# 安全儀控系統設計_評估分析階段

簡村德 / 呂信忠

長春企業集團

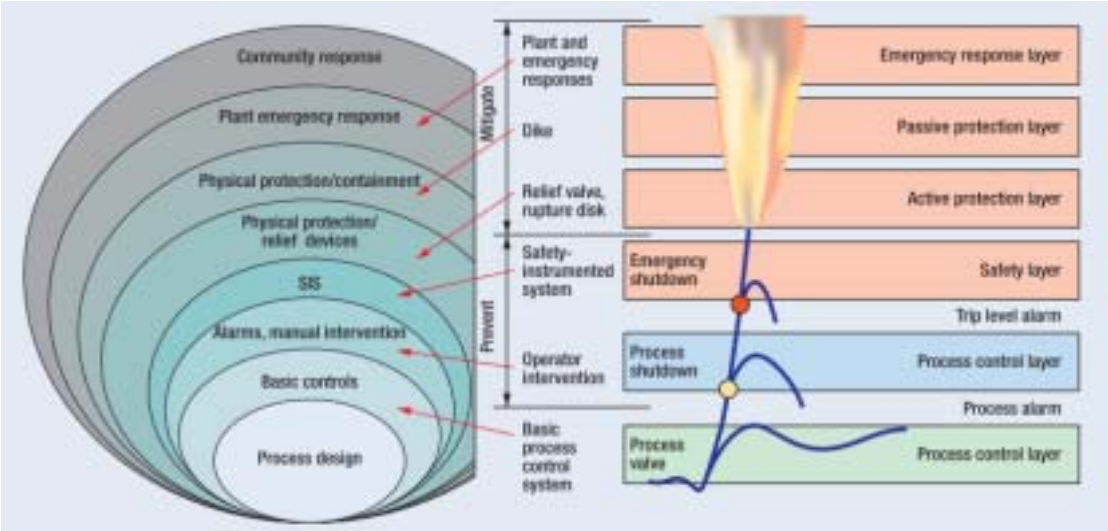
針對『製程控制類別』使用之安全儀錶系統(SIS)標準 IEC-61511 已於 2003 年發布，並將『生命週期』概念導入安全儀控系統中，而 ISA 標準 84.01-1996 亦於 2004 年將 IEC-61511 的標準原封不動的置入其標準裡，成為 ISA 84.00.01-2004，至此一個全新且廣被接納的技術已然成形，設計人員可依標準內容設計出符合公司安全標準要求而又不至於過度設計的安全儀控系統，在經濟、有效且合理可行的前提下來確保公司/工廠的安全在可接受的範圍內進行最後一道防線的把關工作。

IEC-61511 SIS safety life cycle 共有三個主要工作層面(11 個工作階段)，分別為 Analysis phase、Realization phase 與 Operation phase，本文即針對第一個工作層面 analysis phase 來進行探討，以標準內所提及的五個評估方法來決定製程系統所需要安全儀表功能(SIF)的安全完整性等級(SIL)。

五個評估方法分別為：Fault Tree/Event Tree、Safety layer matrix、Calibrated risk graph、Risk graph 與 Layer of Protection analysis (LOPA)，經比較各項評估方法與考慮實際應用概況，長春公司採用第五種方法-保護層分析來進行新建廠的安全儀表系統設計需求評估，並藉此一評估結果進行第二個工作層面的基本設計、驗算與安全需求規格的開立等。

