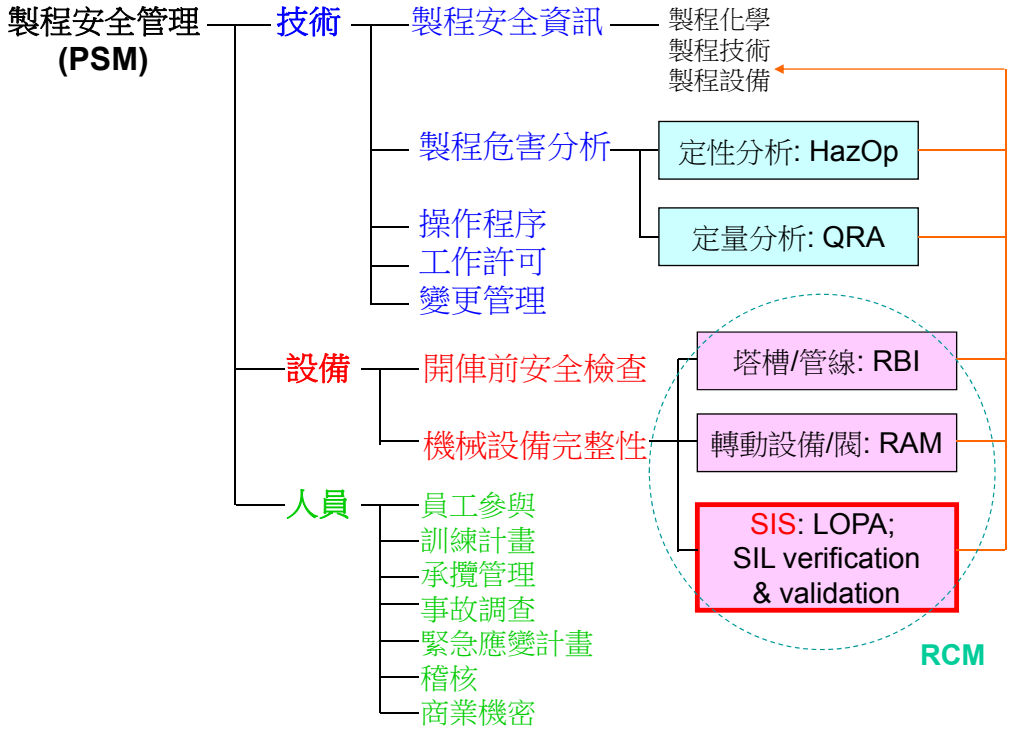
社團法人台灣安全研究與教育學會_系列課程

機械完整性介紹和實務技術研討會

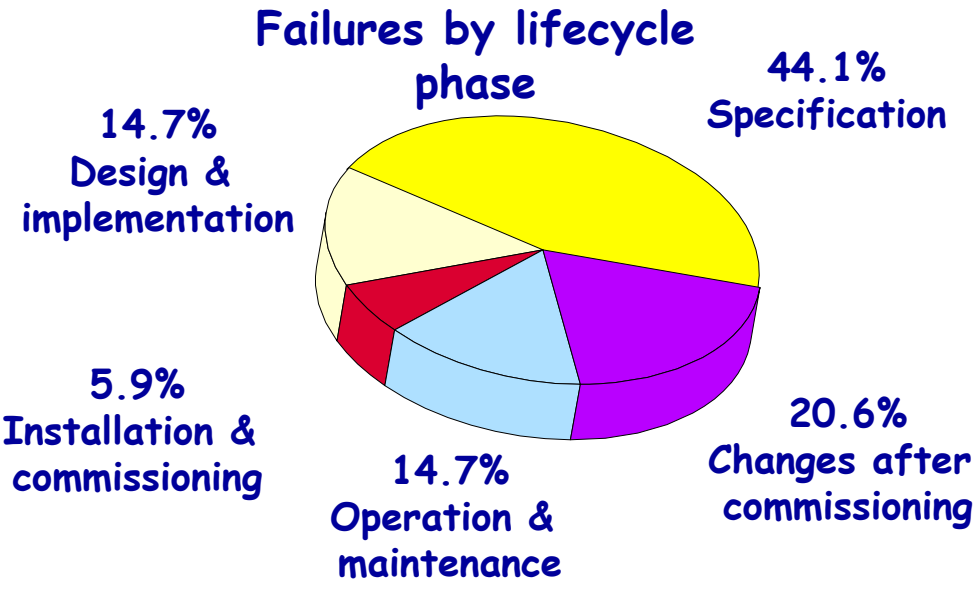
儀控機械完整性 (MI)相關技術和實務

製程安全解決方案



英國HSE針對34件控制系統故障事故的原因分析

HSE "Out of Control" publication



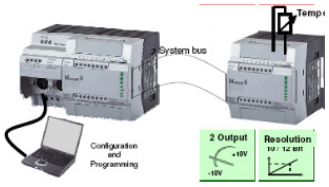
IEC 61508與功能安全

Title: Functional safety of electrical, electronic & programmable electronic safety-related systems….

A seven Part international standard covering all safety lifecycle activities...concept..... specification...design...implementation…operation maintenance & modification

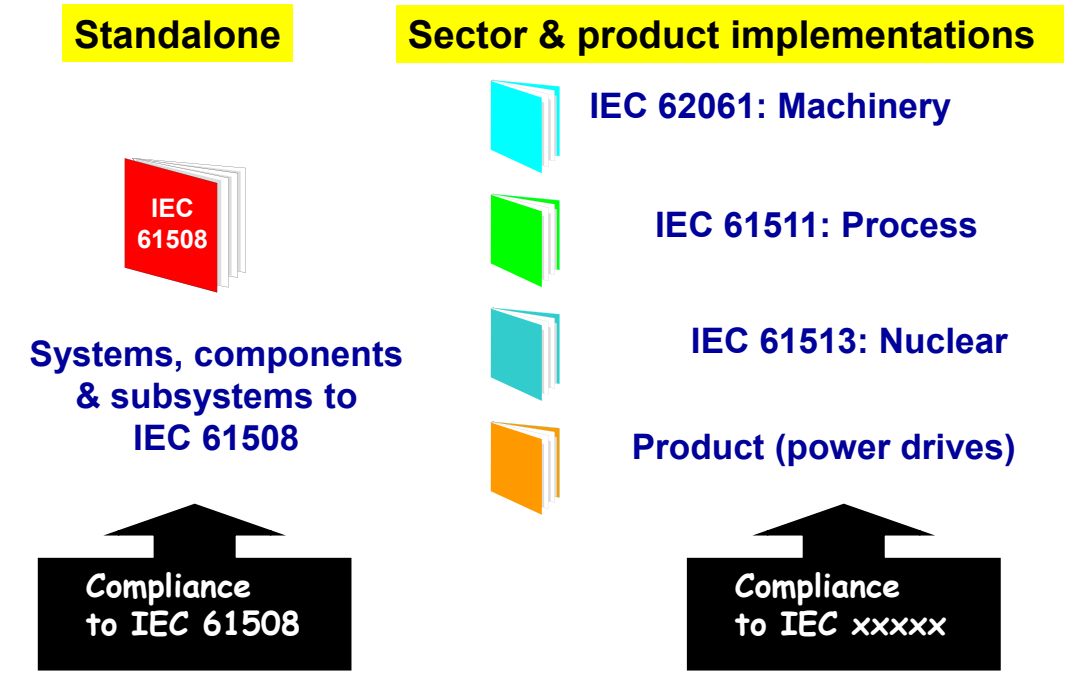
IEC 61508標準共分7個部分

- 第1部分：一般要求
  - 說明主要概念、組織、安全生命週期、文檔編制、引導證據及SIL定義
- 第2部分：電氣/電子/可程式電子安全系統的要求
  - 包括對設備和系統的要求，很多內容與第7部分的鑒別方法的應用有關，並解決隨機失效或系統失效問題
- 第3部分：軟體要求
  - 說明避免失效的方法，與第7部分的附錄相關



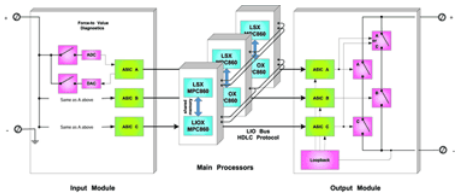
- 第4部分：定義和縮略語
- 第5部分：需求安全完整性等級決定方法與案例
- 第6部分：第2及第3部分之應用指南
- 第7部分：技術與方法概要
  - 說明相關技術、評估、檢驗及測試方法，並提供部分參考書目

