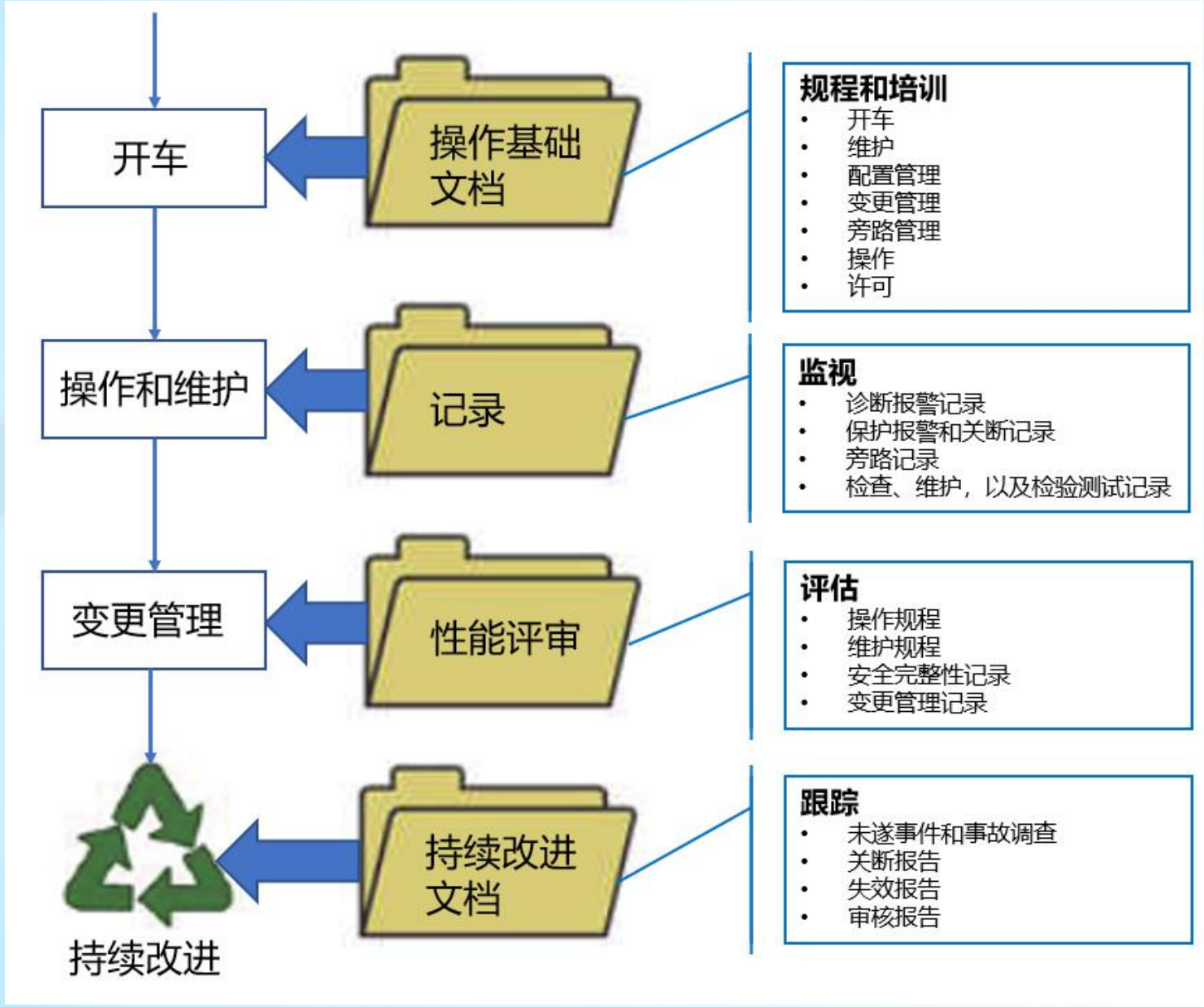
- 制定计划、并按照计划完成**可靠性分析，监控SIS的安全性能**。

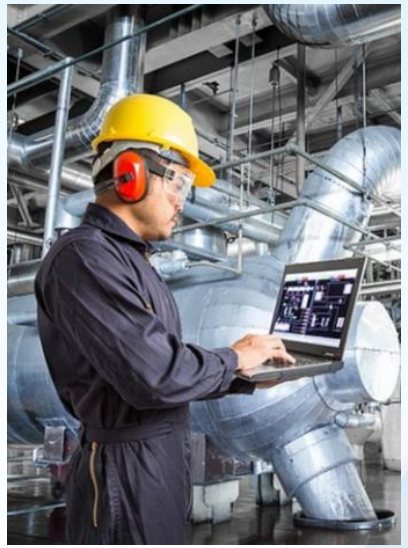
监控SIS的安全性能

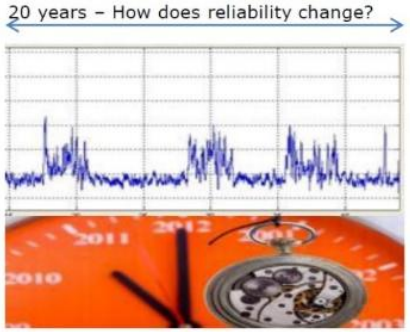


- 应定期评估/审核（A&A）SIS的实际性能是否与预期性能存在差异；
- 当识别出性能缺口时，应进行根本原因分析，以便 (1)确定失效是如何引起的，(2)确定失效的影响，(3)确定失效的根本原因，(4)实施纠正措施，(5)查验纠正措施是否有效地解决了问题；
- 反映SIS性能的主要指标：
  - ✓ 工艺过程“要求”，
  - ✓ 旁路时间，
  - ✓ 平均恢复时间，
  - ✓ 危险失效率，
