从邦斯菲尔德事故谈
化工企业安全仪表系统应用典型问题

张建国

正高级工程师、TUV Rheinland 高级功能安全专家

中石化 – 霍尼韦尔（天津）有限公司

2020年7月31日

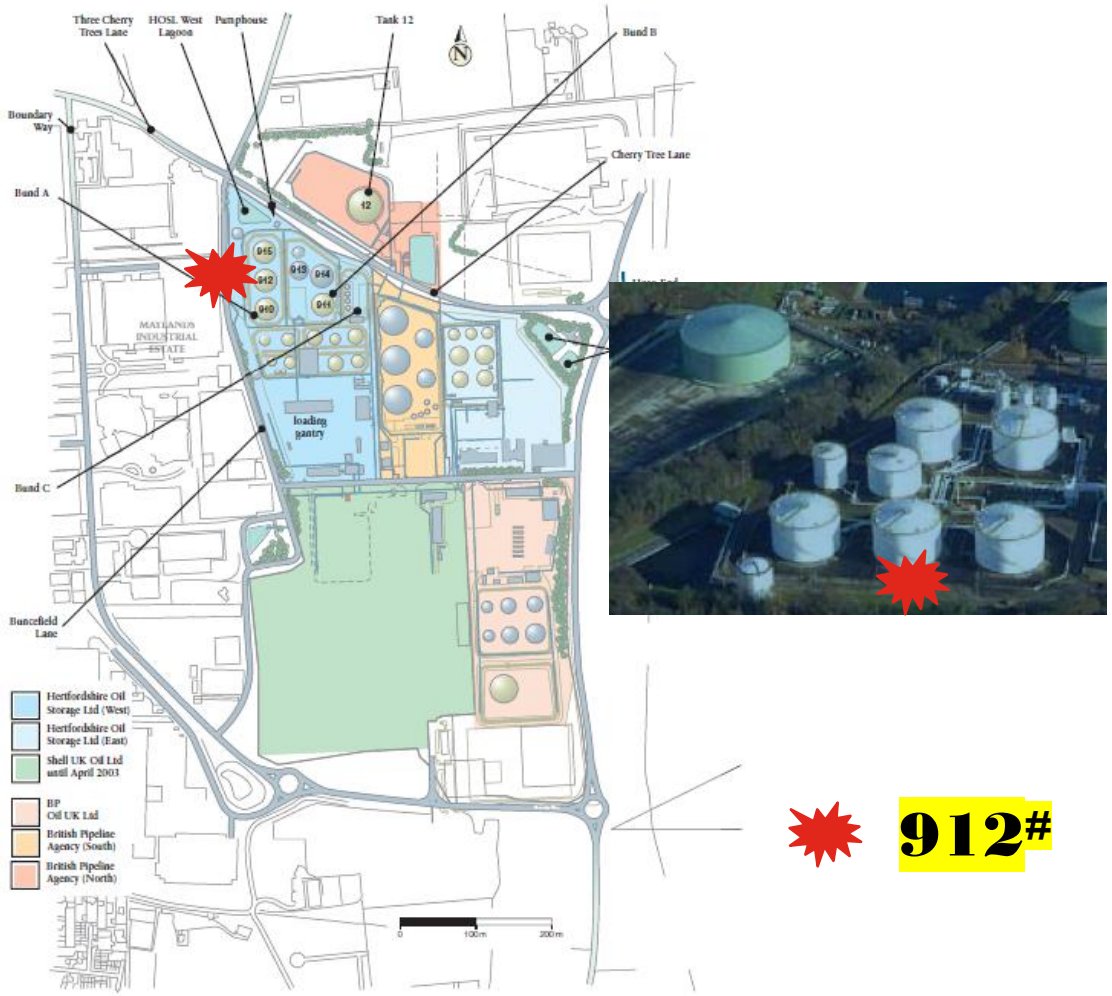
1. 邦斯菲尔德油库事故分析
2. 事故调查报告给出的建议
3. SIS应用的典型问题

邦斯菲尔德油库概况

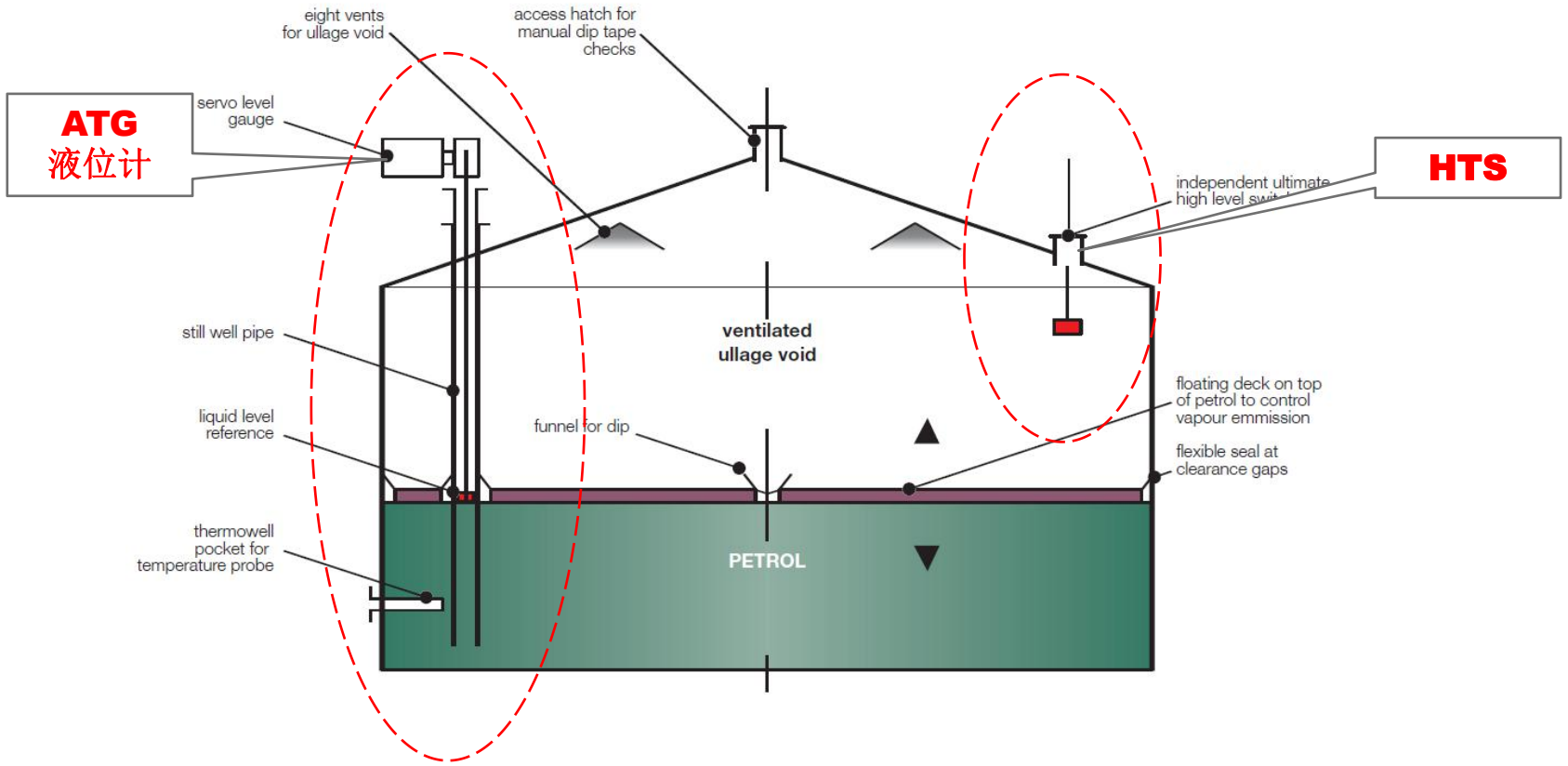
邦斯菲尔德油库坐落于英格兰赫特福德郡（Hertfordshire）的赫默尔亨普斯特德（Hemel Hempstead），靠近M1高速公路的8号路口。

整个油库有三个罐区：

- 赫特福德郡石油储存有限公司(HOSL)，道达尔和雪佛龙合资，道达尔负责日常管理。现场分为东、西两个场地。
- 英国管道代理有限公司(BPA)，英国石油公司（BP）和壳牌（Shell）合资，资产归英国石油管道有限公司(UKOP)所有。罐区也分为两部分：北部部分和位于HOSL东西之间的一部分。
- 英国石油公司(BP)，位于油库的南端。