IEC 61508標準系列

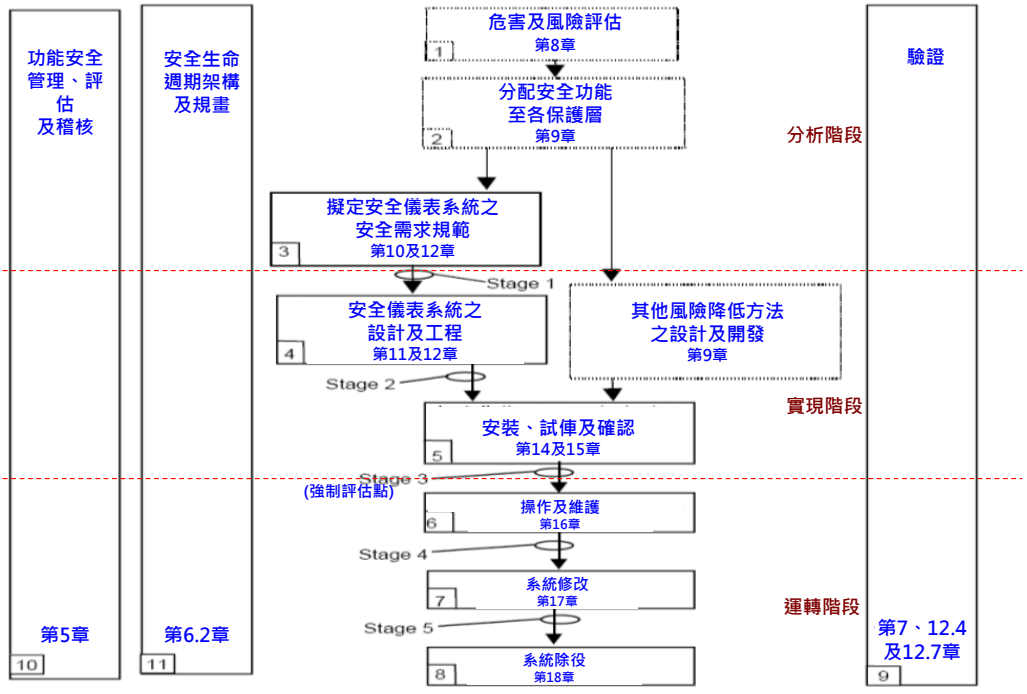


IEC 61511標準共分3個部分

- 第1部分：整體框架、定義、系統、硬體和軟體要求
  - 說明SIS的規範、設計、安裝、營運和維護要求，確保該系統能將製程置於或保持在某個安全狀態
- 第2部分：第1部分的應用指南
  - 為滿足IEC61511第1部分中定義的儀錶安全功能及其相關的SIS的規範、設計、安裝、操作和維護的要求所必要的實現指南
- 第3部分：確定所需安全完整性等級
  - 內容包括風險的基礎概念、風險與安全完整性的關係、允許風險的確定，以及確定儀錶安全功能的安全完整性等級的各種不同方法



IEC 61511 SIS安全生命週期管理



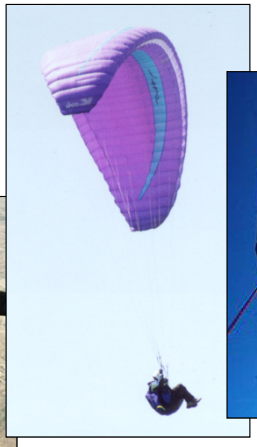
名詞解釋

- 風險及可容忍風險
- 保護層及保護層分析(LOPA)
- 功能安全(Functional Safety)
- 安全儀錶功能(SIF)
- 安全完整性等級(SIL)
- 安全需求規範(SRS)

何謂可容忍風險?

事件	平均個體風險 (死亡數/年)
觸電	5.3E-6
閃電擊中，美國 1990	2.8E-6
酒精，輕度飲酒	2.0E-5
汽車意外，行人	4.2E-5
汽車意外，全部	2.4E-4
時常飛行	5.0E-5
家庭意外	1.1E-4
空氣污染，美國東部	2.0E-4
全部癌症	2.8E-3
抽煙者，每天一包	3.6E-3

You Must Know Both F & C
To Make Informed Decisions



風險評估基準-風險矩陣(Risk Matrix)

風險評估矩陣		可能性							
		1	2	3	4	5	6	7	8
嚴重性	7	4 SIL1	5 SIL2	6 SIL3	7 SIL4	7 B	7 B	7 B	7 B
	6	3 A2	4 SIL1	5 SIL2	6 SIL3	7 SIL4	7 B	7 B	7 B
	5	2 A1	3 A2	4 SIL1	5 SIL2	6 SIL3	7 SIL4	7 B	7 B
	4	1	2 A1	3 A2	4 SIL1	5 SIL2	6 SIL3	7 SIL4	7 B
	3	1	1	2 A1	3 A2	4 SIL1	5 SIL2	6 SIL3	7 SIL4
	2	1	1	1	2 A1	3 A2	4 SIL1	5 SIL2	6 SIL3
	1	1	1	1	1	2 A1	3 A2	4 SIL1	5 SIL2

風險評估基準-嚴重性等級(Severity)

嚴重性分類		人員	設備/設施(包括停爐損失), NTD(元)	洩漏
7	極度嚴重(Extra Catastrophic)	＞50人死亡或永久全失能傷害	＞100億	發生國際污染事件： ＞1,000,000bbl oil spill或 廠外安全事件： ＞5人死亡或永久全失能傷害(執行F-N Curve分析)
6	嚴重(Catastrophic)	5～50人死亡或永久全失能傷害	10億～100億	發生國家級污染事件： ＞100,000bbl oil spill或 廠外安全事件： 1～5人死亡或永久全失能傷害(執行F-N Curve分析)
5	擴大的(Extensive)	2～5人死亡或永久全失能傷害	3億～10億	發生區域性污染事件： ＞10,000bbl oil spill或 廠外安全事件： 永久部份失能傷害或暫時全失能傷害≧5(執行F-N Curve分析)
4	重大(Serious)	1人死亡；或≧5人永久部份失能傷害或暫時全失能傷害	3000萬～ 3億	未污染社區，污染局限在廠內
3	高度(Considerable)	永久部份失能傷害≧1或暫時全失能傷害＜5；或損失工時傷害≧5	300～ 3000萬	工藝單元外泄
2	中度(Marginal)	1≦損失工時傷害＜5	30～ 300萬	工藝區(工段)外泄
1	可忽略的(Negligible)	急救傷害≧1	3～ 30萬	單一設備外泄

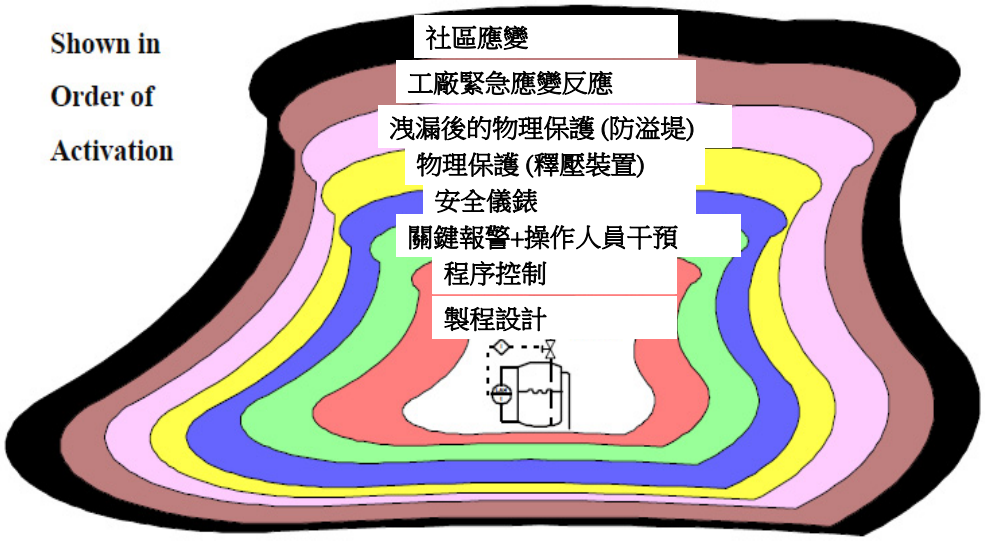
風險評估基準-可能性等級(Likelihood)

可能性分類		預期發生頻率
8	非常頻繁的	＞1
7	經常的	10^{-1}～1
6	非常可能的	10^{-2}～10^{-1}
5	可能的	10^{-3}～10^{-2}
4	也許的	10^{-4}～10^{-3}
3	稀少的	10^{-5}～10^{-4}
2	很稀少的	10^{-6}～10^{-5}
1	極不可能的	10^{-7}～10^{-6}

