從危害控制分析談重大危害事件管理

游輝祥 博士/核可功能安全專家(CFSE)
英能科技(股)公司
電話: +886+3+3565317
傳真: +886+3+3562482
網址: http://www.energywell.com.tw

主　旨

- 瞭解事故預防和製程安全策略的演變
- 瞭解如何有效架構製程安全管理要素
- 瞭解何謂公認和普遍接受的良好工程實務(Recognized and Generally Accepted Good Engineering Practices, RAGAGEP)及其在US OSHA製程安全管理法規的定義
- 瞭解何謂製程安全管理危害控制分析(Hazard Controls Analysis, HCA)的層次結構
- 如何透過層次結構的HCA進行安全屏障(Safety Barrier)和安全關鍵要素/設備(Safety Critical Elements/Equipment, SCE)的績效保證和完整性管理
- 瞭解如何應用領結(蝴蝶結)方法(Bow-tie Method)進行API RP 754製程安全績效指標(Process Safety Performance Indicators, PSPI)的P-D-C-A管理

講題綱要

- 講題一：製程安全管理實施架構簡介(09:20-10:50)
  - 製程安全與工作場所安全的差異
  - 事故預防和製程安全策略的演變歷史
  - 如何有效架構製程安全管理?

- 講題二：RAGAGEP簡介(11:00-12:00)
  - 何謂RAGAGEP?
  - RAGAGEP實施例簡介
  - RAGAGEP在製程安全管理中所扮演的關鍵角色－風險控制的基石與動態風險管理

講題綱要(續)

- 講題三：製程安全管理的危害控制分析簡介(13:00-14:30)
  - 何謂危害控制分析?
  - 危害控制分析在製程安全管理所扮演的關鍵角色
  - 使用領結(蝴蝶結)方法進行結構層次的危害控制分析建模與管理

- 講題四：領結(蝴蝶結)方法在製程安全風險管理的P-D-C-A應用簡介(14:40-15:40)
  - 領結(蝴蝶結)方法建模流程簡介
  - 領結方法結合保護層分析(Layer of Protection Analysis, LOPA)應用簡介
  - 使用領結方法進行安全屏障與和安全關鍵要素/設備的績效保證和完整性管理簡介(SCE-MI)
  - 使用領結方法結合API RP 754製程安全績效指標管理簡介

講題一

製程安全管理實施架構簡介

風險控制策略

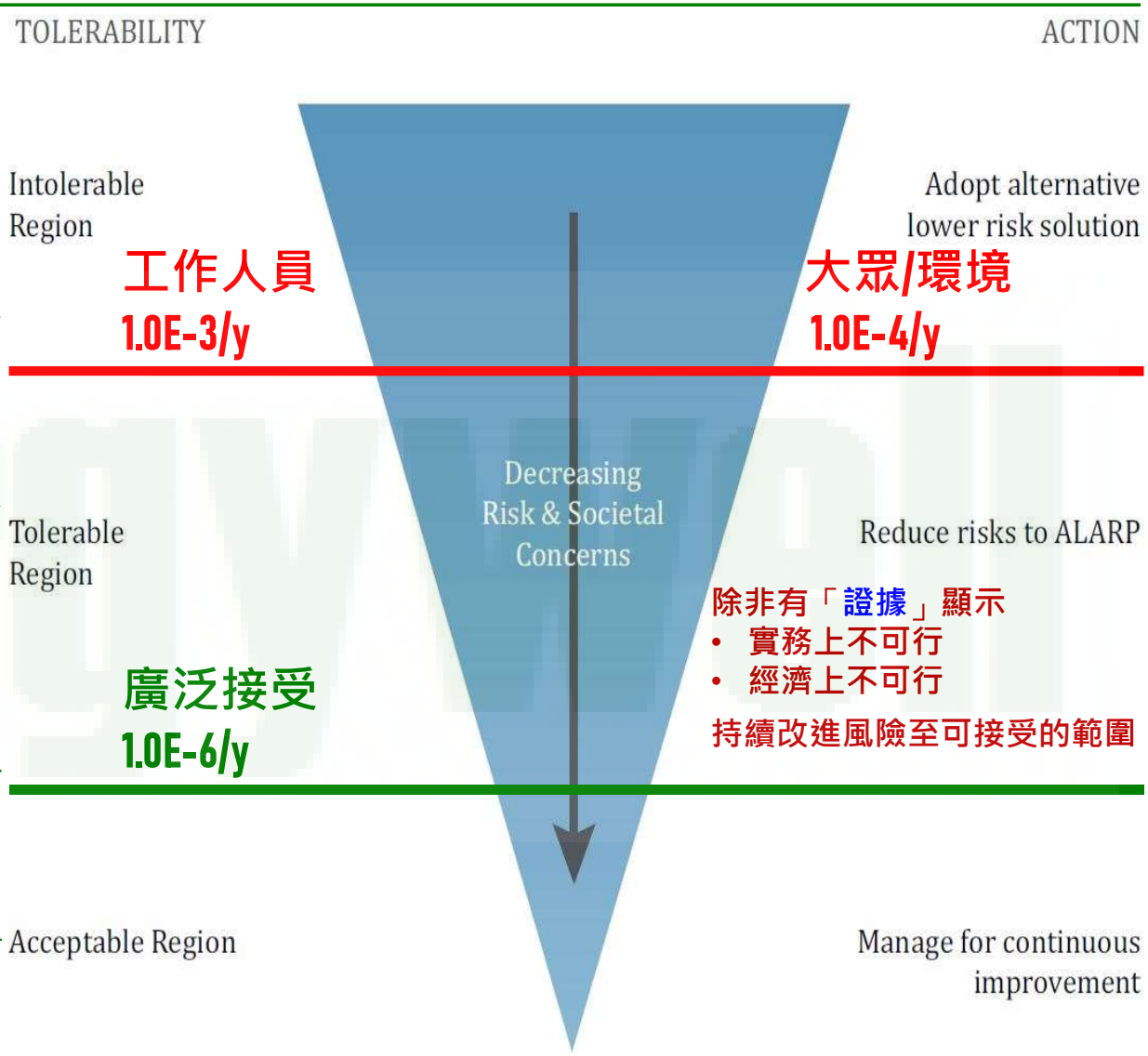
- 廣泛接受的風險控制策略如下:
  - 採用本質安全設計
  - 預防 - 考慮避免危害的措施
  - 透過工程設計、檢查、維護和工作實踐降低發生概率
  - 減輕後果 - 儘量減少不必要事件的後果
  - 緊急應變 - 使得能夠恢復到受控狀態

風險控制策略(續)

- 一般透過以下方式減輕升級風險:
  - 消除 - 從設計中移除受影響的設備
  - 分離 - 增加火源和爆炸源與易受攻擊目標之間的距離
  - 工程 - 設計足夠堅固的結構以承受設計意外負荷(Design Accidental Load, DAL)爆炸爆震波負載
  - 工程 - 在源和易受攻擊的目標之間引入額外的物理屏障
  - 工程 - 最小化洩漏路徑，以減少啟動事件和優化幾何(結構和/或設施配置)的可能性，以最大限度地降低火焰衝擊的風險
  - 工程 - 緊急停機(Emergency Shutdown, ESD)、緊急減壓(Emergency Depressuring, EDP)、被動和主動防火
  - 透過危險區域分類、維護等控制潛在的點火源
- 成本效益分析(Cost-Benefit Analysis, CBA)可用於確定緩解措施的有效性，以防止涉及生產或資產損失的升級

最低合理可行(ALARP)原則

- 一種常見的方法是將風險分為三個範圍:
  - 一個風險較高的區帶
    - 無論其活動帶來什麼好處，風險等級都被認為是不可容忍的
    - 無論其成本如何，風險處理都是必不可少的
  - 考慮成本和效益的中間帶(或「灰色」區域)
    - 將機會與潛在後果相平衡
  - 一個風險較低的區帶
    - 其風險等級被認為可忽略不計或很小，以至於不需要採取風險處理措施



ALARP: As Low As Reasonably Practicable

降低風險的三角模型

資料來源: ISO/TS 16901:2015
UKOOA 1999; HSE RR 063:2001

重大事故/事件(Major Accident)

- 在英國2015年海上設施(海上安全指令)(安全案例等)條例的原始定義，意指
  - (a) 涉及火災、爆炸、井失控或釋放危險物質的事件，該危險物質對安裝或從事某項活動與之相關的人員造成、或可能造成死亡或嚴重人身傷害;
  - (b) 對裝置或裝置的結構造成重大損壞的事件，或裝置穩定性的任何損失，或對裝置上或從事與之相關活動的人員造成、或可能造成死亡或嚴重人身傷害的任何損失;
  - (c) 與安裝有關的潛水作業的生命支持系統的失效，及用於此類作業的潛水鐘的分離，或潛水員受困潛水員鐘罩或其他用於此類作業的海底艙室;
  - (d)因工作活動或從事與其有關的活動所引起的任何其他事件，於安裝工程活動中導致五人或五人以上死亡或嚴重人身傷害;或
  - (e) 前款(a), (b)或(d)段所述及的任何事件所引致的任何重大環境事故，
  - 並且，為了確定某事件是否構成(a), (b)或(e)款規定的重大事故，通常無人看管的設施應被視為有人