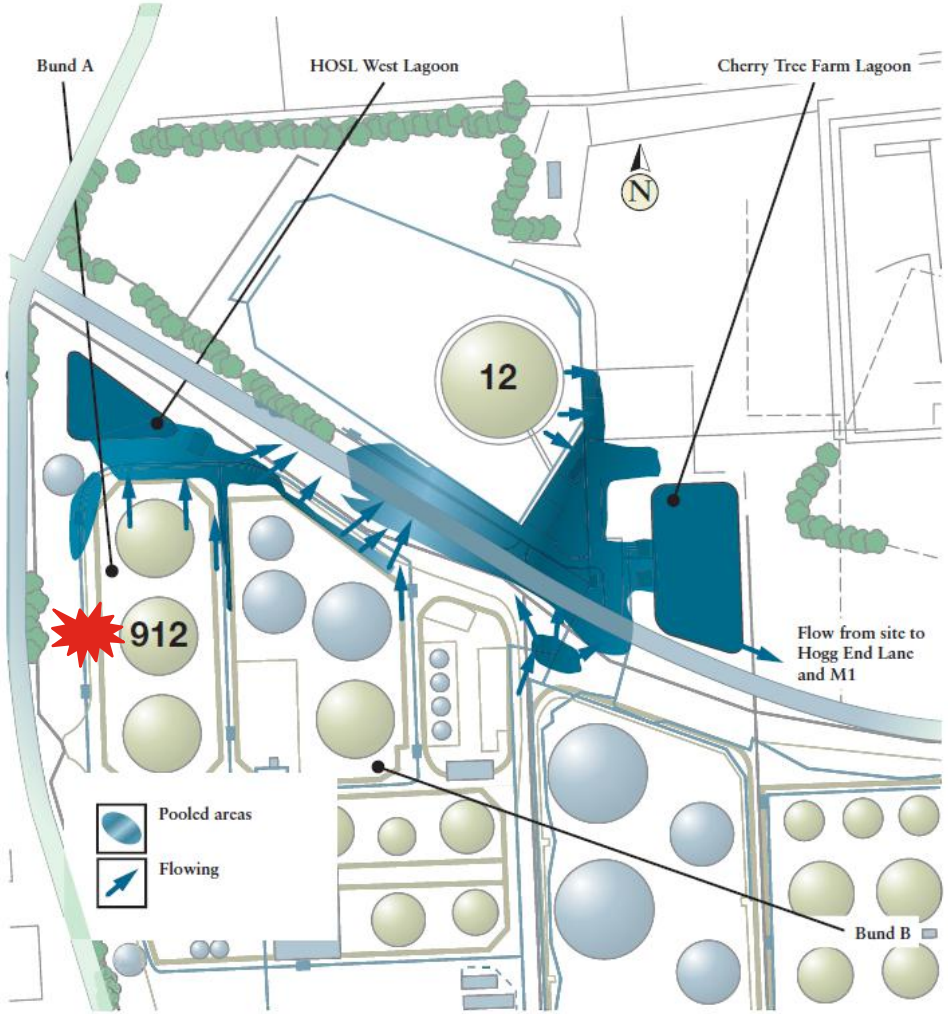
出事故的912#储罐仪控系统配置



- 912#罐容6000m³；装有自动储罐计量系统(ATG)，并在控制室操作站显示液位。BPCS
- 储罐上安装有独立的高液位开关(IHLS)，液位达到设定值时，自动关闭入口管道上的阀门，并给出声音报警。SIS/AOPS(自动防溢流系统)

事故发生时间轴（2005年12月10~11日）

- 12月10日18:50 – 开始向912#罐输送无铅汽油；
- 12月11日03:05 – ATG液位显示不再变化。3个ATG报警：“用户液位”“高液位” 和“高-高液位“也随之失效。
- 真实液位达到高液位开关(HLS)设定值时，该液位开关也处于失效状态，未能启动自动关停和报警。
- 12月11日05:37 – 液位超过其极限容量，汽油开始从罐顶的通风孔溢出。



油品流动和聚集区域

注：ATG – Automatic Tank Gauging System; AOPS – Automatic Overfill Protection System

事故发生时间轴（2005年12月10~11日）

- 闭路电视查证显示，围绕着罐体形成了直径约360m的白色气云（碳氢和冰晶混合物）。
- 罐区外等候拉油的油罐车司机发现了该气云并通知了现场的员工。
- 12月11日06:01 - 按下消防报警按钮，报警响起并启动消防泵。“蒸汽云爆炸”几乎同时发生，可能是由于消防泵启动引起的火花点燃。
- 爆炸发生时，已经有250m^3汽油从油罐泄漏出来。
- 从ATG液位失灵到事故发生，历经3个小时。

注：ATG – Automatic Tank Gauging System; AOPS – Automatic Overfill Protection System

事故发生前与事故发生后

- 大火持续燃烧了好几天，20个大型储罐被大火吞没，并对罐区外周边造成大量的破坏。
- 43人受伤，好在并不严重。
- 630家企业、机构受到严重财产损失。

事故处理中发现的问题

- 爆炸的严重程度远远超出了合理的预期。
- 泄漏的燃油和消防化学品从渗漏的围堰流入下水道和“渗水坑井”，造成重大的环境破坏。
- 由于事故发生在周日早上，包括附近的工业区没有造成人员丧生。
- 事故污染物液体渗透到周边的土壤以及提取饮用水的含水层，对饮用水供应造成威胁。
- **启示：**
  - ✓ 在过程危险分析（PHA）等工作中，要采取更科学严谨的态度和方法，而非仅凭直觉和简单经验，考虑简单的场景。
  - ✓ 在风险评估时，要充分考虑对人员健康、财产、以及环境等多方面的损害和影响。

the Competent Authority

HSE Environment Agency SEPA

问题出在哪里？

- ATG的伺服液位计故障，操作站上的液位显示"冻结"，并没有被及时发现；
- 高液位开关（HLS）功能失效；
- 在火灾期间和之后，"二级"和"三级"密闭系统（诸如围堰）也相继失效；
- 对罐输送量，上下游之间没有足够的监控；
- 多公司参与，对日常作业、安全等关注点分散；
- 人手不足，尤其是在夜班；整个罐区设施老旧，并以最大负荷运行；
- 对所涉及的重大危险源缺乏足够的重视（Buncefield罐区应遵守COMAH法规，类似我国对"两重点一重大"装置或设施的管理规定）；
- ……

注：COMAH – The Control of Major Accident Hazards Regulations 1999. (重大事故危险的控制规定)

