INDUSTRIAL SCIENTIFIC CORPORATION
英思科传感仪器（上海）有限公司

SIL-Safety Integrity Lever (安全完整性等级)基本概念和知识培训课程

SILSafety Integrity Lever (安全完整性等级)基本概念和知识

The questions???

What is SIL?

安全完整性 Safety Integrity

在规定的时间内、在所有规定的条件下,成功 实现所要求的安全功能的平均概率

安全完整性等级：SIL(Safety Integrity Level)

定义：一种离散的等级，用于规定分配给SIS的安全仪表功能的完整性要求

作为衡量安全功能重要因素，是安全系统的核心.

代表着使过程风险降低的数量级

What is SIL represent?

SIL

Safety Integrity Level	Probability of Failure Demand Per Year (Low demand mode of operation)	Risk Reduction Factor
SIL 4	How to calculate SIL? $>=10^{-5}$ to $<10^{-4}$	100,000 to 10,000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10,000 to 1,000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1,000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

Why use SIL concept?

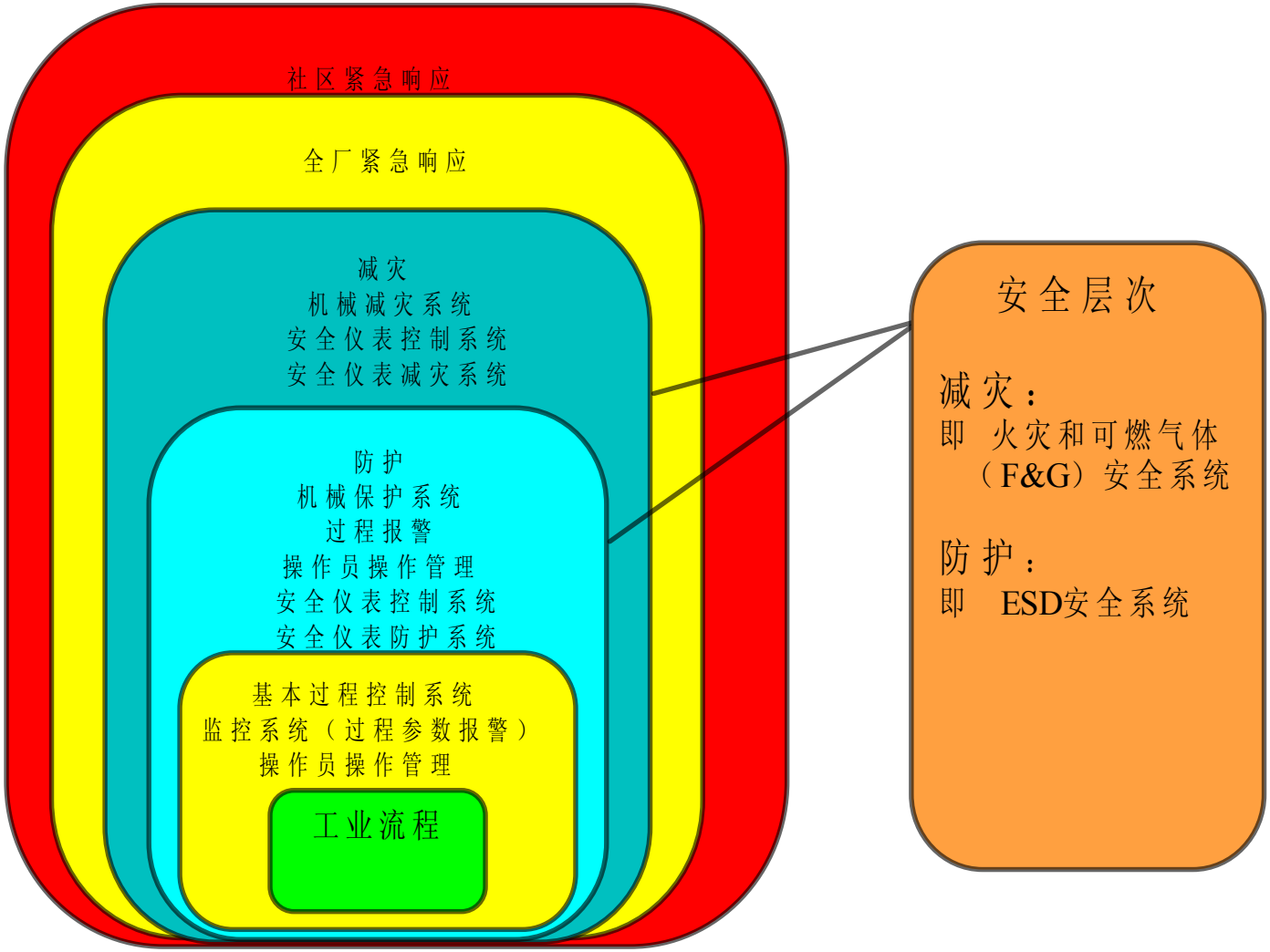
安全对经济,环境和人类自身的健康发展之至关重要.因而安全相关系统 Safety Related System 被广泛应用。

安全相关系统监视生产过程的状态，在危险条件出现时采取相应措施，防止危险环境事件发生，避免潜在危险对人身，设备，环境造成伤害或减轻其后果造成的损失。

安全相关系统是保障生产安全的重要措施，应能在危险发生时正确执行其安全功能。但由于系统结构，硬件，软件及周围环境等原因，安全系统本身会不可避免地存在着安全性问题。

安全系统功能安全主要的研究对象是以保护人身财产安全为目的与安全相关的保护系统，其包括安全控制系统和安全保护系统两大类。随着微电子技术、计算机技术和总线技术以及无线通讯技术的迅速发展，这些技术被越来越多地应用到安全系统以实现安全功能。而安全系统本身，由于无法预计的失效而导致的危险引起了科学家们的注意。由于上世纪七十年代以来在欧美发生了多起工业事故都与安全相关系统失效有关，所以人们意识到安全相关系统的功能安全的重要性。

如何降低风险？ 安全保护层



What is the basic standard for SIL?


IEC
Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

IEC61508

IEC 61508

IEC61508标准，名为《电气/电子/可编程电子安全系统的**功能安全**》,该标准分七部分，涉及1000多个规范。

IEC61508针对由电气/电子/可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统(E/E/PE)的整体安全生命周期，建立了一个基础的评价方法。

IEC 61508主要目标：

1) 对所有的包括软、硬件在内的安全相关系统的元器件生命周期范围提供一个安全监督的系统方法。

2) 提供一个确定安全相关系统安全功能要求的方法。

3) 建立一个基础标准，使其可直接应用于所有工业领域，同时，亦可指导其他领域的标准，使这些标准的起草具有一致性（如基本概念、技术术语、对规定安全功能的要求等）。

4)针对以电子为基础的安全系统提出一个一致的、合理的技术方案，统筹考虑 单独系统(如传感器、通信系统、控制装置、执行单元等)中元件与安全系统组合的问题。

在IEC 61508中将安全关联系统定义为一个履行为EUC(受控设备)实现一个安全状态或为EUC 维持一个安全状态所必需要求的**安全功能**的系统。

安全功能将由E/E/PE安全关联系统来履行。

IEC61508 功能安全相关主要术语

- **安全功能** Safety Function

  针对特点的危险事件，为达到和保持过程的安全状态，由SIS、其他技术安全相关系统或外部设施实现的功能

功能安全 Functional Safety

要求系统本身的安全性（如仪表的本质安全，无辐射等）

安全功能是完整的、可靠的（功能是安全的）

安全仪表系统 SIS(Safety Instrumented System)

用于实现一个或多个安全功能的仪表及仪表系统

包括：传感器、逻辑解算器和最终单元。 SIS 广义/狭义

安全仪表功能 SIF((Safety Instrumented Function)

SIS系统 **所实现的 安全功能。**

什么是功能安全？功能安全是与EUC或EUC控制系统有关的整体安全的组成部分,取决于电气/电子/可编程电子（E/E/PE）安全系统、其它技术安全系统和外界风险降低设施功能的正确行使。

如何来正确行使？主要内容包括管理和技术两方面。既在技术上保证E/E/PE安全系统、其它技术安全系统和外界风险降低设施在需要时能执行安全功能，从另一方面，在管理上保证E/E/PE安全系统、其它技术安全系统和外界风险降低设施在需要时能执行安全功能。

在过程工业领域如石化，化工等，是用安全仪表系统来表述安全相关系统。既SIS(Safty Instrumented Systems)用来实现一个或几个仪表安全功能的仪表系统,可以由传感器、逻辑解算器和终端元件的任何组合组成.