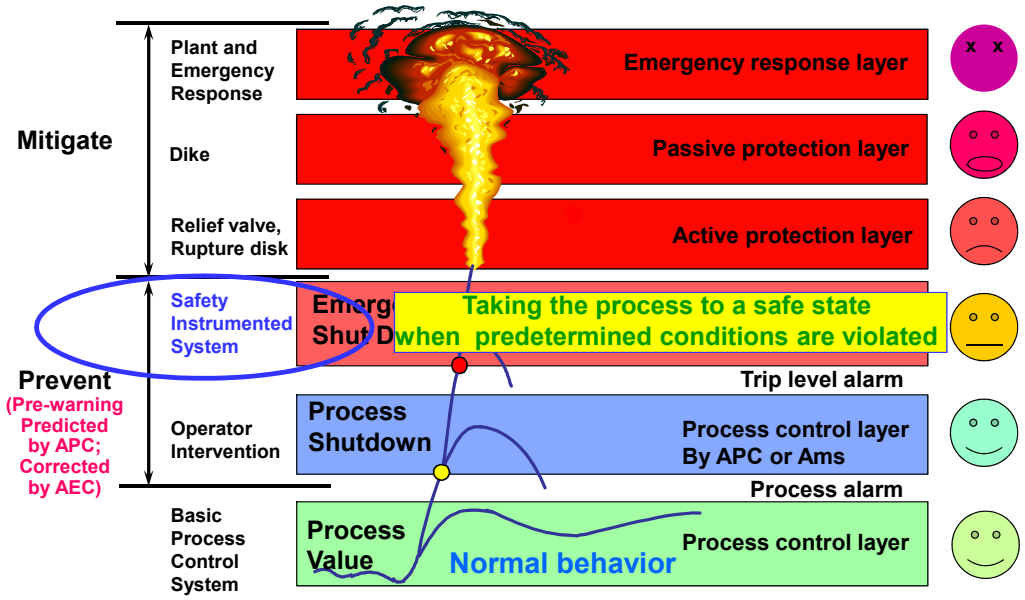
Tolerable Risk Target

嚴重性等級	嚴重性描述	可容忍目標頻率 (/year)
7	極度嚴重(Extra Catastrophic)	＜ 10^{-7}
6	嚴重(Catastrophic)	＜ 10^{-6}
5	擴大的(Extensive)	＜ 10^{-5}
4	重大(Serious)	＜ 10^{-4}
3	高度(Considerable)	＜ 10^{-3}
2	中度(Marginal)	＜ 10^{-2}
1	可忽略的(Negligible)	＜ 10^{-1}

洋蔥模型


Shown in
Order of
Activation
社區應變
工廠緊急應變反應
洩漏後的物理保護 (防溢堤)
物理保護 (釋壓裝置)
安全儀錶
關鍵報警+操作人員干預
程序控制
製程設計

保護層的概念


Mitigate
Plant and Emergency Response
Dike
Relief valve, Rupture disk
Emergency response layer
Passive protection layer
Active protection layer
Safety Instrumented System
Taking the process to a safe state when predetermined conditions are violated
Trip level alarm
Prevent
(Pre-warning Predicted by APC; Corrected by AEC)
Operator Intervention
Process Shutdown
Process control layer By APC or Ams
Process alarm
Basic Process Control System
Process Value
Normal behavior
Process control layer

安全功能及其安全完整性

Safety function — "what has to be done"

Safety integrity of safety function — the "safety performance" of the safety function";

Example

Safety Integrity Level

Safety function: *In order to prevent the rupture of pressure vessel "X", valve "Y" should open in 2 seconds when the pressure in the vessel rises to 2.6 bar.*

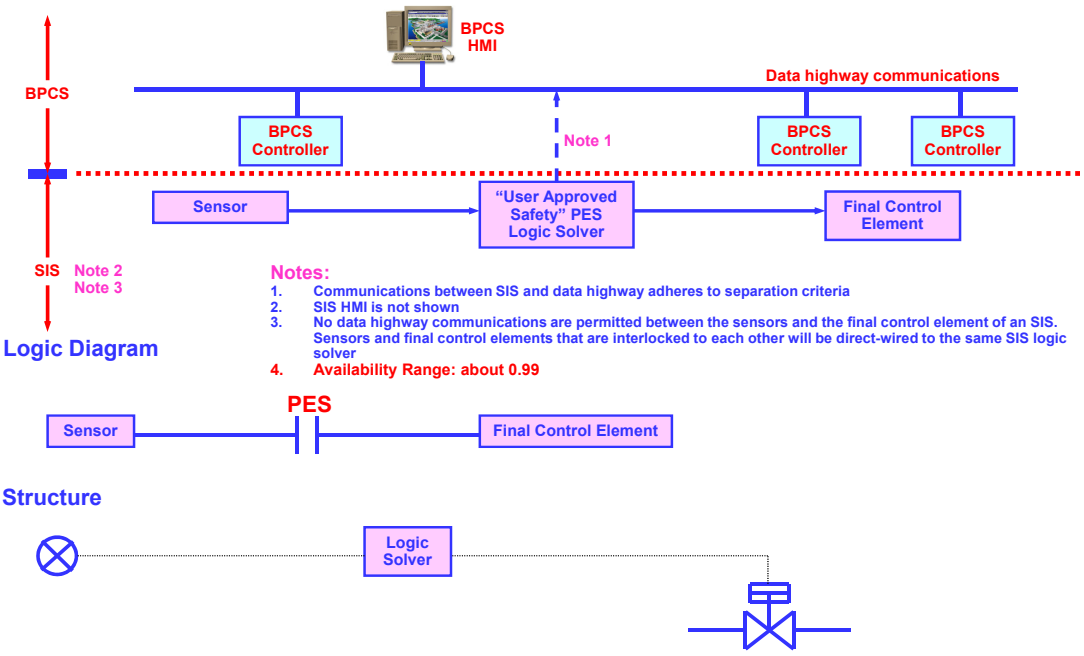
Safety integrity: *The safety integrity of the safety function shall be SIL 2*

IEC61508 安全完整性等級和目標失效考慮

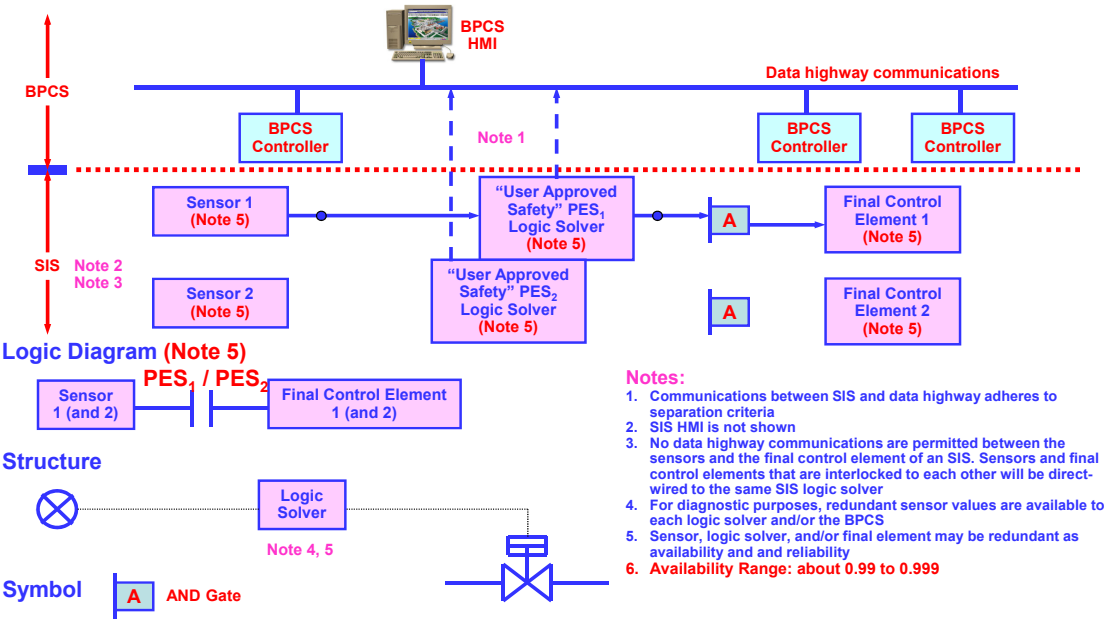
安全完整性等級	低需求模式操作 (需求時之平均失效率) PFDavg	連續/高需求模式操作 (每小時危險失效率) PFH
4	$\geq 10^{-5} \sim < 10^{-4}$	$\geq 10^{-9} \sim < 10^{-8}$
3	$\geq 10^{-4} \sim < 10^{-3}$	$\geq 10^{-8} \sim < 10^{-7}$
2	$\geq 10^{-3} \sim < 10^{-2}$	$\geq 10^{-7} \sim < 10^{-6}$
1	$\geq 10^{-2} \sim < 10^{-1}$	$\geq 10^{-6} \sim < 10^{-5}$

- 需求時之平均失效率(Average probability of failure on demand , PFDavg)
- 每小時危險失效率(Probability of a dangerous failure per hour , PFH)

