安全仪表系统设计应用

黄步余

2010.4

国内石化行业发展概况

- 石化行业处于景气时期，原油价格波动。
- 石化产品需求增长，生产成本提高。
- 世界级规模石化项目建设并投产运行。
- 石化产品产量和质量提高，自给能力增强。
- 石化企业面临机遇和挑战，强化现代化企业管理。
- 降低生命周期成本，节能，环保，获取大的利润。

新建大型炼油项目

- 8 MTA 海南炼油项目
- 8 MTA 福建炼化一体化项目
- 10 MTA 青岛炼油项目
- 10 MTA 独山子炼化一体化项目
- 10 MTA 天津炼化一体化项目
- 10 MTA 抚顺炼化一体化项目
- 10 MTA 钦州炼油项目
- 12 MTA 惠州炼油项目

新型大型乙烯项目

- 900 KTA 上海赛科乙烯项目
- 800 KTA 广东惠州乙烯项目
- 700 KTA 扬巴一体化乙烯项目
- 1,000 KTA 茂名石化乙烯项目（扩建）
- 800 KTA 福建炼化一体化项目
- 1,000 KTA 天津炼化一体化项目
- 1,000 KTA 独山子炼化一体化项目
- 1,000 KTA 抚顺炼化一体化项目
- 1,000 KTA 镇海乙烯项目
- 800 KTA 武汉乙烯项目

控制及信息管理集成系统的总目标

- 健康、安全及环境保护有可靠保证；
- 高质量的过程测量，调节控制，友好人机界面；
- 仪表及控制系统故障引起非计划停车最少；
- 提供准确、无缝的信息数据（实时及历史）；
- 提供维修计划，存量控制和采购计划；
- 提供生产调度优化，满足市场需求；
- 工厂、供应商和客户信息集成互联电子商务平台；
- 降低生命周期成本，获取大的利润。