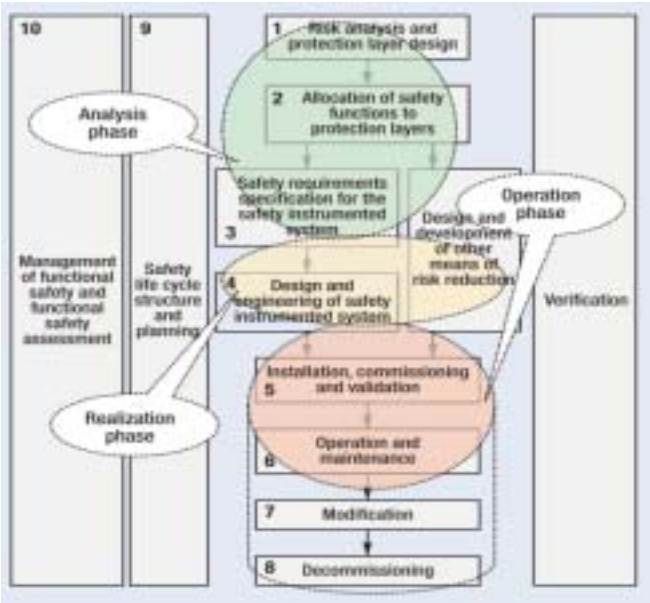
## 一、前言

在製程工廠中為了防止危險事件的發生，會在製程危險條件出現初期採取適當的措施以避免該事件危害人員安全、汙染環境或造成設備/經濟上的損失，舉凡分散式連鎖控制系統、警報裝置、洩漏偵測裝置、安全閥/呼吸閥、消防系統等都是常見的製程控制與安全防護裝置，其中有關安全儀表系統(Safety Instrument System, SIS)則是預防嚴重事件發生的最後一道防線，在安全閥啟動或洩漏偵測警報啟動之前，將製程系統引導至安全狀態(如圖一)。




圖一 獨立保護層[1]

安全儀表系統目前在石油化學工業已被廣泛應用，應用依循的標準為 IEC-61511 或 ANSI/ISA-84.00.01-2004，兩個標準的內容完全相同，在包含 Verification 共 11 個工作項目裡，將其區分為主要的三個工作層面(如圖二)，其中首要的工作即是利用風險分析的方法來決定該製程單元需要何種等級的安全儀表系統安全功能，不同等級的安全儀表系統費用可能會相差數倍，所以若評估階段能清楚的定義出該評估點所需的風險降低量(Risk Reduction Factor, RRF)或風險值，則安全儀表系統的設計即可搭配可靠度適當的偵測器/PLC/關斷閥來達成各該製程系統的風險目標值，避免系統可能的安全度不足或過度的安全設計。

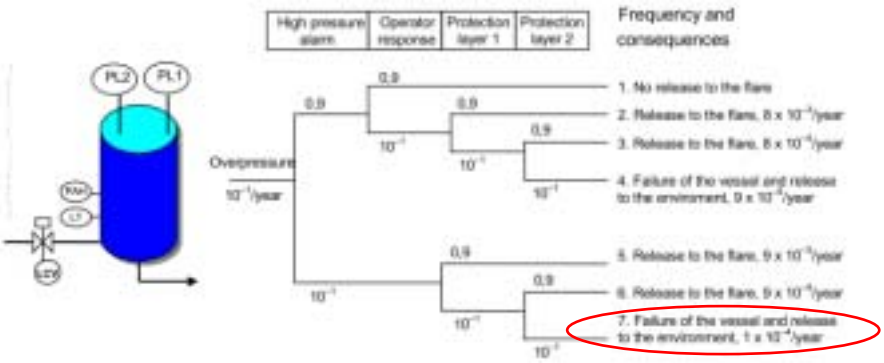



圖二 IEC-61511 SIS safety life-cycle phases[1]

## 二、風險評估方法介紹

### （一）Fault Tree / Event Tree

失誤樹與事件樹互為果因/因果的評估方法，利用此一方法來進行風險降低量的評估與保護層分析方法(LOPA)相當類似，在進行評估之前需要先建立企業所能接受的風險目標值，並藉由失誤樹/事件樹分析評估手法所估算出來的事件發生機率值與風險目標值比對，其中間的差值即為風險缺口，表示系統須再增加其他的降低風險值設計(如增設安全儀表系統)。以圖二使用之事件樹分析為例，假設該設備在既有的各項製程安全操作與防護措施皆失效的情況下發生超壓洩漏事件(發生機率為 $10^{-4}$/year)，若該事件發生的風險目標值為 $10^{-5}$/year，則表示該系統需要新增的風險降低措施，以增設安全儀表系統為例，增設安全完整性等級(Safety Integrity Level, SIL)SIL1 可降低事件的發生機率 10~100 倍，SIL2 可降低事件的發生機率 100~1000 倍，SIL3 可降低事件的發生機率 1000~10000 倍，至於 SIL4 因不會應用在普通的製程工業，故不贅述，讀者可參考表一之說明。本事件只要增設可達 SIL1 之安全儀表系統即可符合風險目標的要求。