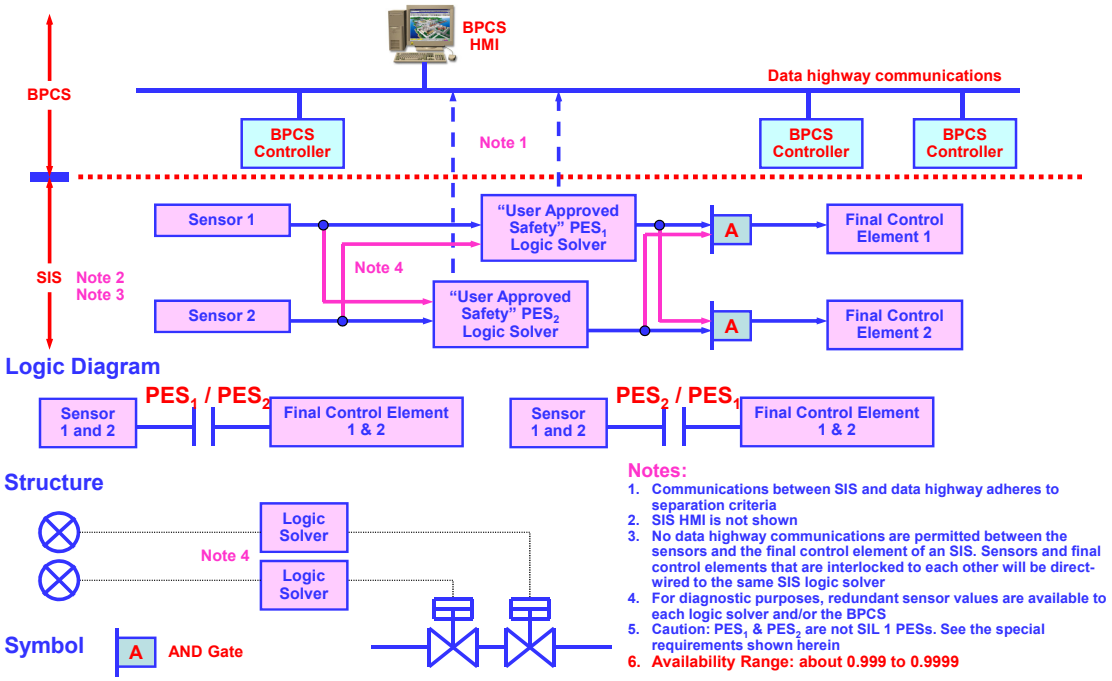
SIL1 SIS架構示意圖



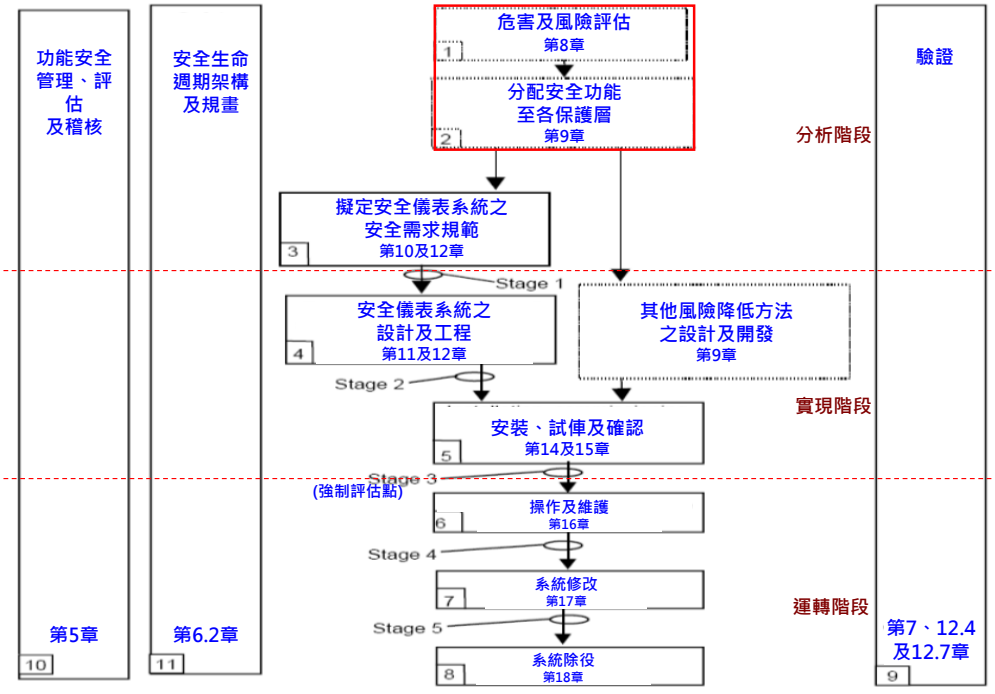
SIL2 SIS架構示意圖



SIL3 SIS架構示意圖



IEC 61511 SIS安全生命週期管理



保護層分析(Layer of Protection Analysis)

- 必須先取得公司無法接受的**風險等級標準**(例如1 x 10^{-6}/年嚴重的結果)
- 列出每一個衝擊事件**起始原因和估計的可能性**
- **列出獨立保護層(IPLs)**，即:DCS、警報和程序、SIS等
- 各**獨立保護層(IPLs)**均被指定一個**需求時失效機率(PFD)**

IEC 61511-3 附錄F: 獨立保護層定義

- 是**獨立的**
- 典型的PFD數值為 1 x 10^{-2}
- **可信賴的(可靠的)**
- 是專門設計成一個獨立保護層
- 能夠被稽核

CCPS: LOPA 獨立保護層規則

- 如果起始原因是一個DCS回路，則該DCS不能算作 IPL
- **DCS發出的警報不是獨立於DCS之外的**
- 一個DCS回路，若其正常的控制可以補償起始原因，則該DCS可以算作一個 IPL

額外的消減獨立保護層(IPLs)

- 泄壓閥
- 破裂盤
- 溢出至安全位置的措施
- 疏散程序
- 自動噴水滅火系統

保護層分析(LOPA)

事件發生的可能性

＝起始失效事件的可能性×獨立保護層(IPLs)的需求時失效機率(PFDs)

IEC 61511-3 附錄F – LOPA工作表

圖F.1

#	1	2	3	4		5		6	7	8	9	10	11
					保護層								
	事件後果F.3	嚴重性等級F.4	起始失效事件F.5	起始失效事件可能性F.6	一般製程設計F.7	基本程序控制系統F.7	警報F.7	額外消減措施，限制進入F.8	獨立保護層F.9	中間事件可能性F.10	SIF完整性等級F.11	消減後事件可能性F.12	註
1	蒸餾塔破裂引起火災	S	冷卻水流失	0.1	0.1	0.1	0.1	0.1	PRV 0.01	10^{-7}	10^{-2}	10^{-9}	高壓引起塔破裂
2	蒸餾塔破裂引起火災	S	蒸汽控制回路失效	0.1	0.1	1	0.1	0.1	PRV 0.01	10^{-6}	10^{-2}	10^{-8}	高壓引起塔破裂

IEC 61511-3 附錄F – LOPA工作表
事件後果F.3

- 使用圖F.1時，從HAZOP分析所確定的每個事件後果描述被填在第1列中

LOPA要求的資訊	HAZOP所導出的資訊
影響事件	後果
嚴重性等級	後果嚴重性
起始失效事件	原因
起始失效事件可能性	原因頻率
保護層	現有保護措施
要求的額外消減措施	建議的新保護措施

IEC 61511-3 附錄F – LOPA工作表
起始失效事件F.5

- 圖F.1第3列引出了事件後果的所有起始失效事件。事件後果有許多起始失效事件，把它們全都羅列出來是重要的

典型起始原因之頻率 (1/3)

項次	閥(Valves)	可能性 (1/yr)
1	逆止閥未能完成止逆(Check valve fails to check fully)	1
2	Check valve sticks shut	0.01
3	墊片或迫緊破裂(Gasket or packing blows out)	0.01
4	調壓閥故障(Regulator fails)	0.1
5	安全閥開啟或嚴重洩漏(Safety valve opens or leaks through badly)	0.01
6	馬達或閥門誤動作的所有原因(Spurious operation of motor or pneumatic valves - all causes)	0.1

項次	容器及儲槽(Vessels and Tanks)	可能性 (1/yr)
1	常壓儲槽故障(Atmospheric tank failure)	1×10^{-3}
2	球槽發生沸騰液體蒸發膨脹爆炸(Sphere BLEVE)	1×10^{-4}
3	容器洩漏(小孔徑≦2")(Small orifice (≦2") vessel release)	1×10^{-3}

典型起始原因之頻率 (2/3)

項次	公用設備(Utility)	可能性 (1/yr)
1	冷卻水故障(Cooling water failure)	0.1
2	電力故障(Power failure)	1
3	儀錶氣源故障(Instrument air failure)	0.1
4	氮氣(或惰性氣體)系統故障(Nitrogen (or inerting) system failure)	0.1

項次	機械故障(Machinery Failure)	可能性 (1/yr)
1	泵軸封故障(Pump seal fails)	0.1
2	多組的泵及轉動設備(損失流量)(Pumps and other rotating equipment with redundancy (loss of flow))	0.1
3	冷卻風扇或翅扇停止(Cooling fan or fin-fan stops)	0.1
4	往復式泵或壓縮機停止(Motor-driven pump or compressor stops)	0.1
5	壓縮機或渦輪因裂縫而超速(Overspeed of compressor or turbine with casing breach)	0.1

典型起始原因之頻率 (3/3)

項次	操作失誤(Operator Error)	可能性 (1/yr)
1	操作失誤-沒有壓力(正常操作)(Operator error-no stress (routine operations))	0.1
2	操作失誤-有壓力(警報、啟動、停機等)(Operator error-stress (alarms, startup, shutdown, etc.))	1

項次	儀錶故障(Instrumentation Failure)	可能性 (1/yr)
1	BPCS回路故障(BPCS loop fails)	0.1

項次	外部事件(External Events)	可能性 (1/yr)
1	閃電擊中(Lightning hit)	0.001
2	大型外部火災之所有原因(Large external fire (all causes))	0.01
3	小型外部火災之所有原因(Small external fire (all causes))	0.1

IEC 61511-3 附錄F – LOPA工作表
保護層F.7 (1/2)