石油化工企业面临的安全挑战

- 生产装置安全评估；
- 防止非计划停车；
- 人员伤害、经济损失、环境污染；
- 缩短恢复生产时间；
- 保障人身和设备安全。

石油化工企业安全解决方案

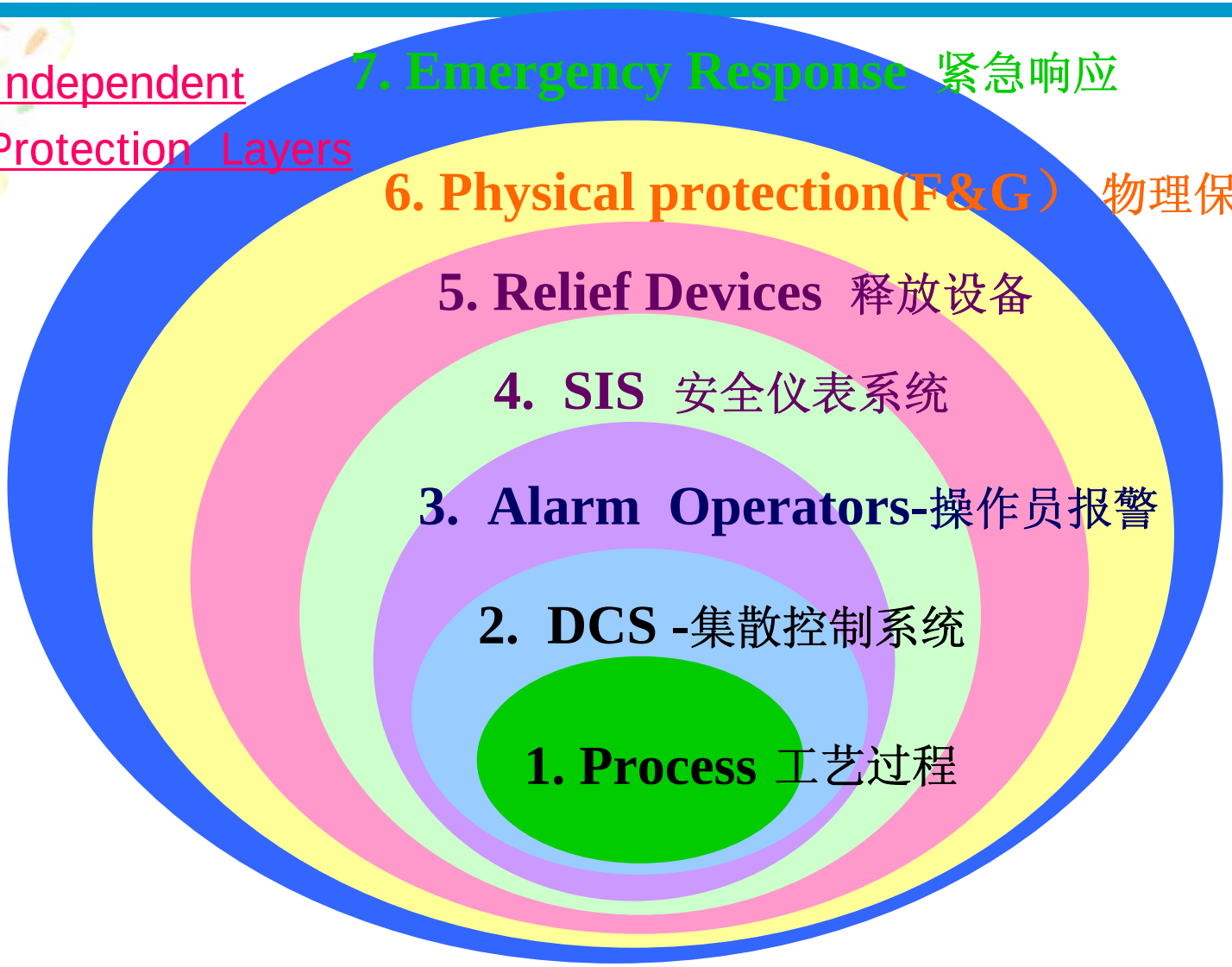
- 安全评估 （安全生命周期，风险评估，功能安全管理）；
- 风险预防 （对人身、设备及环境的损害，重复事件减到最少）；
- 安全仪表系统 （减少不必要的停车，故障原因分析，损失减少）；
- 快速恢复生产 （缩短恢复生产时间，避免相同故障重复发生）。