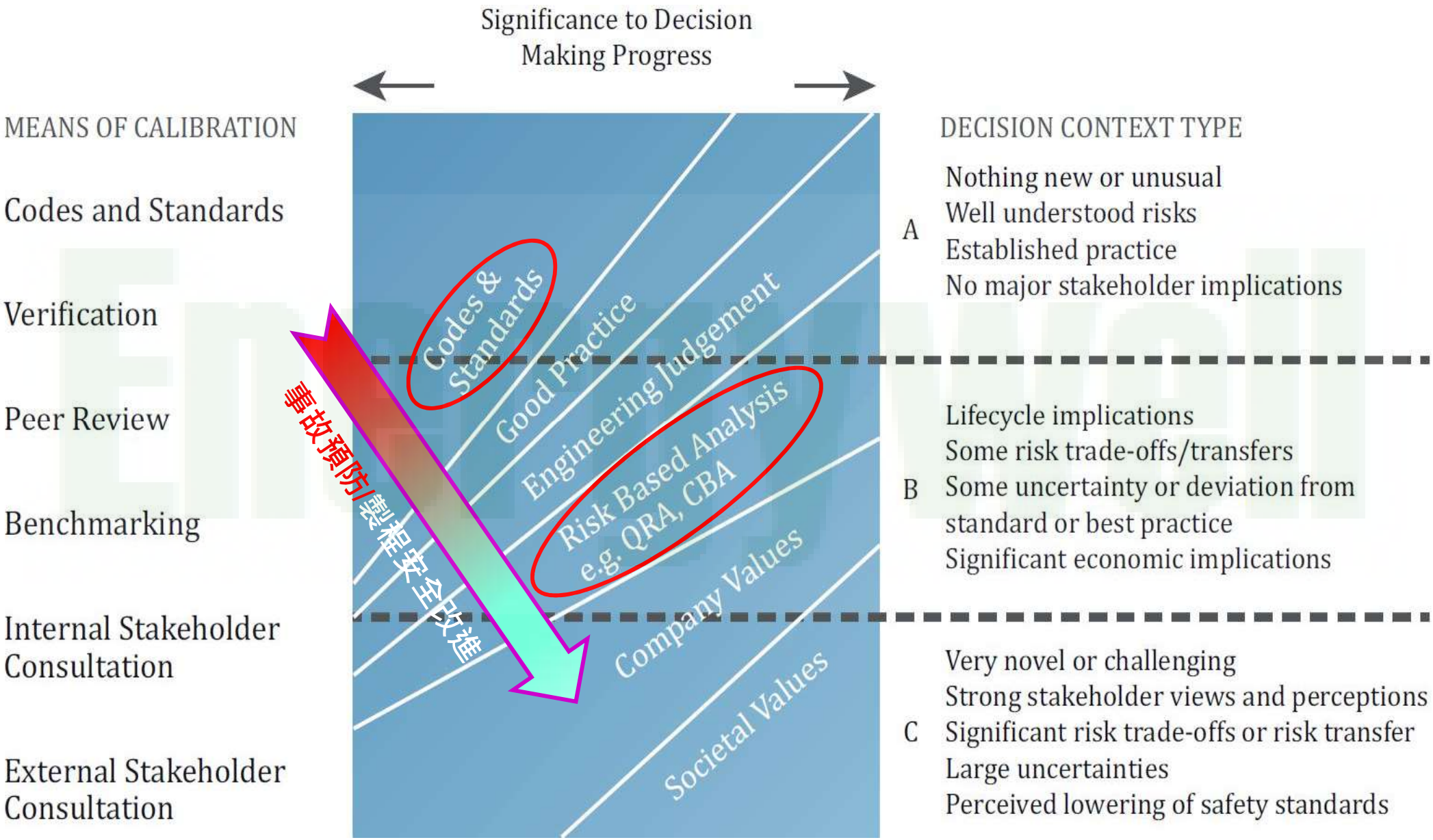
- 重大事故危害(Major Accident Hazard, MAH)是可能導致重大事故的潛在危險源

–管理重大事故危害(MAH)是安全營運的基礎

重大職業災害

- 勞動檢查法施行細則(民國103年06月26日)
  - 第 31 條 - 本法第二十七條所稱重大職業災害，係指左列職業災害之一:
    - 一、發生死亡災害者
    - 二、發生災害之罹災人數在三人以上者
    - 三、氨、氯、氟化氫、光氣、硫化氫、二氧化硫等化學物質之洩漏，發生一人以上罹災勞工需住院治療者
    - 四、其他經中央主管機關指定公告之災害
- 職業安全衛生法(民國102年07月03日)
  - 事業單位勞動場所發生下列職業災害之一者，雇主應於八小時內通報勞動檢查機構:
    - 一、發生死亡災害
    - 二、發生災害之罹災人數在三人以上
    - 三、發生災害之罹災人數在一人以上，且需住院治療
    - 四、其他經中央主管機關指定公告之災害
  - 勞動檢查機構接獲前項報告後，應就工作場所發生死亡或重傷之災害派員檢查

重大事故風險管理決策支援框架



資料來源: ISO/TS 16901:2015
UKOOA 1999; HSE RR 063:2001

風險矩陣範例

Consequence					Increasing probability			
Severity rating	People	Assets	Environ-ment	Reputation	A	B	C	D
					Has occurred in E&P industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero impact	Manage for continued improvement			
1	Slight injury	Slight damage	Slight effect	Slight impact				
2	Minor injury	Minor damage	Minor effect	Limited impact				
3	Major injury	Local damage	Local effect	Considerable impact				
4	Single fatality	Major damage	Major effect	Major national impact	Incorporate risk-reducing measures		Fail to meet screening criteria	
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact				

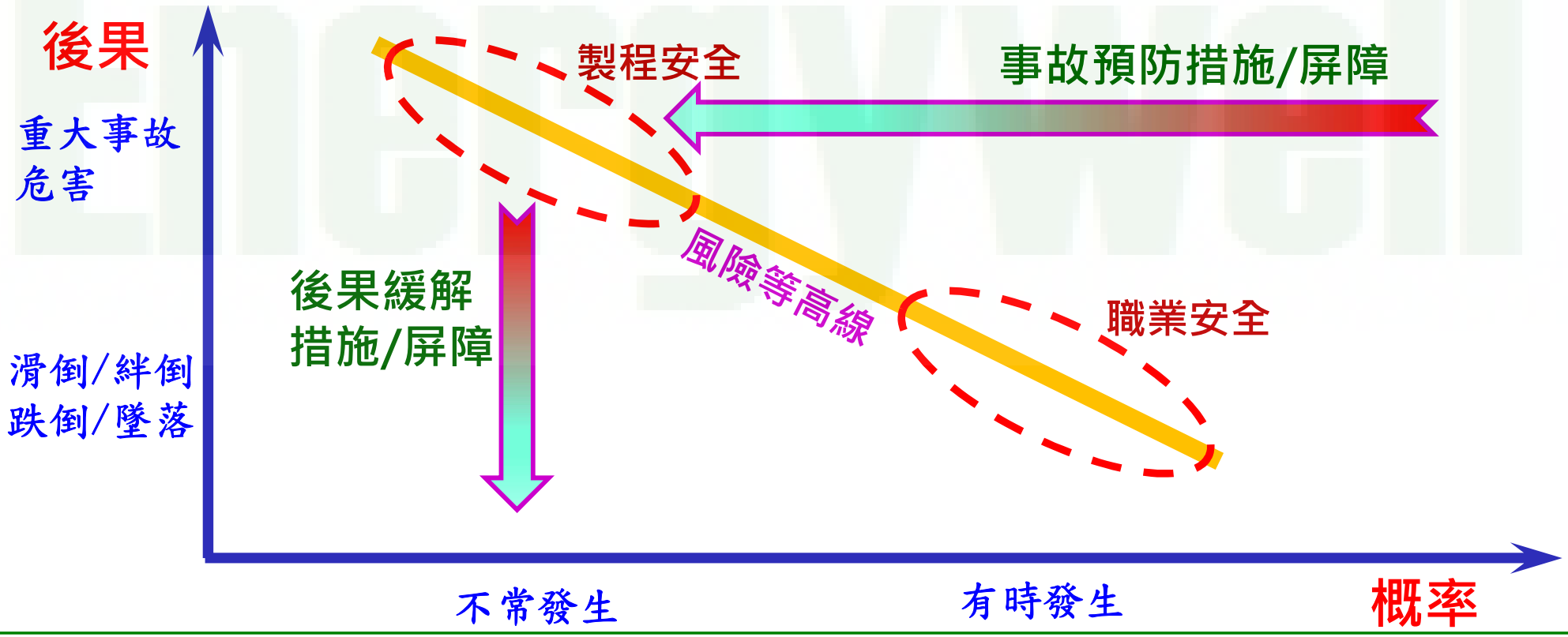
資料來源: ISO 17776, A.1
E&P: 探勘與生產(Exploration & Production)