- 本章開始時介紹的圖，”典型保護層”，表示了製程中通常配備的多個保護層（PL）。每個保護層都由一組設備和/或其功能與其他一些保護層有關的管理級控制設備組成。能以高可靠性執行其功能的保護層可看作獨立保護層（IPL）(見F.9)
- 圖F.1的第5列列出了用於在發生一個起始失效事件時降低發生一個事件後果的可能性的製程設計。這種設計的一個例子就是雙套管或是雙層壁的壓力容器。當主管道或壓力容器的完整性受到損害時，外套可防止製程物質的釋放
- 圖F.1第5列的下一項是基本程序控制系統（BPCS）。如果當起始失效事件發生時，BPCS中的一個控制回路可防止事件後果發生
- 圖F.1第5列的最後一項是從警告操作員的警報和利用操作員干預得到的好處。
- 表F.4列出了保護層典型的PFD_{avg}值

IEC 61511-3 附錄F – LOPA工作表
保護層F.7 (2/2)

表F.4 保護層(預防和消減)典型的PFD_{avg}

保護層	PFD_{avg}
控制回路	1.0×10^{-1}
人的執行能力(經訓練的, 不緊張)	1.0×10^{-4}~ 1.0×10^{-2}
人的執行能力(處於緊張狀態下)	0.5 ~ 1.0
操作員對警報的反應	1.0×10^{-1}
容器壓力額定值超過來自內部和外部壓力源的最大極限值	1.0×10^{-4}或更好，在保持容器完整性（即瞭解腐蝕，按檢查計畫執行檢查維護）

IEC 61511-3 附錄F – LOPA工作表 額外消減措施F.8

- 這一層消減措施通常有機械的、建築上的或程序的。其例子有：
  - 釋壓裝置；
  - 堤（堰）；和
  - 限制接近
- 這一層消減措施可以降低事件後果的嚴重性，但不能防止事件後果的發生。其例子有：
  - 防火或防煙霧釋放用的噴水系統；
  - 煙霧報警器；和
  - 撤離程序
- LOPA小組應確定所有這一層消減措施的恰當的PFD並把它們列入圖F.1的第6列中

IEC 61511-3 附錄F – LOPA工作表 IPL獨立保護層F.9

- 圖F.1第7列中列出了滿足IPL準則的保護層
- 把一個保護層（PL）看作一個IPL的準則是：
  - 提供的保護大量降低已識別的風險，即最小降低100倍；
  - 提供可用性程度很高（0.9或更高）的保護功能；
  - 它具有以下重要特點：
    - a) **專一性**：IPL只被設計用來防止或減輕一個潛在的危險事件（例如失控反應、有毒物質的釋放、安全殼損壞或者火災）的後果。由於多種原因都可能導致同一危險事件，因此多個事件情景都可由一個IPL來啟動動作
    - b) **獨立性**：IPL是與已驗明的危險相關的其他保護層相獨立的
    - c) **可信性**：可信任IPL能執行所設計的那些功能。在設計中處理了隨機失效和系統失效兩種失效模式
    - d) **可審核性**：它被設計成能有助於定期確認保護功能。安全系統的檢驗測試和維護是必要的
- 只有滿足可用性、專一性、獨立性、可信性和可審核性測試的那些保護層才可被歸類為獨立保護層

典型的IPL失效機率

系統或措施	失效機率
Sprinkler system	5×10-2
VESDA	5×10-2
Automatic CO2 system	5×10-2
Relief valve	1×10-2
Rupture disc / Relieving door	1×10-2
Blast wall	1×10-3
Fireproofing	1×10-2
Tank overflow line	1×10-2
Dike	1×10-2
Drainage system	1×10-2

IEC 61511-3 附錄F – LOPA工作表
中間事件可能性 F.10

- 起始失效事件可能性（圖F.1第4列）乘以保護層和消減層的PFD（圖F.1第5列～第7列）即可得出中間事件可能性。算出的數值單位為事件/年，並被填入圖F.1的第8列中
- 如果中間事件可能性小於你公司的該嚴重性等級的事件的準則，則可不用附加的PL。但是如經濟上合適的話，還應進一步降低風險
- 如果中間事件可能性大於你公司的該嚴重性等級的事件的準則，則需要額外的消減措施。在使用安全儀錶系統（SIS）型式的附加保護層之前，應考慮本質較安全的方法和解決辦法。如果能進行本質安全設計的改變，則應更新圖F.1並重新計算中間的事件可能性，以確定它是否低於公司準則。如果不能通過上述方法降低中間事件可能性至公司準則之下，則要求增加一個SIS

IEC 61511-3 附錄F – LOPA工作表

安全系統完整性需求F.11 &消減後的事件的可能性F.12

- **安全系統完整性需求F.11**
  - 如果需要一個新的SIF，則可由該事件後果嚴重性等級的公司準則除以中間事件可能性來計算所需的完整性等級。低於此數的SIF的一個PFDavg被選作SIS的最大值並填入第9列中
- **消減後的事件的可能性F.12**
  - 把第8列和第9列的數值相乘就可計算出消減後的事件的可能性，結果填入第10列中。這種計算一直進行到小組算出每個已識別能查明的事件後果的消減後的事件的可能性為止

HazOp Example -1.1

製程偏離	可能原因	危害/後果	既有防護措施	嚴重性	可能性	風險等級	改善建議
高流量	無具危害之發現						
低/無流量	氫氣來源供應不足	F-3001燒毀造成氫氣外泄火災爆炸	1.F-3001進口端設有FT-3003A~C(2oo3)低低流量警報與連鎖IS-3009關停F-3001 2.F-3001設有TAHH-3007，TI-3005/3006/3007高溫警報	5	2	3	1.CHECK FALL-3003操作範圍是否符合低低流量需求 2. FT-3003A~C(2oo3)低低流量警報與連鎖IS-3009關停F-3001安全儀錶功能規格需達SIL 1
流動方向錯誤	無具危害之發現						

HazOp Example -1.2

製程偏離	可能原因	危害/後果	既有防護措施	嚴重性	可能性	風險等級	改善建議
逆流	無具危害之發現						
錯誤組成	無具危害之發現						
高濃度	上游工廠一氧化碳來源濃度過高	R-3003高溫失控導致洩漏，氫氣引起局部火災	1. 由S31/32取樣分析判斷是否挾帶過多雜質 2.要求上游工廠建立聯繫機制 3. TI-3009監測溫度	4	4	4	R-3003出口TE-3009改為TT-3009，增加兩個TT及IS(2oo3)作動IS-3009關停F-3001並同時關斷進料閥PV-3034. 並做高溫及高高溫警報，此SIF之等級需達SIL 1

HazOp Example -1.3

製程偏離	可能原因	危害/後果	既有防護措施	嚴重性	可能性	風險等級	改善建議
高溫	1.TT/TIC/JC-3003 故障 2. 3.同低/無流量	1.F-3001燒毀造成氫氣外泄火災爆炸 2.造成R-3003觸媒結焦	1.F-3001設有TE-3007A/B及TE-3005A/B高高溫警報與連鎖IS-3009關停F-3001 2.F-3001出口端設有TT-3068A~C(2oo3)高高溫警報與連鎖IS-3009關停F-3001	5	2	3	
低溫	無具危害之發現						

HazOp結合保護層分析(LOPA) -1

事件後果	嚴重性	起始失效事件	起始失效事件可能性	一般安全設計	基本程序控制系統	警報	額外消減措施	獨立保護層	中間事件可能性	安全儀錶系統完全性等級	消減後的事件可能性
F-3001燒毀造成氫氣外洩火災爆炸	5	氫氣來源供應不足	1E-1	0.1	0.1 (TIC-3003)	0.1 (TAHH-3007，TI-3005/3006/3007高溫警報)	1	1	1E-4	1E-1 (SIL 1)	1E-5
R-3003高溫失控導致洩漏, 氫氣引起局部火災	4	上游工廠一氧化碳來源濃度過高	1E-2	0.1	1	1	1	1	1E-3	1E-1 (SIL 1)	1E-4