石油化工企业安全生命周期

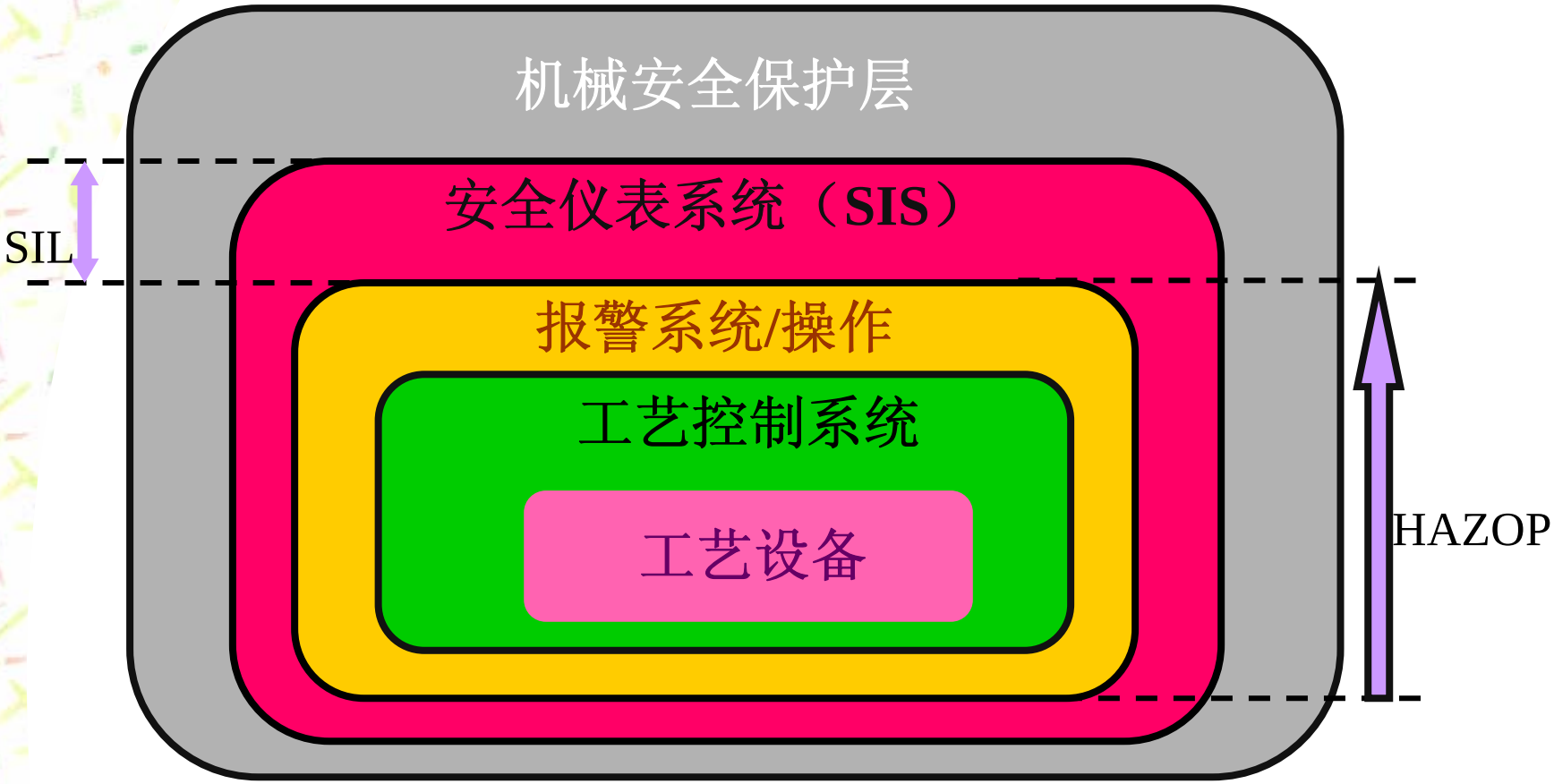
- 风险评估
- 安全功能分配
- 安全需求规格
- 设计及其工程
- 安装、开车、确认
- 操作维护
- 修改或处理
- 确认
- 功能安全管理

石油化工企业安全保护级别

- Independent
- Protection Layers



SIS系统对风险的控制



危险与可操作性审查
(HAZard and Operability study-HAZOP)

- 对生产装置的安全性和操作性进行设计审查;
- 根据标准、工艺参数等按工艺流程（PID）进行系统分析，正常/非正常工况可能出现的问题、产生的原因、可能导致的后果及应采取的措施;
- 有生产经验、工艺、安全、设备、电气、仪表、环保、经济等专家共同研究;
- HAZOP作业流程:选择研究节点→选择工艺参数→选择引导词→发现有价值的偏差→分析产生偏差的原因、后果及现有措施→评估风险→提出控制风险建议。

风险合理化控制(ALARP)
(As Low As Reasonable Practice)

- 根据风险矩阵识别关键设施和操作，位于高风险区的设施研究；
- 降低风险设施投资的合理性的研究；
- 方案投资费用与风险的比选优化。

安全保护级别分析

- 集中研究后果严重和高频发事件；
- 考虑识别的引发事件和原因；
- 确认对各引发事件有效的保护层；
- 有效分配降低风险的资源；
- 确定安全仪表系统（SIL）等级。

安全仪表系统(SIS)

安全仪表系统（Safety Instrumented System - SIS)