仪表安全功能(Safty Instrumented Function)就是具有某个特定SIF的,用以达到功能安全的安全功能,它既可以是安全保护系统,也可以是安全控制系统.

What is SLC?

IEC 61508 最核心的概念和内容

Safety Life Cycle　　SLC

整体安全生命周期

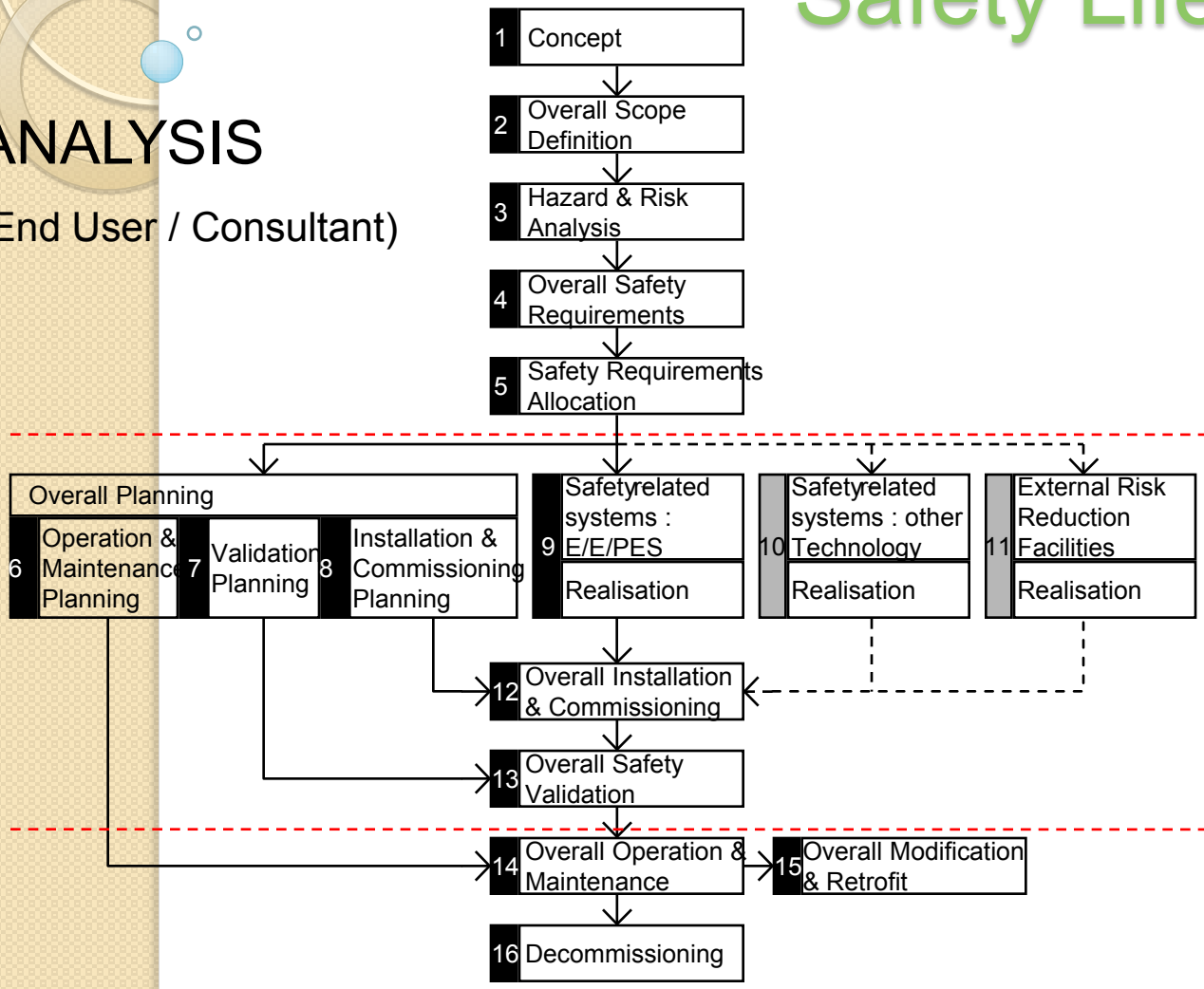
整体安全生命周期包括：概念、整体范围定义、危险和风险分析、整体安全要求、安全要求分配、整体的安全计划编制（操作和维护计划、整体安全确认计划、整体安装和试运行计划）、E/E/PES安全相关系统的实现、其他安全相关系统的实现、外部危险降低设施的实现、整体安装和试运行、整体安全确认、整体操作维护和维修、整体修改和改型、停用和处理。

在整体安全生命周期的各阶段都有各自相关的功能安全活动和要求。其中E/E/PES安全相关系统的实现包括两个部分既硬件的实现和软件的实现，这个阶段是通过设计满足系统的SIL要求。所以，我们说功能安全是设计出来的。

Key Concept: Safety Life Cycle

ANALYSIS

(End User / Consultant)



REALIZATION

(Vendor / Contractor / End User)

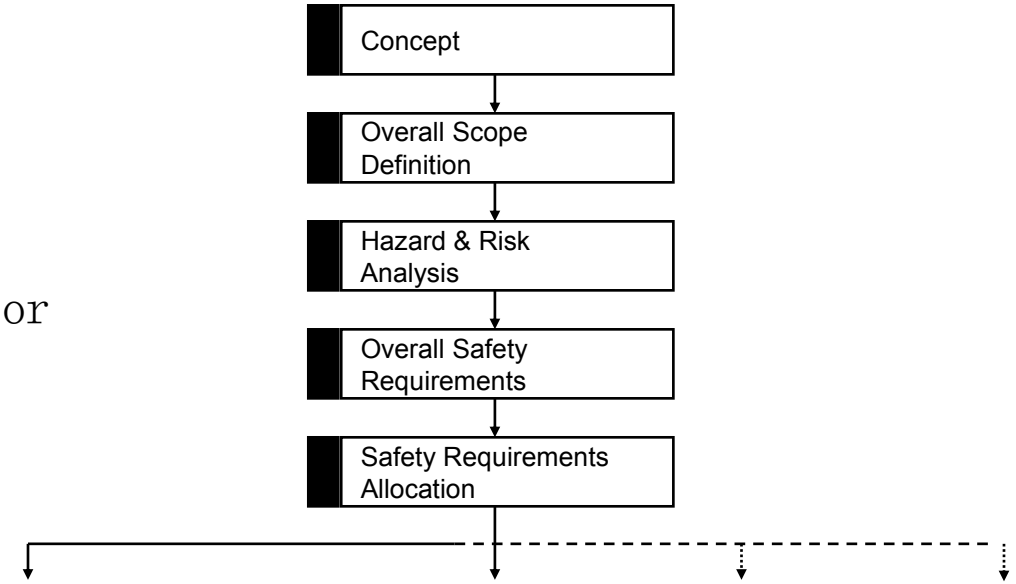
OPERATION

(End User / Contractor)

SLC Analysis Phase

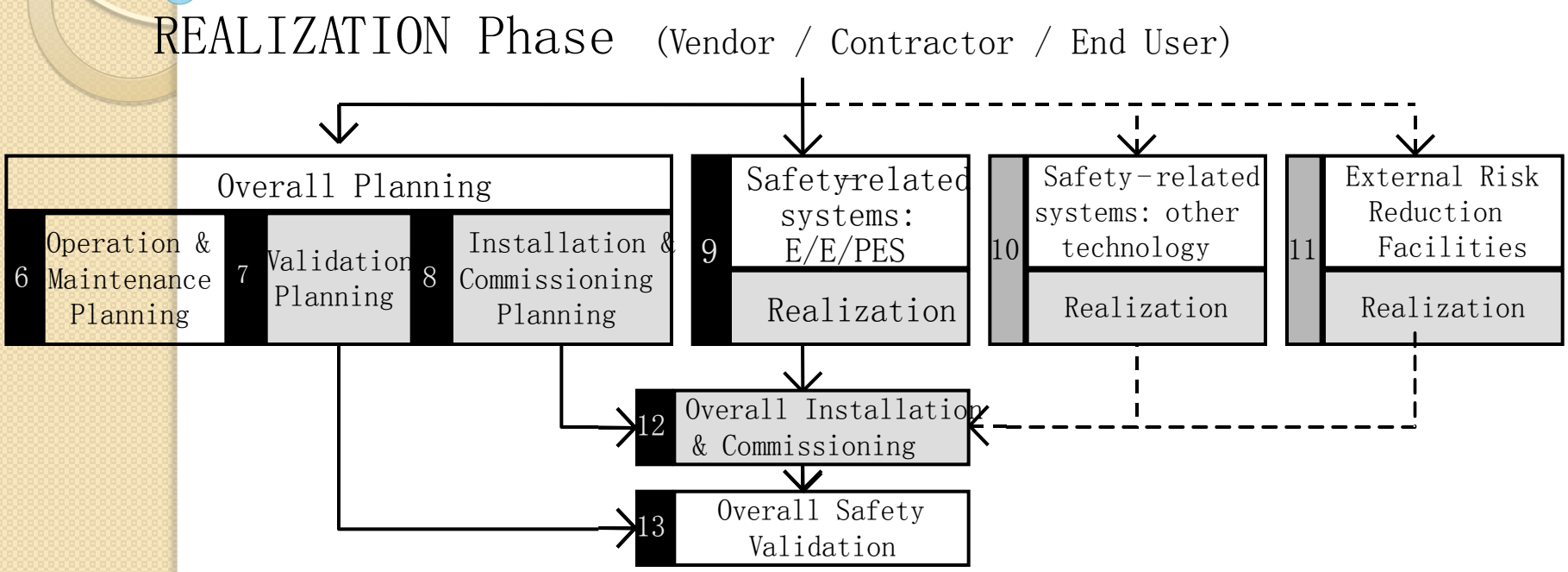
ANALYSIS Phase

(End User / Contractor / Consultant)