圖二 超壓洩漏事件樹應用範例[2]

表一 安全完整性等級風險降低表

| Safety Integrity Level (SIL) | Target Failure Measures for a safety function allocated to an E/E/PE safety-related system | |
|---|---|---|
| | Low demand mode of operation<br>Average probability of failure/demand | High demand/continuous mode of operation<br>Dangerous failure rate [per hour] |
| 4 | >=$10^{-5}$ to <$10^{-4}$ | >=$10^{-9}$ to <$10^{-8}$ |
| 3 | >=$10^{-4}$ to <$10^{-3}$ | >=$10^{-8}$ to <$10^{-7}$ |
| 2 | >=$10^{-3}$ to <$10^{-2}$ | >=$10^{-7}$ to <$10^{-6}$ |
| 1 | >=$10^{-2}$ to <$10^{-1}$ | >=$10^{-6}$ to <$10^{-5}$ |

（二）Safety layer matrix

安全保護層矩陣以既有的危害性與可操作分析為基礎，藉著將可能性(高、中、低)與嚴重性(非常嚴重、嚴重、輕微)各分為三級，以 3×3 的矩陣搭配現有存在的獨立保護層數量來決定需要的安全儀表系統功能等級。

表二 以 Safety layer matrix 來決定系統 SIF 等級[2]

| Number of PL's | SIL level required | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | | | | | | | c) | 1 | 1 |
| 2 | c) | c) | 1 | c) | 1 | 2 | 1 | 2 | b) 3 |
| 1 | c) | 1 | 2 | 1 | 2 | b) 3 | b) 3 | b) 3 | a) 3 |
| Hazardous event likelihood | Low | Med | High | Low | Med | High | Low | Med | High |
| | Minor | | | Serious | | | Extensive | | |
| | Hazardous event severity rating | | | | | | | | |

表二為 Safety layer matrix 主要的依循表格，倘若評估小組已先將系統風險的嚴重度與可能性定義出來(假設嚴重度為非常嚴重-Extensive、可能性為中等-Med)，再找出系統設計中是否有獨立保護層的存在(假設有三個-)，則根據表二此處需要一 SIL1 的安全儀表系統功能。表二 a:代表此處除需要設計一 SIL3 的 SIF 外，還需要其他的風險降低措施；b:代表此處除需要設計一 SIL3 的 SIF 外，可能還需要其他的風險降低措施；c:代表此處不需要設置 SIF。

（三）Calibrated risk graph

標準化的風險圖像方法使用了四個主要的判定參數來決定系統可能需要的 SIF 等級，分別為 C:嚴重度(Consequence)、F: 曝露率(Occupancy)、P:事故發生率(Probability of avoiding the hazard)與 W：需求率(Demand rate)，茲將此四個參數應用簡要說明如下:

1. 嚴重度(Consequence):

   嚴重度可區分為人員傷害與環境影響(財物損失未列在標準中故不談論)，人員傷害部分搭配傷害率 V(Vulnerbility)與事故現場人員數量(Numbers of people present when the area exposed to the hazard)來進行分類，以洩漏量為基礎，小量可燃物或毒性物質洩漏則 V 值設定為 0.01、大量可燃物或毒性物質洩漏則 V 值設定為 0.1、劇毒性物質或可燃物著火機率高者則 V 值設定為 0.5、設備/反應器破裂或爆炸則 V 值設定為 1，以 V 值與曝露人員數量相乘，所得之積若小於 0.01 則屬 Minor injury，分類表以 $C_A$ 來表示；乘積為 0.01~0.1 則以 $C_B$ 來表示，乘積為 0.1~1 則以 $C_C$ 表示，乘積為 1 以上則以 $C_D$ 表示。

