製程安全危害辨識風險管控措施

從危害辨識、風險分級到現場管控

講師：尹邦碩

主講人簡經歷

專業經歷

- 專業單機構工業安全衛生師
- 教育訓練機構安全衛生講師
- 前台中市政府勞動檢查處勞動檢查員(危險性機械設備)
- 前台中市政府勞動檢查處安全衛生輔導員(營造業)
- 職業安全衛生心智圖解析一作者群

專業證照

- 專技人員高等考試職業衛生技師
- 專技人員高等考試工業安全技師
- 公務人員高等考試工業安全類
- 職業衛生管理師甲級
- 職業安全管理師甲級
- 職業安全衛生管理員乙級
- ISO 45001主導稽核員

著作

從安全意識到安全價值

個人的選擇，累積成組織的文化

1 個人安全意識

察覺異常｜拒絕麻木｜主動行動

2 組織安全文化

即時回報｜彼此提醒｜主管支持

3 共同安全價值

系統屏障｜全員承諾｜安全優先

» 從『我知道』到『我們做到』，讓安全成為每一次決策的共同價值

面對風險，打造安全

忽視風險

未落實製程安全管理

洩漏｜火災｜爆炸

恐懼・不安

落實製程安全管理

教育訓練

風險評估

設備管理

人人參與・每日落實

正視風險

安全｜安心｜穩定

製程安全
系統運作正常

安全不會憑空出現，而是每個人每天努力打造出來

沒有受傷，就代表製程安全嗎？

沒有受傷 ≠ 沒有製程安全事件

認知、評估、控制、驗證

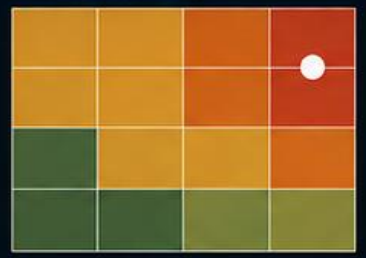
① 認知

哪裡可能失控

② 評估

失控後會發生什麼

風險評估矩陣



洩漏　火災　爆炸

③ 控制

什麼措施真正能擋住事故

氣體偵測　聯鎖停機　隔離洩壓　物理屏障

④ 驗證

控制措施是否持續有效

維修保養紀錄

- ☑ 2024/01/15
- ☑ 2024/04/15
- ☑ 2024/07/15
- ☑ 2024/10/15

功能測試

- 氣體偵測測試 ☑
- 聯鎖功能測試 ☑
- 洩壓功能測試 ☑

趨勢追蹤

有效性｜再現性

避免危險物質與能量失控

第1章

製程安全與職業安全的差異

製程安全與職業安全的差異

都是安全，但切入點不同

職業安全

控制人員作業危害

墜落｜感電｜夾捲｜暴露

墜落

感電

夾捲

暴露

共同管理介面

人員

承攬

作業許可

訓練

製程安全

預防重大失控與災難性後果

毒性｜反應性｜易燃性｜爆炸性

毒性

反應性

易燃性

爆炸性

兩者重疊，但不能互相取代

製程安全與職業安全的差異

事件頻率與後果尺度不同

頻率：由高 → 低

後果嚴重度：由低 → 高

	事件	頻率	後果	領先／落後指標
 職業安全	滑倒｜割傷｜墜落｜夾捲	相對常見 高機率	多集中於個人 相對低嚴重度	多為傷害結果指標 失能傷害｜可記錄傷害
 製程安全	大量洩漏｜火災｜爆炸｜毒性擴散	頻率較低 低機率	多人｜跨廠｜長時間 高嚴重度	事件與屏障指標 失去主圍阻｜異常停車 關鍵警報／聯鎖動作｜屏障失效

不能只用工傷數字，判斷製程是否安全

製程安全週期管理

源頭管理 × PDCA持續改善

PDCA戴明循環

P 規劃 — 防災設計

物料｜反應｜最大庫存
設計界限｜安全系統

D 執行 — 操作訓練

程序｜訓練｜交接
異常處置｜承攬管理

源頭管理

C 查核 — 變更管理與保養維護

MOC｜機械完整性
開車前安全審查

A 改善 — 評估稽核

事故調查｜稽核
績效指標｜定期再評估

設計 → 操作 → 維護／變更 → 學習改善 → 回到設計

第2章

製程危害特性與事故形成

製程危害從哪裡來？「失控源」

物質

易燃｜毒性｜腐蝕｜反應性｜低溫

能量

壓力｜溫度｜電力｜位能｜旋轉動能

失控源

製程

反應失控｜混料｜超量｜逆流｜相變化

介面

人機｜承攬商｜交接｜程序｜組織決策

想一想：哪些物質，會在製程條件下變得危險？

為何重大事故容易被低估？

低頻率

多年未發生，
不代表不會發生

連鎖性

一處失控，
可能升級至
相鄰設備

重大事故風險

高後果

多人傷亡、
停產與廠外影響

潛伏性

腐蝕、疲勞與
警報失效長期累積

複合性

設備、人員、
程序與管理缺口
交互作用

藏在零事故下的製程風險

安全績效良好，不代表製程風險受到控制

表面績效
零工傷｜表面平靜
0 工傷件數
本月累計

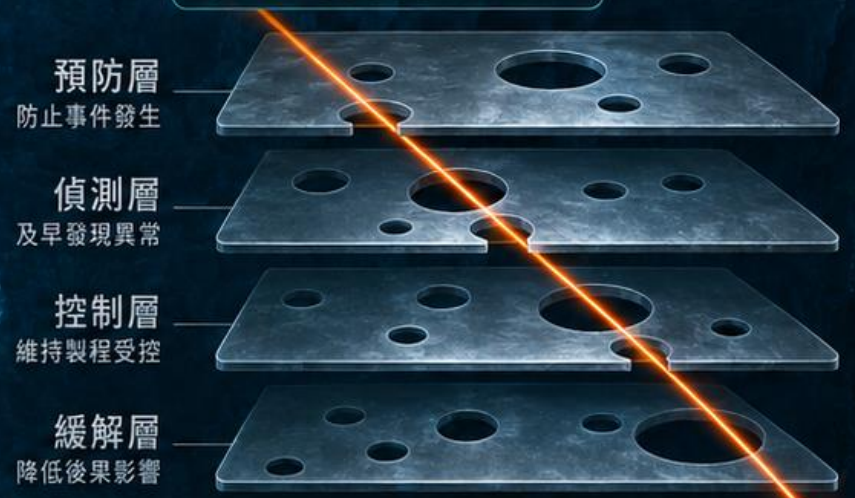
看得見的結果

受傷件數受人員暴露頻率影響

安全屏障逐漸失效

- 自動檢查未落實
- 警報旁通（Bypass）
- 法蘭洩漏
- 製程操作超限
- MOC逾期未結案
- 關鍵設備追蹤改善

多重屏障同時失效



零事故 ≠ 零風險；要看屏障是否持續有效

LNG危害不是只有「會燃燒」

超低溫

凍傷｜材料脆化｜密封失效

無加臭

嗅覺不能取代洩漏偵測

LNG液化天然氣
約−162°C

大量氣化

液態氣化後，體積約增為600倍
可燃雲｜缺氧環境

液封升壓

封閉管段內受熱氣化
可能造成快速超壓

儲槽與水域情境

蒸發氣管理｜翻滾（Rollover）
與分層｜快速相變｜
依場域評估

Bow-tie：一張圖看懂事故發展與安全屏障

失誤樹｜威脅與預防

威脅

- 接頭未鎖妥
- 軟管劣化
- 車輛移動
- 錯誤閥序
- 超壓

屏障

- 接頭確認
- 車輛防移動
- ESD／拉斷閥

頂端事件

LNG失去主圍阻

事件樹｜後果與減災

屏障

- 偵測
- 隔離
- 疏散

後果

- 低溫噴濺
- 可燃雲
- 點燃
- 缺氧
- 設備升級

屏障的任務： 避免威脅演變成頂端事件，並阻止後果持續擴大

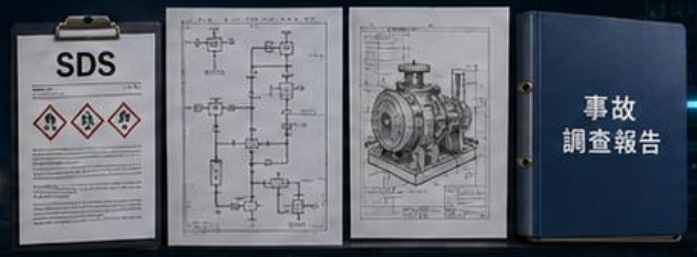
第3章
製程安全危害辨識方法

製程安全的開始

危害辨識六步驟

1 定義範圍與分析節點

2 蒐集物料、流程、設備與事故資料



3 組成跨專業團隊

4 提出偏離／失效情境

5 確認原因、後果與既有屏障

6 形成建議、責任人、期限與追蹤證據

建議行動	責任人	期限	證據	已結案
更新操作程序	張志明	2025/06/30		✓
更換洩壓閥	李建國	2025/07/15		✓
校驗壓力變送器	王小華	2025/07/10		✓
加強人員訓練	陳雅雯	2025/06/25		✓

最常見的失敗 ｜ 範圍模糊 ｜ 資料過期 ｜ 團隊不完整 ｜ 建議未結案

如何設置安全的製程?