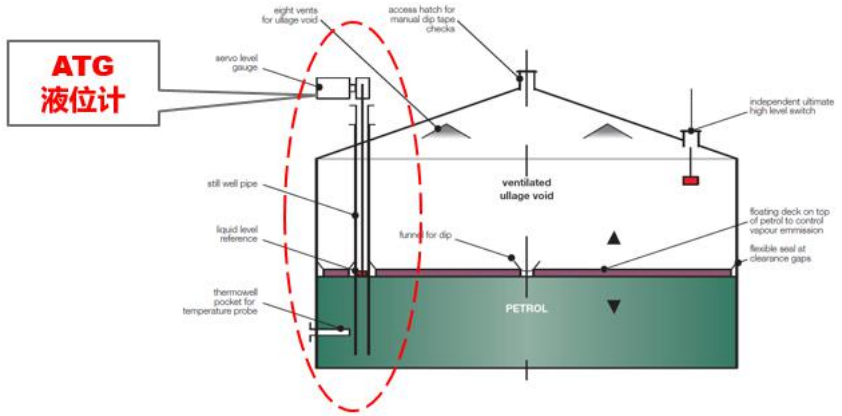
仪表问题 - 1

- ATG伺服液位计失灵，是此次事故的直接原因。

LOPA: 触发事件（IE）- BPCS

- 据报告，该液位计从8月31日维修后到12月11日发生事故，不到3个半月，共有14次出现类似故障。

- ATG系统的故障一直没有彻底解决，厂商也没有找到故障原因。



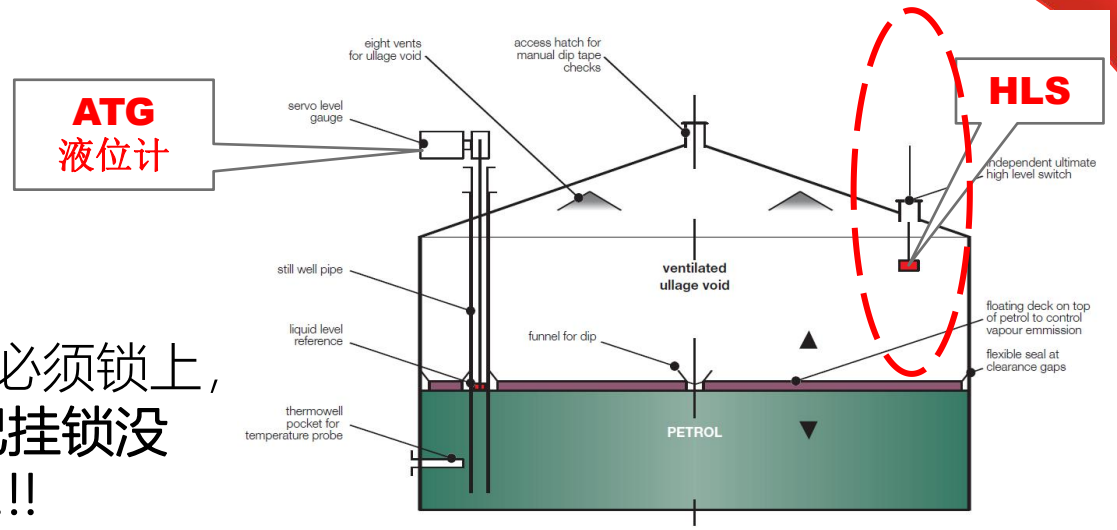
- **问题思考：**
  - ✓ 规章制度、规程是否足以杜绝此类问题？
  - ✓ 人员能力是否胜任这些仪表设备的处理？
  - ✓ 在LOPA分析时，通常将BPCS IE假设为10-1/年，并非想当然，这需要怎样的前提？
    - ➢ 检验、测试和预防性维修（ITPM）任务的计划安排是否满足这样的假设？
    - ➢ 当发现失效，或者在校验或诊断出初始失效状态时，要及时进行修复（基于状态维护）；
    - ➢ IE频率通过历史性能表现予以验证。

摘自《Guidelines for Initiating Events and Independent Protection Layers in LOPA, CCPS》

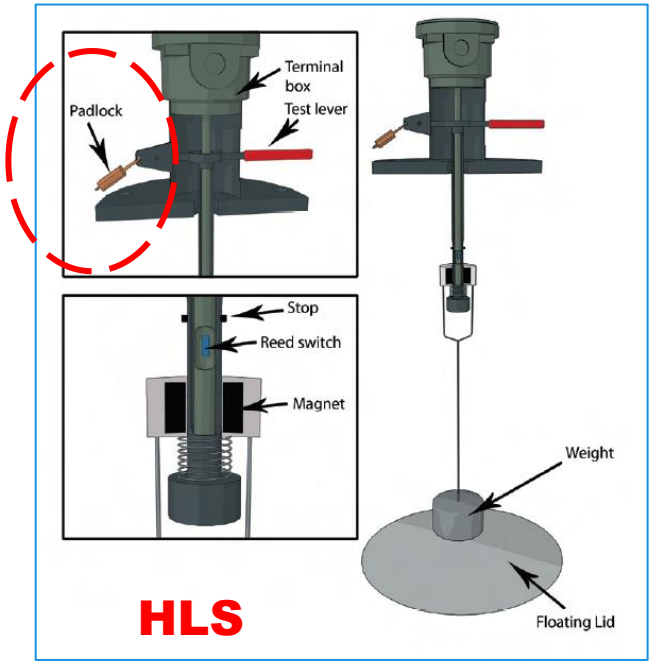
仪表问题-2

- 高液位检测开关（HLS）功能失效

LOPA：SIF保护层失效



- 液位开关上的 Padlock （挂锁），在正常操作时，必须锁上，将测试杆（Test Lever）固定并处于水平位置；**这把挂锁没有安装！从供货商到用户没有人知道它的真实用途!!!**
- *‘除了HLS的制造商和承包商的问题之外，现场业主方没有对订单、安装和测试规程进行充分的监督。在对开关进行定期测试时，现场没有人员知道测试完成后需要挂锁，以便将测试杆固定在正确的位置。现场业主方应该对关键的安全操作和设备进行更严格的监管，以便相关人员充分了解其工作原理，…”– 摘自事故报告*



- **问题思考：**
  - ✓ HLS失效并非硬件本身可靠性差；
  - ✓ 它由人为因素造成，在SIS应用中，它被分类为**系统性失效**；
  - ✓ *这样的问题，在SIL验证的PFDavg计算中，能体现出来吗?*

控制系统的其他问题

- 显示画面 – 多个罐的ATG系统只有1台显示器，一次只能调取1个罐的操作画面。在事故发生当晚，有关912#罐的操作画面堆栈排在其他4个罐的画面后面。

- 在罐的操作画面上设计了一个红色的“停止”紧急切断按钮。共有3条输油管道，该按钮可关闭其中两条管道上的阀门。但是该急停按钮从没有用过，也没有测试过，也没有相应的操作规程；另一条管道在现场控制室有单独的急停按钮。

- 系统的访问权限：任何人都可以修改ATG系统的任何参数，包括更改报警设定值。（虽然与本次事故没有关系）

- 当时的ATG系统没有在液位测量和灌装数据不一致时给出报警的功能，该报警功能能够辨识罐表出现测量值冻结这样的故障。

其他问题 – 输送量控制 -1

- 油品接收共有3条管道，现场操作主管可以对一条管道的物料及其”批次“的量值完全管控，而另外两条管道（UKOP），由于历史原因，控制权在其他地方。

- 罐区现场人员无法了解UKOP两条管线上游的SCADA监控系统的信息，包括管道是否在用，以及输送流量。

- 由于管道存量、码头状态、多个罐同时作业等工况，现场人员很难通过输送量计算灌装的液位变化速度。另外，也没有适当的计划调度系统，输送量的改变也没有通知罐区现场。例如，在爆炸前不久，UKOP南线的流量从550立方米/小时改变到900立方米/小时，现场并不知情。

- UKOP管道紧急关停的方式:
  - ✓ **打电话到上游终端**
  - ✓ 依赖储罐上HLS的动作
  - ✓ **启动现场临近的手报开关**

- **对于依赖人工操作本应进行风险评估，但没有进行。**

其他问题 – 输送量控制 - 2

- **问题思考：**

  ✓ 在HLS之外，紧急切断很大程度上依赖人工操作。要充分考虑**人因的影响**：人员是否有足够的能力及时发现问题？是否有足够的响应时间？是否有完备的操作规程？是否接受过相应的培训？

  ✓ 在LOPA分析，“报警 + 人员操作”作为PL，一般假定为风险降低能力（RRF）10倍。

表 F.4　保护层(预防和减轻)典型的 PFD_{avg}

保护层	PFD_{avg}
控制回路	1.0×10^{-1}
人的执行能力(经培训的、不紧张)	$1,0 \times 10^{-1} \sim 1,0 \times 10^{-2}$
人的执行能力(处于紧张状态下)	0.5～1.0
操作员对报警的响应	1.0×10^{-1}
容器压力额定值超过来自内部和外部压力源的最大极限值	10^{-4}或更好，在保持容器完整性(即了解腐蚀、按日程表执行检查、维护时)

GB/T21109 （IEC61511）附录F

Data Table 5.46. Human response to an abnormal condition

IPL description
Human response to an abnormal condition
Generic PFD suggested for use in LOPA
0.1
Special considerations for use of generic PFD for this IPL
• When the trigger for the human response is a safety alarm, the alarm is clearly understandable and available to the operators in their usual work location(s). • When the trigger for the human response is a check or field sample, a procedure indicates the need for this check or sample and the required frequency. There is also written guidance on what to do if the check shows the reading to be out of a tolerable range. Readings are recorded in a checklist, on an appropriate form, or in some form of database. • The operator has sufficient time available to respond to the indication of an abnormal condition and complete the required action, and this time is less than the time that it takes for event to become unavoidable. See Section 3.3.3. • There are clear procedures for the operator to follow to complete the response. The response task is low-complexity, with step-by-step instructions and minimal diagnostics or calculations. • The operator is trained on the response task. • The operator taking the corrective action can do so without being put into a dangerous situation to accomplish the action. • The human factors related to oral communication, human system interface, and work environment have been reasonably optimized. (See Appendix A for performance shaping factors to control.)
Generic validation method
• Testing of any sensors, alarms, and final control elements used by the operator in the response procedure is performed to ensure that they function properly. (See the Safety Alarm Section 5.2.2.1.1 for details.) • Verification of the procedures, training, and control of human factors ensures continuing effectiveness of human response. • Tabletop exercises, drills, and use of a process simulator are techniques that can be used to provide refresher training or to demonstrate response effectiveness.
Basis for PFD and generic validation method
Consensus of the *Guidelines* subcommittee. See NUREG CR-1278 – *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report*, Table 15-3 (Swain and Guttmann 1983).