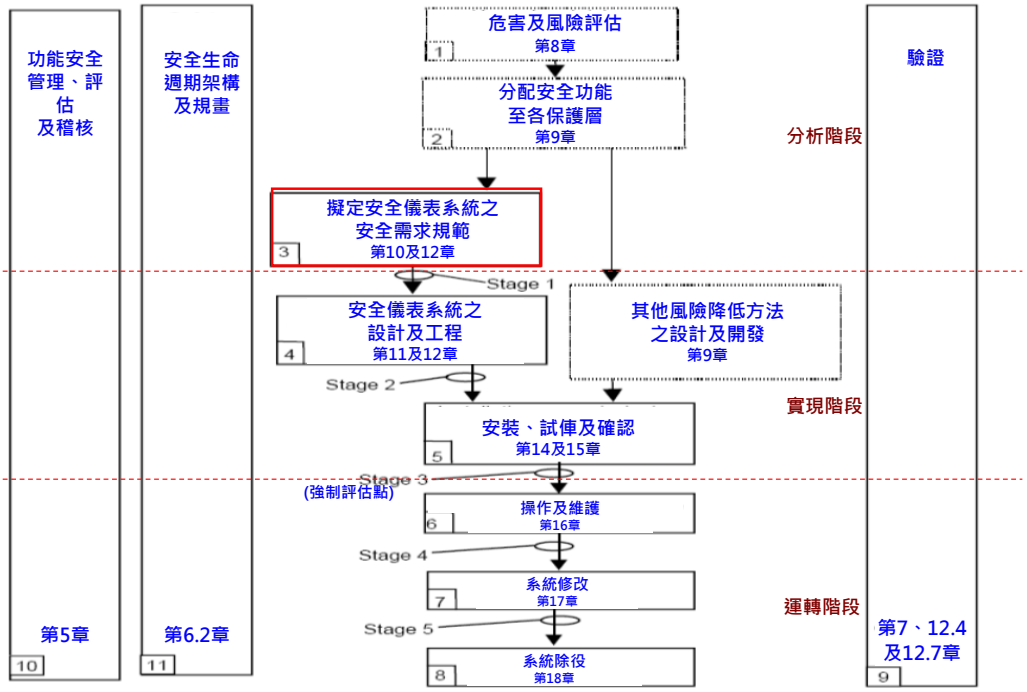
HazOp Example -2

製程偏離	可能原因	危害/後果	既有防護措施	嚴重性	可能性	風險等級	改善建議
低/無流量（氣相甲醇）	1.FT/FIC/FV-E201故障開度過小或全關；2.上游單元甲醇進料泵P-3710A/B故障；3.LT/LIC/LV-E401故障開度過小或全關。	反應器催化劑失去流化，導致死床、悶床，嚴重時局部過熱或溫度失控，造成反應器燒穿，烯烴外洩造成火災爆炸。	1.FIRSA-R101低警報及低低警報並聯鎖關HV-R101、開HV-R102，大量補蒸汽；2.反應器內壁襯隔熱耐磨襯裡；3.反應器附近設有可燃氣體檢測器。	5	3	4	1.TIC-R107A~D/TIC-R110A~D增設八取三高高溫警報，並聯鎖作動IS-01，安全儀錶功能需SIL2；2.增加一條與HV-R102平行的LS3管線與閥門；3.HV-R101密封等級(TSO)4級以上；4.甲醇進料泵P-3710A/B運轉狀態送至FMTP製程中控室顯示。
低/無流量（液相甲醇）	FT/FIC/FV-R107故障開度過小或全關。	催化劑結焦，導致再生器負荷增加。	反應器反應段設有多組溫度計。	1	4	1	

HazOp結合保護層分析(LOPA) -2

事件後果	嚴重性	起始失效事件	起始失效事件可能性	一般安全設計	基本程序控制系統	警報	額外消減措施	獨立保護層	中間事件可能性	安全儀錶系統完全性等級	消減後的事件可能性
反應器催化劑失去流化，導致死床、悶床，嚴重時局部過熱或溫度失控，造成反應器燒穿，烯烴外洩造成火災爆炸。	5	1.FT/FIC/FV-E201故障開度過小或全關；2.上游單元甲醇進料泵P-3710A/B故障；3.LT/LIC/LV-E401故障開度過小或全關。	2.5E-1	0.1 反應器內壁襯隔熱耐磨襯裡	1	1	0.1	1	2.5E-3	4E-3 (SIL 2)	1E-5

IEC 61511 SIS安全生命週期管理



安全儀錶功能(SIF)表實例

安全儀錶功能名稱/編號	安全儀錶功能說明	危害/後果	安全儀錶功能設計架構	安全完整性等級
MCR反應器保護/IS-01	**Causes:** FIRSA-R101低低流量； TIC-R107A~D/TIC-R110A~D高高溫 **Effects:** 關斷HV-R101、PV-E401；開HV-R102、HV-R102B(新增)大量補蒸汽	反應器催化劑失去流化，導致死床、悶床，嚴重時局部過熱或溫度失控，造成反應器燒穿，烯烴外洩造成火災爆炸。	**Sensor:** Group 1: FIRSA-R101 (1oo1) Group 2: TIC-R107A~D/TIC-R110A~D (3oo8) Group voting: 1oo2 **Final actuator:** Group 1: HV-R101、PV-E401 (1oo2) Group 2: HV-R102、HV-R102B (1oo2) Group voting: 2oo2	**SIL 2**

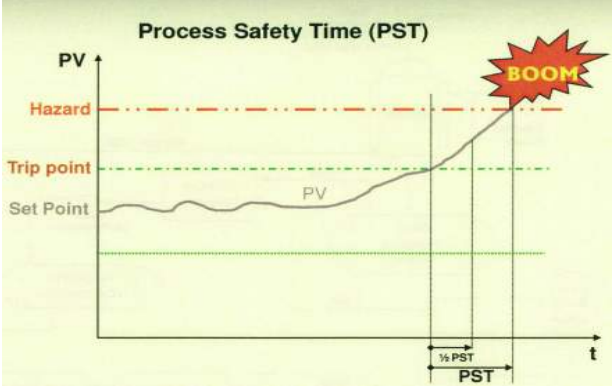
安全需求規範(SRS)要項 (1/4)

- 達到需求的功能安全所必須的所有儀錶安全功能的描述
- 識別和考慮共同原因失效
- 對每個確定的儀錶安全功能的製程安全狀態的定義
- 儀錶安全功能需求和需求率的假定來源
- 檢驗測試週期
- SIS 使製程進入某個安全狀態的回應時間要求

SRS要項 (2/4)

■ 製程安全時間 (PST)

- PST是由製程化學及製程動態的決定因素
- PST數據的唯一來源是製程工程師
- PST是在設計SIS過程中，須考慮的基本因素
- SIF應該有一個比1/2 PST更佳的反應時間



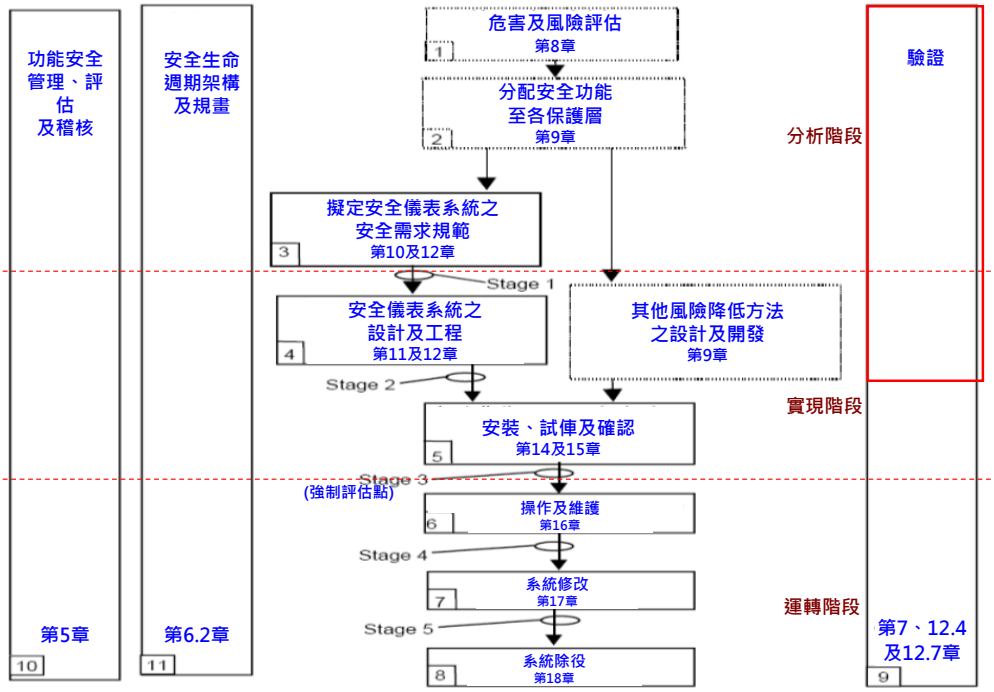
SRS要項 (3/4)

- 安全完整性等級和操作模式(低需求/連續)
- 測量和它們的作動點(trip point)的描述
- 輸出動作和成功操作準則的描述，例如關斷閥的密封要求
- 輸入和輸出之間的功能關係，包括邏輯功能、數學功能和任何要求的許可
- 手動停機要求
- 與致能(energize)或失能作動(de-energize)有關的要求
- 停機後復歸SIS的要求
- 最大允許誤作動率
- 失效模式和要求的SIS 回應(如警報、自動停機)
- 與起動和重新起動SIS 程式有關的任何特殊要求

SRS要項 (4/4)

- SIS 和任何其他系統(包括BPCS 和操作員)間的所有介面
- 凌駕/抑制/旁路要求，包括怎樣復歸
- 在檢測到SIS 中的故障事件時，達到和保持某個安全狀態所必需的任何動作的規範。任何這樣的動作都應考慮相關人員的因素
- 平均修復時間
- 需要避免的SIS 輸出狀態的危險組合
- 應識別SIS 可能遇到的所有極端環境條件。需考慮的有：溫度、濕度、污染、接地、電磁干擾/射頻干擾、衝擊/振動、靜電放電、用電區等級、水災、雷電和其他有關因素
- 任何能承受重大意外事故的儀錶安全功能要求的定義，例如在火災事故中閥門保持可操作性的時間要求