從規劃到運轉，每一階段都必須被驗證

1 規劃與可行性

選址｜產能｜物料｜法規｜資源

2 風險評估與安全設計

辨識危害，決定安全系統

8 緊急應變演練

情境｜通報｜隔離｜疏散｜復原

3 安裝與組配

材料｜方向｜焊接｜支撐｜施工品質

7 維護與完整性管理

檢查｜保養｜校驗｜缺陷追蹤

4 耐壓與氣密試驗

確認強度、密封性與洩漏

安全製程

6 操作與運轉管理

程序｜訓練｜交接｜操作界限

5 機械與氣體試運轉

分階段驗證設備與製程功能

安全不是完工時才加入，而是每個階段都要被驗證

製程安全資訊PSI之蒐集

資料正確，危害分析才有正確的起點

危害化學品資訊

毒性 | 容許暴露濃度 | 物理數據

反應性 | 腐蝕性 | 熱與化學安定性

不相容物質與混合危害

製程技術資訊

方塊流程圖 | 製程流程圖

化學反應 | 預期最大存量

操作界限與偏離後果

製程設備資訊

建造材料 | P&ID | 防爆區域

釋壓 | 通風 | 安全連鎖與偵測

設計規範、標準與證明文件

資料驗證

文件蒐集 → 現場走查 → 圖面核對 → 確認最新版本

關鍵提醒

P&ID、閥號或連鎖邏輯若與現場不一致，再完整的分析也可能是錯的

請問學員

風險評估前，
有先到現場走查
並核對圖面嗎？

製程安全評估｜如何選擇分析方法？

初步危害分析發現潛在危害後，應依問題類型進行細部安全評估。

初步危害分析 → 發現潛在危害 → 選擇細部評估方法

細部安全評估

- **檢核表 Checklist**
  快速確認法規、標準與必要項目是否完整
- **危害及可操作性分析 HAZOP**
  系統辨識製程參數偏離、原因與後果
- **如果–結果分析 What-if**
  用假設問題探索可能事故情境
- **故障樹分析 FTA**
  由頂端事件反推失效原因與組合路徑
- **如果–結果／檢核表 What-if / Checklist**
  兼顧情境探索與標準化查核
- **失誤模式與影響分析 FMEA**
  逐項分析設備失效模式及其影響
- 其他經中央主管機關認可、具有同等功能之安全評估方法

方法選擇考量

- 評估目的
- 製程階段
- 資料完整度
- 問題複雜度

⚠ **沒有單一方法適用所有問題；必要時可組合運用**

製程危害分析與方法介紹

先問要解決什麼問題，再選擇適合的方法

問題類型	適用方法	適用階段
 初步篩選與快速檢核	Checklist | What-if	規劃 | 建造試俥 | 除役
 連續製程的操作偏離	HAZOP	製程設計 | 操作與變更
 設備與元件失效模式	FMEA	設計工程 | 維護與變更
 程序與人員操作步驟	JSA | Procedure HAZOP	建造試俥 | 操作與維護
 事故路徑與屏障失效	Bow-tie | FTA／ETA	設計 | 操作 | 事故調查

製程生命週期


規劃


製程設計


設計工程


建造試俥


操作／維護／變更


終止或廢棄

沒有最好的分析方法，只有最適合問題與階段的方法

如何設計一份有效的檢核表？

先決定要查什麼，再決定怎麼問

兩種設計起點

A 參考既有檢核表

法規 | 標準 | 同業 | 設備商 | 內部經驗

確認依據、版本、範圍與現場適用性

B 依現場自行設計

製程節點 > 操作步驟 > 危害 > 關鍵屏障 > 所需證據

檢核表設計五步驟

1 定義目的、範圍與查核對象

- 確定檢核目的與預期成效
- 界定製程範圍與查核對象
- 排定查核情境與頻率

2 蒐集現況、文件與事故經驗

- 蒐集SOP、設計圖、P&ID
- 彙整製檢紀錄與維修紀錄
- 檢視事故/虛驚事件與教訓

3 找出危害、關鍵控制與驗證證據

- 辨識危害與後果
- 確認關鍵控制與屏障
- 明確可驗證之證據來源

4 設計題目、答案與判定標準

- 一題只問一件事
- 定義可接受標準與判定邏輯
- 指定證據類型(現場/文件/照片)

5 現場試用、修正、核准與版本管制

- 現場試用並檢視可行性
- 修正題目與標準
- 核准發布並執行版本管制

題目改寫範例

✕ 模糊

設備是否安全？

✓ 可驗證

軟管接頭鎖定銷是否到位，並有現場標記或照片可確認？

好題目的四個條件

可觀察 | 可回答 | 可舉證 | 可改善

設計圖例

- 青色＝既有依據
- 橘色＝現場風險
- 綠色＝可驗證題目
- 紅色＝模糊題目

一題只問一件事；異常時要能指出位置、證據、責任與處置

檢核表分析的意義

把經驗轉成可重複執行的查核問題

核心概念

由具經驗的專業人員，
將法規、標準、程序與
事故經驗轉成查核題目

1. 建立題目
2. 現場查核
3. 回答並記錄證據
4. 形成建議與追蹤改善

LNG灌裝現場範例

檢核題目		結果
	接頭是否鎖妥？	✓
	車輪擋塊是否到位？	!
	ESD功能是否正常？	✓
	氣體偵測器是否有效？	✗

結果圖例

綠色	紅色	橘色	灰色
＝符合	＝不符合	＝待改善	＝不適用

方法特性

以定性分析為主；
加入權重或分數後，
可作為半定量工具

適用範圍

設計｜施工｜試車｜
運轉｜維護｜除役

重要限制

檢核表只能找出清單問到的問題，
不能取代團隊對新危害的分析

檢核表的製備與更新流程

從經驗清單、轉化為可驗證、可追蹤的管理工具

資訊來源

- 法規、規範與標準
- PSI與必要文件
- 操作與維護程序
- 設備手冊
- 事故與虛驚事件
- 有經驗的跨專業人員

1. 彙整資訊與查核目的
2. 擬定開放式檢核表
3. 現場試評與蒐集證據
4. 題目是否清楚、可觀察且與風險相關？
   - 修正後再試評
   - 通過
5. 形成封閉式與混合式檢核表
   - A 封閉式檢核表
   - B 混合式檢核表
6. 核准、發布、教育訓練與版本管制
7. 定期檢討與更新