Guidelines for Initiating Events and Independent Protection Layers in LOPA, CCPS

其他问题 – 罐区吞吐量增大

- 自上世纪60年代末投产，罐区处理量已增长了4倍。储罐之间转移批次以防止溢流的缓冲库容在操作上面对着相当大的压力.

- 在事故发生当晚，现场人员甚至搞不清楚哪条管道在与哪个储罐进行输送作业。原因包括：

  ✓ 换班交接程序存在问题
  ✓ ATG系统操作画面叠加层面太多

- **问题思考：**

  ✓ 交接班是重要的管理环节。类似问题出现事故的典型案例 – 1988年英国北海的派普艾尔法(Piper Alpha)海上平台事故，造成167人丧失，£17 亿损失。

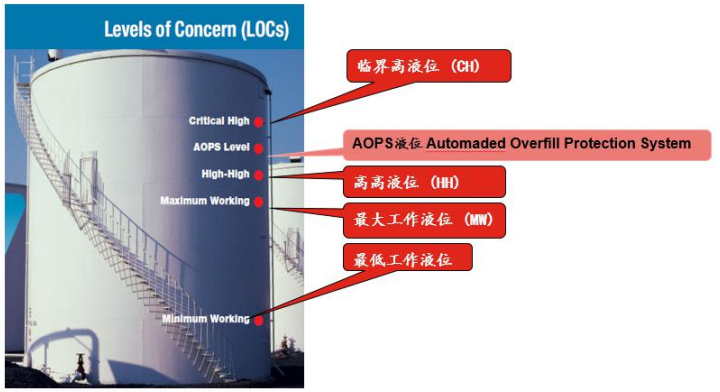
  ✓ “工作流程和人员安排应该定义如何跨班次、下班、周末和节假日的管理维护活动”“报警应以适当的时间间隔自动重复激活，以确保每一个班次都被通知到当前的工况状态”。

Piper Alpha's location in the North Sea, around 193 kilometres (120 miles) north-east of Aberdeen, Scotland

其他问题 – 灌装规程

- 由于一次只能调取一个储罐的操作画面，操作员必须有意识地决定监视哪个画面；在液位测量上也设计了一系列的声光报警。基本上有3个液位报警：

  ✓ “用户高液位” – 每个批次的最高液位，由操作主管设定。
  ✓ “高液位” - 设置为储罐最大允许操作液位以下。
  ✓ “高-高液位” - 设置为HLS设定值以下。



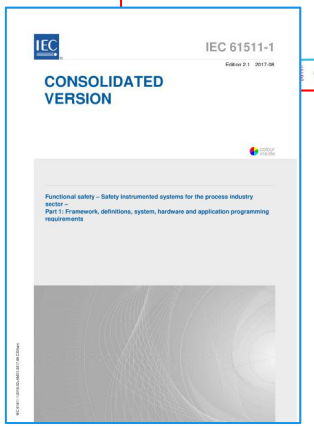
- 现场操作依赖这些报警控制灌装过程。不过，由于生产的要求，对这些报警应用很随意。例如，有时允许液位超过“高液位报警”；有时允许液位上升到“高-高”，甚至超过该设定值。

- 书面操作规程缺乏细节描述，对于上述的液位选择和报警使用没有给出任何具体指导。

液位	含义	需要的动作
极端高液位（CH）-必须	造成危害的最高液位	激出管理紧急响应
自动防溢流系统激活液位（AOPS）	在CH到达之前能够自动切断的最高液位	AOPS激活
高高液位（HH）-必须	在CH到达之前能够启动切断的最高液位	报警和切断响应
最大的工作液位（MW）-必须	在正常情况下可能达到的最高液位	无
最小的工作液位	在正常情况下可能达到的最低液位	无

- **问题思考：**
  ✓ 本案例现场没有真正意义上的储罐灌装系统。
  在溢流这样的重大事故危险管控上，存在严重的管理失缺失。
  ✓ 必须以一致、安全的方式控制灌装作业，报警限的设置必须明确其含义。

其他问题 – 仪控承包商问题



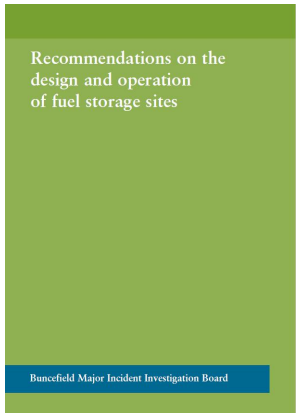
- 本案例的ATG的维护、HLS的供货和安装委托给了一家公司。
- 2004年审核机构给出的意见：承包商人员必须有能力履行有关职能，其能力要求应与合同的风险水平挂钩。承包商人员应接受培训。
- 本案例业主方没有对承包商人员的技术能力和培训进行评估。
- **问题思考：**
  - ✓ 合同应该明确安全关键工作的期望目标。
  - ✓ 应该有有效的报告和记录所有重大故障及其解决办法的系统。这个系统应该被合同双方理解并实施。
  - ✓ ……
- “提供产品或服务的供应商，应有质量管理体系并应制定规程以证明其充分性”“供应商应有功能安全管理体系，以符合IEC61511的功能安全管理要求，应制定规程证明其功能安全管理体系的充分性”“功能安全管理体系应满足IEC61508-1:2010的条款6”。摘自IEC61511-1:2016

注：IEC61511对应GB/T21109；IEC61508对应GB/T20438

邦斯菲尔德事故调查报告给出的建议

调查报告给出了25条在罐区设计和操作方面的建议，可分成六个主题：

- 安全完整性等级要求的系统性评估（建议1）
- 采用高完整性系统防止一级密闭的丧失（建议2-10）（储罐罐体的防溢流）
- 通过工程实施，应对一级密闭丧失的逐步升级（建议11-16）
- 通过工程实施，应对二级和三级密闭的丧失（建议17-18）（围堰及其外围围堵措施）
- 企业的管理体系、规程、人员能力等方面（建议19-22）
- 安全文化和领导力（建议23-25）



邦斯菲尔德重大事故调查委员会发表了45页的报告，给出了25条关于燃料储存罐区设计和操作方面的建议。

与SIS应用有关的建议解读

建议1:

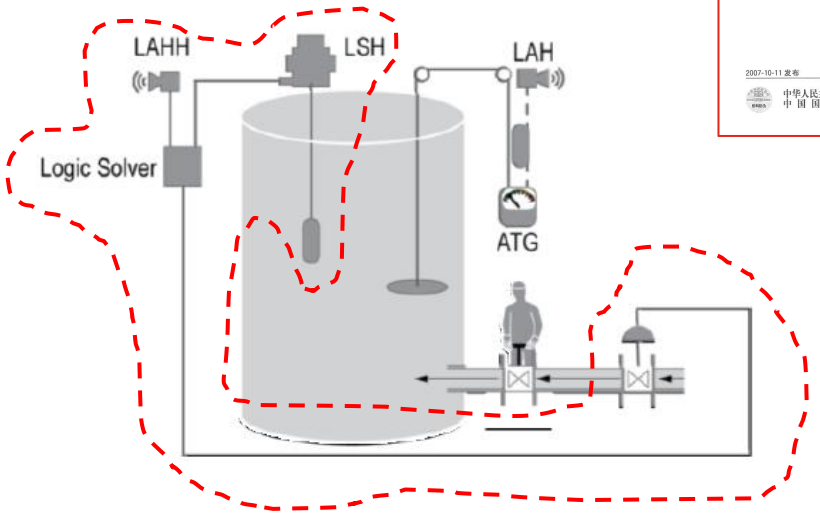
- 按照最新的国际标准，设置高完整性的防溢流系统，具有足够的独立性，确保及时地安全切断，防止储罐的溢流。

- 根据BS EN 61511 （IEC61511，我国GB/T21109）第3部分给出的规则，制定防溢流系统安全完整性等级（SIL）定级的通用方法。该方法应考虑:

  - ✓ 罐区周边敏感资源或人口的存在
  - ✓ 罐区操作的特性和强度
  - ✓ 储罐计量系统(ATG)预期的可靠性水平
  - ✓ 操作人员监控的范围和严格程度

解读:

- 设置独立的储罐自动防溢流系统（AOPS）
- AOPS的SIL等级定级：HAZOP/LOPA
- 现代防溢流设计：标准API 2350:石油设施储罐的溢流保护



AOPS

注：ATG – Automatic Tank Gauging System; AOPS – Automatic Overfill Protection System

与SIS应用有关的建议解读

建议2～25要点：

- 高安全完整性的自动防溢流系统（AOPS），应与ATG系统物理和电气隔离。
- AOPS的工程实施、操作和维护，遵循IEC61511。
- 通过适当的检查、测试、维护，特别是周期性检验测试，确保其安全完整性水平持续保持。
- 保存维护记录，并周期性审查。
- 确保有完善的规程、足够的人员能力。
- 安装可燃气体探测系统。
- 安装CCTV系统，帮助操作人员早期检测异常工况。


GB

中华人民共和国国家标准

GB/T 21109.1—2007/IEC 61511-1:2003

过程工业领域安全仪表系统的功能安全 第1部分：框架、定义、系统、硬件和软件要求

Functional safety—Safety instrumented systems for the process industry sector—Part 1: Framework, definitions, system, hardware and software requirements

(IEC 61511-1:2003, IDT)

2007-10-11 发布　　2007-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

- **企业要成为“高可靠性组织”(HRO)**：具有强烈安全文化的强健组织，长期保持高水平的安全、可靠、工作质量。

- 建议6：确保接收终端（而不是发送端）对储罐的灌装有最终控制能力。接收端应能够安全地终止或转移输送，而不依赖于远程第三方的行动，也不依赖于远程通信的有效性。
需要考虑与上游管网、炼油厂、或其他关联设施的相互影响。

注：ATG – Automatic Tank Gauging System;　AOPS – Automatic Overfill Protection System

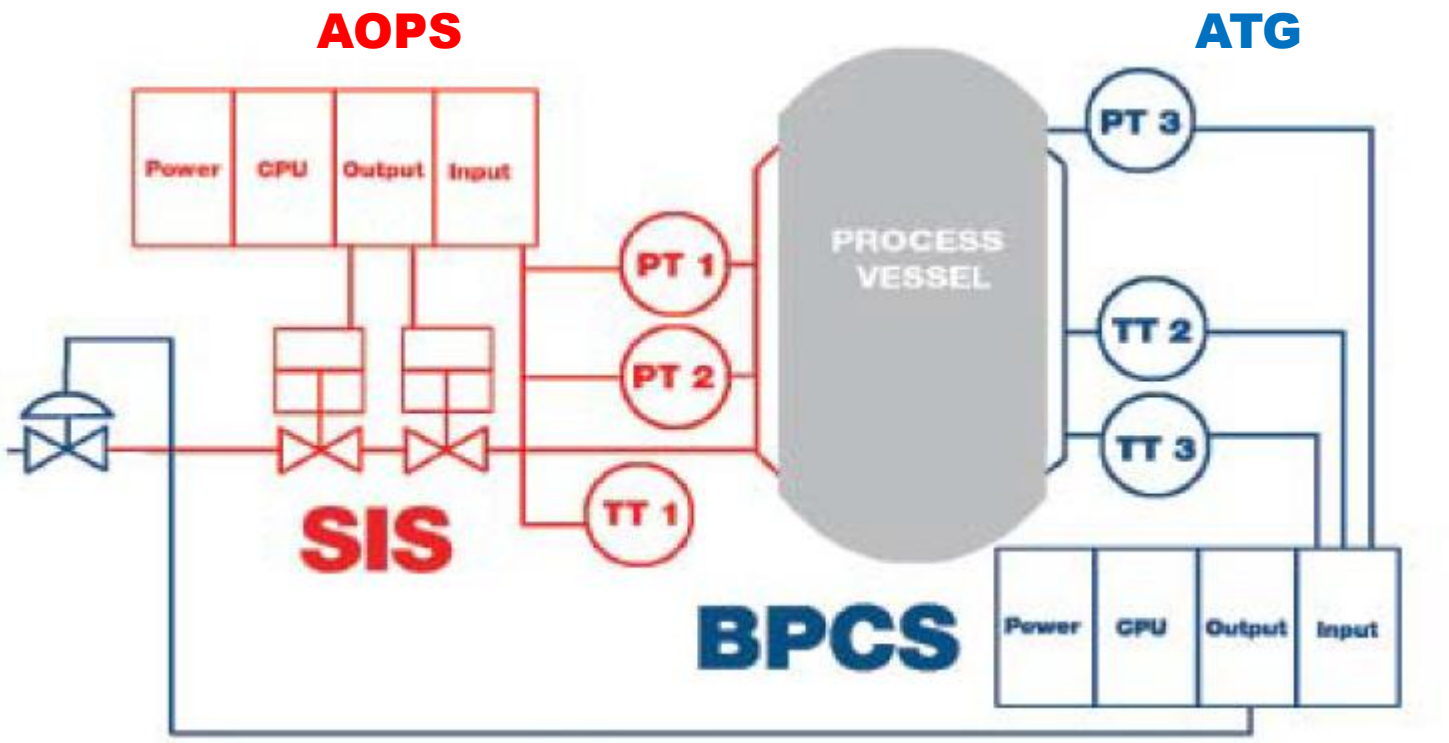
几个思考点

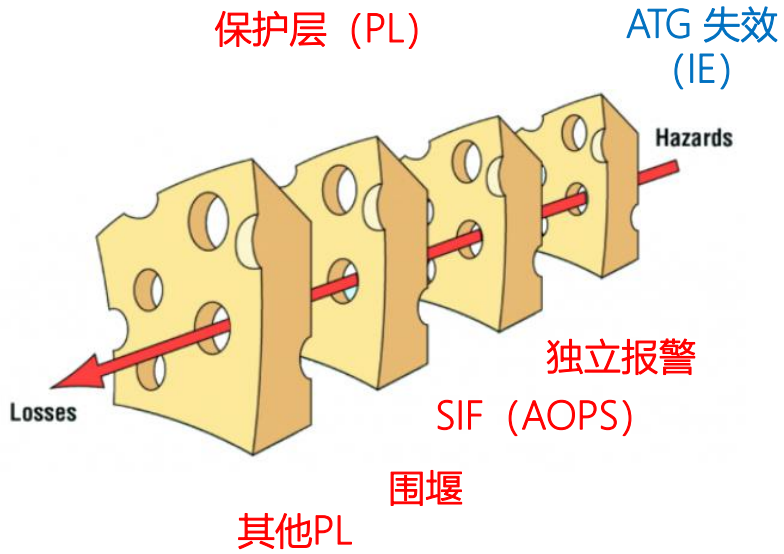
- 传统的防溢流设计，如本案例的HLS切断，与今天基于GB/T21109（IEC61511)，有何不同？为什么要进行SIL定级？

- 本案例的HLS失效是由于人为错误（挂锁缺失），在SIL验证时能体现出来吗？进一步地，什么是SIL？
- SIS的操作和维护如何确保SIL的持续保持？
- 根据原安监总局安监总管三【2014】116号文要求，企业对涉及“两重点一重大”的化工装置和危险化学品储存设施，普遍进行了过程危险和风险分析、SIL定级，以及SIL验证等评估，下一步应该做什么？

以上几个思考点，将结合到下面有关SIS的典型概念和关注问题之中

1. SIS应独立于BPCS





- IEC61511 条款9.4.1：应对保护层的设计进行评估，确保各保护层之间、保护层与BPCS之间的共因、共模，以及从属性失效的可能性足够低。
- 独立性是SIF/PL的核心属性之一。

避免出现多米诺（Domino）现象

2. 什么是安全完整性？SIL不仅仅是PFD!