製程安全與職業安全

- 製程安全
  - 著重於能源釋放的重大事故管理
- 職業安全－工作場所安全
  - 著重於管理影響個人的事件

實務上，重大危害事故的預防應(Shall)或宜(Should)設計

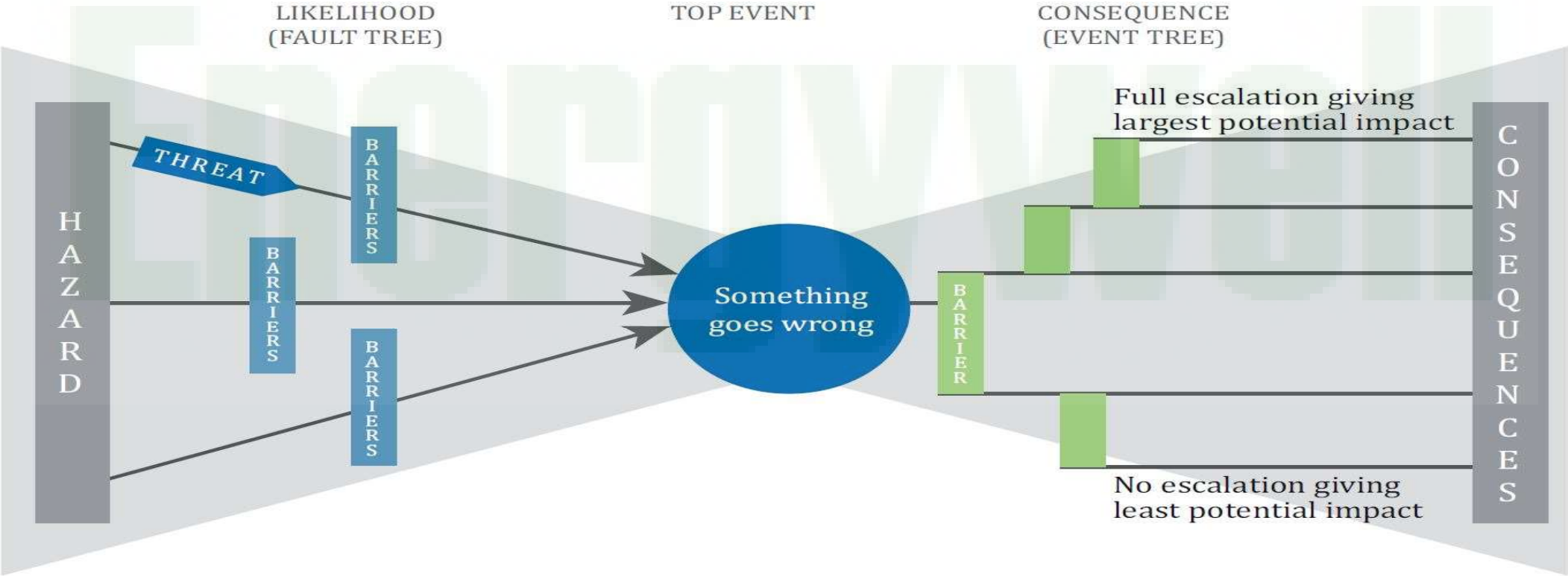
工程控制類別的安全屏障



註: Shall, Should, May, Can這裡引用財團法人全國認證基金會(TAF)的標準用語翻譯

領結(蝴蝶結)(Bow-Tie)分析

- 領結是一種設計工具，可用於評估阻止頂端事件發生的屏障和恢復措施，以減少後果
- 它基於一個模型，該模型表示如何釋放危險、升級以及如何控制危害



The *identification, design, installation* and *maintenance* of threat and escalation barriers are *HSE Critical Activities*

資料來源: ISO/TS 16901:2015

展現ALARP所需的屏障數

Barriers	High risk hazards	Medium risk hazards with potential fatalities	Other medium risk haz-ards
Total number of barriers from threat to consequence	5 controls + recovery measures	4 controls + recovery measures	3 controls + recovery measures
Controls (threat)	3 controls to be in place for each identified threat. *Alternative:* 4 controls	2 controls to be in place for each identified threat. *Alternative:* 3 controls	2 controls to be in place for each identified threat
Recovery measures (consequence)	2 recovery measures required for each identi-fied consequence. *Alternative:* 1 recovery measure	2 recovery measures required for each identi-fied consequence. *Alternative:* 1 recovery measure	1 recovery measure required for each identi-fied consequence

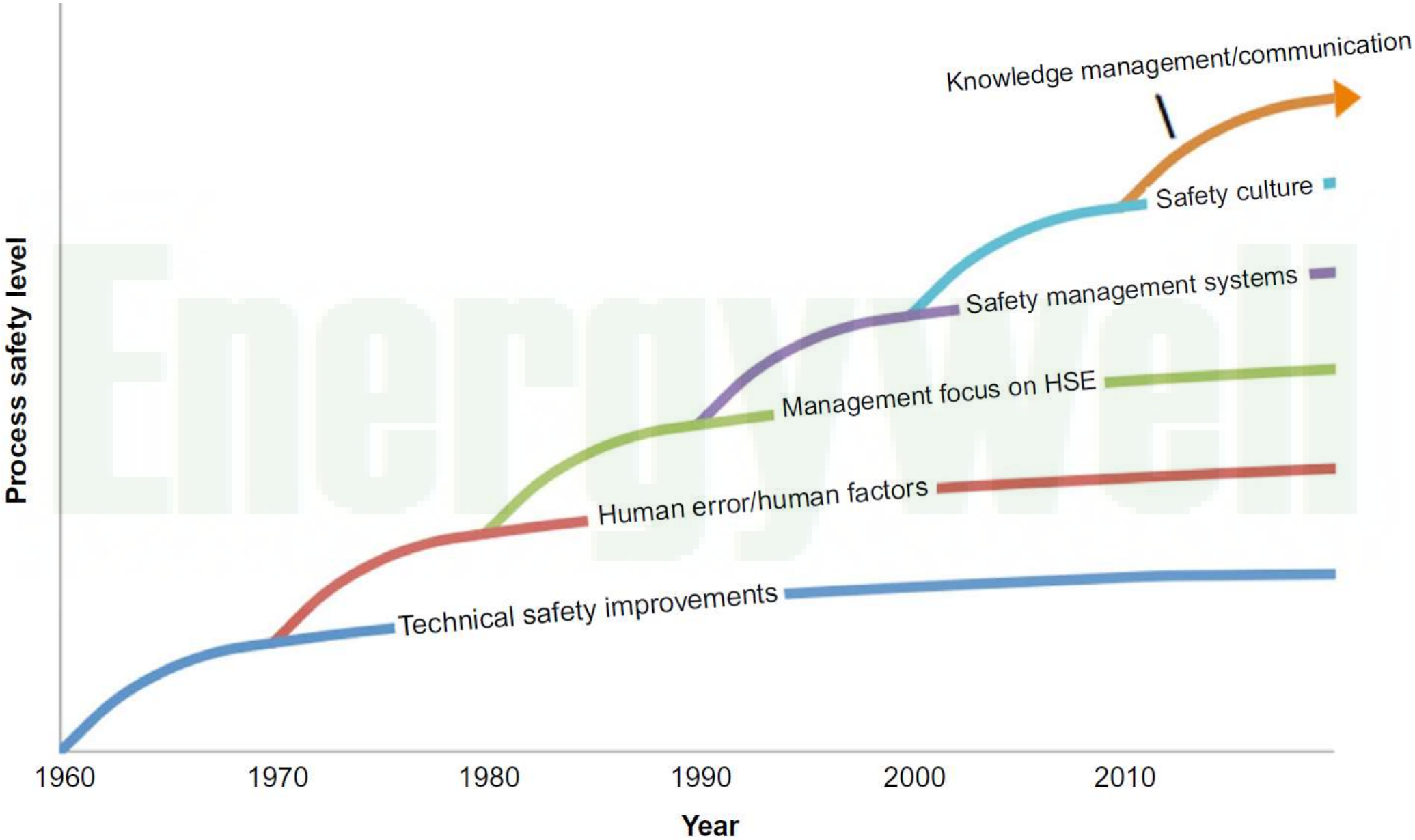
- 在大多數情況下，一個屏障僅能採計為「一個」
  - 經驗豐富的保護層分析(Layer of Protection Analysis, LOPA)危害分析師可以根據最佳實務給予特定屏障額外的風險削減績效
  - 例: 對於安全完整性等級(Safety Integrity Level, SIL) 2的安全儀錶系統，可以視為兩個屏障
- 需要嚴謹考慮屏障之間的獨立性
  - 共同原因故障(Common Cause Failure, CCF)分析
  - 電力/電子/可編成電子(E/E/PE) - 安全相關系統: 具有SIL績效的安全儀錶功能和系統

資料來源: ISO/TS 16901:2015

風險屏障

- 屏障可以是(例如):
  - 設計特徵 - 例如分離距離
  - 硬體 - 例如減壓閥、火災探測
  - 關鍵作業管制程式 - 例如上鎖/掛簽(Lot-out/Tag-out, LOTO)
  - 操作員介入的任務 - 例如工廠監視/關斷/停車
  - 組合任務 – 群組功能: 例如警報加操作員操作
- 應確定管理每種威脅的適當屏障
  - 要使屏障有效，它應為:
    - 有效防止頂端事件或後果
    - 能夠防止特定威脅釋放危害
    - 可核實 - 例如透過稽核維持有效屏障所需的環安衛(ESH)關鍵活動
    - 獨立於同一威脅線內的其他屏障

製程安全演變的重大貢獻



Ref.: Faisal Khan, Methods in Chemical Process Safety, Volume 1, Academic Press (2017)

事故預防和製程安全策略的演變

基於標準的策略 → **基於合規的策略** → **持續改進的策略** → **基於風險的策略**

我該怎麼做?

我需要做什麼?

如何根據自己的經驗進行改進?