流程圖例

- 青色 = 資訊輸入
- 橘色 = 設計與試評
- 綠色 = 核准發布
- 紅色 = 修正回饋

更新觸發

- 法規變更
- MOC
- 設備或程序改變
- 事故經驗
- 稽核發現

檢核表不是一次完成，必須隨現場、變更與事故經驗持續更新

檢核表分析的優點與限制

簡單好用，但不能把清單以外的風險當作不存在

優點

適用範圍廣

設計｜施工｜試車｜運轉｜維護｜除役

快速且成本低

方法簡單、容易使用，
可快速完成初步篩選

標準化與訓練

可作為操作訓練依據，
協助新進人員掌握重點

符合性與追蹤

適合確認法規、程序與
設備要求，並追蹤改善

限制

受清單內容限制

沒有完美的檢核表，
未被提問的危害可能被漏掉

高度依賴編製品質

結果受編寫者的經驗、
專業知識與更新程度影響

無法模擬事故

不適合單獨分析事故路徑、
發生頻率與後果嚴重度

不能單獨完成風險判斷

不宜作為事故調查唯一依據，
也無法單獨量化與分級

適合使用

初步篩選｜例行巡檢｜符合性查核｜教育訓練

需要搭配

HAZOP｜FMEA｜Bow-tie｜風險矩陣｜事故調查

圖例

綠色＝優勢　橘紅＝限制

青色＝適用　白色＝補充方法

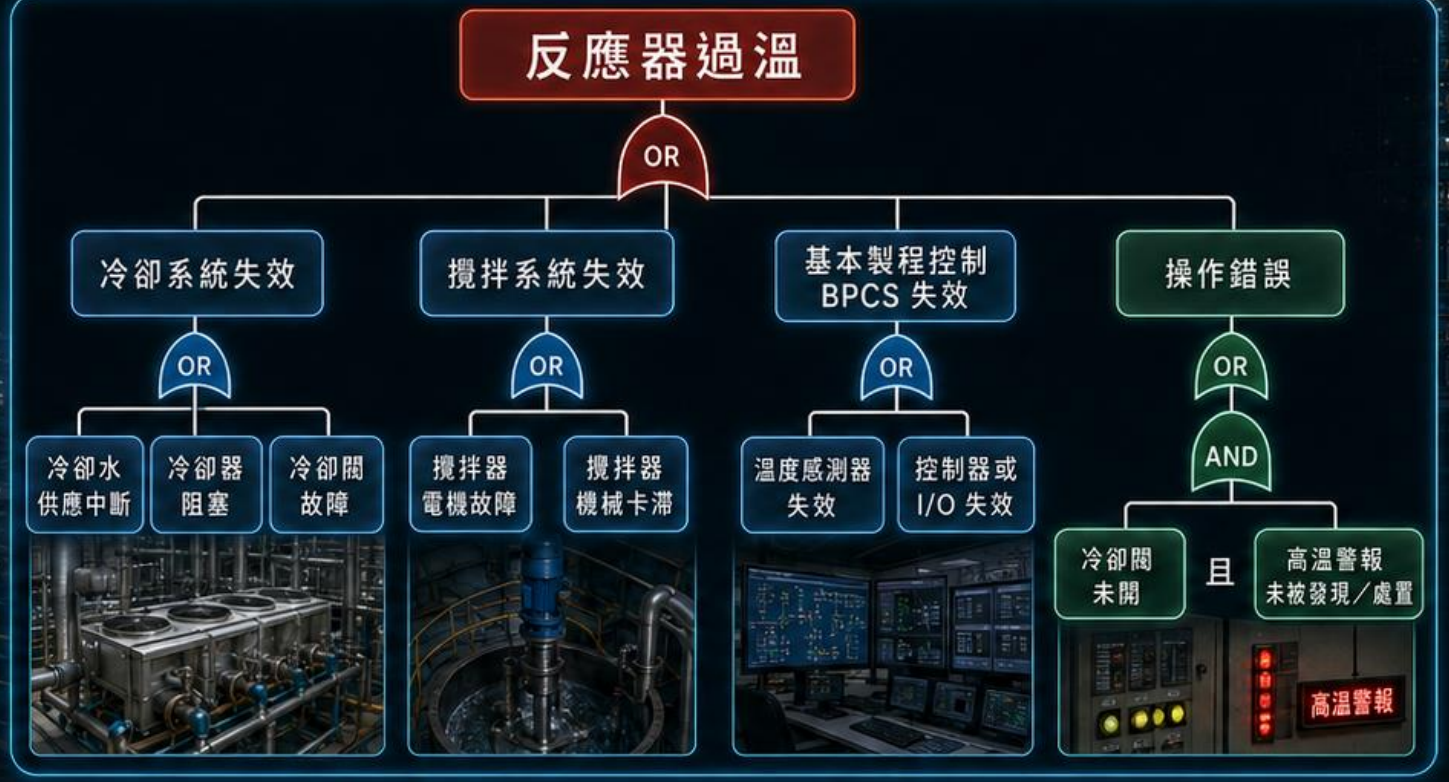
用檢核表守住已知風險，再用系統性分析找出未知與複合風險

複雜起始事件頻率｜用 FTA 拆解失效組合

當一個起始事件由多項設備、人員與控制失效共同造成時

為何使用 FTA？

- 起始事件不是單一設備故障
- 需展開設備、人員、程序及共同原因
- 避免重複計算或忽略相依性



FTA 計算規則

OR 閘：
任一事件發生即可導致上層事件

AND 閘：
所有輸入事件同時發生才導致上層事件

只有在獨立等假設成立時，才可直接使佈簡化加總或相乘

定義頂端事件 → 展開失效原因 → 確認邏輯與相依性 → 估算起始事件頻率 IEF → 帶入 LOPA

FTA 與 LOPA 的連結

FTA：
回答起始事件如何發生、發生多頻繁

LOPA：
檢查事故路徑中的 IPL 是否足夠

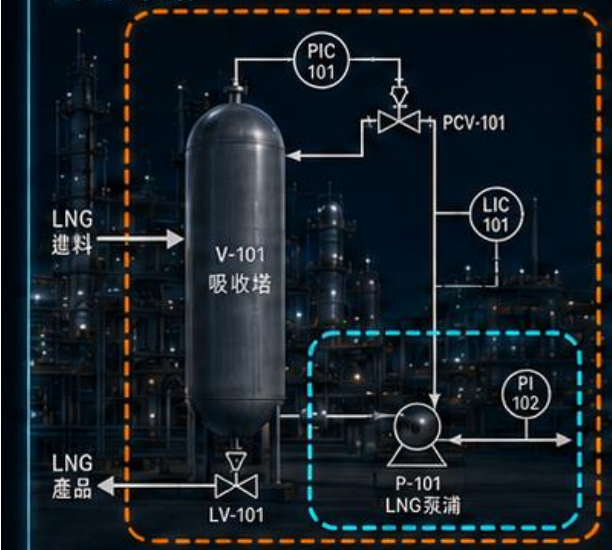
FTA 提供可信的起始事件頻率；LOPA 再評估防護後風險

HAZOP：用引導詞系統化找出製程偏離

逐節點、逐參數、逐引導詞，系統性詢問『如果偏離會怎樣？』

① 定義節點與設計目的

拆分節點



大節點
範圍過廣、設計目的多，討論容易發散

適當節點
邊界清楚、設計目的單一、資料足夠

設計目的

這個節點原本要完成什麼？

節點不是越小越好，重點是設計目的單一且邊界清楚

② 產生製程偏離

製程參數
流量｜壓力｜溫度｜液位｜組成

引導詞
No｜More｜Less｜Reverse｜Other than

引導詞 + 製程參數 = 製程偏離

範例

No	+	Flow	=	No Flow
More	+	Pressure	=	High Pressure
Reverse	+	Flow	=	Reverse Flow
Other than	+	Composition	=	Wrong Composition

評估原則

① 偏離｜僅考慮本節點
② 原因｜僅考慮本節點
③ 後果｜考慮任何地方
④ 風險等級｜考慮後果嚴重性與發生可能性
⑤ 專注於｜重大潛在危害或工廠特別關切項目
⑥ 著重｜危害辨識，而非重新設計

③ 分析與輸出

製程偏離 → 原因 → 後果 → 既有保護 → 改善建議

工作表示例

節點	設計目的	偏離	原因	後果	既有保護	建議
泵浦入口管段	穩定供應 LNG	無流量	閥門關閉／過濾器堵塞	泵浦氣蝕或跳車	低流量警報／聯鎖	強化開車確認

HAZOP工作流程

選定節點 → 確認設計目的 → 選擇參數 → 套用引導詞 → 討論原因與後果 → 檢視屏障與提出建議

⚠ HAZOP不是問設備有沒有問題，而是問設計目的可能如何被偏離

HAZOP Consequences（可能後果）定義

後果不是一個名詞，而是從偏離走向最嚴重可信損失的演變路徑

定義

偏離發生後所造成的結果，
可能影響人員、設備、營運、環境與廠外

人員 | 設備 | 營運 | 環境 | 廠外

後果演變範例

撰寫原則

- 描述完整的演變過程
- 寫到最嚴重的可信後果
- 先不假設既有保護一定成功
- 說清楚影響對象與範圍

① 生產後果

製程緊急停車｜直火設備熄火｜
觸媒中毒｜產品不合格

② 化學品釋放

排放至緩衝槽｜強酸鹼外洩｜
大規模洩漏｜毒氣擴散

③ 火災

火雨：燃燒塔噴出燃燒物

④ 爆炸

燃燒 → 熄火 → 爆炸

⑤ 環境污染

PM2.5與刺激煙塵｜溫室氣體｜
BOD／COD｜油污｜重金屬｜
病原體｜酸鹼鹽

⑥ 其他後果

酸鹼噴濺｜物體投射｜感電｜
反應失控｜設備損壞

描述後果時至少回答 如何發展？ | 影響誰？ | 範圍多大？ | 最嚴重可信結果是什麼？

先描述後果，再檢視屏障；不要因為已有保護就縮短事故演變

HAZOP Consequences（可能後果）說明

分析後果時，先假設有效的安全防護失效

警報系統 Alarm → 洩壓閥 Relief Valve → 安全閥 Safety Valve → 聯鎖系統 Interlock → 操作員 Operator → 最嚴重後果

防護措施失效

後果需考慮

1. 任一地方的後果
2. 所有防護措施失效的後果
3. 最嚴重的後果

後果描述原則

1. 後果宜作具體性的描述
2. 須定性描述人員受傷比例與程度

範例｜分離槽 V-1234

⚠ 不要因為有防護措施，就縮小事故後果

HAZOP Causes（原因）定義

係指偏離何以發生的可能理由；原因一旦具體化，偏離才具有分析意義。

人為因素

操作錯誤｜閥位錯誤｜
未依程序確認

設備失誤

設備故障｜儀表失準｜
閥件卡死｜洩漏

外在因素

電力喪失｜公用系統中斷｜
火災或環境干擾

評估節點 Node

製程偏離

例如：組成改變

可能後果

原因辨識原則

1. 僅考慮與所評估節點偏離直接相關的原因
2. 列出所有可能原因，再逐一評估其後果
3. 不要只寫「設備故障」，應具體指出故障設備與失效模式

人員／設備／外在因素 → 辨識所有原因 → 確認製程偏離 → 評估可能後果

⚠ 先問：這個偏離為什麼會發生？

HAZOP Safeguards（保護措施）定義

工程系統或行政管理措施，用來阻斷事故發展或降低損失。

工程系統 | 行政管理措施

原因 → ① 預防機制 → 製程偏離 → ② 調解機制 → 事故發生 → ③ 緩解機制 → 後果

減少偏離起因的發生機率

防呆設計｜設備保養｜程序與訓練

起因發生後，及時介入避免演變為事故

警報｜聯鎖｜操作員處置｜緊急停車

減輕已發生後果的傷害程度

消防系統｜圍阻｜隔離｜疏散

防護有效性必須經過驗證

有效防護

定期維護 | 功能測試 | 檢查紀錄 | 缺失改善

無效防護

缺乏定期維護的滅火系統

⚠ **設備存在 ≠ 防護有效；必須有可追溯的驗證證據**

Procedural HazOp | 把操作步驟當成分析節點

主要目的：辨識操作風險情境

分析節點 Node

1. **角色職責** — 操作人員 / 覆核人員
2. **操作動作** — 確認、連接、開啟、關閉
3. **設備對象** — 接地夾、軟管、閥件、ESD
4. **安全系統驗證** — 狀態、標準值、警報與聯鎖

偏離示例

1. 未確認接地
2. 提前開閥
3. 只完成部分連接
4. 操作錯誤閥件

分析重點

- 步驟可觀察性
- 接受標準
- 前後相依
- 異常復原能力

適用作業：開停車 | 取樣 | 裝卸 | 切換 | 清洗 | 旁通 | 緊急操作

LNG 灌裝研究經驗　高度仰賴人員操作時，步驟『**未確認或未執行**』常是重要風險來源。

SOP 只寫『確認正常』不夠 → 應明確寫出：確認什麼 | 標準值多少 | 由誰確認 | 異常如何停止

第４章
風險評估與風險分級

風險矩陣｜先充分了解規則，再開始評估

色塊只是分級工具；真正的答案是對應的行動、核准與期限

可能性 L	1 輕微	2 中度	3 嚴重	4 重大	5 災難
5 頻繁	5	10	15	20	25
4 很可能	4	8	12	16	20
3 可能	3	6	9	12	15
2 不太可能	2	4	6	8	10
1 罕見	1	2	3	4	5

嚴重度 S

1–4 低	5–9 中	10–16 高	17–25 極高

分級後必須採取行動

- **低**：依程序作業，維持控制
- **中**：排定改善，主管核准並追蹤
- **高**：停止或限制作業，優先改善
- **極高**：立即停止，重新設計或高階核准