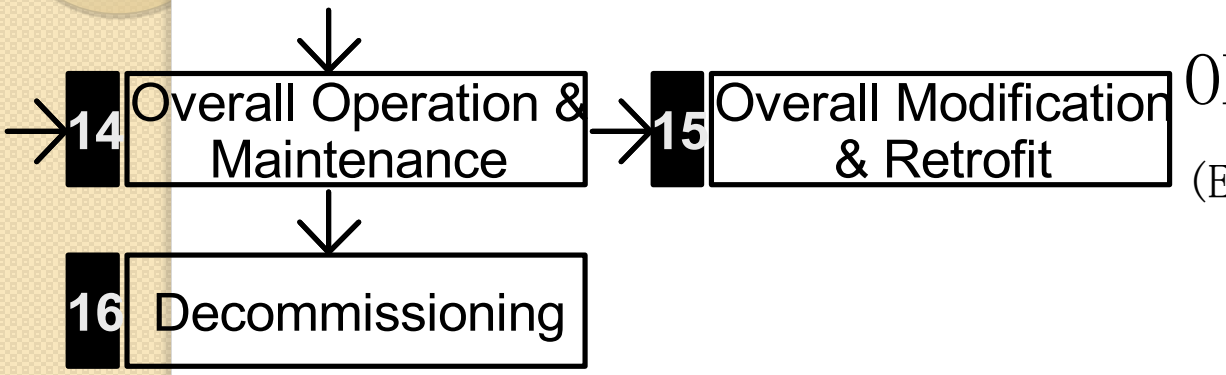
- Concept and Scope
- Hazards and Operability (HAZOP) Study
- Layers of Protection Analysis (LOPA)
- Fault Tree Analysis, Process Failure Modes and Effects Analysis
- Definition of Safety Functions (Cause and Effect Charts)
- Safety Integrity Level (SIL) Targets

SLC Realization Phase



- Architectural / Detail Design
- SIL Verification: Fault Trees / Markov Models
- Operation and Maintenance Planning
- Validation Test Planning
- Installation and Commissioning
- Validation Testing

SLC Operation Phase



OPERATION

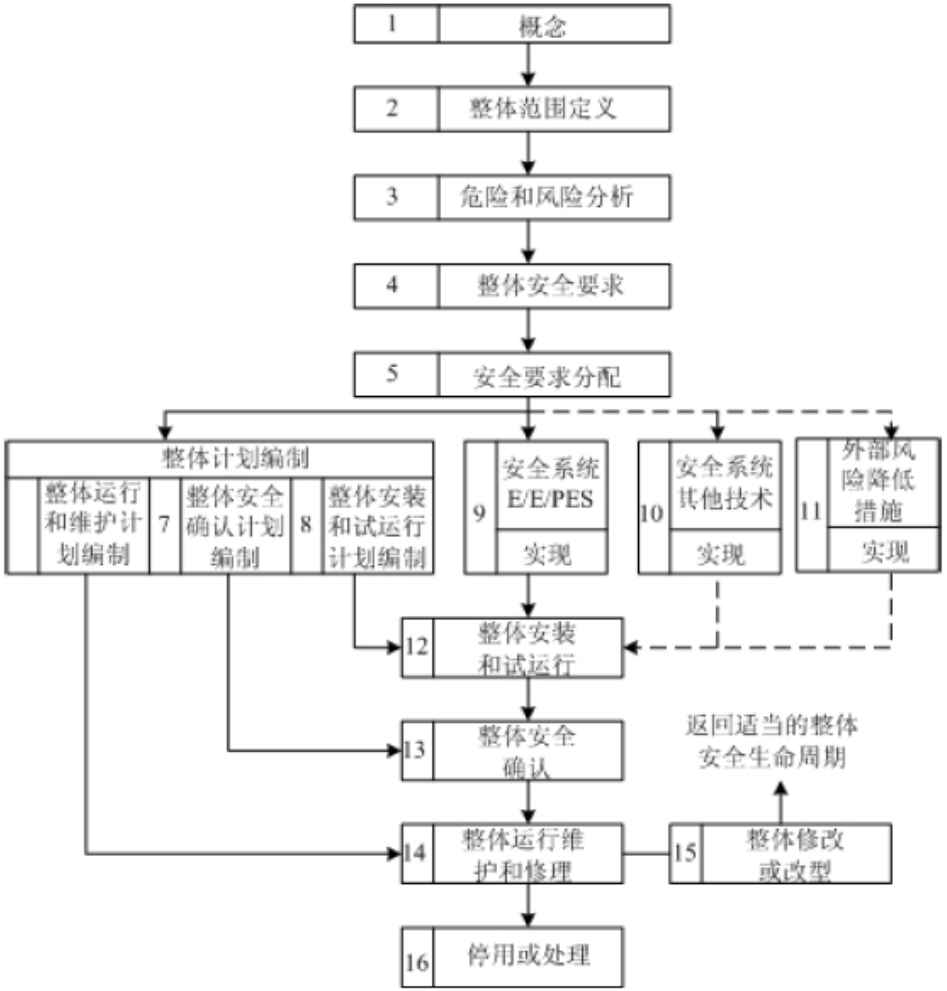
(End User / Contractor)

- Operation
- RiskBased Maintenance
- Periodic Inspection and Testing
- Modification Process and Retrofit
- Decommissioning

Overall SLC Objective

- To systematically structure the different phases to achieve the required functional safety of E/E/PE Systems
- To provide a framework for safer, more reliable systems
- To document key information relevant to functional safety
- To reduce system implementation cost

•安全生命周期 Safety Life Cycle 不仅覆盖安全相关系统的设计，还包括安全相关系统的规划、设计、安装、调试、运行、维护、停运等所有主要的阶段。其基本思想是功能安全相关的所有活动都是按照一个有计划的系统的方法进行管理。