如何更好地管理風險？

製程安全

- 倚賴並仰仗團隊的共同努力
- 瞭解自己的角色並與同事一起保護自己和他人
- 瞭解與混合、分離或存儲製程物料相關的危害，包括:
  - 哪種化學物質具有反應性或能夠引起失控反應
  - 與製程化學品相關的有毒、火災或爆炸危害
  - 在事故或異常過程中如何處理

製程安全(續)

- 注意設備操作和維護要求，包括:
  - 腐蝕、洩漏或其他設備問題的跡象或徵候
  - 當您發現問題時，誰應被提醒或被通知
- 瞭解您的製程:
  - 遵循操作、安全和緊急程序
  - 隨時瞭解程序、設備和化學品的最新變更
  - 提供回饋 - 報告所有的事件和未遂(或虛驚)事件

如何有效實施製程安全管理

- 幾個常見的問題:
  - PSM是管理系統嗎?
  - PSM有涵蓋一個製程的全生命週期嗎?
  - 如何進行風險基準的PSM?
  - 如何進行製程安全績效的量化管理?
  - PSM可以一步到位嗎?
  - 有無系統工程的方法，有效實施PSM?
- 答案只有一個
  - 達成這樣的目標，僅能仰仗您自己，包括您的決心、承諾、資源投入、紮實基礎，與持之有恆的支持

六個重要的疑問

- 回饋安全屏障管理
  - 您知道您工作場所的主要危害嗎?
  - 您知道您工作場所的主要危害事件或代表事件群組和事件列及其相關情境嗎?
  - 您知道哪些是您工作場所的安全關鍵要素/設備(SCEs)?
  - 您知道每一個主要危害事件的關鍵安全屏障嗎?
  - 這些關鍵的安全屏障有無被妥善的確保績效，及進行管理?
  - 您如何知道它們正確安裝且有效運作? 如何確保它們維持功能正常?

如何架構並實施有效的PSM

- 必須完整嵌入並架構在事業體的職業安全衛生管理系統(ISO 45001)之下
  - 在品質管理系統(ISO 9001)高階結構的統一框架之下，朝向整合管理系統(Integrated Management System, IMS)邁進
  - 可以進一步整合包括:
    - 環境管理系統 – ISO 14001
    - 能源管理系統 – ISO 50001
    - 資訊安全管理系統 – ISO 27001
    - 資產完整性管理(AIM)系統 – ISO 55001
    - 設施管理系統 – ISO 40001
  - 引用ISO 31000:2018風險管理－原則與指導綱要
    - 全生命週期風險管理
    - 風險基準的風險管理
    - 動態風險管理
  - 必須能夠被有效驗證(Verification)和確認(Validation)
    - 系統工程(System Engineering)方法論的引用

如何架構並實施有效的PSM (續)

- 在職業安全衛生管理系統或IMS之下，發展並建立良好的HSE計畫(HSE Plan)
  - 遵循高位階的HSE計畫，建立安全管理系統(Safety Management System, SMS)及其相關的程序文件
  - 在SMS之下，嵌入並在適當的階段和任務中，實施PSM的各項要素
- 有效的SMS有五個主要元素:
  - 安全文化
  - 參與
  - 井場(wellsite)分析
  - 危害預防和控制
  - 教育和培訓

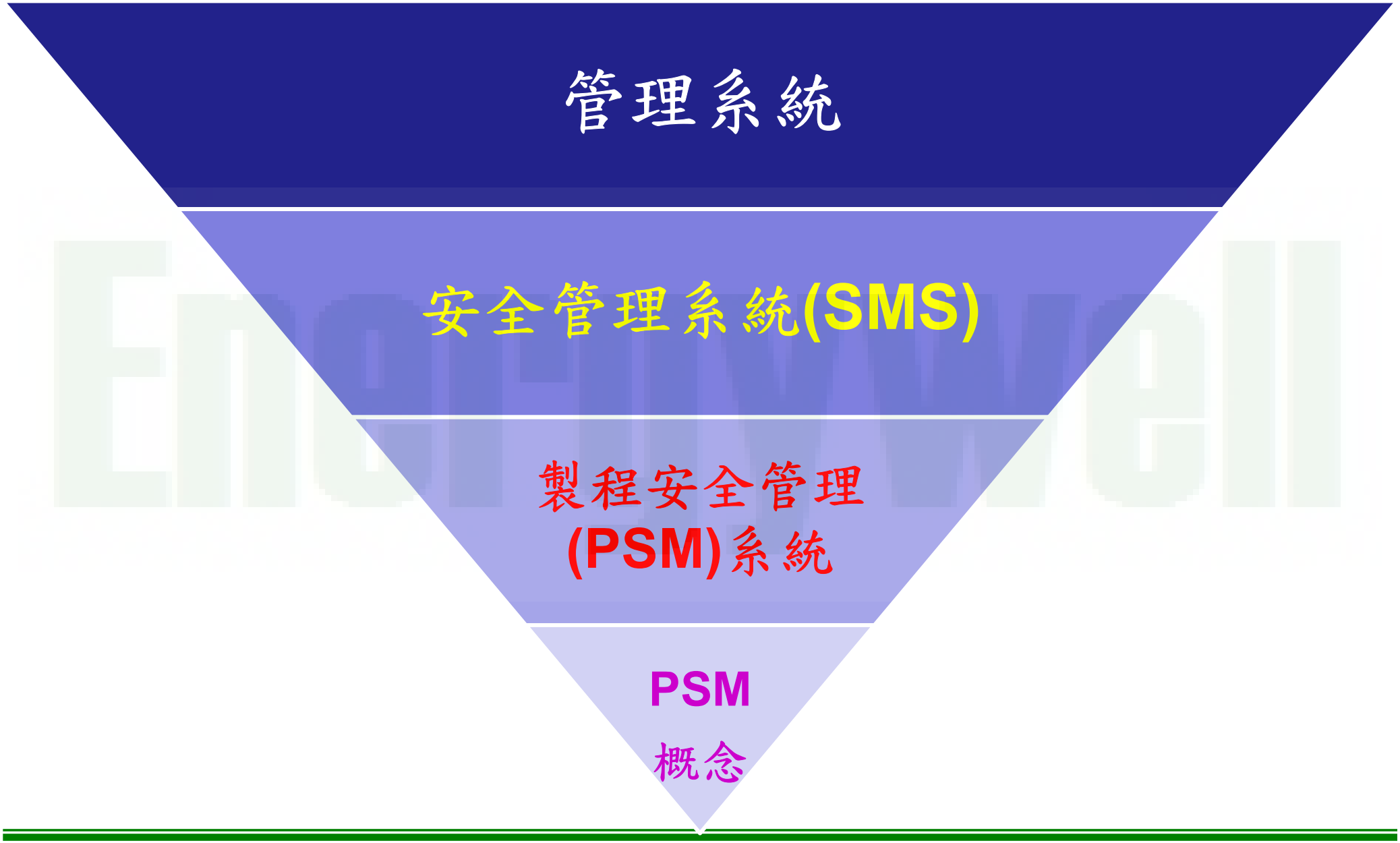
如何架構並實施有效的PSM (續)

- 有用的資訊用以實施PSM (這必須仰賴您的團隊努力瞭解有用的知識來源)
  - AIChE CCPS (2016) - Guidelines for Implementing Process Safety Management Systems
  - AIChE CCPS (2016) - Guidelines for Integrating Management Systems and Metrics to Improve Process Safety Performance
  - AIChE CCPS (2016) - Guidelines for Asset Integrity Management
  - AIChE CCPS (2007) - Guidelines for Risk Based Process Safety
  - AIChE CCPS (2011) - Guidelines for auditing process safety management systems
  - AIChE CCPS (2012) - Guidelines for Engineering Design for Process Safety
  - AIChE CCPS (2013) - Guidelines for Managing Process Safety Risks During Organizational Change
  - AIChE CCPS (2015) Guidelines for Defining Process Safety Competency Requirements
  - AIChE CCPS (2018) - Bow ties in risk management - A Concept Book for Process Safety
  - AIChE CCPS (2018) - Guidelines for Siting and Layout of Facilities
  - AIChE CCPS (2018) - Guidelines for Integrating Process Safety into Engineering Projects
  - AIChE CCPS (2018) - Essential Practices for Creating, Strengthening, and Sustaining Process Safety Culture
  - AIChE CCPS (2018) - Dealing with Aging Process Facilities and Infrastructures
  - AIChE CCPS (2018) - Recognizing and Responding to Normalization of Deviance
  - EI PSM - High level framework for process safety management
  - EI PSM - Guidance on meeting expectations of EI Process safety management framework element 1~20

典型SMS手冊的章節安排

- 詞彙表
- 出版物/文獻
- 簡介
- 安全管理基礎
- 安全文化
- 安全績效管理
- 安全數據收集和處理系統
- 安全分析
- 保護安全數據、安全資訊和相關來源
- 事業(企業)的安全管理
  - 整合至上層位階的職安衛管理系統
- 安全管理系統
  - 簡介
  - SMS框架
  - 安全政策和目標
  - 安全風險管理
  - 安全保證(Safety Assurance)
    - 引用系統工程的驗證(Verification)和確認(Validation)保證方法
  - 安全促進
  - 實施計畫