- **安全完整性** - SIS在需要时执行所需SIF的能力。 (IEC61511-1:2016术语3.2.68)

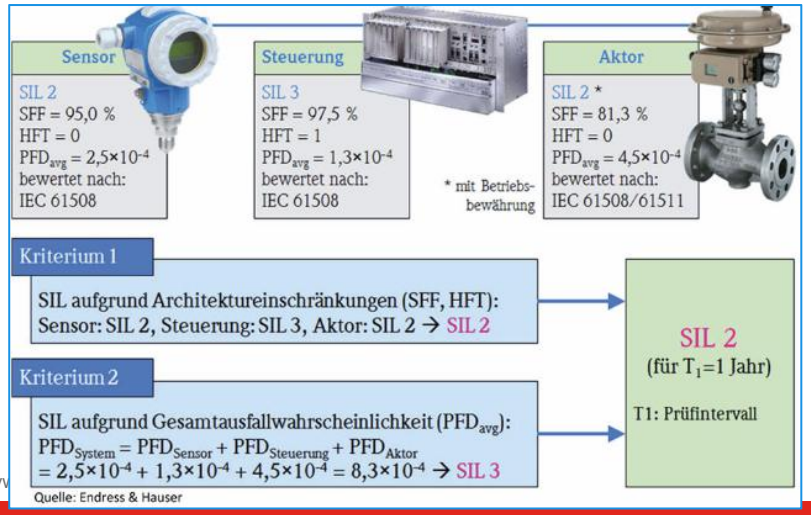
  注4: 安全完整性包括***硬件安全完整性***和***系统性安全完整性***，也要考虑由硬件和系统性问题交互结合造成的复杂失效。

- **硬件安全完整性** – 与SIS在危险失效模式下、与随机硬件失效有关的、安全完整性的一部分。用危险失效的平均频率（PFH，连续操作模式），或者“要求”时的平均失效概率（PFDavg，要求操作模式）表征。 (IEC61511-1:2016术语3.2.26)

✓ “要求（Demand）”，例如：ESD系统在工艺条件达到“HH（高高）”或“LL（低低）”时，需要联锁关停；

✓ PFDavg由6个设计参数确定：

- 危险失效率（ λ_D）
- 表决架构（MooN）
- 自动诊断覆盖率（DC）
- 检验测试时间间隔（TI）
- 在线平均维修/恢复时间（MTTR）
- 公共原因失效的影响（β）

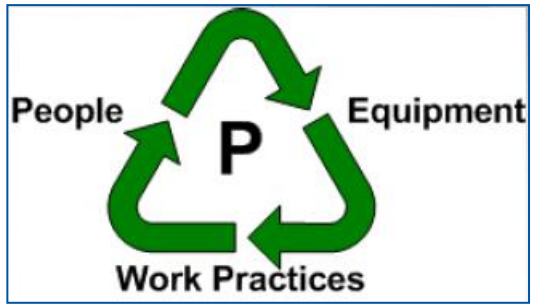


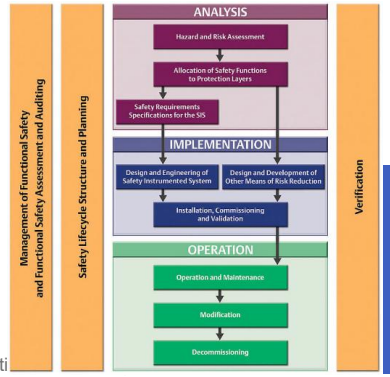
2. 什么是安全完整性？SIL不仅仅是PFD!

- **系统性安全完整性** – 与SIS在危险失效模式下、与系统性失效有关的、安全完整性的一部分。系统性安全完整性通常不能被量化 (有别于硬件安全完整性)。 (IEC61511-1:2016术语3.2.82)

✓ 所谓的“系统性（Systematic）失效”，也就是“体系性失效”，是在设计、建造、操作和维护过程中，“人为因素”导致的失效。其失效的原因包括规程、依据的文档，以及人员能力等。

- **很显然，邦斯菲尔德油库中的“高液位检测开关（HLS）”失效，属于系统性失效，只能通过建立严格的管理体系、规程，以及提高人员的能力解决。在SIL验证（PFDavg计算）中反映不出这些问题！**





3. 安全生命周期（SLC）

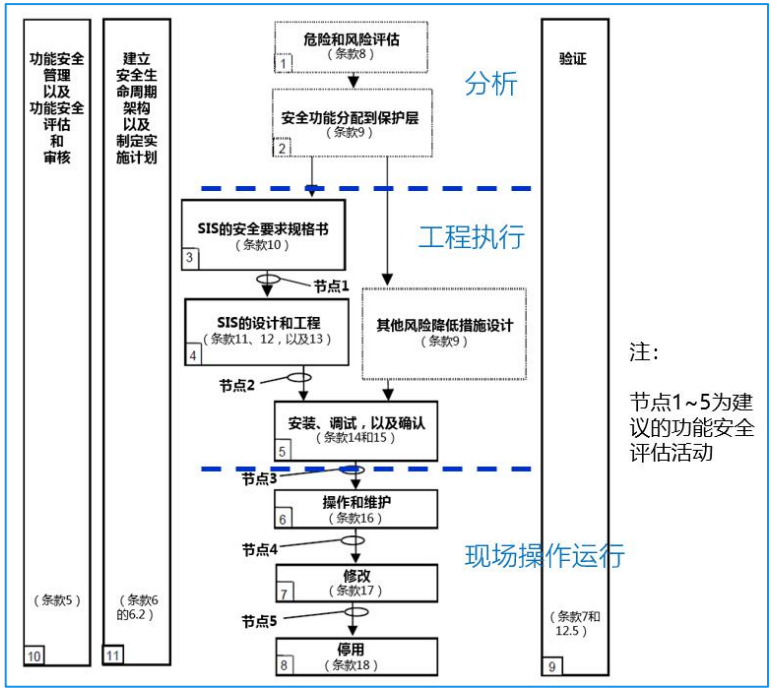
- SIS功能安全标准GB/T21109（IEC61511）是在数十年工程实践的基础上，形成的一套方法论。
- 该标准的体系，围绕两个基本概念：**SIS的安全生命周期（SLC）**和**安全完整性等级（SIL）**。

- SLC分为三个阶段：

✓ **分析阶段**：通过HAZOP/LOPA等方法，确定SIL的目标值（定级）。
✓ **工程实施阶段**：以SIL为指针，设计、建造SIS系统，使安全性能目标要求转化为SIS的内在品质。
✓ **操作阶段**：确保SIL目标得以持续保持。

❑ SLC并非简单的工作流程描述，它为工作流程规定了一套质量管理体系，目的是：*避免或控制系统性失效。*
❑ SLC三个阶段并非割裂的，它们之间存在内在的、有机关联，体现SIL的价值传递。
❑ **传统的防溢流设计，例如邦斯菲尔德的HLS关断，基于经验；今天通过HAZOP/LOPA等系统性的方法，就可以实现：**

✓ **恰如其分地确定安全要求，避免“过设计”或者“欠设计”。**
✓ **优化SIS/SIF与其他保护层之间的关系。**



安全生命周期（SLC， IEC61511）

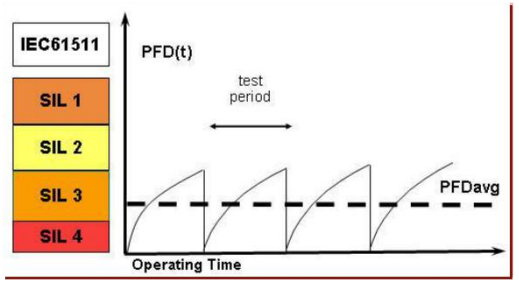
4. 检验测试（Proof Test）

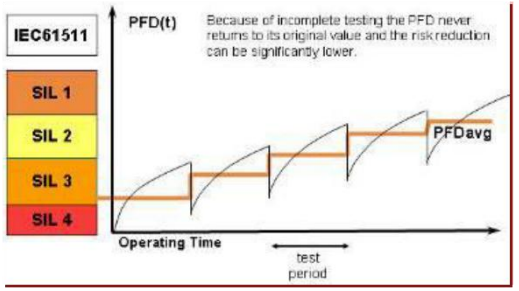
- **检验测试** - 为检测SIS中隐蔽的危险失效而进行的周期性测试，如有必要，通过维修使系统恢复到"如新"状态，或者尽可能接近这种状态。（IEC61511-1:2016 术语3.2.56）

- "（七）加强化工企业安全仪表系统操作和维护管理……要按照符合安全完整性要求的检验测试周期，对安全仪表功能进行定期全面检验测试，应详细记录测试过程和结果……"
（原国家安监总局安监总管三【2014】116号文）