IEC 61508 最核心的概念和内容

RiskReduction------- Tolerable Risk

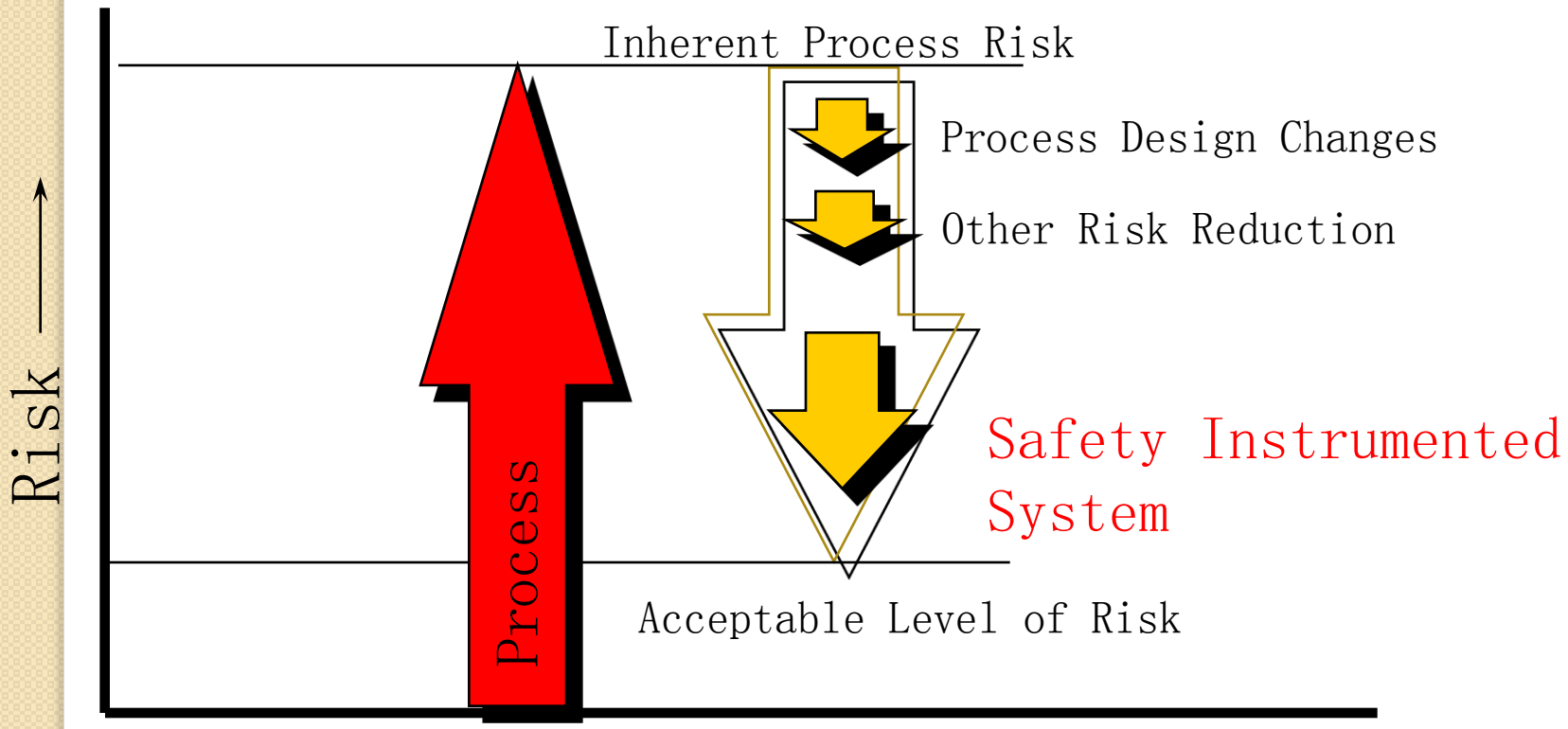
可容忍的风险（允许风险）

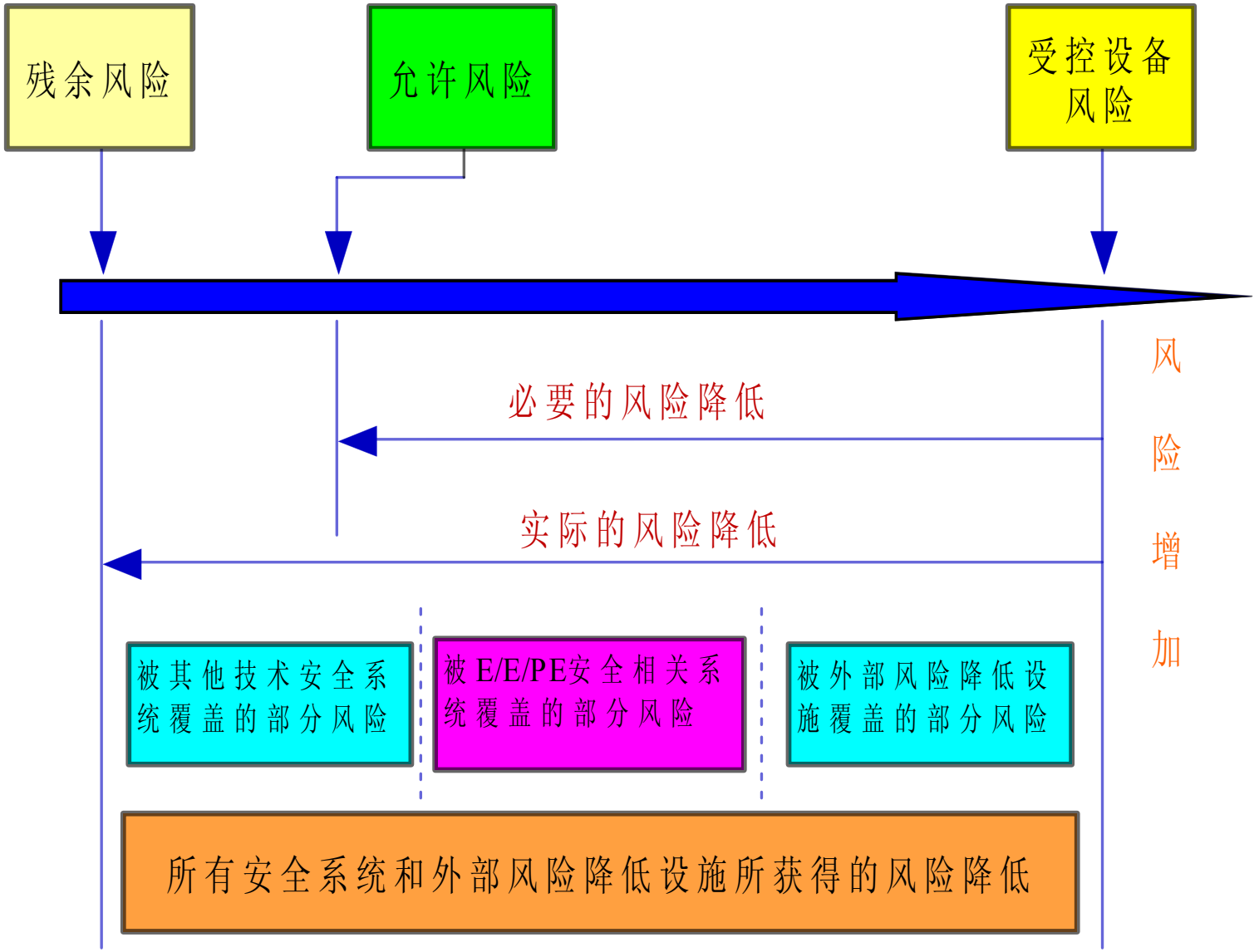
以定量的方法作为一个目标值明确给出

从而可以清晰确定适合的SIL

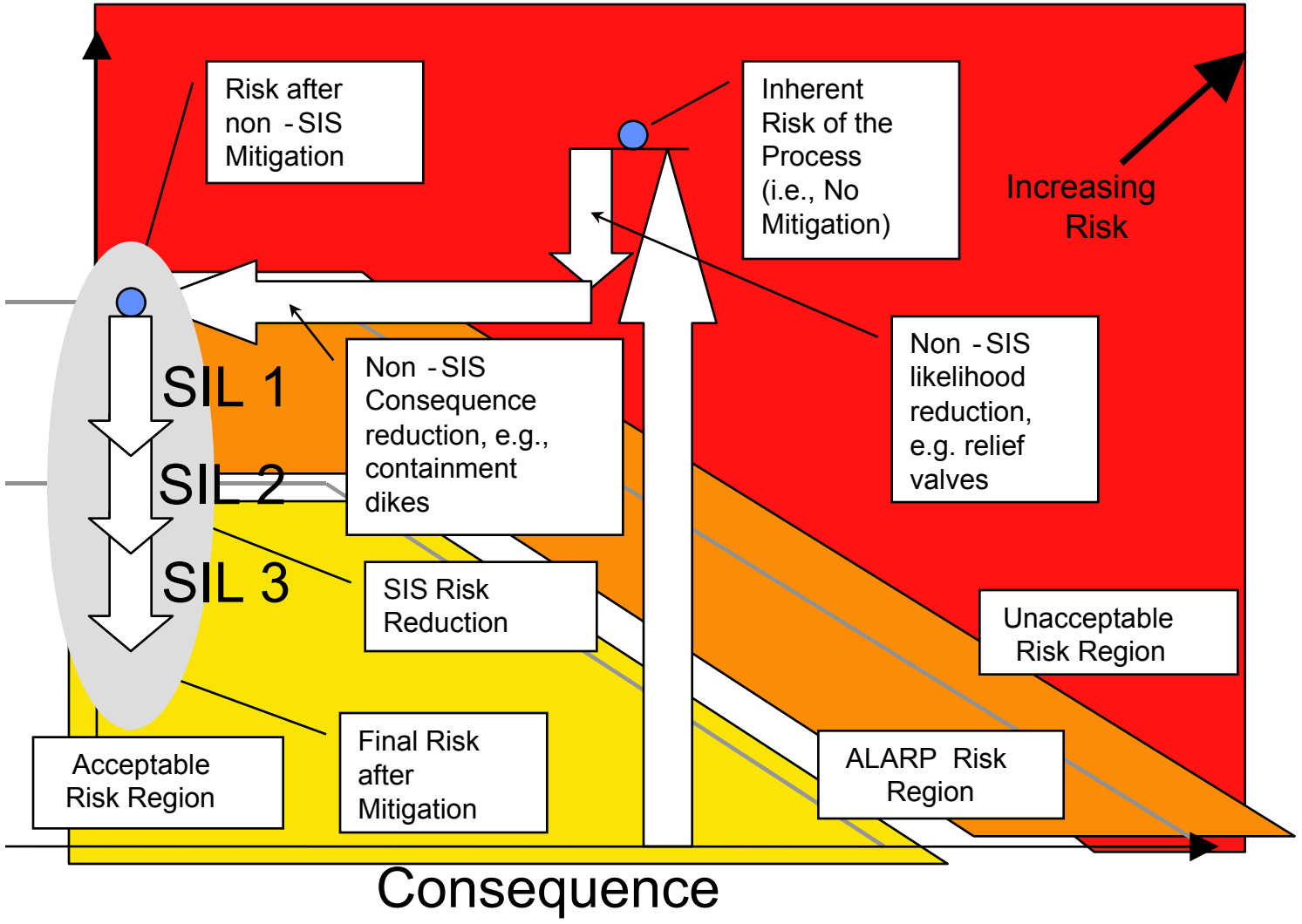
Key Concept: Risk and Safety Instrumented Systems