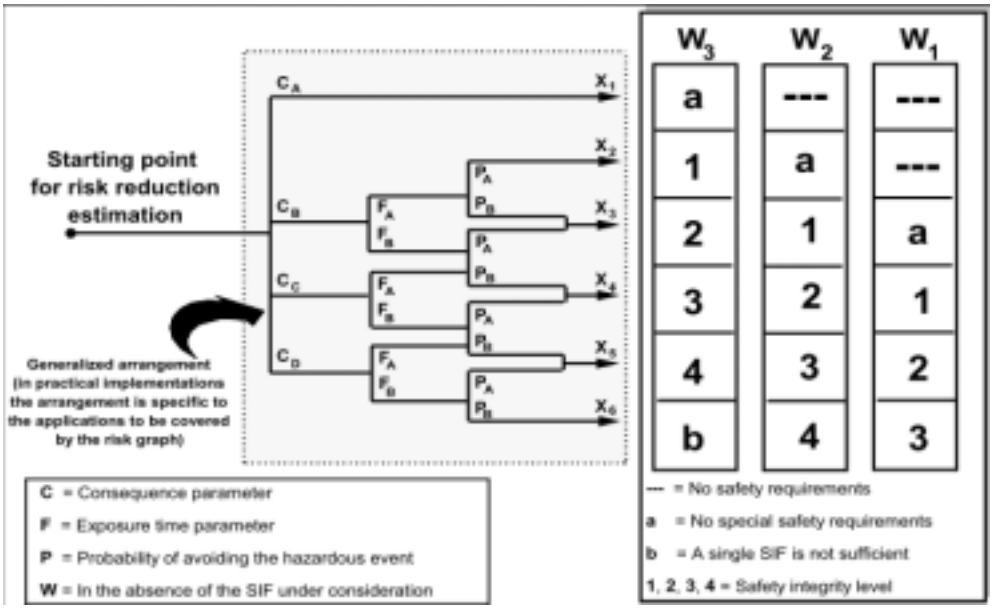
2. 曝露率(Occupancy):

   曝露率指的是在正常的工作週期內，人員會在該評估的事故地點出現的時間比率，比如一天 24 小時內有 12 小時會有人員在該地點工作，則曝露率則為 0.5，如曝露率小於

0.1，則屬於低曝露率以 $F_A$ 表示，若大於 0.1 則屬於經常性的高曝露率以 $F_B$ 表示。

3. 事故發生率(Probability of avoiding the hazard):
   事故發生率是指若異常事件發生，可避免該異常事件演變為意外事故的機率，若 a. SIS 失效可發出警示給操作人員、b. 獨立的設施作動可避免危害發生或人員可全部撤離至安全區預、c.警報發出後操作人員尚有超過一小時或有足夠的時間進行處理等三項全部成立時則認為該事件造成人員的傷害可有效被避免並以 $P_A$ 表示，若條件無法成立則以 $P_B$ 表示。
4. 需求率(Demand rate)
   需求率指該異常事件在一年週期內且不考慮 SIF 的情況下可能的發生次數，評估時可將現有的控制系統納入考量，唯若控制系統未依 IEC-61511 進行設計與維護則可靠度不可超過 SIL1。若需求率低於 0.1D/year(D 為校正因子，可容許的殘餘風險值)則以 $W_1$ 表示，介於 0.1D~1D/year 以 $W_2$ 表示，介於 1D~10D/year 以 $W_3$ 表示，若需求率大於 10D/year 則需要高等級的 SIF。