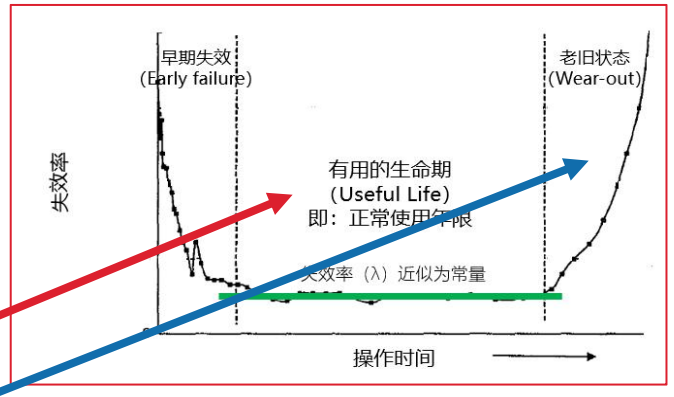
- 检验测试是确保SIS安全性能最重要的维护活动，是SIL验证（PFDavg计算）重要参数之一。

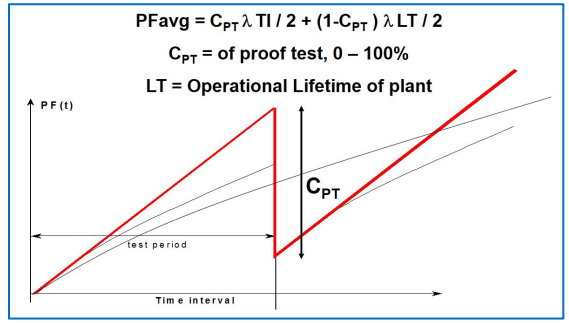
- 检验测试有三个关注点：
  - ✓ 时间间隔（TI）
  - ✓ 检验测试的覆盖率（C_{PT}）
  - ✓ 适时调整维护策略





ISA-TR84.00.03-2012



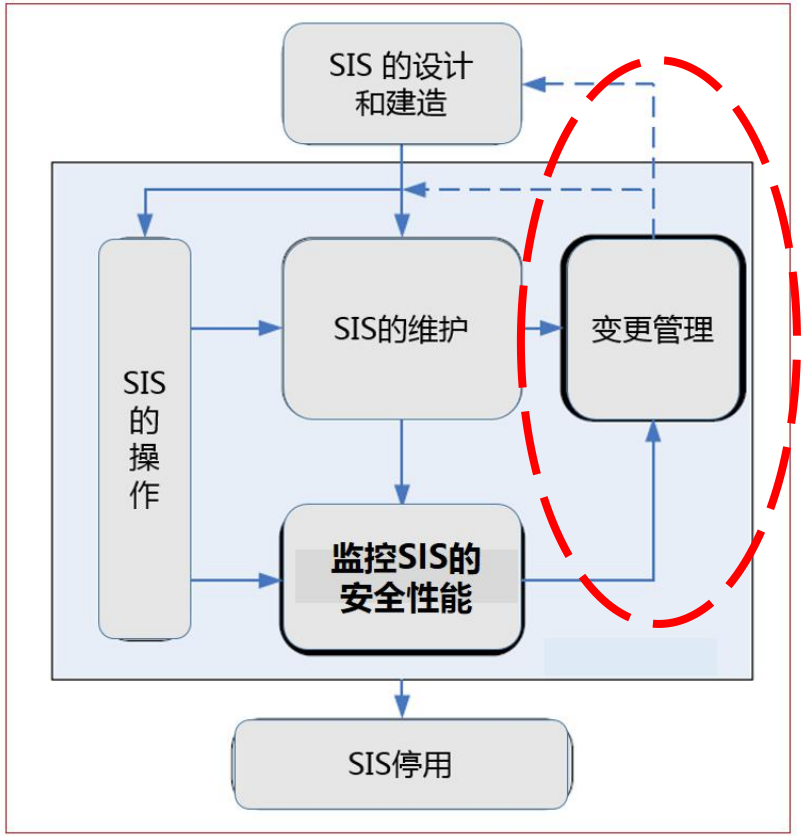


PFDavg计算

仪表设备处于"老旧状态"，要适时调整维护策略，此时PFDavg计算已没有实质意义。

5. 变更管理（MOC）

- 变更管理是SIF/PL 核心属性之一
- 建立变更管理流程时，进行”影响分析“是重要的步骤。



SIS操作阶段的活动及其关系（摘自挪威SINTEF）

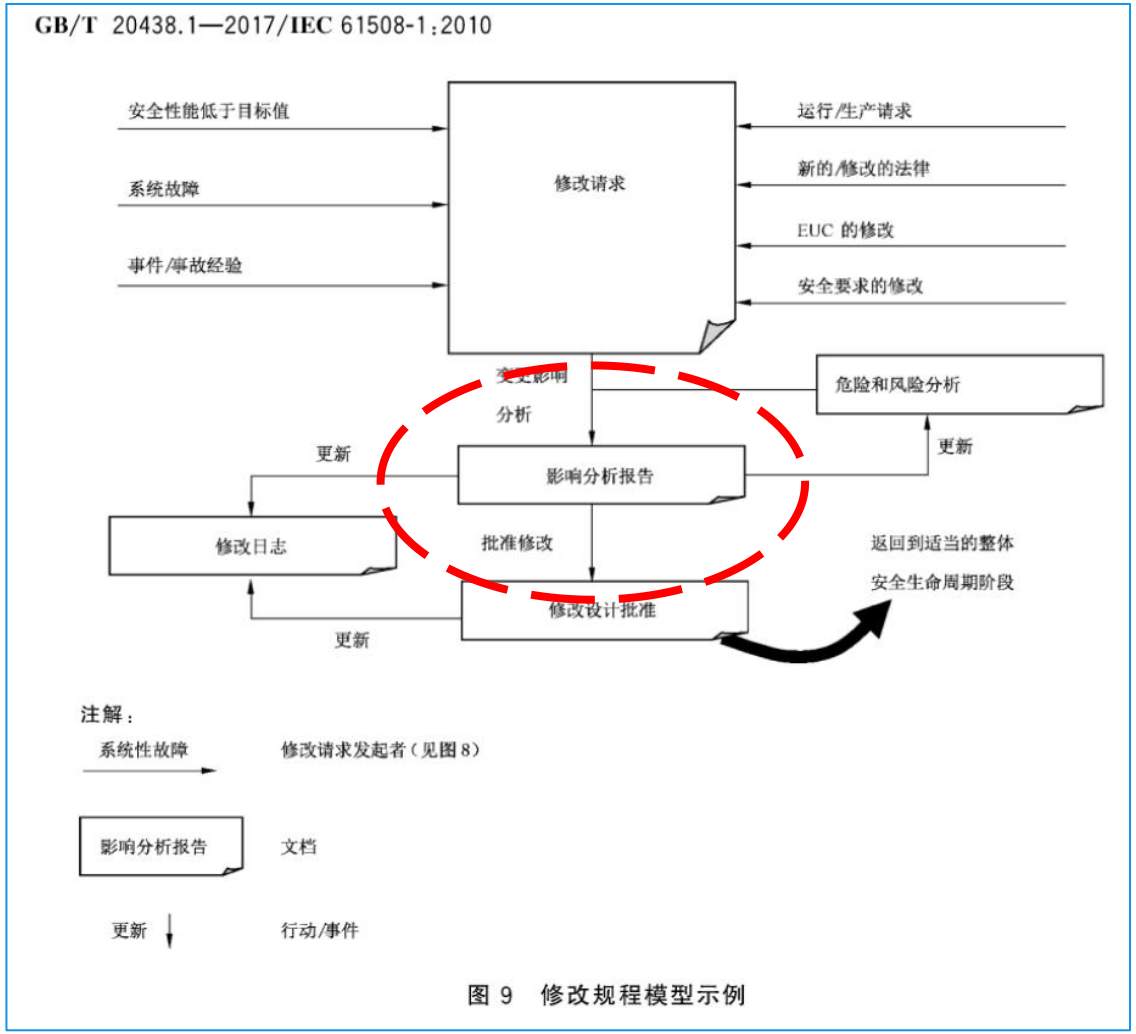


图 9 修改规程模型示例

6. SIL认证与以往使用（Prior Use）

- IEC61511-1:2016 条款11.5.2.1 - 选择用做SIS的组成部分、并具有特定SIL的仪表设备，应遵循IEC61508关于硬件和软件的要求；或者根据需要，遵循本标准的“以往使用”规则。
  注：根据IEC 61508 评估的设备，应按照“系统能力（SC）”要求使用。