〔仪表保护系统(Instrument Protection System- IPS）〕

〔安全联锁系统（Safety Interlocking System - SIS）〕

〔紧急停车系统（Emergency Shut-Down System - ESD）〕

仪表系统用于实现1个或多个安全仪表功能，安全仪表系统包括传感器（Sensor）、逻辑运算器（Logic solver）和最终执行元件(Final element）。

目前SIS采用标准规范

- IEC 61508 Functional Safety of electrical / electronic /programmable electronic safety-related system
- IEC 61511 Functional Safety Instrumented systems for the Process Industry Section
- IEC 61131 Programmable Controllers
- ANSI/ISA-84.01 Application of Safety Instrumented Systems for the Process Industries
- DIN V 19250 Programmable Safety System
- SH/T3018 石油化工安全仪表系统设计规范（中华人民共和国石油化工行业标准）

  Design code for safety instrumented system in petrochemical industry

SIS功能及要求

- 安全仪表系统（SIS）在生产装置的开车、停车阶段，运行以及维护操作期间，对人员健康、装置设备及环境提供安全保护。无论是生产装置本身出现的故障危险，还是人为因素导致的危险以及一些不可抗拒因素引发的危险，SIS系统都应立即作出正确反应并给出相应的逻辑信号，使生产装置安全联锁或停车，阻止危险的发生和事故的扩散，使危害减少到最小。
- SIS系统应具备高的可靠性（Reliability）、可用性（Availability）和可维护性（Maintainability）。当SIS系统本身出现故障时仍能提供安全保护功能。

SIS与DCS区别

- DCS用于生产过程的连续测量、常规控制（连续、顺序、间歇等）、操作控制管理，保证生产装置的平稳运行；

  SIS用于监视生产装置的运行状况，对出现异常工况迅速处理，使危害降到最低，使人员和生产装置处于安全状态；

- DCS是“动态”系统，始终对过程变量连续进行检测、运算和控制，对生产过程进行动态控制，确保产品的质量和产量；

  SIS是“静态”系统，正常工况时，始终监视生产装置的运行，系统输出不变，对生产过程不产生影响；非正常工况时，按照预先的设计进行逻辑运算，使生产装置安全联锁或停车；

- SIS比DCS在可靠性、可用性上要求更严格，IEC61508、IEC61511、ISA S84.01、SH/T3018强烈推荐SIS与DCS硬件独立设置。

安全（SIL）等级 Safety Integrity Level

IEC61508	DINV 19250	说明
SIL 1	1,2	财产和产品一般保护
SIL 2	3,4	主要财产和产品保护，可能损害人
SIL3	5,6	保护人员
SIL 4	7	灾难性伤害

危险等级

- I 级　无法忍受的严重危险（Intolerable risk）
- II级　较严重危险（Undesirable　risk）
- III级　可以忍受的危险（Tolerable　risk ）
- IV级　轻微的危险（Negligible　risk）

危险性分组

危险等级		说明
因果关系（C）	C1	轻微伤害
	C2	严重伤害，会导致1人或多人死亡
	C3	造成多人死亡
	C4	造成很多人死亡
危险出现的频率	F1	长期出现
	F2	经常出现
避免危险事件发生的可能性	P1	在一定条件下可能出现
	P2	有可能出现
意外事故发生的可能性	W1	几乎不可能
	W2	有可能
	W3	很可能

SIS系统设计选用原则

- SIS独立于过程控制系统(PCS），独立完成安全保护功能。当过程达到预定条件时，SIS系统动作使过程转入安全状态；
- 根据对过程危险性及可操作性分析，人员、过程、设备及环保要求，确定SIS的功能等级；
- 设计成故障安全型；
- 采用经TUV安全认证的PLC系统；
- 具有硬件、软件诊断和测试功能；
- 构成中间环节最少；
- 传感器、最终执行元件宜单独设置；
- 能和DCS、MES等进行通信；
- SIS实现多个单元保护功能时，其公用部分应符合最高安全等级要求；