製程安全管理的要素結構



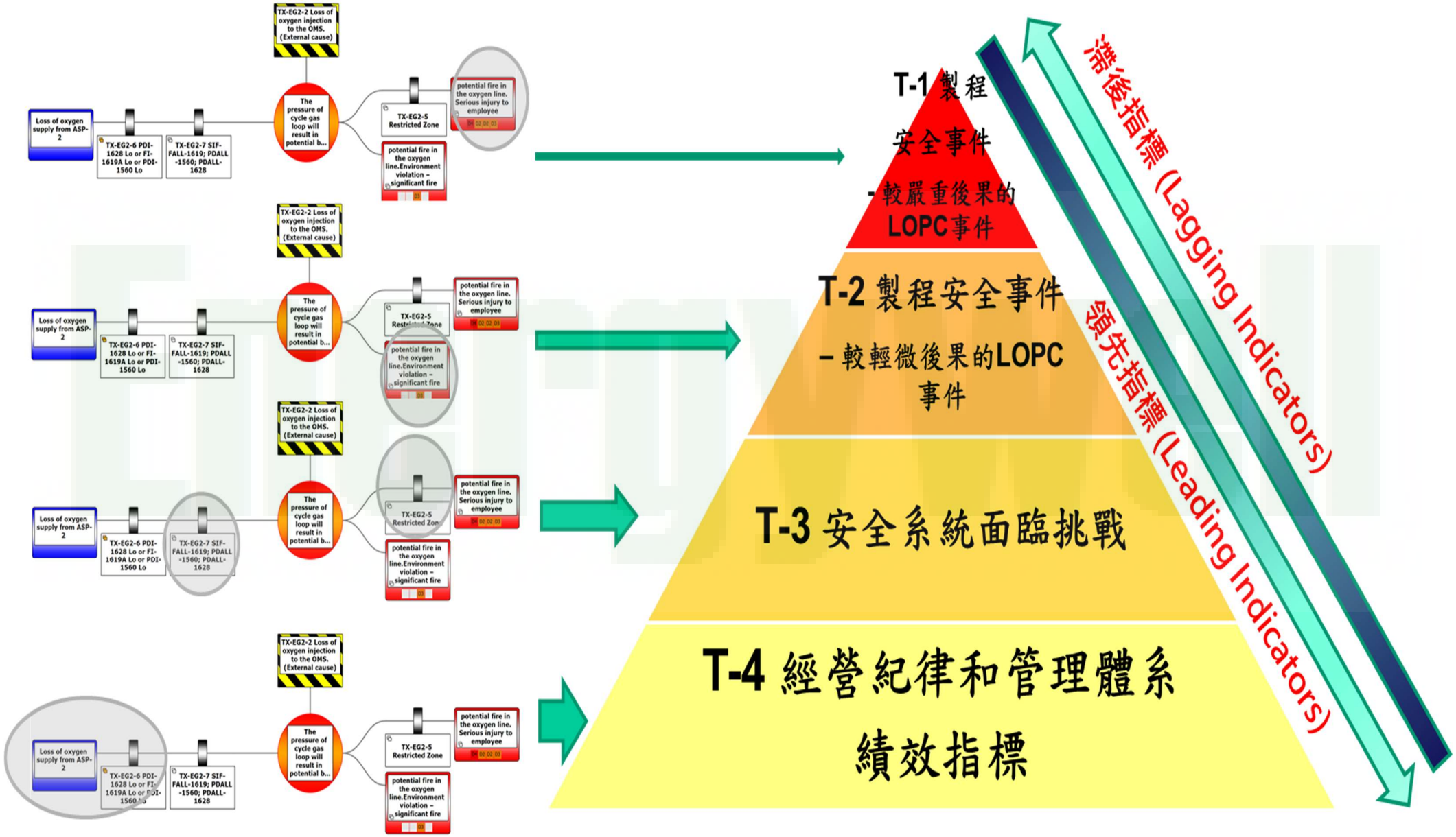
對安全負責

- 雇主安全問責制應該有六個要素:
  - 正式的績效標準
  - 充足的資源和社會心理支持
  - 績效衡量系統
  - 應用有效的結果論
  - 適當應用結果論
  - 持續評估問責制

關注安全管理系統(SMS)的一般目標

- 查核以下須包含在SMS中的一般目標:
  - 指定合格的安全人員來協調該計畫
  - 使用書面的工作安全分析(Job Safety Analysis, JSA)來規劃安全
    - 透過風險評估和方法聲明(Risk Assessment & Method Statement, RA & MS)分級管制作業安全
  - 定期進行駐井(wellsite)安全檢查並進行健康監測
  - 遵守安全程序和規則
  - 提供持續的安全培訓
  - 實施安全規則並使用適當的紀律

PSM績效量測 – 製程安全績效指標(PSPI)



註: US OSHA PSM強制實施危害控制與分析(HCA)、Bow-tie方法為AIChE/CCPS推薦的PSM HCA之RAGAGEP最佳實務

執行製程安全管理任務的PDCA方法示例

方法(以製程危害評估為例)		規劃(P)	執行(D)	查核(C)	行動(A)
辨識	辨識危害: 檢核表、危害與可操作性研究、故障模式與影響效應分析、如果-結果又如何等 辨識製程安全目標、辨識監管法規要求				
實施	本質安全設計 檢查計畫、修復和更換、晶相變化 安全和控制系統以降低事故發生頻率 • 基本製程控制系統 • 警報和人員介入處理 • 安全儀錶系統 • 緊急停車裝置 • 壓力釋放裝置 緩解措施和系統以降低事故影響後果 • 實體圍堵性設備(防溢堤、防爆牆、消防系統等) • 工廠和社區緊急應變				
措施	事故後果影響評估 事故發生概率評估 風險評估				
評價	ALARP (成本效益分析(CBA)、效益-成本比率分析(BCR)、淨現值(NPV)分析) 保護層分析(LOPA)、安全完整性(SIL)評估				
監測	領先指標、滯後指標				
管理	績效/效能標準、稽核程序、安全文化				
維持	基於更新的資訊，重複執行P-D-C-A循環				

Ref.: Faisal Khan, Methods in Chemical Process Safety, Volume 1, Academic Press (2017)

製程安全與資產完整性

- 製程安全
  - 著重於能源釋放的重大事故管理
- 資產管理
  - 可以實現資產的價值
  - 無論任何行業，透過使用具有類似核心特徵的分析方法和實施流程來達成價值實現
- 資產完整性
  - 資產在保護生命和環境的同時履行其功能的能力
- 資產績效
  - 資產能夠在最大化事務/業務/商務績效的同時執行其功能

整體製程安全管理

Source: MMI, Process Safety & Barrier Management – Lessons from major hazard industries, Engineers Ireland, Fire & Safety Division Conference

講題二

RAGAGEP簡介

什麼是RAGAGEP?

- 源自US OSHA PSM法規
  - 自1992年起，即已規定，迄今並無新的規則(No New Rules)
  - 29 CFR 1910.119 (d)(3)(i)(F)
    - 採用的規範/標準
  - 29 CFR 1910.119 (d)(3)(II)
    - 符合RAGAGEP
  - 29 CFR 1910.119 (d)(3)(III)
    - 既有一般不常使用設備的安全
  - 29 CFR 1910.119 (J)(4)(II)
    - 遵循RAGAGEP實施檢查/測試(Inspections/Tests, I/T)
  - 29 CFR 1910.119 (J)(4)(III)
    - I/T的實施頻率

US OSHA關於RAGAGEP的第一次解釋

- 標準解釋符合PSM和ANSI/ISA-S84.01的安全儀錶系統(Safety Instrumented System, SIS)
  - 發佈於2000年
    - 參考網址資訊:
      - https://www.osha.gov/laws-regs/standardinterpretations/2000-03-23
  - 亦即IEC 61511標準
    - 台灣實務上常提到的安全完整性等級(Safety Integrated Level, SIL)、功能安全工程(Functional Safety Engineering, FSE)、功能安全管理(Functional Safety Management, FSM)
  - 解釋標準號:
    - 29 CFR 1910.119 (d)(3)
    - 29 CFR 1910.119 (f)(1)(iv)
    - 29 CFR 1910.119 (j)

RAGAGEP為何重要?

- PSM標準是強調「績效/性能(Performance)」的標準
  - 雇主擁有很多自由度以執行PSM的合規性
  - 雇主有責任證明其PSM實施的績效/性能與合規性
    - 如何證明和展現(Demonstration)呢?
    - 透過RAGAGEP要求的實施提供了雇主選擇適用規範/標準的自由度，並據此實施結果證明和展現其實施PSM的績效/性能
- 一個簡單的問題:
  - 您有一個堅實的安全管理系統(Safety Management System, SMS)嗎?
    - 說出您做了些什麼? (識別並寫下來、並承諾)
    - 做您所說的內容 (實施/執行)
  - 如果您以這麼做，那麼您已經實施了RAGAGEP

RAGAGEP的適用選擇權

- 雇主擁有選擇適用RAGAGEP規範/標準的權利
  - 除法規已強制規定的部分例外
  - 此原則，亦適用於台灣的法規要求與業界實做的實務應用
- 非常重要:
  - 並非所有被強制要求的RAGAGEP或者所有被選擇適用的RAGAGEP都在使用中
  - 只有適用於特定工作場所應用程序的RAGAGEP被使用
- US OSHA官方解釋RAGAGEP的參考資訊
  - US OSHA: RAGAGEP in Process Safety Management Enforcement 5/11/2016
    - https://www.osha.gov/laws-regs/standardinterpretations/2015-06-05-0

US OSHA PSM RAGAGEP的例子

- 廣泛採用的規範
  - 某些共識標準已被聯邦、州或市轄區廣泛採用
    - 許多州和市政建築和其他規範包含或採用諸如國家消防協會(National Fire Protection Association, NFPA)的NFPA 101生命安全和NFPA 70國家電氣規範等
    - 例如:
      - ASME B&PV Code
      - NFPA-70 / NFPA 85/86 / NFPA 101
      - NEC
      - IBC
      - etc.