- **以往使用** - 用户根据以往在类似操作环境中的操作经验，对设备适合在SIS中使用，并能满足所需的功能和安全完整性要求进行的书面评估。（IEC61511-1:2016 术语3.2.51）

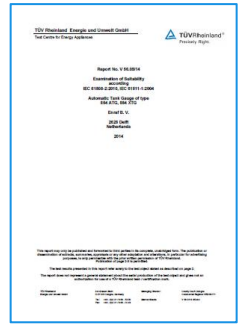
- “（七）加强化工企业安全仪表系统操作和维护管理…… 要规范安全仪表系统相关设备选用，建立安全仪表设备准入和评审制度以及变更审批制度，并根据企业应用和设备失效情况不断修订完善。”（原国家安监总局安监总管三【2014】116号文）

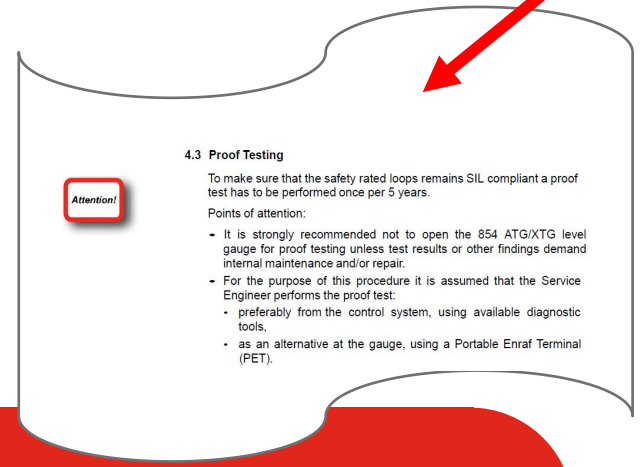
- 目前，SIS设备选型普遍看重基于IEC61508的SIL认证。认证产品有三个必要文件：证书、测试报告，以及安全手册（Safety Manual）。

- **未来SIS设备选型应立足于SIL认证与“以往使用”相结合。**

用于AOPS的 Honeywell Enraf Radar / Servo

TÜVRheinland
SIL-2 approved





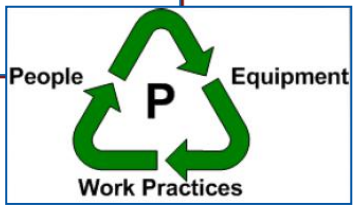
7. 安全完整性管理

- CCPS/ISA技术指南，大都沿用"机械完整性（MI - Mechanical Integrity）"概念。

- SIS的MI管理，主要关注**SIS的现场操作和维护**阶段，其目标是确保SIS的功能安全得到持续保持。

- MI – 确保设备以安全的方式检查、维护、测试、以及操作，并与分配的风险降低要求保持一致的**管理体系**。

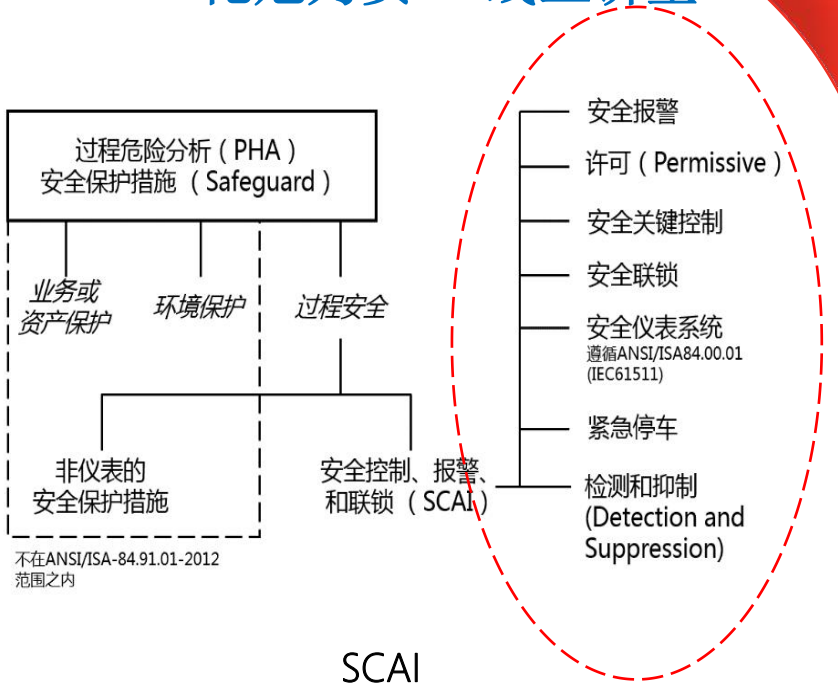
- SIS的安全完整性管理有两个方面：
  1. 通过设计和建造，将可靠性融入到SIS中；
     - ✓ 在**分析**和**工程**阶段，确保将**独立性**、**完整性**、**功能性**，以及**可靠性（过程可用性）**成为SIS的**内在品质。**
  2. 通过检验、测试、维护，以及运行状态监控，确保SIS的安全完整性得以保持，并在出现失效和性能降级时，及时成功地予以校正。
     - ✓ 在SIS**操作和维护**阶段，将**可审核性**、**访问的权限管理**、MOC 融入到管理体系中。
     - ✓ 简言之：人员有能力、做事有章法（计划、规程）、结果有跟踪确认，并不断改进、提高管理水平。



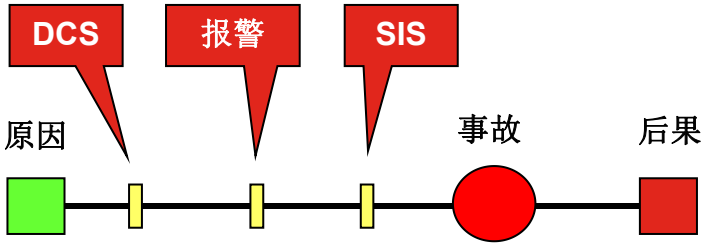
邦斯菲尔德油库事故，不仅仅是设备问题，也是管理体系和人员能力的缺失！

8. SCAI的安全管理

- SCAI - 通过**仪表和控制方式**实施的过程安全保护措施，针对特定的场景，提供所需的风险降低，实现或维持工艺过程的安全状态。(ANSI/ISA 84.91.01 - 2012)；
- SCAI是**安全控制**、**报警**、**联锁**的缩写（Safety Control, Alarm, and Interlock）。简言之，**SCAI就是在LOPA分析中确定的仪表和控制防护层**：
  - ✓ 安全仪表功能（SIF）
  - ✓ BPCS认定为PL的控制回路、联锁、或者报警
  - ✓ 独立的安全报警
- SIF之外的BPCS、独立报警PL，与SIF具有相同的属性，相同的角色，因此，要参照SIF进行管理：
  - ✓ 相关文档，要与其他仪表系统明确区分。
  - ✓ 根据良好的工程实践原则，对其进行周期性检验测试；纳入安全完整性管理体系。
  - ✓ 对其进行的检验和测试，要留存完整的书面记录。
- “（九）加强过程报警管理，……，与安全仪表功能安全完整性要求相关的报警可以参照安全仪表功能进行管理和检验测试。
  （十）加强基本过程控制系统的管理，与安全完整性要求相关的控制回路，参照安全仪表功能进行管理和检验测试，……”
  （原国家安监总局安监总管三【2014】116号文）



SCAI



仪表和控制PL

9. 培育安全文化

- 什么是安全文化？安全文化是企业文化的一部分，是雇员在工作场所共享的、与安全有关的态度、信念、认知，以及价值观，它体现了工作的行为和方式。

- 邦斯菲尔德油库事故调查报告、美国BP得克萨斯炼油厂事故的“贝克报告，2007”，都阐述了培育安全文化的重要性。

- 智慧的安全文化（英文四个E）：

❑ 把安全作为核心价值（Establish safety as a core value）
❑ 向所有人授权（Empower everyone），即安全生产，人人有责
❑ 鼓励安全倡导者，排除反对者（Elevate safety advocates and eliminate opposition）
❑ 在所有行动中，体现对安全的承诺（Exhibit a commitment to safety in all actions）

- 安全水平的提升是日积月累、不断完善的过程：
  - ✓ 短期目标：根据116号文等规定的工作节点要求，完成评估和整改。
  - ✓ 中期目标：完善管理体系建设。
  - ✓ 长期目标：培育安全文化。

- *新的理念*
- *新的解决方案*
- *新的技术*

谢谢大家的线上参与和支持！ 请批评指正！