SIS传感器设计选用

- 独立设置原则：
  - 1级　SIS传感器可与DCS共用；
  - 2级　SIS传感器宜与DCS分开；
  - 3级　SIS传感器应与DCS分开；
- 冗余设置原则：
  - 1级　SIS传感器可采用单一的传感器；
  - 2级　SIS传感器宜采用冗余的传感器；
  - 3级　SIS传感器应采用冗余的传感器；
- 冗余选择原则：
  - 保证系统的安全性时，采用“或”逻辑结构；
  - 保证系统的可用性时，采用“与”逻辑结构；
  - 当系统的安全性和可用性均需保证时，采用“三取二”逻辑结构；
- 传感器宜采用隔爆型的变送器（压力、差压、差压流量、差压液位、温度），不宜采用开关型传感器；传感器由SIS系统供电。

SIS逻辑运算器设计选用

- SIS逻辑运算器：可编程序电子系统，混合系统；
- 可编程电子系统用于I/O点较多,逻辑功能复杂，与DCS、MES通信等场合；
- 可编程电子系统是经TUV认证的PLC系统；
- 独立设置原则：1级SIS逻辑运算器宜与DCS分开；
  2级SIS逻辑运算器应与DCS分开；
  3级SIS逻辑运算器必须与DCS分开；
- 冗余设置原则：1级SIS可采用单一的逻辑运算器；
  2级SIS宜采用冗余或容错逻辑运算器；
  3级SIS应采用冗余容错逻辑运算器；

SIS执行元件设计选用

- 执行元件：　　气动切断阀（带电磁阀），气动控制阀（带电磁阀）；

- 独立设置原则：1级 SIS 阀门可与DCS共用，应确保SIS优先于DCS动作；
  2级SIS阀门宜于DCS分开；
  3级SIS阀门宜于DCS分开；
- 冗余设置原则：1级 SIS 可采用单一阀门；
  2级宜采用冗余阀门；如采用单一阀门，电磁阀宜冗余配置；
  3级宜采用冗余阀门；可采用一个控制阀和一个切断阀；
- 电磁阀设置原则：电磁阀应采用长期带电，低功耗，隔爆型；由SIS系统供电。

SIS工程设计中注意的问题

- I/O模件应带光/电或电磁隔离，带诊断，带电插拔；
- 来自现场的三取二信号应分别接到三个不同的输入卡；
- 现场变送器或执行元件应由SIS系统供电；
- 当变送器信号同时用于SIS、DCS时，应先接到SIS系统后接到DCS系统；
- SIS 不宜采用现场总线通信方式；

SIS工程设计中注意的问题

- 负荷不应超过50%；
- 电源应冗余配置；
- 采用等电位接地。
- 传感器及执行元件，正常时应带电（励磁）；非正常时应失电（非励磁）；
- 电磁阀冗余配置时，有两种连接方式：

  并联连接 -- 可用性好；

  串联连接 -- 安全性好。

SIS维护

- 预防性维护到预测性维护 （工业以太网、HART等）；
- 提高维护效率和自动化程度 （基于工具软件、管理软件等）；
- 维护工作从现场移到控制室 （现场数据采集到服务器、远程维护）；
- 预防计划外的停车 （预测诊断功能、仪表工作情况）。