  - ✓ 误关停率，
  - ✓ 人员能力、对管理规定和作业规程的依从性（管理体系指标）
- 通过表单记录留存相关信息和进行可靠性分析所需的数据。例如：
  - ✓ 停车记录和调查分析报告
  - ✓ 仪表设备（例如变送器、阀门）失效分析报告
  - ✓ 仪表设备检查表（巡检、介入检查）- 发现问题时用
  - ✓ 仪表设备校验记录表
  - ✓ 检验测试记录表
  - ✓ 旁路审批表
  - ✓ 延期测试审批表

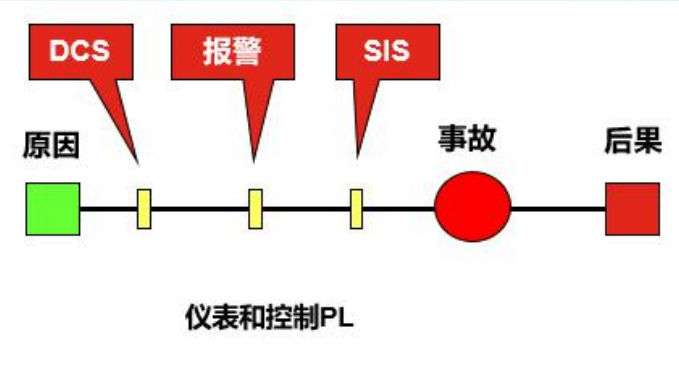
SIS的现场操作和维护阶段信息收集和评审







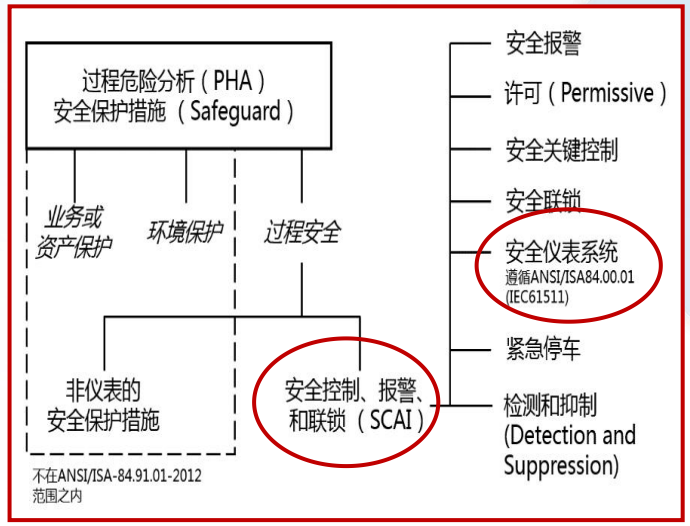
- SCAI：用仪表和控制方式执行的过程安全保护措施，根据所关注特定场景的风险降低需要，用于实现或保持过程的安全状态;