US OSHA PSM RAGAGEP的例子

- 共識文件
  - 某些組織如美國機械工程師協會(American Society of Mechanical Engineers, ASME)遵循美國國家標準協會(American National Standards Institute, ANSI)的基本要求
    - 制定共識標準和推薦做法時，美國國家標準(基本要求)的正當程序要求
    - 根據ANSI和類似要求，這些組織必須證明他們擁有多元化且具有廣泛代表性的委員會成員資格
    - 共識文件的例子包括ASME B31.3製程管線規範和國際氨製冷研究所(International Institute of Ammonia Refrigeration, IIAR)
      - ANSI / IIAR 2-2008 - 閉環路氨機械製冷系統的設備、設計和安裝
    - 這些共識文件被業內的人廣泛用作RAGAGEP的來源
    - 例如:
      - NFPA 30
      - API RP 752
      - IIAR-2

US OSHA PSM RAGAGEP的例子

- 非共識文件
  - 一些行業使用不符合ANSI基本要求的流程開發非共識工程文檔
  - 在適用的情況下，這些文件中描述的做法可被廣泛接受為良好實務
    - 例如，氯研究所(Chlorine Institute, CI)的「小冊子」側重於氯和次氯酸鈉(漂白劑)的安全性，並被一些處理這些原物料的公司使用
  - 請注意，OSHA還認可「適用的」製造商關於RAGAGEP潛在來源的建議
  - 例如:
    - CI的小冊子
    - 緊急排放系統設計研究所(Design Institute for Emergency Relief System, DIERS)
    - 關於特定危害的技術論文

US OSHA PSM RAGAGEP的例子

- 內部標準
  - PSM標準的序言承認雇主可以制定內部標準，以便在其設施內使用
  - 序言部分說明了相關部分
    - 規則制定參與者提出的短語：「公認和普遍接受的良好工程實務」與OSHA的意圖一致
    - 原子能機構還認為，這一短語將包括適當的設施內部標準…
  - 內部制定的標準仍然必須代表公認和普遍接受的良好工程實務

RAGAGEP的「應(Shall)」用語

- RAGAGEP中使用的「應」、「必須(Must)」或類似用語反映了開發人員的觀點
  - 即該實務是控制危害的強制性最低要求
  - 同樣地，「不應(Shall not)」、「禁止(Prohibited)」或類似的用語參考或描述了不可接受的方法或做法
  - 如果雇主偏離了雇主自己所採用的RAGAGEP適用的「應」或「不應(Shall not)」的要求，US OSHA將推定其為違規行為
  - 根據US OSHA現場作業手冊(CPL 02-00-159, 1/10/2015)第3章中描述的檢查程序
    - 雇主將有機會解釋偏離的理由，以及它認為其方法反映公認和普遍接受的良好工程實務

註: Shall, Should, May, Can這裡引用財團法人全國認證基金會(TAF)的標準用語翻譯

RAGAGEP的「宜(Should)」用語

- 在RAGAGEP中使用術語「宜」或類似的語言表示反映可接受和優選實務的建議
  - 如果雇主選定的RAGAGEP中的「宜」條款適用於所涵蓋的製程或特定情況，US OSHA會假定雇主遵守建議的方法是可以接受的
  - 如果雇主選擇包含「宜」條款，但不遵守規定的RAGAGEP，US OSHA不會推定其為違規行為
    - 此情況合規安全和衛生官員(Compliance Safety and Health Officer, CSHO)「宜」評估雇主的方法是否反映了公認和普遍接受的良好工程實務，以及雇主是否紀錄其設備符合RAGAGEP
    - 如果雇主紀錄其設備符合RAGAGEP，則雇主不需要紀錄與「宜」聲明的差異

註: Shall, Should, May, Can這裡引用財團法人全國認證基金會(TAF)的標準用語翻譯

RAGAGEP的「宜(Should)」用語

- 如果雇主選擇包含「不宜(Should not)」條款的RAGAGEP (或描述不受歡迎做法的類似用語)，然後遵循不受歡迎的做法，US OSHA將不會推定其為違規行為
  - 在這種情況下，CSHO「宜」評估雇主的方法是否反映了公認和普遍接受的良好工程實務，以及雇主是否紀錄其設備符合RAGAGEP
  - 如果雇主紀錄其設備符合RAGAGEP，則雇主不需要紀錄與「不宜」聲明的差異

註: Shall, Should, May, Can這裡引用財團法人全國認證基金會(TAF)的標準用語翻譯

RAGAGEP中的規範和信息要求

- 強制性的規範(Normative)要求與建議性或參考性的信息(Informative)要求
  - 規範和共識文件通常包含提供補充信息和/或要求的附錄或附件
  - 這些附錄或附件的內容可以是「規範性的(Normative)」或「信息性的(Informative)」
    - 規範性部分通常解釋如何遵守規範和/或共識文件的要求，並且可能包含「應」和「宜」的用語
      - 「應」表示開發人員認為規範性聲明是強制性的觀點，而「宜」表示反映可接受和優選實務的建議
    - 信息性部分通常提供關於規範和/或共識文檔要求的背景和參考信息，但也可以識別和/或解決危害或可接受的減排手段
  - 雇主宜閱讀並考慮這些部分，但US OSHA並不希望雇主查閱信息部分或附錄中引用的所有來源

最常引用的PSM RAGAGEP違規行為

- 29 CFR 1910.119 (d)
  - 製程安全資訊(Process Safety Information, PSI)
  - 用於所有製程設備的設計

- 29 CFR 1910.119 (j)
  - 機械完整性(Mechanical Integrity, MI)
  - 用於(j)(1)所述設備的檢查和測試(I/T)方法和頻率

RAGAGEP – PSI

- 使用的設計規範和標準文檔
  - (d)(3)(i)(F)
- 製程設備符合RAGAGEP的文檔
  - (d)(3)(ii)
- 非使用標準(Out-of-use Standards)建造的既有設備是安全的確定紀錄文檔
  - (d)(3)(iii)
- 雇主應制定並保存書面PSI的彙編
  - (d)(3)(i)(F)
  - 與製程中的設備有關的資訊應被包括
  - 所採用的設計規範和標準
  - 應說明您做了些什麼?

RAGAGEP – PSI (續)

- 雇主應紀錄該設備符合公認和普遍接受的良好工程實務
  - (d)(3)(ii)
  - 雇主選擇他將使用/遵守的適用和保護性的RAGAGEP
    - 不是主管機關替您選擇 (法規強制規定或要求者除外)
  - PSI要求與涵蓋製程中的設備有關
  - 設備必須實際遵守RAGAGEP，以便雇主紀錄合規情況
  - 不僅僅是文檔要求還需要實踐
    - 做您所說的話
  - 簡單的概念
    - 您無法紀錄您尚未做的事情

RAGAGEP – PSI (續)

- 對於根據一般不再使用的規範、標准或慣例設計和建造的既有設備，雇主應確定並紀錄設備的設計、維護、檢查、測試 ，並以安全的方式運作
  - (d)(3)(iii)
- RAGAGEP可以隨時間改變
  - ASME規範壓力容器安全係數(由於更好的合金、檢查方法而降低)
  - API 510 (最新版本:2014)和API 570 (最新版本: 2016)壓力容器與管線檢查規範
  - API RP 2219真空卡車在石油服務中處理易燃和可燃液體的安全操作(最新版本:2016)
- 在美國，除非RAGAGEP明確追溯，否則US OSHA不能要求雇主將其設備更新為當前的RAGAGEP
  - 雇主必須確定並紀錄其製程設備是否安全
  - US OSHA希望雇主考慮將RAGAGEP中的相關變更作為風險管理活動的一部分

RAGAGEP – MI

- 檢查和測試實務應遵循RAGAGEP
  - (j)(4)(ii)
  - 已發佈用於檢查大多數PSM/MI所覆蓋設備的標準/實務
- 您的MI程序是否以適當的MI RAGAGEP為基礎?
  - (j)(2)
  - MI請說明您做了什麼?
    - 提出做您所說的話的證據和展現文檔
- 旨在確保在發生故障之前檢測到符合機械完整性要求的製程設備的缺陷
  - (j)(4)(ii)
  - US OSHA通常希望雇主在RAGAGEP更改/升級後的合理時間/時段內(不固定時間區段)更新其檢查和測試實務
  - 譬如: 您有多久沒有審視API 510和570，並確認其最新版本更新後是否存在差異?

RAGAGEP – MI (續)

- 製程設備的檢查和測試頻率應符合適用製造商的建議和良好的工程實務，並且如果既往的操作經驗確定是必要的，則宜更頻繁
  - (j)(4)(iii)
  - 當操作經驗表明有必要時，I/T必須更頻繁地執行
    - 發現排放/釋壓閥在正常的I/T間隔內被污染或腐蝕時
    - 發現管線或壓力容器腐蝕比預期更快或變異更大時

如何判定內部標準符合RAGAGEP?

- 當內部開發的標準保護效力或程度不如公佈的規範、標準或實務
- 當基本要求不遵循規範、標準或實務中的「應」、「不應」、「宜」、「不宜」用語，而是使用替代方法來控制危害
- 如果內部標準與常用的已發布文檔一致，則可能是可接受的
- 簡單的規則
  - 法規強制要求適用的規範、標準、實務應遵循
  - 除非同業經常引用的RAGAGEP不存在或不適用或無法適用時，「可(May)」或「能(Can)」自行依據RAGAGEP制定原則發展，但應聲明
  - 所引用的規範、標準、實務其內部標準用語不應被降級要求
    - 譬如:「應」改為「宜」或「可」或「能」(視為違規)
    - 譬如:「宜」改為「可」或「能」(不被視為違規，但必須仍為RAGAGEP，應聲明)
    - 相反地，升級用語要求為符合RAGAGEP
    - 不能低於製程技術設計廠商之安全要求或設備製造商建議之實務要求