行動門檻、核准層級與期限，應依公司制度校準。

不要為了讓工作繼續而調低分數；有疑義時記錄假設並採保守評估。

評估結果須連結責任人、暫行措施、完成期限與驗證證據。

既有風險、剩餘風險與追蹤改善

改善完成不等於風險下降；必須確認措施已上線、有效且有證據

1 既有風險

不考慮既有控制｜看見危害本質

危害 × 暴露

控制措施

2 現況風險

只計入已存在且有效的屏障

確認有效性

改善＋驗證

3 剩餘風險

改善完成並驗證後，仍存在的風險

驗證後重評

建議追蹤五要素

- 措施
- 責任人
- 期限
- 暫行措施
- 完成證據

優先處理

- 高後果情境
- 僅靠單一屏障
- 已出現失效徵兆
- 多人暴露

風險登錄表至少保留

情境｜假設｜分數｜屏障｜建議｜結案證據

只有措施真正上線、功能驗證完成並重新評估，才能宣告剩餘風險下降

製程安全控制層級｜先減源頭改善，最後才依賴人員

優先選擇不需要人在壓力下每次都做對的控制

優先／
可靠度提高

對人員依賴提高

1 本質較安全

消除｜減量｜替代｜緩和｜簡化

2 被動工程

圍阻｜耐火｜間距｜排液坡度｜物理隔離

3 主動工程

聯鎖｜ESD｜偵測｜洩壓｜抑制／消防

4 行政管理

SOP｜作業許可｜雙人確認｜訓練｜稽核

5 PPE與緊急應變

降低暴露後果，
不能取代源頭控制

哪一個較不依賴人？

增加告示牌

需人員看見並
正確反應

增加自動隔離

偵測後
立即切斷

工程控制通常更穩定，
但仍須測試與維護

先問能否移除或減少危害，再依序建立被動、主動與管理防線

本質較安全

本質安全不依賴控制系統動作

在增加防護層之前，先問：危害能不能被消除、減少或變得更溫和？

1 Minimize 減量

能否減少危險物庫存、管段容積或滯留量？

2 Substitute 替代

能否改用較低危害物質、條件或技術？

改善前｜複雜、高庫存、高壓

從源頭改變危害

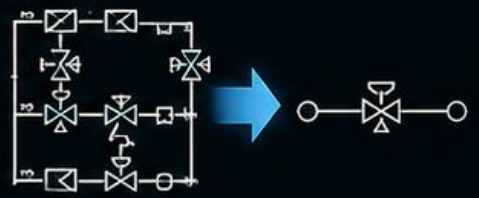
改善後｜減量、低壓、簡化

3 Moderate 緩和

能否降低壓力、溫度、濃度或反應強度？

4 Simplify 簡化

能否減少閥件、旁通、人工切換與易錯步驟？



最可靠的事故預防，是讓危害不存在、數量更少、條件更溫和、流程更不易犯錯

LOPA 後果分析｜先定義終點，再評估風險

沒有明確後果，就無法判斷防護層是否真正有效

1 1｜事故情境

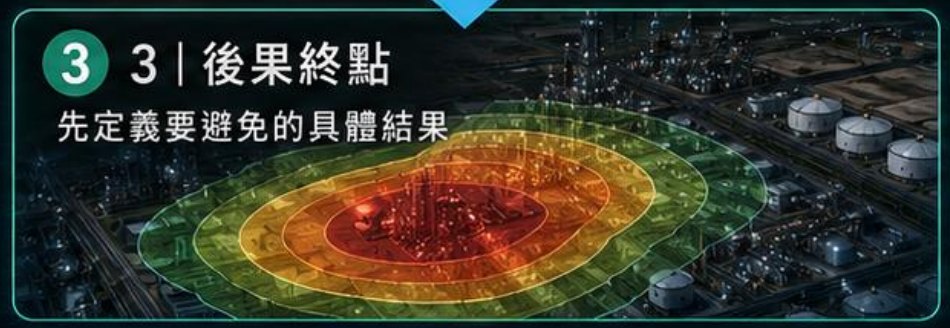
設備、物料、操作與環境條件

2 2｜不良後果

火災／爆炸｜有毒物質釋放｜人員傷害｜設備損壞

3 3｜後果終點

先定義要避免的具體結果



應評估哪些後果？

A 事故情境風險

後果越嚴重，
評估應越深入

B 風險評估方法

依組織方法、
影響範圍與
分析深度選擇

C 可投入資源

時間、人力、
資料品質與
專業能力

後果分析深度

定性描述

以文字說明
可能後果與影響範圍

半定量分級

低／中／高
或風險矩陣

定量後果分析

熱輻射、超壓、
擴散範圍與
受影響人數

⚠ 後果不可只寫「洩漏」或「火災」，
應描述物質、範圍、演變與受影響對象

先界定後果終點，再依風險、方法與資源決定評估深度

LOPA 是什麼？

用數量級估算事故情境風險，判斷獨立防護層是否足夠

1｜基本定義

LOPA＝保護層分析
（Layer of Protection Analysis）

介於定性危害分析與完整
定量風險分析之間的**半定量**方法

2｜如何評估風險

- 起始事件頻率 **IEF**
- 後果嚴重度
- 獨立防護層 **IPL** 與失效機率 **PFD**
- 以**數量級**估算特定情境風險

3｜分析基礎

- 通常承接 **PHA／HAZOP**
  已辨識的事故情境
- 每次分析一組
  單一原因－後果配對

4｜主要目的

- 確認現有防護是否足夠
- 判斷情境風險是否可接受
- 找出仍需降低的**風險缺口**

事故情境

已辨識的特定事故情境
（原因－後果配對）

起始事件

造成事故情境的
起始事件

起始事件頻率 IEF

獨立防護層 IPLs

警報 | 關鍵儀表安全系統 | 安全閥 | 操作程序與人員 | ...

各 IPL 的失效機率 PFD

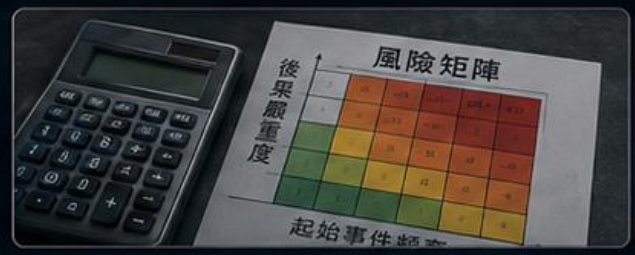
防護後風險

以數量級估算
情境風險

風險決策

可接受

不可接受



LOPA 不只是列出保護措施，而是驗證每一層能否取得風險降低額度

用 LOPA 做風險決策｜維持、改善或放棄風險

辨識情境 → 計算剩餘風險 → 與風險準則比較 → 決定行動

辨識情境
(蝴蝶結 / 情境)

計算
剩餘風險

與風險準則
比較

決定行動
(維持 / 改善 / 放棄)