Riskis a measure of both how often something bad happens, and how bad it will be if it does.




残余风险
允许风险
受控设备风险
风险增加
必要的风险降低
实际的风险降低
被其他技术安全系统覆盖的部分风险
被E/E/PE安全相关系统覆盖的部分风险
被外部风险降低设施覆盖的部分风险
所有安全系统和外部风险降低设施所获得的风险降低

Paths to Risk Reduction



IEC 61508 最核心的概念和内容

SIL Safety Integrity Lever

安全完整性等级

How SIL works with SLC?

SIL是在风险评估之后确定的。因此安全仪表系统必须满足系统风险分析后所要求的SIL。SIL不仅是安全仪表系统安全性能的衡量标准，而且是整个安全生命周期的主线。其选择应该恰到好处，过高会造成成本的浪费，过低会使风险不可接受。SIL的选择为保障安全仪表系统执行其安全功能提供了系统科学的方法。

安全完整性指在规定条件下、规定时间内、成功实现所要求的仪表安全功能的**平均概率。**

安全完整性等级是用来规定分配给SIS安全功能的安全完整性要求的分离等级,记为SIL共分4个等级,SIL4为最高等级IEC61508-1规定了目标失效量。

在确定安全完整性时,应包括导致非安全状态的所有失效因素(硬件随机失效和系统失效)。

安全相关系统使用方式,按要求产生的频率可分为:低要求模式(≤1次/年)和高要求或连续模式(>1次/年)。低要求模式和高要求模式SIL的目标失效量是不同的，见表1。

安全完整性等级：低要求模式和高要求模式 SIL 的目标失效量

SIL	风险降低	低要求操作模式下 PFDavg(平均失效概率)	高要求或连续操作模式下 PFH(每小时危险失效概率)
1	10-----100	≥10-2 至＜10-1≥	10-6 至＜10-5
2	100----1000	≥10-3 至＜10-2	≥10-7 至＜10-6
3	1000----10000	≥10-4 至＜10-3	≥10-8 至＜10-7
4	10000---100000	≥10-5 至＜10-4	≥10-9 至＜10-8

要求时平均失效概率：PFDavg

(average Probability of Failure on Demand)

连续时危险失效概率：PDFperhour

(Probability of Dangerous Failure)

Key Concept: Safety Integrity Level

Safety Integrity Level	Probability of Failure Demand Per Year (Low demand mode of operation)	Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100,000 to 10,000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10,000 to 1,000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1,000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

IEC 61508 中对安全完整性等级SII的定义为：在一定时间，一定条件下，安全相关系统执行其所规定的安全功能的可能性。选择安全完整性等级水平的目的是通过降低风险发生的概率把系统的风险降低到一个可以接受的水平。

How to calculate SIL?

安全仪表系统的失效模式

安全仪表系统的失效可能导致其不能对过程危险状况作出响应,也就是说不能完成保护功能.另一方面,安全仪表系统的失效也有可能造成系统的误停车,使得正常生产中断.这些不同的失效方式被称作失效模式.

安全仪表系统的失效 λ

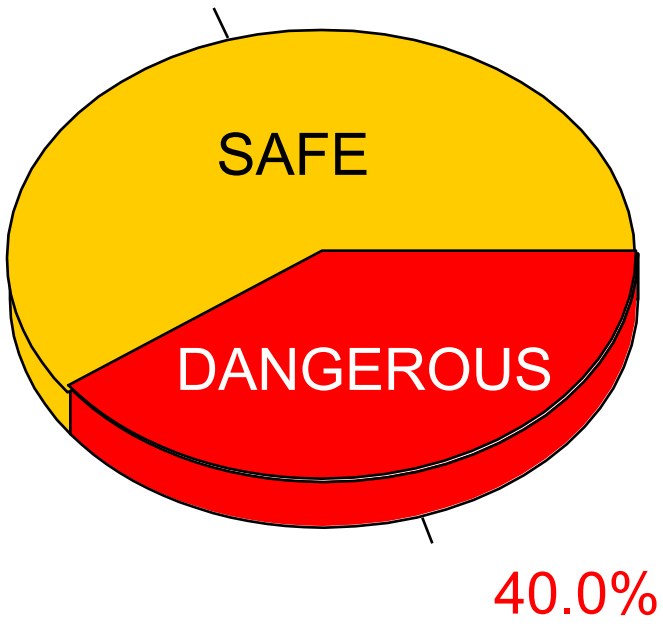
- 安全失效 λ^{S}
- 危险失效 λ^{D}
- 检测到的失效 λ^{DD}
- 未检测到的失效 λ^{DU}