SIS质量保证

- 安全等级认证（SIS系统相关I/O 、CPU、通信等）
- 防爆等级认证
- ISO 9000质量认证
- CE 标志
- 主要部件的产地
- 质量保证程序

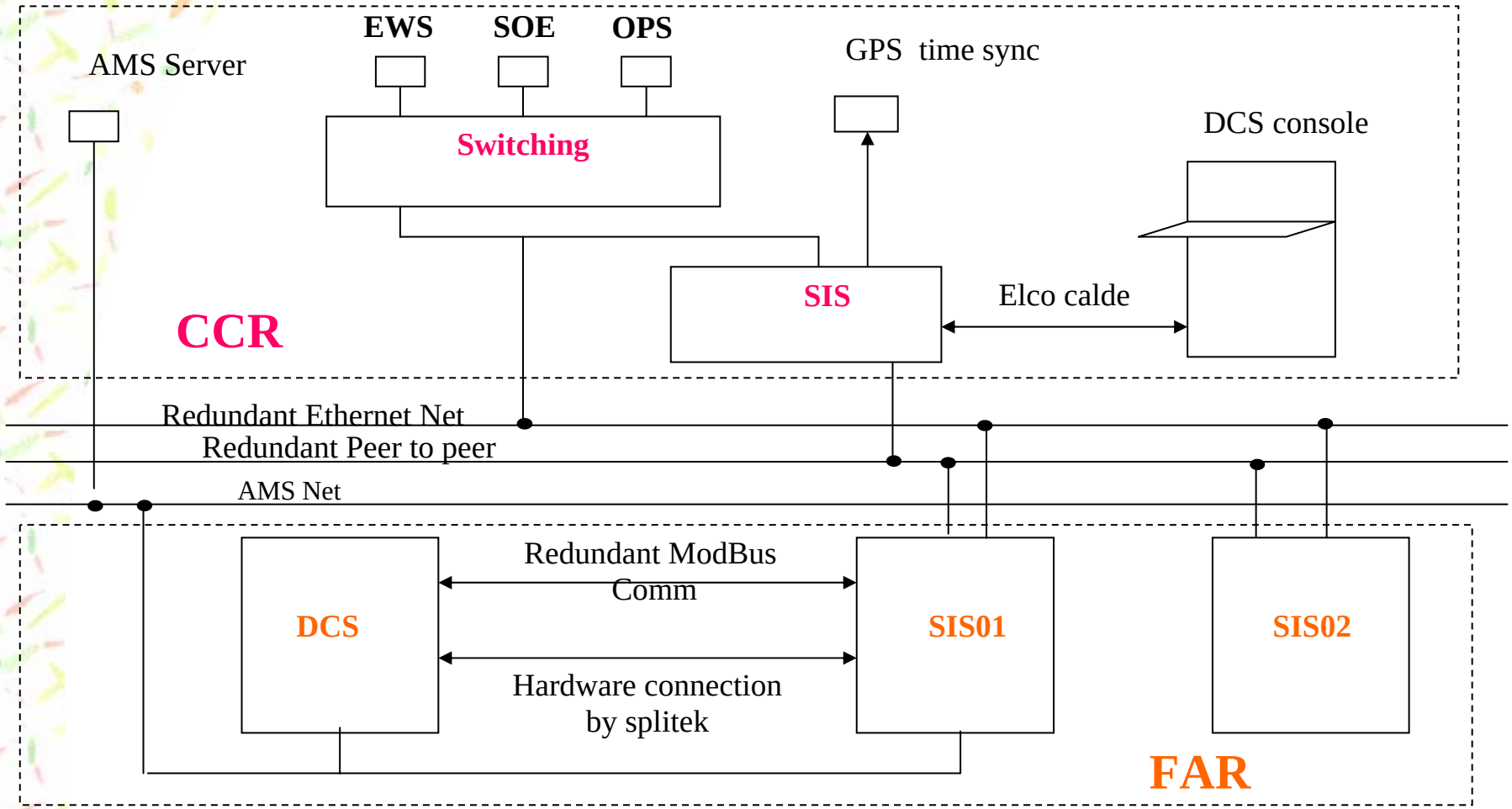
SIS故障分析

（在生命周期阶段）

- 技术规格 44 %
- 调试后变更 20 %
- 设计和实施 15 %
- 操作和维护 15 %