註: Shall, Should, May, Can這裡引用財團法人全國認證基金會(TAF)的標準用語翻譯

常見的RAGAGEP例子

	Boilers	Pressure Vessels	Piping	Valves	Aboveground Storage Tanks	Safety/Safety Relief Valves	Pumps	Instrumentation and Controls	Pipelines (49 CFR-186-199)
2. DESIGN OR CONSTRUCTION CODES:	ASME I ASME IV	ASME VIII DIV. 1 & 2	ASME B31.1 ASME B31.3	ASME B16.34 API 600 API 609	API 12B API 650 API 620	ASME I ASME IV ASME VIII API 2000	API 610 API 574-676	VARIOUS ISA STANDARDS AND RP 551	B31.4 B31.8 API 1104
3. INSPECTION, REPAIR, ALTERATION, RERATING, OR FITNESS FOR SERVICE CODES:	NBIC	NBIC API 510 API 579	API 570 API 579	API 598 API RP591	API 653 API 579	NBIC API RP 576	API RP683 MFG STDS	ISA/MFG STANDARDS	ASME B31G
4. "SUPPORT" OR "REFERENCED" CODES OR PUBLICATIONS:	ASME II, ABCD ASME V ASME VI & VI ASME IX API RP 573 5NT-TC-1A	ASME II, ABCD ASME V ASME IX API RP 572 API IRE II 5NT-TC-1A	ASME II, ABCD ASME V ASME IX API RP 574 ASME B16.5 5NT-TC-1A	API RP 574 ASME V ASME IX	API 651 API 652 API 2016 API 2207 API RP 575 ASME V ASME IX 5NT-TC-1A	ASME PTC-25 API 627 ASME V ASME IX	MFG. STANDARDS AWS D14.5	INSTRUMENT ENGINEER'S HANDBOOK MFG. STANDARDS	ASME V ASME IX

Source: Oneok Partners

常見的RAGAGEP例子 (續)

- 加熱爐/燃燒管理系統(BMS)允許操作互鎖設計

		NFPA 85	NFPA 86	S84-TR5	API 556
1.1	**Fuel block valves proved closed**	✓	✓	✓	✓
1.2	**Absence of flame proved**	✓	✓	✓	✓
1.3.1	**Pre-purge flow proved**	✓	✓	✓	✓
1.3.2	**Pre-purge timer complete**	✓	✓	✓	✓
1.4	Air proved at low fire rate	✓		✓	✓
1.5	Fuel pressure in correct range	✓		✓	✓
1.6	Pilot flame detected within time	✓	✓	✓	
1.7	Main fuel set at low fire position	✓	✓	✓	
1.8	Main flame detected within time	✓	✓	✓	
1.9.1	Post purge flow proved	✓			
1.9.2	Post purge timer complete	✓			
1.10.1	Adequate process level			✓	
1.10.2	Adequate process flow				✓

Source: Oneok Partners

常見的RAGAGEP例子 (續)

- **BMS點火/空氣/燃料控制安全聯鎖設計**

		NFPA 85	NFPA 86	S84-TR5	API 556
2.1	**Loss of flame**	✓	✓	✓	✓
2.2	**Loss of combustion air**	✓	✓	✓	✓
2.3	Low furnace pressure				✓
2.4	High furnace pressure	✓			✓
2.5	**Low fuel pressure**	✓	✓	✓	
2.5.1	Low fuel pressure – at pilot	✓		✓	✓
2.5.2	Low fuel pressure – at main burner	✓			✓
2.6	**High fuel pressure**	✓	✓	✓	
2.6.1	High fuel pressure – at pilot	✓		✓	✓
2.6.2	High fuel pressure – at main burner	✓			✓
2.7.1	Loss of atomizing medium	✓	✓	✓	N/A
2.7.2	Heated oil – Low temp/High visc	✓	✓		N/A
2.7.3	High heated oil temperature	✓	✓		N/A

Source: Oneok Partners

常見的RAGAGEP例子 (續)

- **BMS燃燒控制系統和製程安全聯鎖設計**

		NFPA 85	NFPA 86	S84-TR5	API 556
3.1	**Loss of actuating energy**	✓	✓	✓	✓
3.2	**Power failure**	✓	✓	✓	✓
3.3	Emergency Shutdown	✓	✓		✓
4.1	Low (water) level	✓		✓	✓
4.2.1	**Excess (steam) pressure**	✓	✓	✓	✓
4.2.2	**Excess (water) temperature**	✓	✓	✓	✓
4.3	Low process flow		✓	✓	✓
4.4	High furnace discharge temp			✓	✓
4.5	High skin temperature				✓

Source: Oneok Partners

常見的RAGAGEP例子 (續)

- 安全儀錶系統功能安全管理(FSM)
  - 安全管理系統(SMS)
  - 安全管理計畫(SMP)
  - 安全儀錶功能(SIF)清單
    - SIF的SIL判定/配當分析程序/報告
    - 危害辨識/危害風險評估程序/報告
    - LOPA分析程序/報告
  - 安全要求規格(SRS)
  - SIL驗證(Verification)計算程序/報告
  - 因果圖(C&E Diagram)
  - P&IDs、SIS邏輯圖
  - 迴路圖、SIS設計規格書
  - 控制盤體布置圖
  - FAT/SAT程序/報告
  - 驗證/確認(Validation)程序/報告
  - 功能安全評估(FSA)
  - 安裝與核可程序/QA/QC紀錄
  - 操作與維護程序/紀錄
  - 驗證測試程序(Proof-test Procedure)/定期實施報告
  - SIS需求/故障報告、分析及矯正措施系統(FRACAS)與紀錄
  - FSM稽核計畫/報告
  - FSM MOC程序/紀錄與衝擊分析
  - 訓練紀錄

註: 藍色字體顯示者為台灣現況實務欠缺實做或者較不完備者

大哉問 ...

- 前述的例子說明
  - 我們目前沒有很有系統的整理企業引用的內部標準或RAGAGEP清單
  - 如果不嫻熟RAGAGEP實務的實際要求內容，如何有效查核雇主是否遵循RAGAGEP?
    - 不禁發出的疑問是: 何謂「合格的PSM稽核人員」或「合格的PSM符合性稽核或檢驗人員」?
  - 即便在台灣，要求IEC 61511功能安全(或泛稱SIL工程)已非常普遍，但真的有符合IEC 61511的「應(Shall)」RAGAGEP用語嗎?
- 前述問題的答案，明顯證明
  - 我們離RAGAGEP的落實還有非常大的差異與距離....

風險控制的堅實基礎 - RAGAGEP

請您務必記得 ...

基於標準的策略 → 基於合規的策略 → 持續改進的策略 → 基於風險的策略

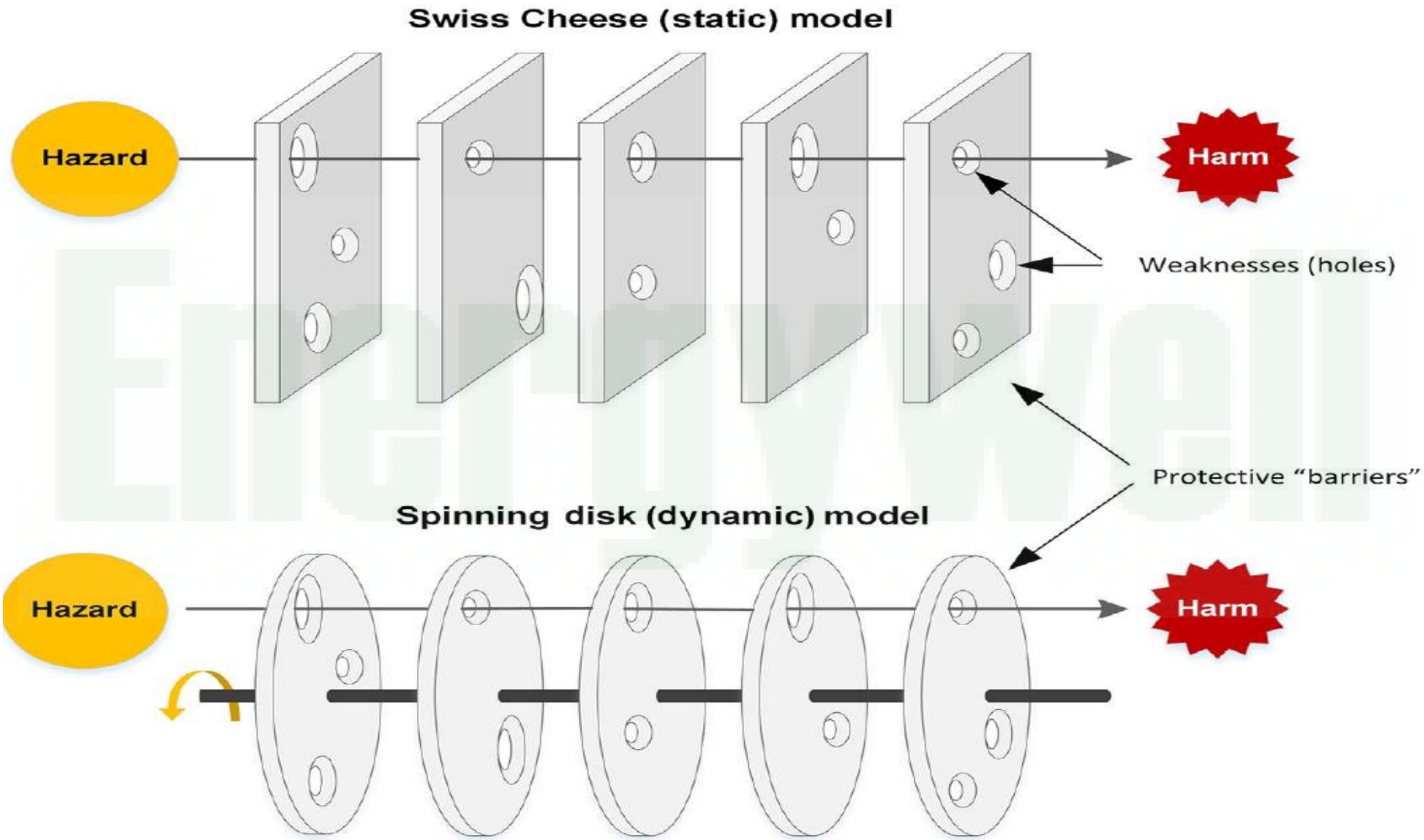
我該怎麼做?