- **共因失效， ß**

IEC61508 part 6 --ISATR84.02 Method

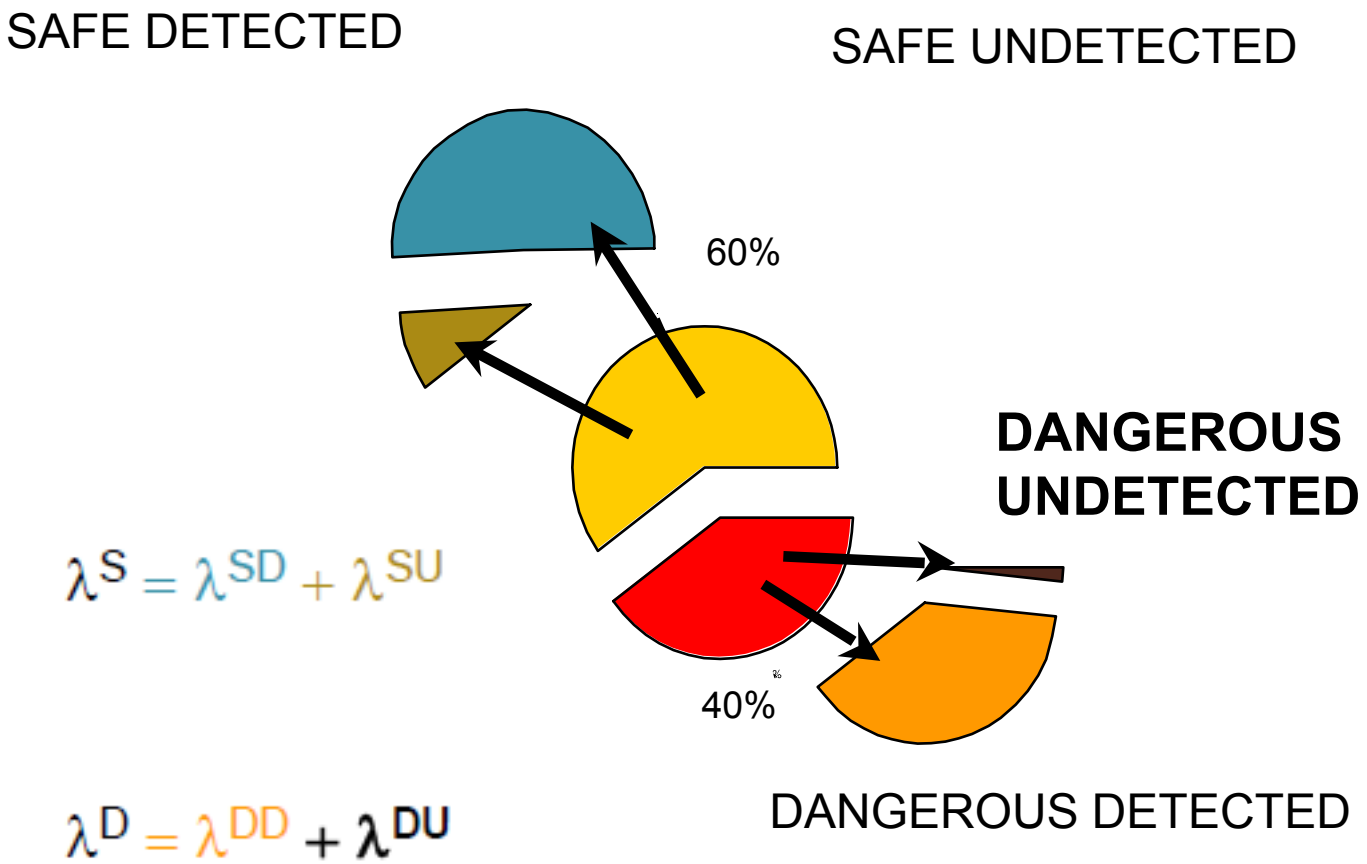
Divide failure rate into failure modes

$$\lambda = \lambda^S + \lambda^D$$



SD/SU/DD/DU

Divide each failure rate into “detected” and “undetected” (by on line tests)



$$\lambda^{S} = \lambda^{SD} + \lambda^{SU}$$

$$\lambda^{D} = \lambda^{DD} + \lambda^{DU}$$

Failure Modes Effects and Diagnostics Analysis FMEDA
失效模式,影响和诊断分析

FMEDA 是一种系统的技术,用来识别设备中存在的问题.它是一种自底向上的方法,以一份设备中的详细列表开始..比如:某电阻的失效会不会造成设备安全失效,危险失效或失准?如果A/D 转换到微处理的串行通信线路短路,设备会出现什么状况?

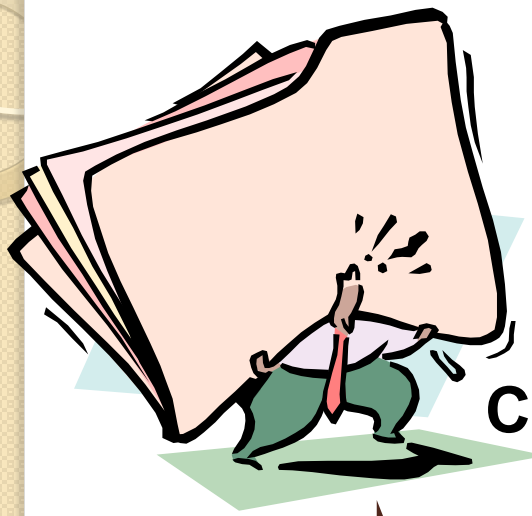
FMEDA 最终结果失效数据,包括每一种失效模式的失效率,检测到的和未检测到的失效概率,安全失效的比例等等,通常还包括在安全验证中如何使用这些数据.

Failure Modes Effects and Diagnostics Analysis FMEDA
失效模式,影响和诊断分析

通过FMEDA 可以得到某一设备某一失效模式的失效率,安全失效和危险失效的比例,诊断覆盖率也可以相当准确的得到.与工业数据库和经验估计相比,FMEDA 的结果是针对具体设备的,具有更高的准确性.

FMEDA 的测试和结果,是设备/系统获得SIL等级认证的基础.

Four categories of failure rates



% Safe

C^S （安全失效的诊断覆盖率

C^D(危险失效的诊断覆盖率

Manufacturer’s FMEDA

λ

$$\lambda^{SD} = C^S * \lambda^S$$

$$\lambda^{SU} = (1-C^S) * \lambda^S$$

$$\lambda^{DD} = C^D * \lambda^D$$

$$\lambda^{DU} = (1-C^D) * \lambda^D$$

Manufacturer's FMEDA

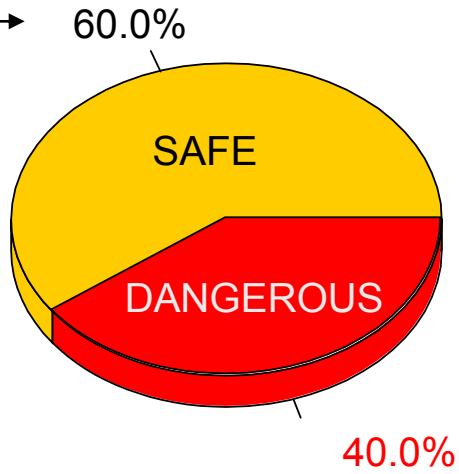
Manufacturer's FMEDA

% Safe

C^S

C^D

λ



Failure category				Failure rate (in FITs)
Fail Safe Detected				118
Fail Safe Undetected				209
Fail Dangerous Detected				1537
	Fail Detected (int. diag.)	1324		
	Fail Low (detected by the logic solver)	188		
	Fail High (detected by the logic solver)	25		
Fail Dangerous Undetected				123
No Effect				436
Annunciation Undetected				0