- 安装和调试 6 %

摘自<Health & Safety Executive HSE-UK>

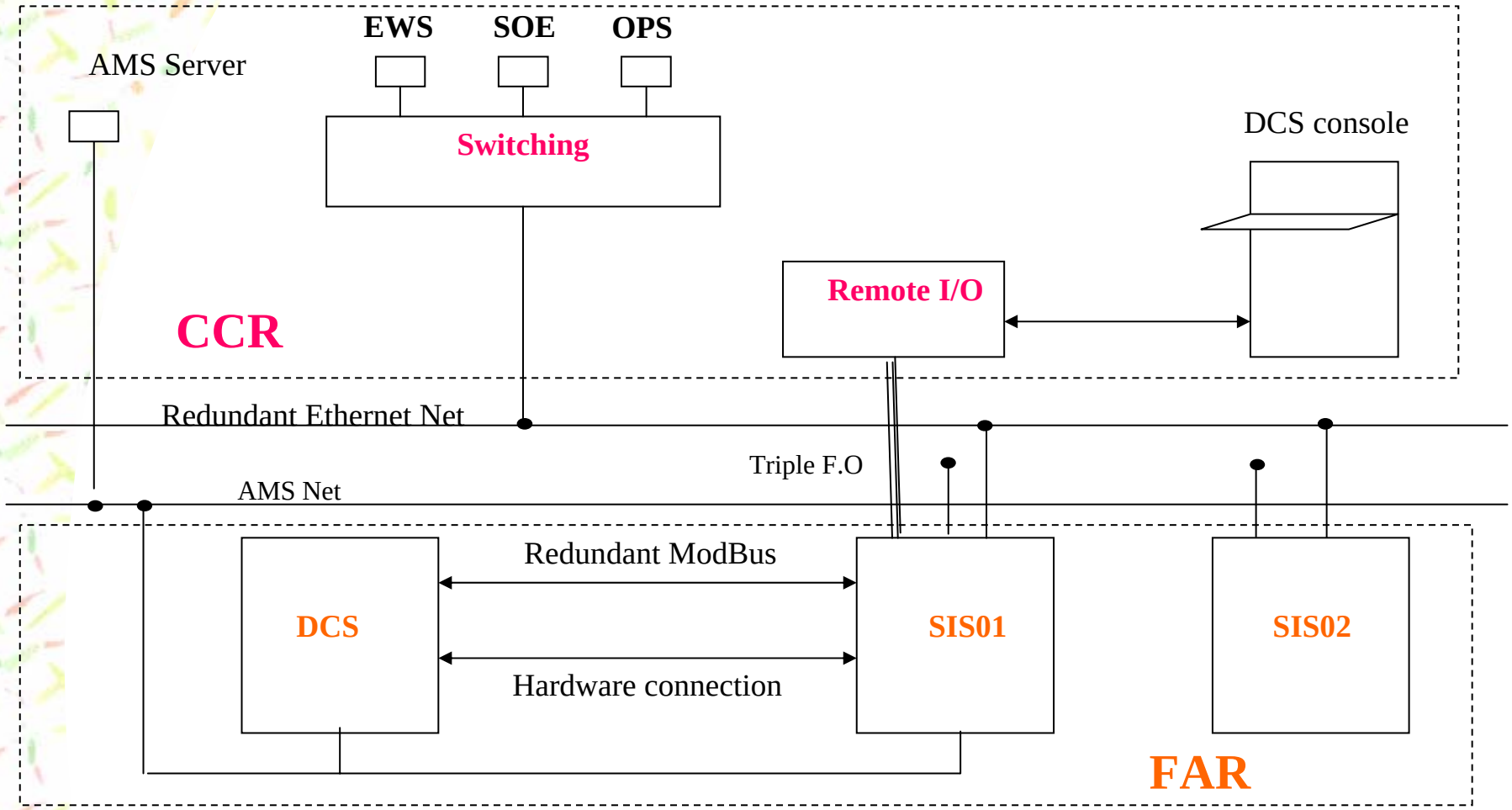
SIS系统网络原理图(1)



注：在CCR内，每个装置用一个独立的SIS系统

。

SIS系统网络原理图(2)



注：在CCR内，每个SIS系统对应一个Remote I/O系统。

谢　　谢！