1 維持剩餘風險

- 風險已在可接受範圍
- 持續測試、維護與稽核
- 確認假設及暴露條件未改變

風險在可接受範圍

2 降低／修正風險

- 風險暫可容忍，但仍須改善

風險暫可容忍，持續改善

3 不可接受風險

- 立即停止、限制或重新設計
- 不得以降低評分取代改善
- 必要時放棄該操作或情境

風險不可接受

決策核心

1. 比較剩餘風險與公司準則
2. 確認核准層級
3. 設定責任人與期限
4. 追蹤至措施驗證結案

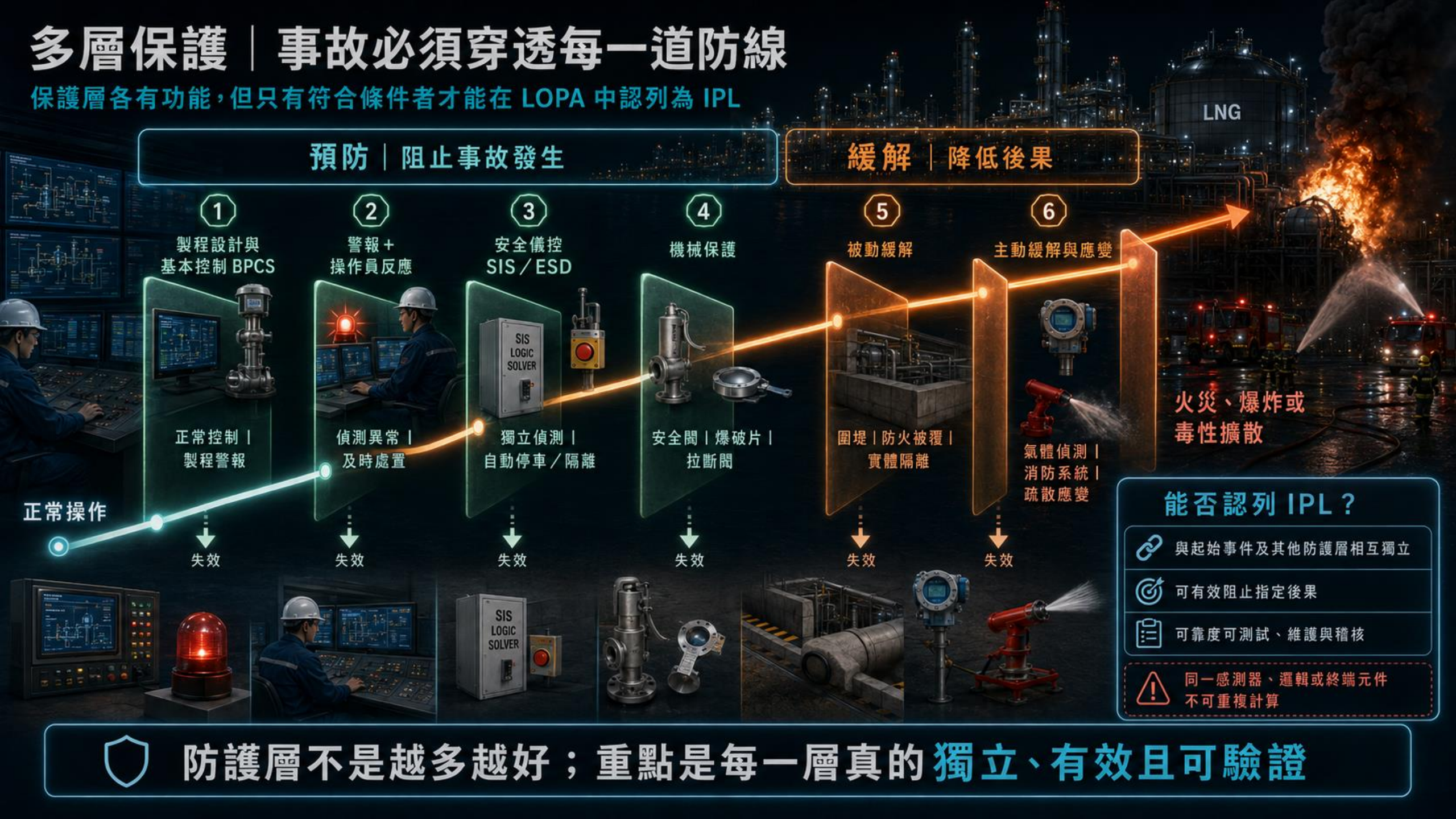
LOPA 的價值不只在計算風險，更在支持是否接受、如何降低或停止風險的決策

第5章

風險管控層級與實務措施

多層保護｜事故必須穿透每一道防線

保護層各有功能，但只有符合條件者才能在 LOPA 中認列為 IPL



能否認列 IPL？

- 與起始事件及其他防護層相互獨立
- 可有效阻止指定後果
- 可靠度可測試、維護與稽核

⚠ 同一感測器、邏輯或終端元件不可重複計算

防護層不是越多越好；重點是每一層真的獨立、有效且可驗證

從 HAZOP 到 LOPA

主要目的：判斷事故情境的風險是否可接受，以及防護層是否足夠

HAZOP 找出值得擔心的情境；LOPA 判斷現有防護是否足夠

不是所有 HAZOP 情境
都需要進入 LOPA

HAZOP → LOPA → SIS｜三階段如何銜接

從危害情境辨識，到防護充分性評估，再到安全儀控需求

HAZOP｜找出可能出錯之處

製程可能如何偏離？

- 系統性辨識危害
- 分析原因、後果與既有保護

輸出

事故情境清單與改善建議

LOPA｜判斷防護是否足夠

這個情境的風險可接受嗎？

- 選定重大事故情境
- 確認 IPL 的獨立性、有效性與可稽核性
- 估算防護後事故頻率

輸出

風險缺口與所需風險降低量

LOPA 分析工作表（範例）

事故情境	初始事件頻率	獨立保護層（IPL）				防護後頻率	風險準則	結果
		IPL 1	IPL 2	IPL 3	IPL n			
反應器超壓洩放火災	高	安全閥	高高壓跳脫	緊急排放	消防水系統	中	可接受	風險可接受

風險高 — 可接受區域 — 風險低

風險缺口仍存在？

- 是 → SIS
- 否 → 風險可接受：維持既有防護，無需新增 SIS

SIS｜提供安全儀控保護

是否需要 SIF？需要多少可靠度？

- 定義安全儀控功能 SIF
- 決定安全完整性等級 SIL
- 感測器｜邏輯控制｜終端元件
- 功能安全生命週期管理

輸出

安全需求規格與驗證依據

⚠ 不是每個 HAZOP 建議都需要 SIS

⚠ 不是每個保護措施都可認列為 IPL

LOPA 是決策橋梁：把 HAZOP 情境轉為可驗證的風險降低需求

LOPA 如何運作？六個核心步驟

從後果定義、情境選擇到風險決策，每一步都必須留下依據

1 確認後果

先確認需要避免的最嚴重可信後果

2 選定事故情境

每次分析一個單一原因－後果配對

3 確認起始事件

辨識起始原因並估算發生頻率 IEF（次／年）

4 確認 IPL 與 PFD

逐層驗證獨立性、有效性與可稽核性
估算各層失效機率 PFD

5 整合資料估算風險

起始事件頻率 × 各 IPL 的 PFD
必要時納入使能條件與條件修正因子

6 評估風險並決策

與容許風險準則比較
維持防護｜改善或新增防護｜進一步分析

核心邏輯： 後果 → 事故情境 → 起始事件 → IPL → 防護後風險 → 決策

LOPA 的一致性，來自固定步驟、明確定義與可追溯資料

LOPA 風險降低｜每一道 IPL 降低多少？

以數量級估算起始事件與獨立防護層，判斷風險缺口

起始事件
高壓蒸氣入口閥卡開

原始情境頻率
10^{-1}／年

IPL 1｜超壓警報＋操作員反應

PFD = 10^{-1}

預期事故頻率：
10^{-3}／年

IPL 2｜安全閥

PFD = 10^{-1}

防護後：
10^{-5}／年

IPL 3｜SIS

PFD = 10^{-2}

安全目標

10^{-5}／年

後果
設備超壓／破裂
火災、爆炸、毒性擴散

$$10^{-1} \times 10^{-1} \times 10^{-1} \times 10^{-2} = 10^{-5}\ /年$$

示例結果：達到安全目標

計算前先確認

- 每一層均符合 IPL 條件
- 警報與操作員反應合併為一層
- PFD 應有測試、維護與資料依據

教學示例｜實際數值及容許風險應依事業單位核准準則

風險降低不是把數字相乘而已；每一個防護額度都必須有證據

Safeguard 與 IPL｜不是每項保護都能取得額度

所有 IPL 都是 Safeguard，但不是所有 Safeguard 都符合 IPL 條件

Safeguard 保護措施

能啟動、中斷、控制或緩解事故發展的設備、系統或人員行動

IPL 獨立防護層

可獨立阻止特定事故情境進入指定後果

必須具備獨立性、有效性、可靠度與可稽核性

兩種分類方式

依動作特性

主動式 Active：需偵測、邏輯或人員動作

SIS 邏輯解鎖 ESD

被動式 Passive：不需啟動即可發揮功能

洩壓閥

防溢堤 (Dike)

依作用時機

預防型 Preventive：在失去主圍阻前介入

高高壓聯鎖

緊急關斷閥 ESD

緩解型 Mitigative：在釋放後降低後果

火炬系統

噴淋系統 (Deluge)