IEC 61511 SIS安全生命週期管理



安全完整性

硬體安全完整性 ＋ 系統安全完整性 ＝ 安全完整性

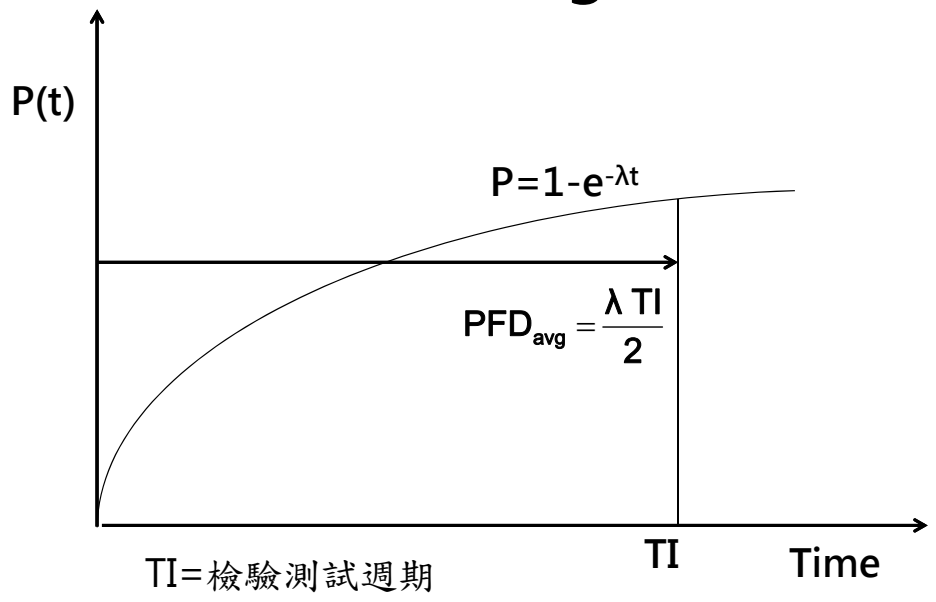
- **硬體安全完整性**

  與隨機硬體失效有關的安全相關系統安全完整性的一部分，例如：繼電器：無法開啟或關閉；二極體，電晶體：正極/負極/發射極斷線，短路；電池老舊；接線耗損；接觸腐蝕造成無法導電；組件隨機失效

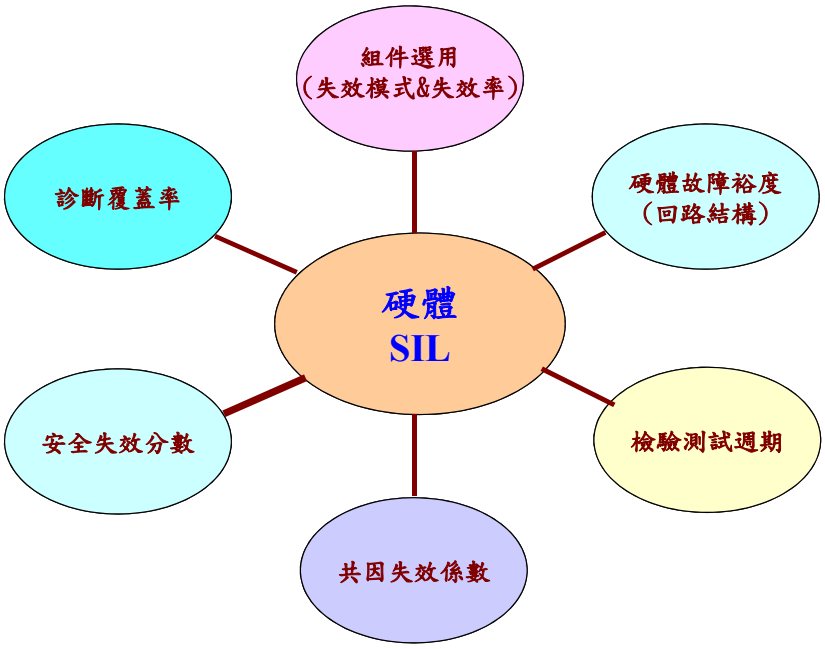
- **系統安全完整性**

  與系統失效有關的安全相關系統安全完整性的一部分，例如：系統設計錯誤；換上不正確的備品；錯誤的配置；軟體病毒；錯誤的軟體版本；操作員關錯開關

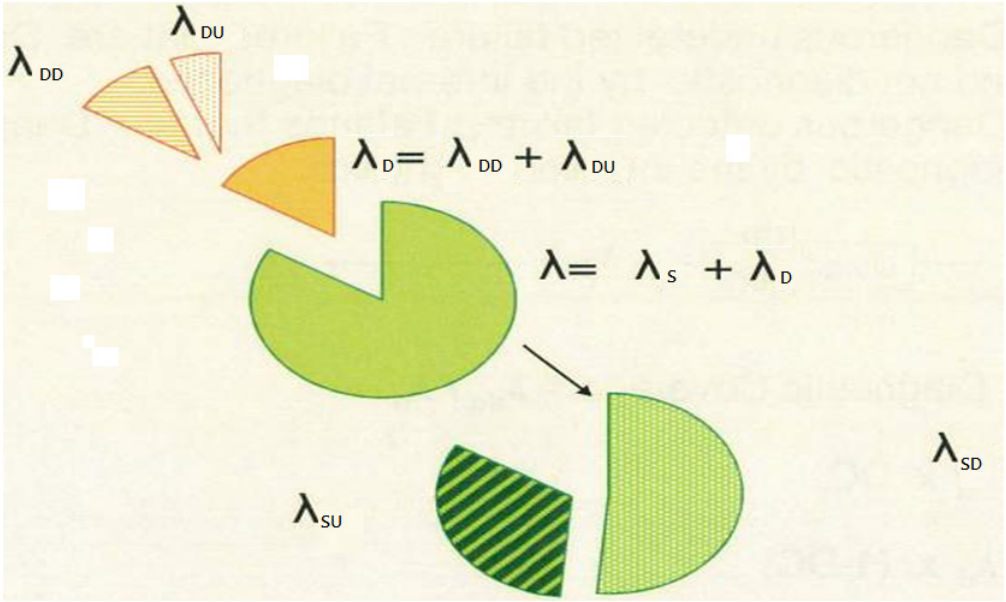
PFDavg



影響硬體SIL驗證的主要變數



危險失效及安全失效組成



終端元件失效模式和類型

- 與安全相關的閥，正常開&正常帶電
- 在失控狀態下，閥必須關閉

安全失效
失電時，自然關閉

未被檢測出

檢測出
通過電壓測試

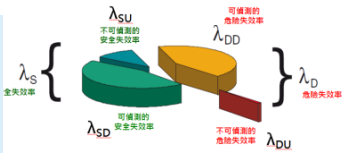
危險失效
卡在開位置

未被檢測出

檢測出
通過閥位“閃動”測試

安全失效分數(Safe Failure Fraction, SFF)

$$SFF = \frac{(\lambda_{su} + \lambda_{sd} + \lambda_{dd})}{(\lambda_{su} + \lambda_{sd} + \lambda_{dd} + \lambda_{du})}$$



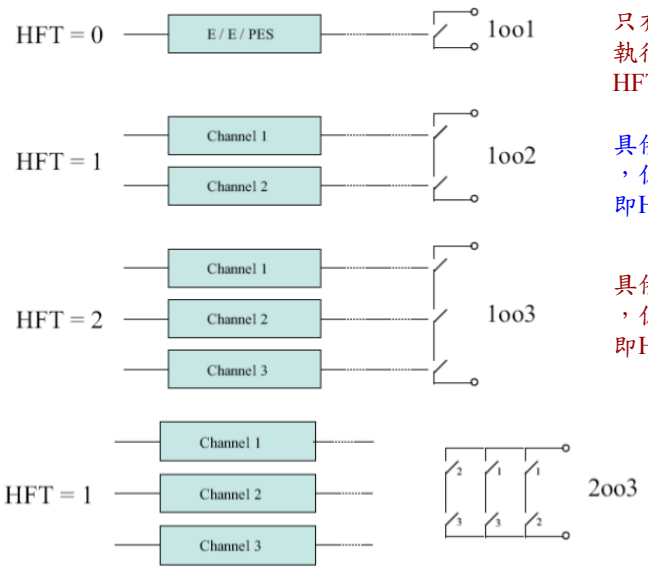
SFF (安全失效分數): 子系統的安全失效率及可偵測危險失效率的總和在子系統全部失效率所占的比例，例如：SFF = 0.9 表示90%的失效故障為安全失效，不會導致安全性喪失

IEC 61511-2 第11.4條款定義SFF為在SIS的運作上，對於冗餘和診斷覆蓋率的需求選擇時的關鍵因素

硬體故障裕度(Hardware Fault Tolerance, HFT)

- 硬體故障裕度 (HFT)：
  - 子系統在一個(或多個)硬體危險失效的情況下，仍能繼續維持安全功能的容錯能力
  - 亦即子系統配置能夠容忍的危險失效數目。
  - HFT = N，表示 N+1 個故障將導致危險失效。
  - HFT 不考慮診斷措施的影響。

HFT (硬體故障裕度)