Simplified Equation PFD

$$F(t) \approx \lambda t$$

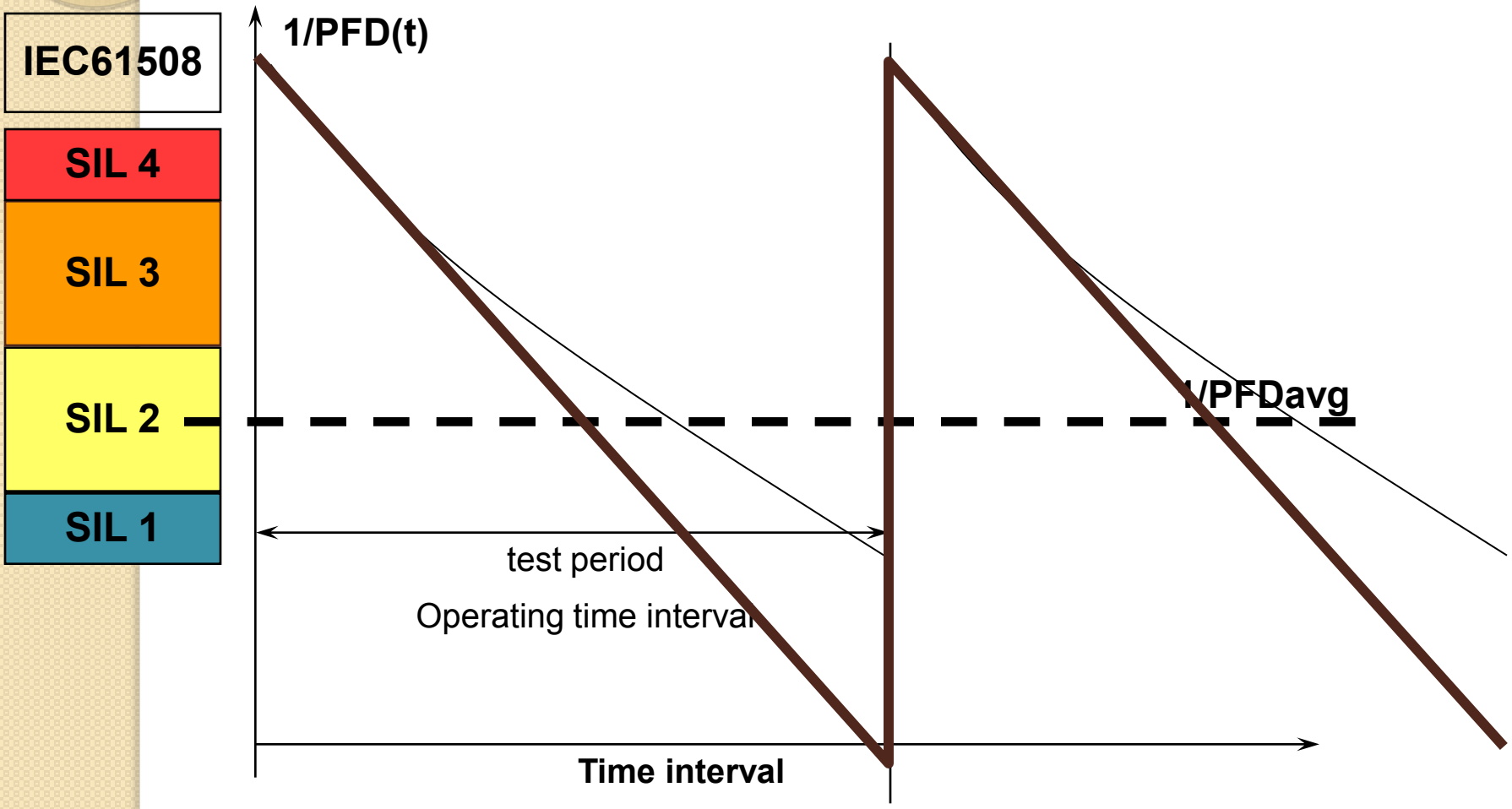
PF = λt

PFD = λ^{DD} RT + λ^{DU} TI

PFD = λ^{DU} TI Simplified

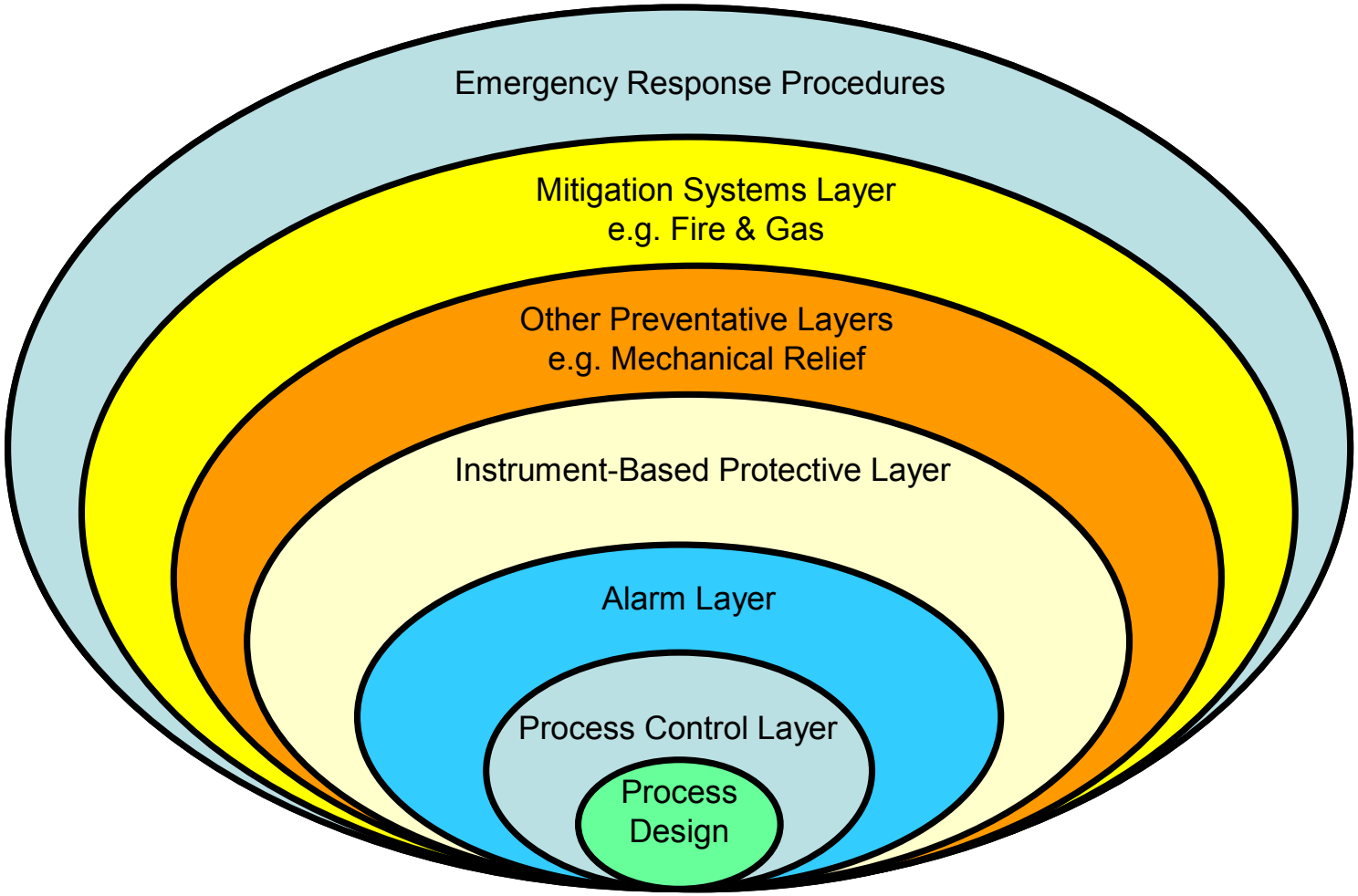
Simplified Equation PFDavg

$$PFD_{avg} = \lambda^{DU} \; t / 2$$

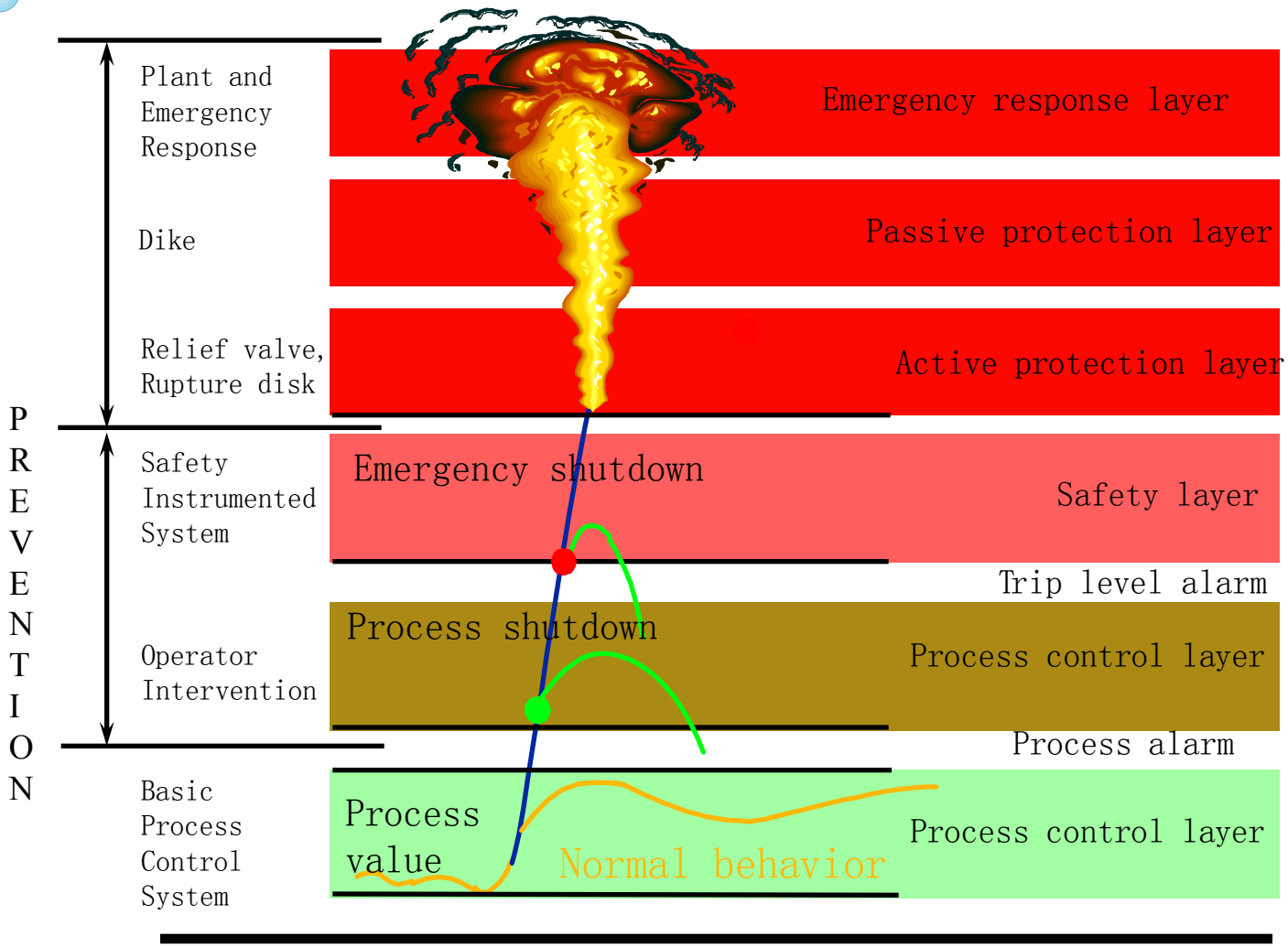


SIL等级在火气系统的应用

Risk Reduction Layers



SIL Identification and Layer of Protection Analysis



SIL等级在火气系统的应用

•在各个保护层都失效或是发生故障以后，火气系统发生效能，用于弥补各个保护层的失效/故障。例如：

- 设计的不完善

  产生的机械故障

  密封失效

  泄露

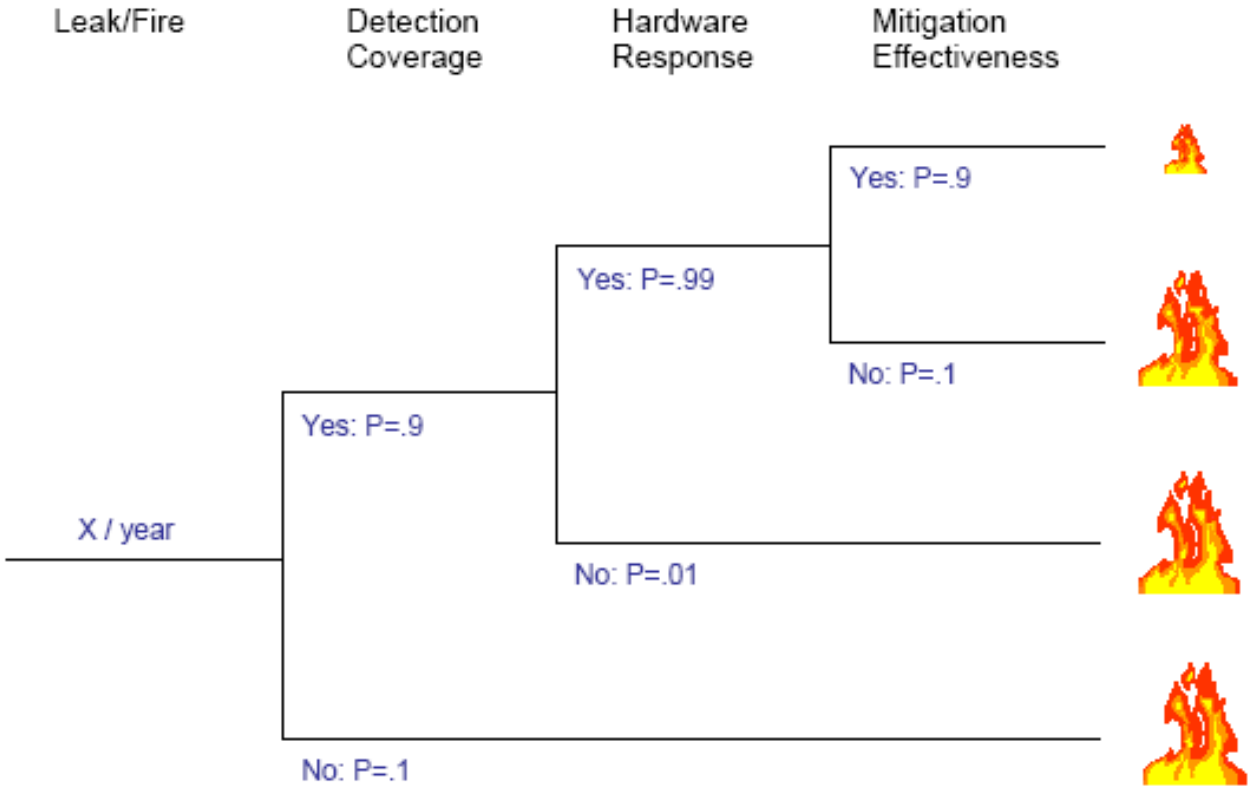
  操作失误

  控制故障

•火气系统作为一个与安全相关的系统，即便在工厂生产停止后，仍然需要能正常工作。

SIL等级在火气系统的应用

树形分析图 -影响火气系统的因素



SIL等级在火气系统的应用

现场传感器:迅速、正确地发现危险的存在，是整个系统最基本的元素。整个系统的产品架构再好，如果不能发现危险的存在，它也不是一套好的系统。

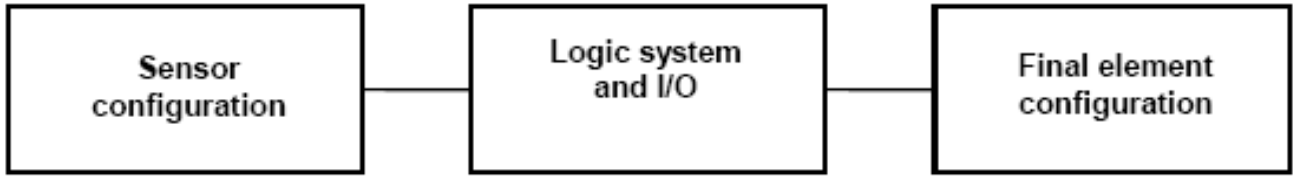
逻辑控制单元:确保系统在发现危险存在后，执行正确命令的可靠性。

执行单元：减低危害的效果，整个系统正确响应并阻止或是减轻危害事件的可能性

SIL等级在火气系统的应用

在火气系统设计选型时，常见的情况是很容易只要求控制器部分的安全性，忽略了现场仪表的安全要求，实际上火气安全仪表系统包括了现场的传感器、逻辑控制单元和执行单元，其故障失效率的计算方法如下：

PFDsis = PFDsensor + PFDlogic + PFDactuator



SIL等级在火气系统的应用

如果控制器达到SIL3，整个火气系统可以达到SIL3 的要求么？

如果现场的传感器达到SIL2，控制器达到SIL2，整个火气系统达到SIL2的要求了么？

SIL等级在火气系统的应用

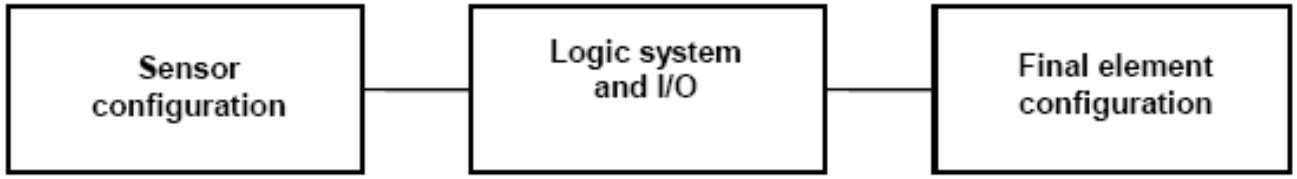
如果一个正常工作的传感器不能够检测到危险的存在？譬如传感器的放置位置不正确，或是设计的点数不够…..

如果一个正常工作的执行单元不能够避免或是减轻危险事件的发生？譬如启动的风机不足以排出泄露的气体….

SIL等级在火气系统的应用

在火气系统设计选型时，常见的情况是很容易只要求控制器部分的安全性，忽略了现场仪表的安全要求，实际上火气安全仪表系统包括了现场的传感器、逻辑控制单元和执行单元，其故障失效率的计算方法如下：

PFDsis = PFDsensor + PFDlogic + PFDactuator