要認列 IPL，還必須確認

- 與起始事件及其他防護層相互獨立
- 能有效處理指定原因並阻止指定後果
- 有測試、維護、旁通與稽核證據
- PFD 額度有核准資料依據

Safeguard 是廣義保護；IPL 是通過條件審查、可量化風險降低的子集合

LOPA 改善建議｜從降低後果、頻率到提升可靠度

先找最能改變風險的地方，不要只想到「再加一道聯鎖」

事故情境 → LOPA 分析 → 找出風險缺口 → 選擇改善方向 → 驗證結案

降低後果嚴重度

- 減少危險物庫存與管段容積
- 降低壓力、溫度或濃度
- 改善圍阻、隔離與安全距離

目的：事故發生時**降低損害**

降低起始事件頻率

- 設備重新設計與失效消除
- 簡化程序與減少錯誤機會
- 機械完整性與預防保養

目的：讓事故**不容易被啟動**

增加或強化 IPL

- SIS／SIF、獨立偵測與隔離
- 洩壓、被動圍阻與耐火保護
- 確認獨立性、有效性與 PFD

目的：補足所需**風險降低量**

提升既有保護可靠度

- 測試週期、維護與功能驗證
- 旁通管理、警報管理與紀錄
- 追蹤改善至證據完整結案

目的：縮小帳面與現場的**落差**

選擇改善方案時同時考量

優先採本質較安全 | 風險降低效益 | 工期與可行性 | 重大影響可進一步做 QRA

LOPA 建議不只是增加聯鎖；應從源頭、事故路徑、保護層與管理可靠度共同改善

LNG 灌裝 LOPA 案例｜哪一道防護真的獨立？

把 HAZOP 情境轉成單一原因－後果配對，逐層驗證防護額度

情境設定

1 起始事件

灌裝中槽車意外移動

2 必要條件

軟管已連接且正在輸送 LNG

3 頂端事件

軟管斷裂，LNG 失去主圍阻

4 最嚴重可信後果

低溫噴濺與可燃氣雲形成，遇火源造成火災或爆炸

候選防護層｜能否認列 IPL？

1 SOP、教育訓練與輪擋確認

✗ 不可直接認列

若與起始人為失誤相依，便不具獨立性

2 車輛防移動聯鎖

✓ 候選 IPL

須確認獨立偵測、動作邏輯及定期測試

3 拉斷閥／緊急脫離裝置

✓ 候選 IPL

須證明可限制洩漏量且維護有效

4 獨立氣體偵測＋ESD 隔離

✓ 候選 IPL

須確認感測、邏輯與終端元件不與其他層共用

小組討論

1. 定義的後果是洩漏、火災，還是人員傷亡？
2. 每一層真的能阻止這個後果嗎？
3. 測試、維護與旁通紀錄能支持所取 PFD 嗎？

同一原因不能同時當防護；有設備也不代表能取得 IPL 額度

MOC 與 PSSR｜變更後，既有風險評估可能失效

任何改變，都可能改寫原有的事故情境與安全屏障

MOC 管理範圍

設備 | 材料 | 設定值 | 軟體 | 程序 | 臨時旁通 | 組織／人力

1 提出變更

- 設備／管線新增或修改
- 參數／設定值調整
- 程序或操作方式改變

2 重新風險評估

- 更新危害辨識
- 重新分析事故情境
- 確認安全屏障有效性
- 評估風險等級

3 MOC 文件／訓練

- 技術依據
- 風險評估
- 文件更新
- 核准
- 操作＋維修部門訓練

4 PSSR 開車前安全審查

5 投入運轉後持續監測

- 監測異常
- 驗證評估假設
- 關閉暫行措施

異常或新變更

變更沒有完成 MOC、文件更新、訓練與 PSSR 驗證，就不應投入運轉

回顧課程重點

從看見失控，到確認每一道控制真的有效

1 零工傷

不等於零製程風險

2 完整路徑

從原因、偏離、失控
到最壞可信後果

3 方法匹配

設備、製程與程序風險，
選擇適合的分析方法

程序風險可用 Procedural HazOp 深入分析

4 有效屏障

矩障只能排序；
屏障有效，風險才會下降

5 證據驗證

優先減少危害
與依賴人的機會

用測試、維護與紀錄
驗證關鍵控制

安全不會憑空出現，而是每天辨識、改善與驗證的結果

製程風險掌握多少？

你知道廠內風險最高的製程，以及擋住事故的關鍵屏障嗎？

1 **辨識**｜風險最高的製程為何？

2 **建立**｜是否有關鍵安全屏障？

3 **驗證**｜如何檢點、測試與保養？

4 **持續**｜如何證明屏障持續有效？

看得見風險、說得出屏障、拿得出證據，才是真正掌握製程安全

課程結束後，我做什麼？

把危害辨識、風險評估與屏障管理，轉成現場行動

1 畫一張 Bow-tie

選一個高風險製程節點

完成：威脅、頂端事件、後果與屏障

2 抽查三項安全屏障

有效性｜獨立性｜可稽核性

氣體偵測器　ESD 閥　安全洩壓閥

在役？逾期？旁通？有測試證據？

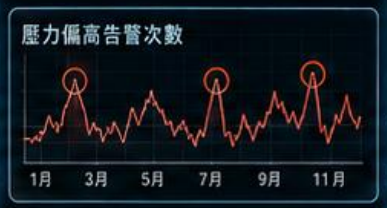
3 挑一份 SOP

確認角色、標準、停留點與異常處置

不只寫「確認正常」

4 回顧近一年異常

虛驚事件＋異常停車



找出重複的製程偏離

5 重排改善優先順序

盤點 MOC 與風險評估建議

高後果情境 RISK HIGH	改善建議：更新安全儀表或增加獨立保護層	Owner：製程部 Due：2025/06/30
中後果情境 RISK MEDIUM	改善建議：優化程序與操作監控	Owner：操作部 Due：2025/08/31
低後果情境 RISK LOW	改善建議：例行維護與文件更新	Owner：維護部 Due：2025/10/31

高後果情境優先

帶回現場的成果

- 1 個 高風險情境
- 3 項 屏障驗證
- 1 份 有責任人與期限的改善清單

安全不會在課堂結束時自動發生；它從下一次走查、下一筆證據、下一項改善開始

U.S. CSB 官方調查報告解析 | 案號：2024-05-I-TX

致命的錯覺：PEMEX 德州煉油廠硫化氫外洩事故調查

設備識別失效如何導致 27,000 磅毒氣外洩與兩名工人喪生

事故儀表板 (Executive Dashboard)

事故時間

2024年10月10日

4:23 p.m.

傷亡慘重

2死/13傷

(分別死於洩漏源頭與下風處相鄰廠區)

外洩規模

27,000 磅

(高濃度 H2S 劇毒氣體，持續外洩近一小時)

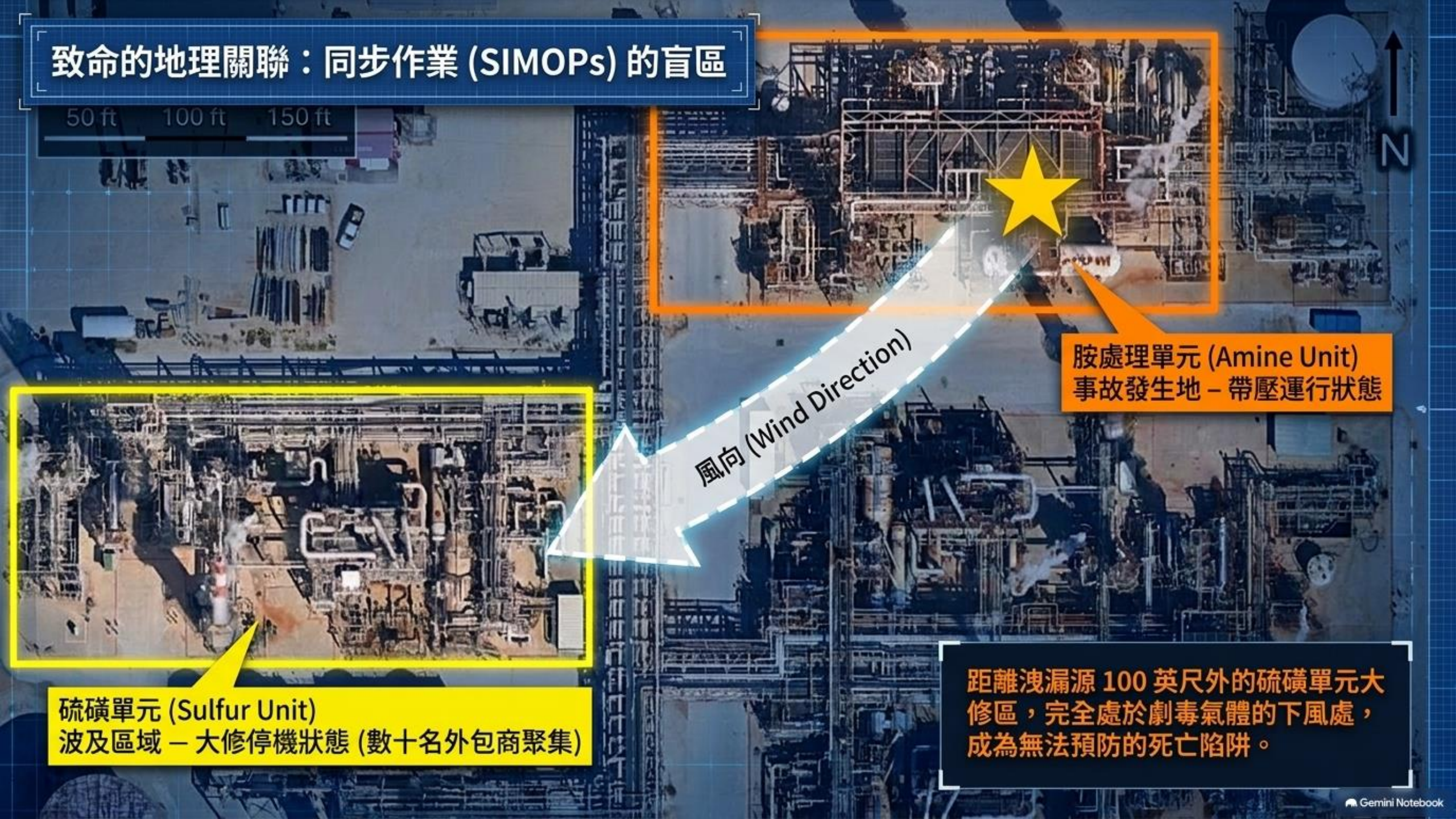
財產損失

$1,230萬美元

(因胺處理單元與下游設備停擺)

事故核心物質：硫化氫 (H2S) — 無色、劇毒、比空氣重。濃度達 1,000 ppm 時，吸入後幾秒內即可致命。

致命的地理關聯：同步作業 (SIMOPs) 的盲區



致命的認知陷阱：環境切換導致的安全盲區

絕對隔離 (大修狀態)

設備狀態
(Physical State)

→ 完全排空、無壓力

危害預期
(Hazard Expectation)

→ 零 (Zero)

工人心理
(Psychological State)

→ 安全放鬆
(以為所有的管線都是空的)

日常維護 (帶壓狀態)

設備狀態
(Physical State)

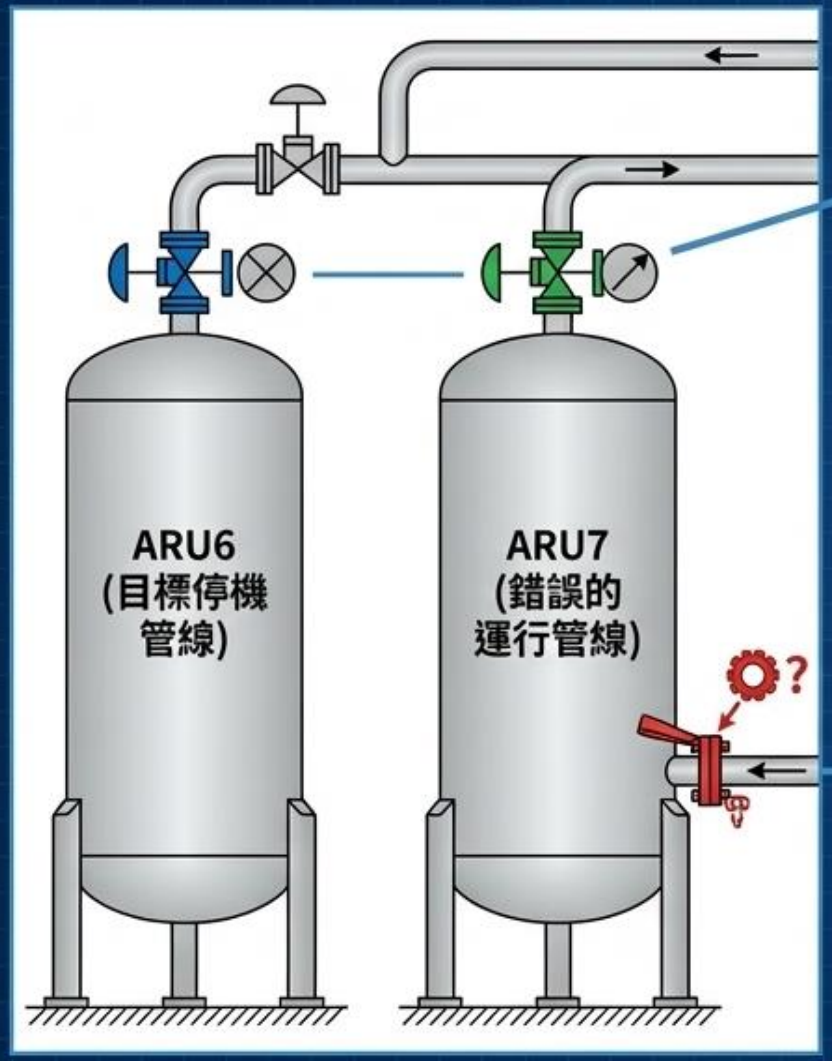
→ 部分停機，相鄰管線
帶有高壓 H2S

→ 極高 (Critical)