決定出四項參數值之後即可利用圖三來決定所需 SIF 等級。

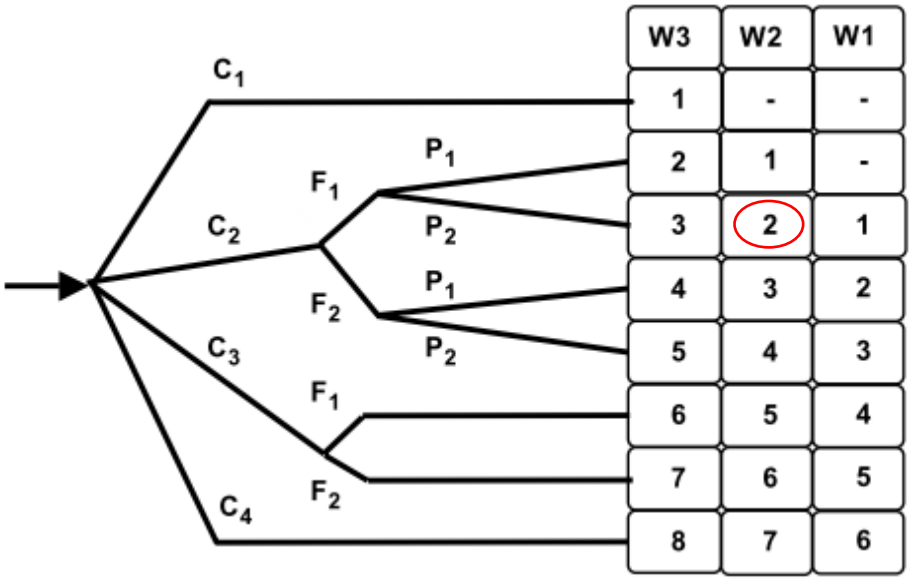



圖三 風險圖(Calibrated risk graph) [2]

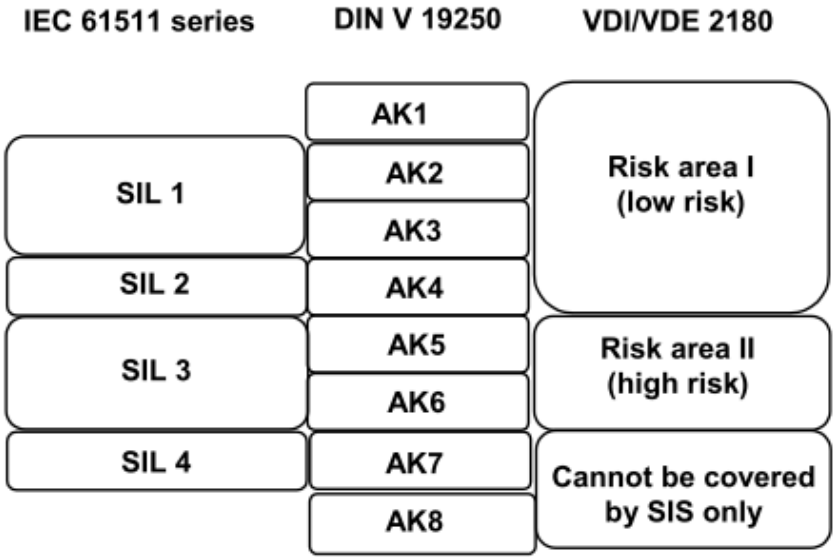
（四）Risk graph

Risk graph 是由德國標準 DIN19250 所發展出來的定性分析方法，與 Calibrated risk graph 同樣都是使用 C：嚴重度(Consequence)、F：曝露率(Occupancy)、P：事故發生率(Probability of avoiding the hazard)與 W:需求率(Demand rate)等四個參數來進行，不同之處在於各項參數的定義與風險圖的路徑，屬於較簡易型的評估方式，茲將此一方法簡要說明如下：

C：$C_1$-輕度傷害、$C_2$-重度永久性傷害/一人死亡、$C_3$-數人死亡、$C_4$-更大量人員死亡；F：$F_1$-低曝露率、$F_2$-經常性曝露；P: $P_1$-可能避免、$P_2$-不可能避免；W：$W_1$-非常低的事件發生機率、$W_2$-較低的事件發生機率、$W_3$-相對較高的事件發生機率。評估小組定義出 C、F、P、W 值後，搭配圖四的風險圖可得到 1~8 的數值(相當於 AK1~AK8)，再利用圖五 IEC-61511 與 DIN V 19250 的相對比較表來決定系統所需要的 SIF 等級，例如評估出來的結果是 $C_2$ -> $F_1$ -> $P_2$ -> $W_2$，所得數值為 2(AK2)，AK2 在圖五的比較表中相當於需設計符合 IES-61511 規範 SIL1 的 SIF。




圖四 風險圖(Risk graph) [2]




圖五 風險圖(Risk graph) [2]

（五）Layer of Protection analysis (LOPA)