只有1個通道，當此通道失效，即無法執行安全功能，造成危險失效，亦即HFT=0。

具備2個通道，即使任一通道功能失效，仍有1個通道能夠執行安全功能，亦即HFT=1 。

具備3個通道，即使任一通道功能失效，仍有2個通道能夠執行安全功能，亦即HFT=2 。

具備3個通道，每個輸出通道皆與其他通道兩兩串聯構成表決電路(可減少例如誤動作的安全失效)，但只要1個通道發生危險失效(造成串聯的另一通道失效)，將只剩1個通道能夠執行安全功能，亦即HFT=1。

子系統的結構約束(IEC 61508-2, Table 2 & 3)

- 硬體的最高安全完整等級會受到子系統的複雜度類型、SIL 聲明限制(SIL claim limit)、安全失效分數(SFF)及硬體故障裕度(HFT)等因素的限制。

A類 (簡單型)

安全失效分數 (Safe Failure Fraction, SFF)	硬體故障裕度 (Hardware Fault Tolerance, HFT)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % -≤90 %	SIL 2	SIL 3	SIL 4
90 % -≤ 99 %	SIL 3	SIL 4	SIL 4
≥99 %	SIL 3	SIL 4	SIL 4

1oo1	1oo2	1003
1oo1(D)	1oo2(D)	1oo3(D)
2002	2oo3	2oo4(D)
NooN	NooN+1	NooN+2

B類 (複雜型)

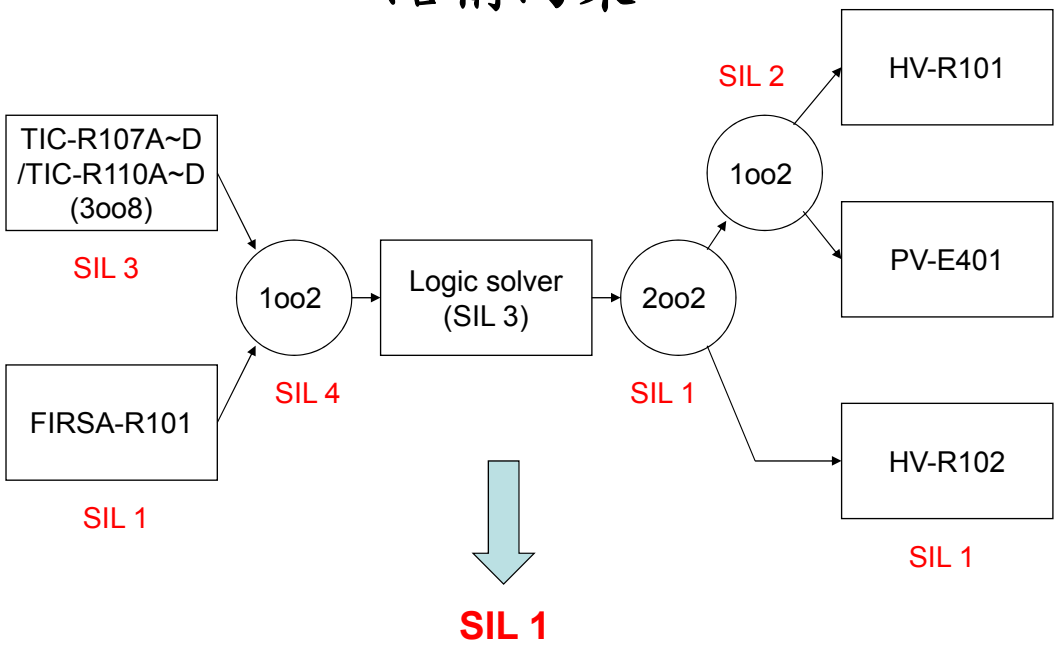
安全失效分數 (Safe Failure Fraction, SFF)	硬體故障裕度 (Hardware Fault Tolerance, HFT)		
	0	1	2
< 60 %	***Not allowed***	SIL 1	SIL 2
60 % -≤90 %	SIL 1	SIL 2	SIL 3
90 % -≤ 99 %	SIL 2	SIL 3	SIL 4
≥99 %	SIL 3	SIL 4	SIL 4

1oo1	1oo2	1oo3(D)
1oo1(D)	1oo2(D)	2oo4(D)
2oo2	2oo3	NooN+2
NooN	NooN+1	

符合IEC 61511的硬體故障裕度 - 感測器和終端元件

IEC 61511- Part 1 表6 感測器、終端元件和非-PE邏輯處理器	
SIL	最小硬體故障裕度
1	0
2	1
3	2
4	適用特別的要求 – 請見 IEC 61508

結構約束



SIL 驗算(Verification)

ISA TR84.00.02

- **Sensor part:**

PFDavg,s1 = PFDavg,s1,i + PFDavg,s1,ccf = 0 + 1/2 $\beta\lambda_{DU}$ t
=0.5x0.05x305x10^{-9}x17520 = 1.34x10^{-4}

PFDavg,s2 = 1/2 λ_{DU} t = 0.5x3600x10^{-9}x17520 = 3.15x10^{-2}

PFDavg,s = PFDavg,s1 x PFDavg,s2 = 1.34x10^{-4} x3.15x10^{-2}
= 4.22x10^{-6}

- **Logic Solver:**

PFDavg,L = 1/2 λ_{DU} t = 0.5x241x10^{-9}x17520 = 2.11x10^{-3}

- **FE:**

PFDavg,v1 = 1/3 (λ_{DU1} λ_{DU2})t^2 = 1/3x(3225x10^{-9}x17520)^2
= 1.06x10^{-3}

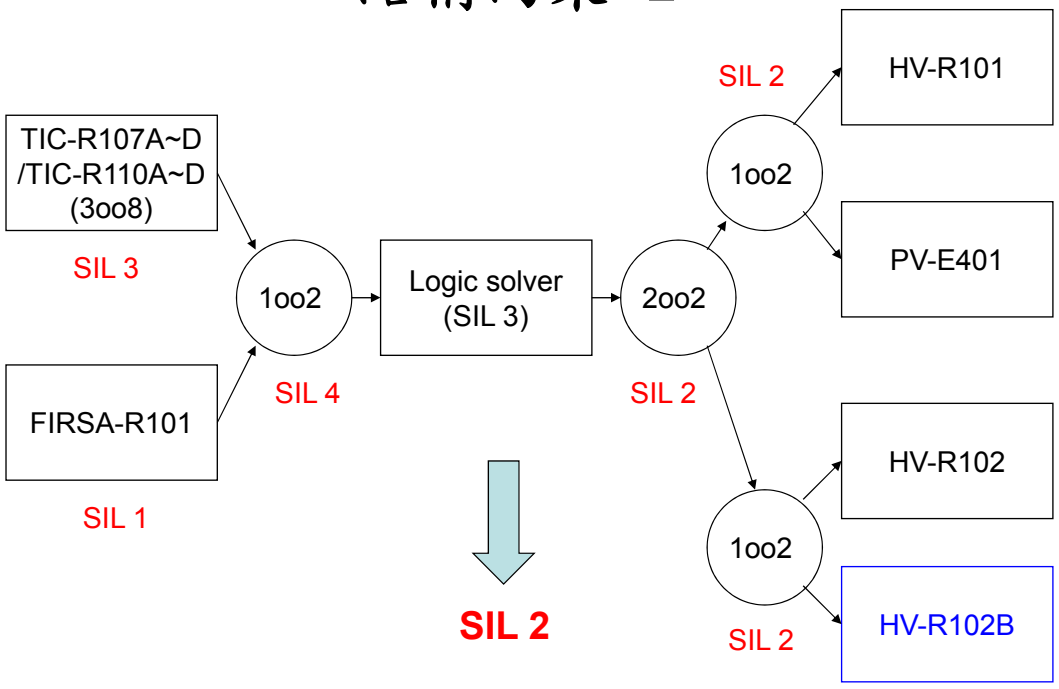
PFDavg,v2 = 1/2 λ_{DU} t = 0.5x1925x10^{-9}x17520 = 1.69x10^{-2}

PFDavg,v = PFDavg,v1 + PFDavg,v2 = 1.06x10^{-3} + 1.69x10^{-2}
= 1.8x10^{-2}

PFDavg = PFDavg,s + PFDavg,L + PFDavg,v = 4.22x10^{-6} + 2.11x 10^{-3}
+ 1.8x10^{-2} = 2.01x10^{-2}

- SIL 2 ?

結構約束 -2



SIL驗算-2

- PFDavg,v2 = 1/3 $((1-\beta)\lambda_{DU}\, t)^2$ + 1/2 $\beta\lambda_{DU}\, t$
- = $1/3\times(0.95\times1925\times10^{-9}\times17520)^2 + 0.5\times0.05\times1925\times10^{-9}\times17520$
- = $3.42\times10^{-4} + 8.43\times10^{-4} = 1.19\times10^{-3}$
- PFDavg,v = PFDavg,v1 + PFDavg,v2 = $1.06\times10^{-3} + 1.19\times10^{-3}$
- = 2.25×10^{-3}
- PFDavg = PFDavg,s + PFDavg,L + PFDavg,v = $4.22\times10^{-6} + 2.11\times10^{-3} + 2.25\times10^{-3} = 4.36\times10^{-3}$
- → SIL 2