→ 未經重新簡報，
仍停留在大修模式

Repcon 外包商從
「死區」突然被調往
「活區」拆卸盲板，
卻無人告知他們新區域
潛藏著高壓毒氣。

找錯目標：失效的視覺線索



步驟 1 (目標):
工人被指派移除 ARU6 上的「407 號盲板」。

步驟 2 (迷失):
操作員將識別標籤掛在「遠處的欄杆上」而非管線上，工人根本沒看到。

步驟 3 (誤導):
工人依靠過去大修的經驗，尋找「紅色法蘭鎖」來辨認辨認目標。ARU7 上剛好有法蘭鎖，且未上鎖。

步驟 4 (致命開啓):
工人誤認 ARU7 為目標，開始拆卸帶有高壓 H2S 的法蘭。

災難爆發：致命的 60 分鐘

4:22 PM

下風處硫磺單元的攜帶型氣體偵測器作響 (>10 ppm)，外包商試圖用對講機警告操作員，無回應。

4:23 PM

ARU7 法蘭爆開，高壓 H2S 猛烈噴發。兩名拆卸工人中，一人撤離失敗當場倒地身亡。

4:24 PM

地面監護員透過對講機通報「人員倒地」。下風處濃度飆升至 500-800 ppm。

4:28 PM

事發 4 分鐘後，胺處理單元的固定式警報器才偵測到異常，控制室警鈴大作。

5:22 PM

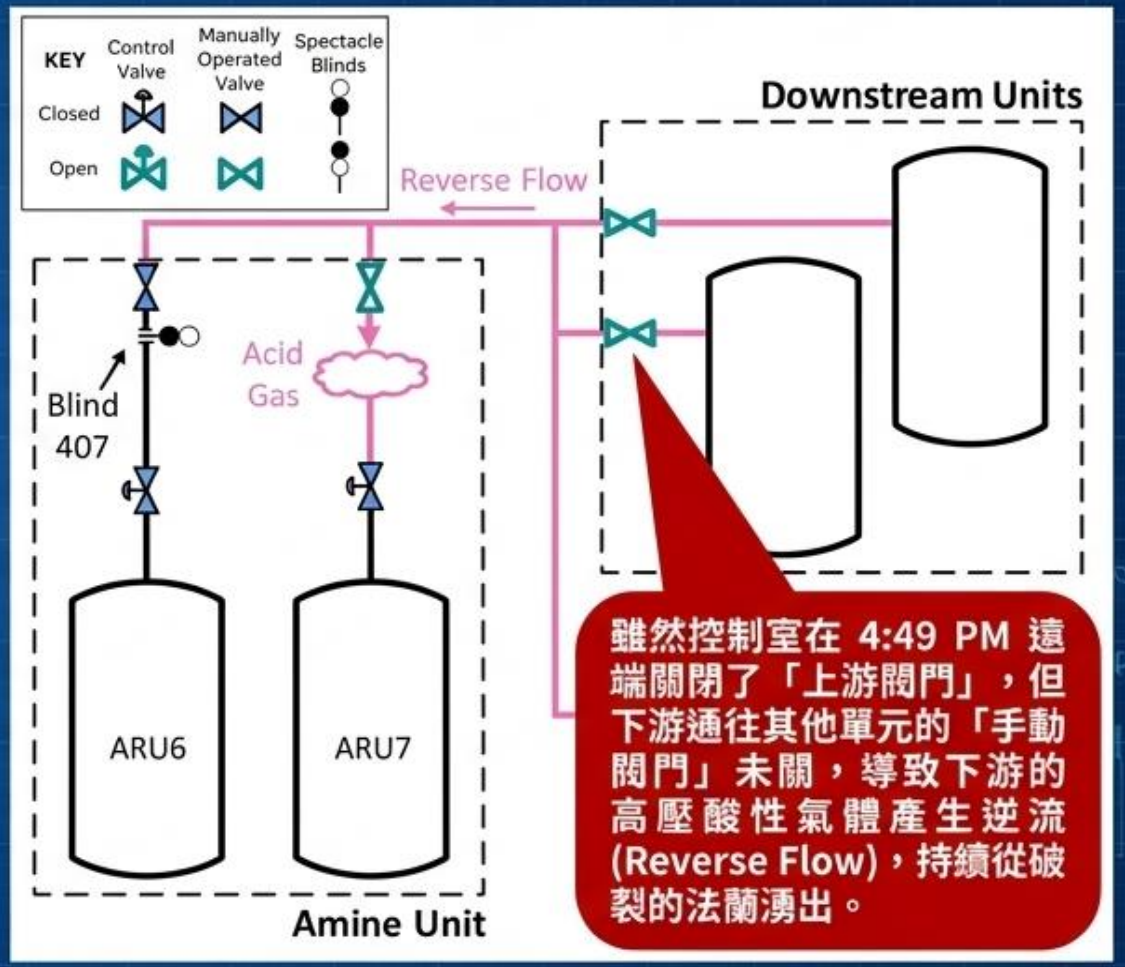
救援人員冒險重新鎖緊法蘭，歷時近一小時才完全止漏。

CSB

擴散與逆流：為何災情難以控制？

毒氣擴散

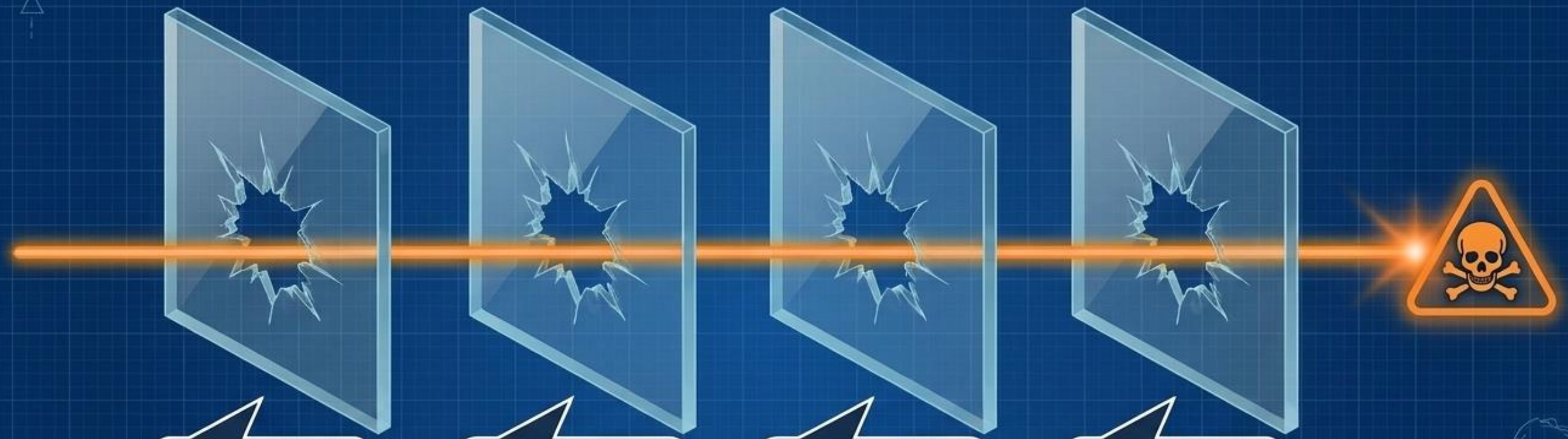
氣體逆流



CSB

Gemini Notebook

系統崩潰：四重安全防線如何被逐一突破

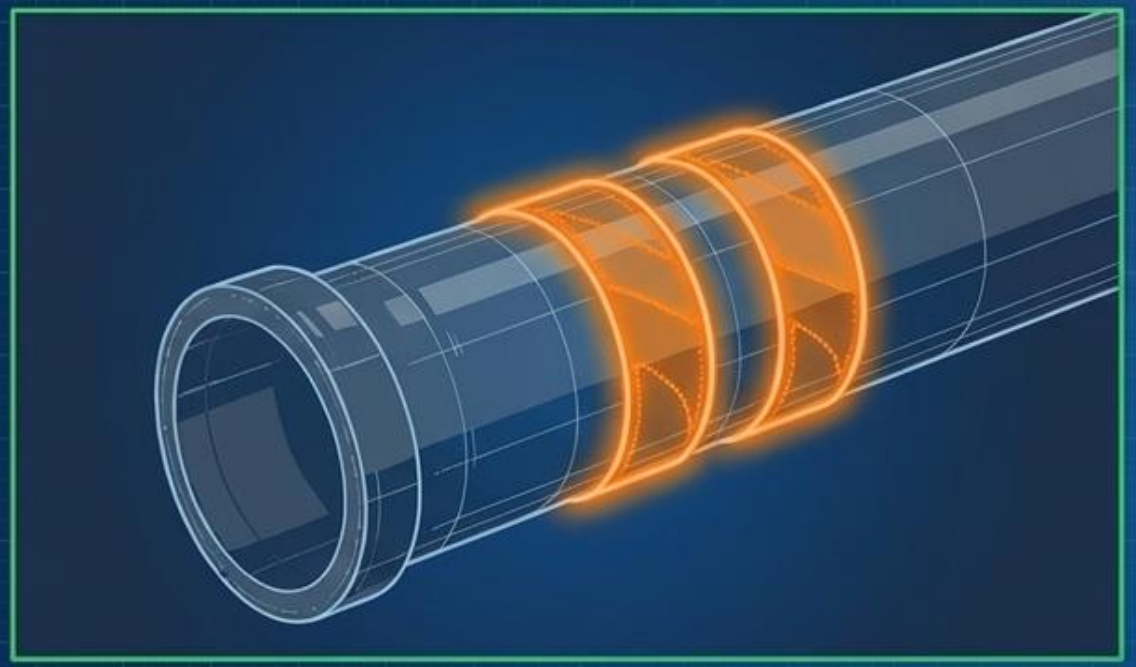


災難並非單一工人的疏忽，而是微小漏洞在特定時刻的完美對齊。

CSB

防線一：設備識別標準的雙標與失效

嚴格規定（切割管線作業）



根據 PEMEX 規定，切割管線必須有操作員與協調員親自到場，並在確切位置貼上醒目「雙圈橘色膠帶」。這套流程能有效防呆。

本次事故（法蘭拆卸作業）

對於致命風險相同的「拆卸法蘭」作業，卻缺乏標準化標示。標籤被隨意掛在遠處的欄杆上，工人被迫在沒有明確指引的情況下，依賴錯誤的「法蘭鎖」來盲目猜測位置。

CSB