SIF Verification Example

***Example*: Gas Detector**

	Lambda DU
Gas Detector	6.9x 10^{-7}failures per hour

No Diagnostics, Test Interval –1 year, SIL2

$$PFD_{avg} = \lambda^{DU} TI / 2$$

$$PFDavg = (0.00000069 * 8760) / 2$$

$$PFDavg = 0.0003$$

$$RRF = 1/PFDavg = 330$$

Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

SIF Verification Example

***Example*: F&G Loop Gas detector + Controller, 1001, SIL2**

	PFD
Gas Detector:	$3X10^{-3}$
Gas Controller:	$2.66x10^{-3}$

Test Interval –1 year,

PFDavg = $0.003+0.00266=0.00566=5.66x10^{-3}$

Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand (Demand mode of operation)	Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

IEC61508 Safe FailureFraction 安全失效分数

$$SFF = \frac{\lambda SD + \lambda SU + \lambda DD}{\lambda SD + \lambda SU + \lambda DD + \lambda DU}$$

IEC61508 Safe Failure Fraction

TYPE A

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % < 90 %	SIL2	SIL3	SIL4
90 % < 99 %	SIL3	SIL4	SIL4
	SIL3	SIL4	SIL4

IEC61508 Safe Failure Fraction

TYPE B

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % < 90 %	SIL2	SIL3	SIL4
90 % < 99 %	SIL3	SIL4	SIL4
	SIL3	SIL4	SIL4

IEC 61508 最核心的概念

- **Safety Life Cycle　　SLC**
  整体安全生命周期
- RiskReduction ---Tolerable Risk
  可容忍的风险（允许风险）
  以定量的方法作为一个目标值明确给出
  从而可以清晰确定适合的SIL
- SafetyIntegrity Lever SIL
  安全完整性等级

Questions?

- Thank you very much！