保護層分析方法主要應用搭配的製程危害分析方法為危害與可操作分析(HazOp)，在執行評估前與 Fault Tree / Event Tree 相同須先設定組織的風險目標，風險目標的設定各公司可能不盡相同，表三為各國政府對風險目標的可接受概況表，讀者可依自身公司的文化/規模/特性自行建立。

表三 各國政府機構引用之個人死亡風險標準表

| 機構及應用 | 最大容許風險 | 可忽視風險 |
|---|---|---|
| 荷蘭(既有工廠或結合新工廠) | $10^{-5}$ / year | $10^{-8}$ / year |
| 英國(既有具潛在危害性工業) | $10^{-4}$ / year | $10^{-6}$ / year |
| 英國(鄰近新社區之既有工廠) | $3\times10^{-5}$ / year | $3\times10^{-7}$/year |
| 香港(新工廠) | $10^{-5}$ / year | 不採用 |
| 美國加州(新工廠) | $10^{-6}$ / year | 不採用 |
| 新南威爾斯(新工廠) | $10^{-5}$ / year | $10^{-7}$ / year |

風險目標除了人員死亡/失能傷害/輕度傷害的風險外，亦可考慮環境影響、可燃性物質洩漏量與毒性物質洩漏量的影響等(必要時亦會導入財物損失、停工天數與公司聲譽等財務性指標)。進行完 HazOp study 後，將 HazOp Form 中的可能危

害/後果、嚴重性、可能原因、可能性、防護措施、改善建議等六個欄位填入保護層分析應用表格(表四)內的欄 1、2、3、4、5、6、7 等欄位中，接下來保護層分析的主要工作即是將各欄位失效率值填入列 1、2 中，失效率值可參考 OREDA(Offshore Reliability Data) handbook、CCPS(Center for Chemical Process Safety of the AIChE )或其他具公信力的參考書籍與文章，亦可使用自廠設備元件的使用經驗值來計算事件發生的總失效率，並填入表四第 8 欄中，再與評估一開始所制定的風險目標作比較，若總失效率值大於風險目標值則須增加保護措施來降低事件的發生機率，保護措施的設計應優先考慮符合經濟效益的其他降低風險方法，最後才進行安全儀表系統的新增設計。

表四 保護層分析應用表格[2]

| # | 1 | 2 | 3 | 4 | | 5 | | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | PROTECTION LAYERS | | | | | | | | |
| | Impact event description F.3 F.14.1 | Severity level F.4 F.14.1 | Initiating cause F.5 F.14.2 | Initiation likelihood F.6 F.14.3 | General process design F.14.4 | BPCS F.14.5 | Alarms, etc. F.14.6 | Additional mitigation, restricted access,F.8 F.14.7 | IPL additional mitigation dikes, pressure relief F.9 F.14.8 | Inter-mediate event likelihood F.10 F.14.9 | SIF integrity level F.11 F.14.10 | Mitigated event likelihood F.12 F.14.10 | Notes |
| 1 | Fire from distillation column rupture | S | Loss of cooling water | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | PRV 01 | $10^{-7}$ | $10^{-3}$ | $10^{-9}$ | High pressure causes column rupture |
| 2 | Fire from distillation column rupture | S | Steam control loop failure | 0.1 | 0.1 | | 0.1 | 01 | PRV 01 | $10^{-6}$ | $10^{-3}$ | $10^{-9}$ | Same as above |
| N | | | | | | | | | | | | | |

## 三、結語

安全儀表系統的設置可有效具體提升製程安全的可靠度，在製程發生異常偏離且危及製程安全時可自動將製程條件導引致安全狀態(Safety sate)，但並非所有製程皆須要應用安全儀表系統，原則上還是以製程的危害特性、危害物質保有量等會造成怎樣程度的影響，搭配現有的操作控制/管理措施來決定評估的系統是否在可允許的接受範圍內，若風險無法接受再來考慮增設可有效降低風險的安全設計。

## 四、參考資料

(1) R.MODI; Implementing a suitable safety instrumented system – part1, HYDROCARBON PROCESSING, 2010.

(2) BS IEC-61511-3, BRITISH STANDARD, 2003,