- 从LOPA的观点，SCAI就是辨识为保护层（PL）的独立安全报警、BPCS中的控制回路/联锁/报警，以及SIF；它们是相同的角色并有相同的特性;

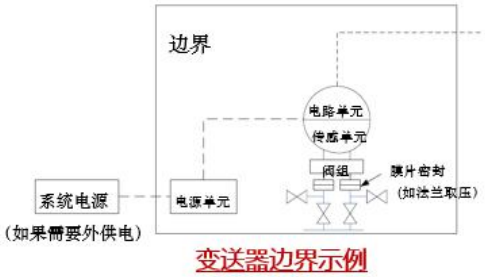
- 原国家安监局116号文：“四、高度重视其他相关仪表保护措施管理”，要求对这些保护层参照安全仪表功能进行管理和检验测试;

- SCAI管理要点：
  - ✓其相关文档应与其他仪表系统明确区分;
  - ✓纳入到安全完整性管理程序中;
  - ✓基于良好的工程实践，进行周期性检查、测试，以及预防性维护，保持在操作环境下的完整性;
  - ✓规程中要明确规定检验和测试记录的应有内容。



可靠性数据 - “经使用证明”与 “以往使用”

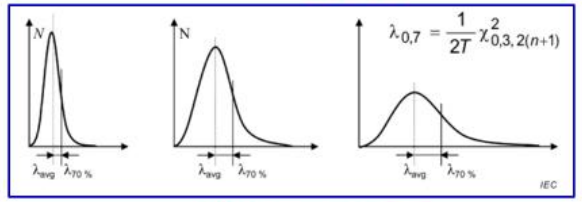
- **经使用证明（Proven in use）**：GB/T20438.4-2017/IEC61508-4:2010中的术语；
  - ✓制造商基于其设备设计基础 （例如，温度极限，振动极限，腐蚀极限，期望的维护支持）进行的论证证明，是仪表设备SIL认证（SIL Claim Limit）的重要评估依据之一，例如：阀门；
  - ✓**基于大量的用户经验，证明仪表设备在特定应用领域具有广泛的适用性**；
- **以往使用（Prior use）**：GB/T21109/IEC61511：2016中的术语；
  - ✓**最终用户**对SIS仪表设备的安全性能进行的书面评估；
  - ✓证明在特定的操作环境下，实际安装使用的仪表设备其安全性能具有高度的确定性；
- 明确仪表设备的边界；明确仪表设备的失效分类，确定 “通过/未通过（PASS/FAIL）“准则；采用适当的数学模型和计算方法；
- 企业采用”以往使用“规则分两步：
  - ✓基于定性评估，建立”用户批准清单“”准入和评审制度“；
  - ✓联合同类企业”建群“，采用共同的失效分类和收集规则，建立通用可靠性数据库，用于量化评估；



变送器边界示例

ISO14224	PERD, CCPS	OREDA
• 关键失效	• 完全失效	• 关键失效
• 降级失效	• 部分失效	• 降级失效
• 初始失效	• 初始失效	• 初始失效

失效分类



失效率70%置信上限

- IEC61511条款11.4.9 - 用于计算失效量的可靠性数据应以不低于70%的统计置信上限确定。

- 安全自动化资产完整性（SAAI – Safety Automation Asset Integrity）管理，是一个大概念，包括：

✓ SIS/SIF;
✓ 非SIF的“仪表和控制方式”保护层;
✓ BPCS:
- BPCS的平稳操作，是安全生产的基础（LOPA中触发事件（IE）之一）；
- SIS的操作和维护，依赖BPCS的支持；
- BPCS中与SIS相同的现场仪表，也是可靠性数据库的重要来源；

- 满足国家安全监管要求：“... 逐步建立相关设备失效数据库。...，建立安全仪表设备准入和评审制度以及变更审批制度，...；
- 对SIS设备的安全性能进行动态跟踪；
- 参照“以往使用（Prior use)”规则，建立企业SIS设备失效数据库以及”准入和评审制度“、“用户批准清单”制度；
- 参照“经使用证明（Proven in use）”规则，探索多企业、同行业等统一的失效数据收集机制，逐步形成我们自己的行业通用SIS设备可靠性数据库。

谢 谢！

直播回看、课件下载请上“中化协安全技能培训平台”
网址：https://ccsa.yunkeonline.cn