防線二：失能的工作許可與 SIMOPs 盲區

範圍過廣 (Broad Scope)

一張許可證涵蓋了 15 個盲板的拆卸作業，未對每一個風險點進行獨立評估。

忽視暫停點 (Ignored Hold Points)

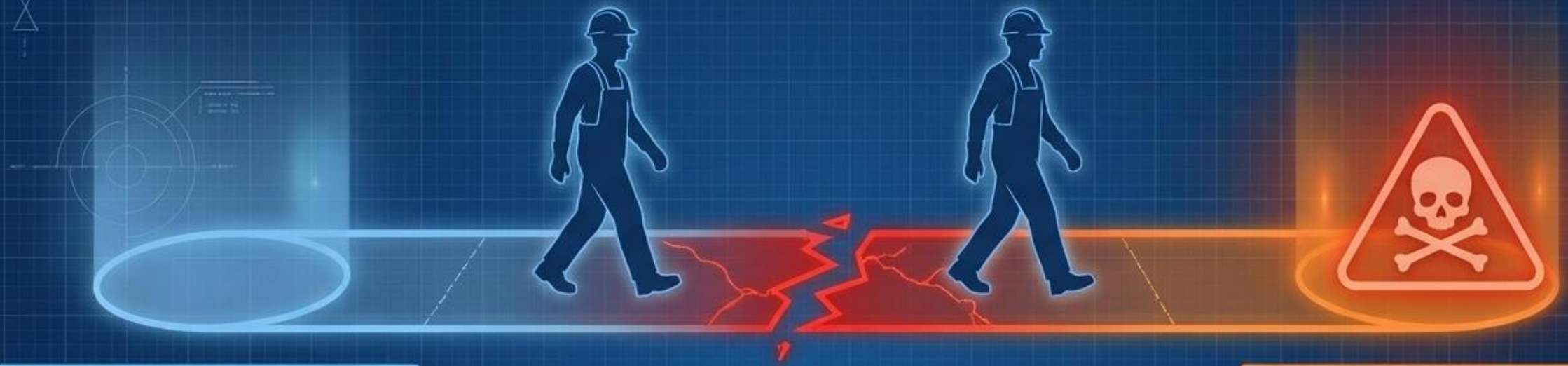
許可證上雖寫著「打開管線前需操作員在場」，但缺乏強制性的暫停查核機制，導致工人直接動手。

同步作業危害 (SIMOPs Failure)

許可審查過程完全沒有考慮相鄰區域正在進行大修。沒有實施交通管制、沒有通知下風處單位，將數十人暴露於未評估的風險中。

CSB

防線三：致命的工作調度與資訊斷層



出發地：硫磺單元大修區

連續工作數天，習慣了「絕對隔離」的無害環境。

盲目跨越（無交接程序）

沒有針對「帶壓運行單元」的危害簡報、沒有更新防護裝備等級。

目的地：胺處理單元

帶壓操作中，相鄰管線充滿高壓 H_2S。

核心痛點：

針對剛入廠的工人有詳盡的「大修安全培訓」，但對於廠內不同區域間的「臨時調度」，卻沒有任何重新提示危害的交接標準。

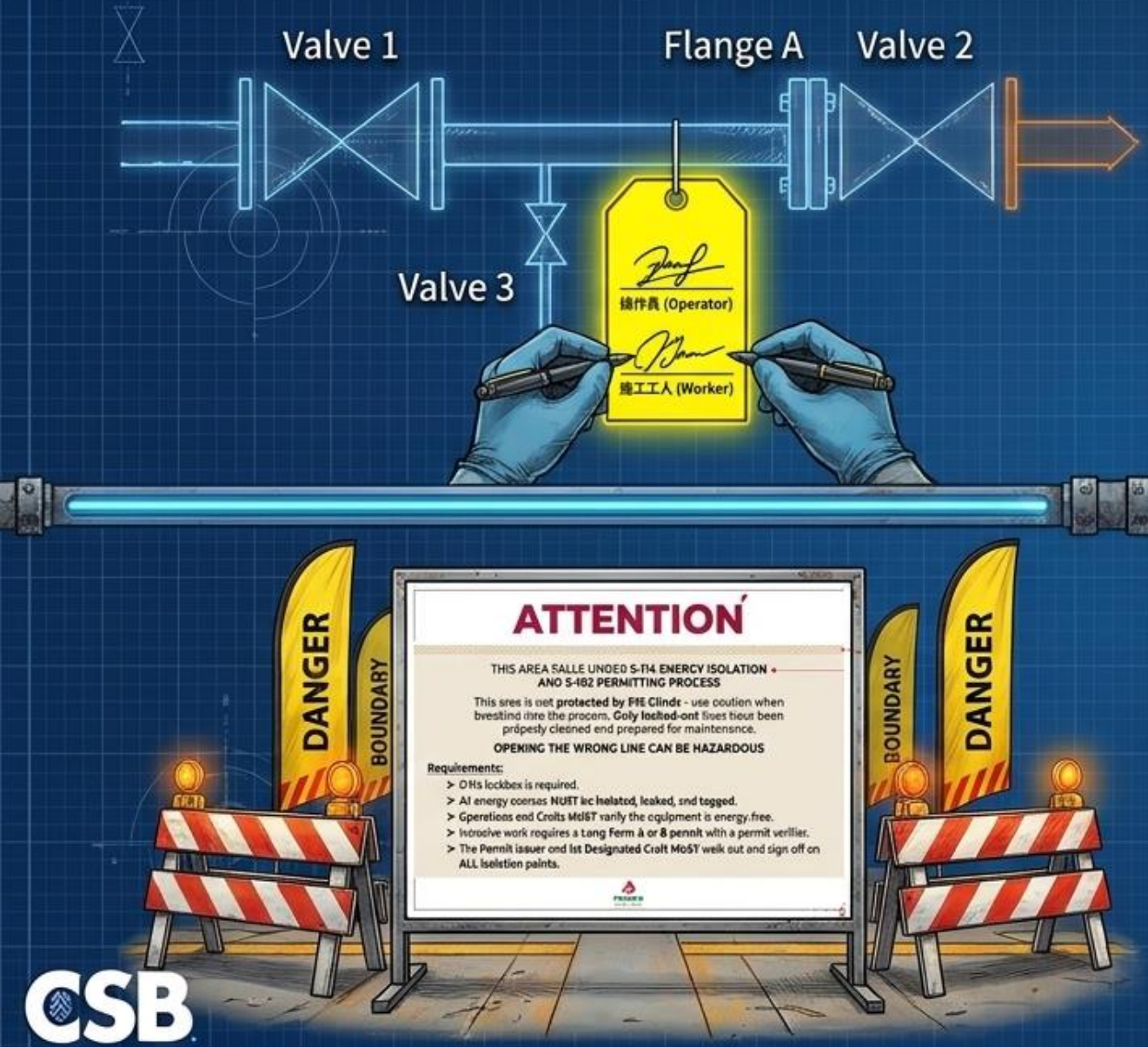
CSB

防線四：操作紀律的崩壞

當公司的「安全文化」容許員工經常性地偏離書面程序，災難只是時間問題。

CSB

立即性防線重建：雙重簽署黃色標籤系統



防呆設計：
廢除將標籤掛在欄杆上的作法。新版黃色標籤 (Yellow Tag) 必須由「設備擁有者 (操作員)」與「實際執行拆卸的工人」在管線上共同確認、雙重簽名。

邊界警示：
在「帶壓運行」與「全面隔離」的交界處，設置實體的羽毛旗與大型警告看板，強制改變工人的心理預期。

CSB

核心教訓：重構防呆的安全系統

> **每一場事故都源於人為錯誤...**
> **操作員往往處於責任鏈的末端，卻承受了所有的指責。我們應該思考的是：那些有能力力改變系統設計與工作方法的人，為何沒有阻止事故發生？**
>
> — Trevor Kletz (化學工程安全先驅)

防範人為錯誤不應僅依靠前線工人的警覺，而是必須建立一個「不會誤導人、強制確認、且容錯」的系統架構。本事故最大的教訓，即是重新審視我們習以為常的標示與許可制度。