我需要做什麼?

如何根據自己的經驗進行改進?

如何更好地管理風險？

安全屏障的靜態與動態模型

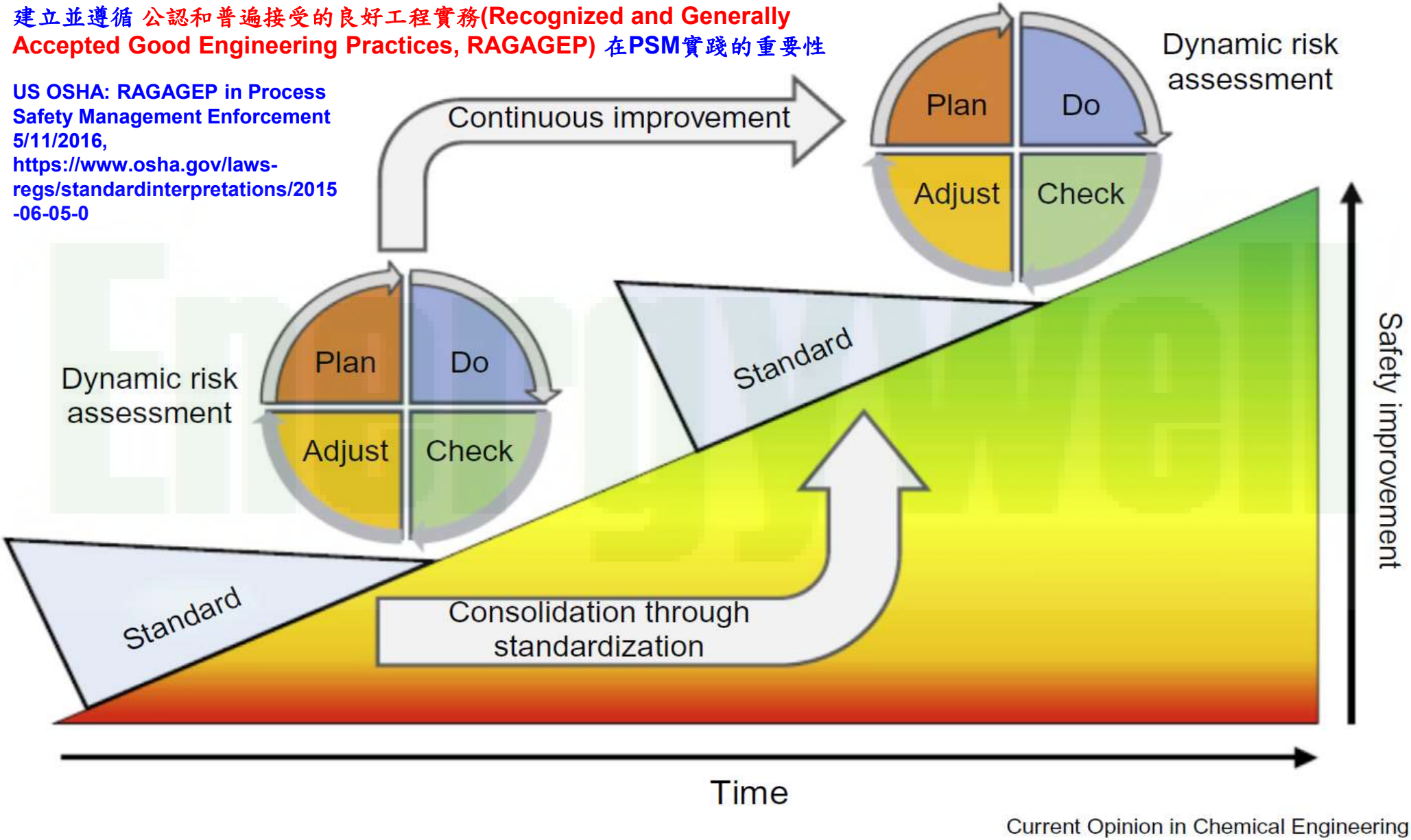


Source: Faisal Khan, Methods in Chemical Process Safety, Volume 1, Academic Press (2017)

經由動態風險管理持續安全改進

建立並遵循 公認和普遍接受的良好工程實務(Recognized and Generally Accepted Good Engineering Practices, RAGAGEP) 在PSM實踐的重要性

US OSHA: RAGAGEP in Process Safety Management Enforcement 5/11/2016, https://www.osha.gov/laws-regs/standardinterpretations/2015-06-05-0



Current Opinion in Chemical Engineering

Source: Faisal Khan, Methods in Chemical Process Safety, Volume 1, Academic Press (2017)

講題三

製程安全管理的危害控制分析簡介

US OSHA PSM實施經驗回饋

- 1992 US OSHA PSM標準
- 1998 US EPA 風險管理計畫(Risk Management Plan, RMP)規則
- 2001 美國化學理事會(American Chemistry Council, ACC)責任照顧管理系統(Responsible Care Management System, RCMS)和RC-14000
- 2005 德克薩斯城煉油廠爆炸
  - 2007 BP貝克小組的報告(Baker Panel Report)
- 2007-2012一些行業倡議涉及貝克小組的經驗回饋
  - CCPS基於風險的製程安全指南
  - API RP 和API RP 752 Rev 3 臨時建築物的設施選址
  - CCPS和API RP 754製程安全績效指標(PSPI)
  - API RP 755疲勞管理
- 2007-2010 US OSHA煉油行業PSM國家重點計畫(National Emphasis Program, NEP)指令
  - 2010 馬康多深水地平線(Macondo Deepwater Horizon)鑽油平台漏油事件、進行化學品行業NEP
- 2013 行政命令(Executive Order, EO) 13650 - 提高化學設施的安全和保安(資安)
  - 2014 加州煉油廠安全報告、 DIR (Department of Industrial Relations)和CalARP (Accidental Release Prevention, ARP)草案規則變更
  - 2014 US OSHA PSM意見徵詢(Request for Information, RFI) and EPA RMP RFI
- 2017加州法規、標題8、第5189.1節煉油廠的製程安全管理(Process Safety Management for Petroleum Refineries)

CalPSM-R 2017強調 ...

- 加州特別強調，且獨立出來的PSM要素項目，亦即是US OSHA執行PSM檢查發現的主要缺失項目或相對較差的項目
  - 損傷(壞)機制審查(Damage Mechanism Review, DMR)
  - 危害控制分析(Hazard Control Analysis, HCA)的層次結構
    - 指定應有層次結構的分析與管理，適用強制性的RAGAGEP
  - 人為因素(Human Factor, HF)
  - 組織變更管理(Manage of Organization Change, MOOC)
  - 製程安全文化評估(Process Safety Culture Assessment, PSCA)
  - 製程安全管理計畫(Process Safety Management Program, PSMP)
  - 事故調查(Incident Investigation, II)
    - 指定根本原因分析(Root Cause Analysis, RCA)，適用強制性的RAGAGEP，IEC 62740:2015是可引用的RAGAGEP
- 以上項目內涵亦包括在US OSHA PSM標準，因此在CalPSM-R:2017的規定之下，相關PSM要素項目的執行是「強制性的」，並且引用RAGAGEP規定也是「強制性的」

CalPSM-R PHA應(Shall)解決…

- 該製程的危害
- 以前公開紀錄的石油煉製和石化工業部門與該製程有關的重大事故
- 製程單元適用的DMR報告
- 製程單元適用的HCA報告
- 製程設備故障的潛在後果
- 設施選址，包括製程、設備、建築物、員工佔用和工作站的安置，以有效保護員工免受製程安全危害
- 人為因素HF報告
- 對製程或製程設備故障可能導致的可能事故的類型、嚴重程度和可能性進行定性評估
- 外部事件的潛在影響，如果適用，包括地震事件
- 與該製程有關的事故調查結果
- 審查自上次製程危害分析(Process Hazard Analysis, PHA)以來適用的變更管理(Management of Change, MOC)文件完成狀況

CalPSM-R PHA製程/製程設備的定義

- 製程
  - 煉油廠的活動，包括使用、儲存、製造、處理、管線或現場移動，涉及高度危險的原物料
  - 如果發生故失效或故障，可能會導致重大事故，公用設施和製程設備應被視為製程的一部分
  - 任何相互連接的塔槽或單獨的塔槽，其位置假若會因為一個塔槽的事故而影響到任何其他的塔槽，則應視為單一製程
    - 此定義包括部分或非計畫停機的製程
    - 此定義不包括輔助管理和支援功能，包括辦公大樓、實驗室、倉庫、維修站和更衣室
- 製程設備
  - 與製程相關的設備，包括壓力容器、旋轉設備、管線、儀錶、製程控制或附屬設備

CalPSM-R PHA操作步驟/模式應包括

- 啟動(開機)
- 正常運轉
- 根據需要進行的臨時行動(譬如故障排除或維修活動)
- 緊急停機，包括
  - 需要緊急停機的條件
  - 規定合格操作人員有權部分或完全停止操作或關閉製程
  - 將責任分配給合格的操作人員

    以確保安全及時地執行緊急停機
- 正常關機
- 調度後、計畫內或計劃外停機或緊急停機後的啟動
- 前述各項操作步驟/程序，亦應納入PSM操作程序要素項目中

CalPSM-R HCA應…

- 雇主應對既有製程執行獨立的HCA
  - 對於既有製程的HCA，分析團隊應在進行HCA時審核PHA
  - 既有製程的HCA應依據以下時間表執行，並可與PHA時間表一起執行:
    - 在CalPSM-R 5189.1節生效之日起三(3)年內，至少完成既有製程的50%
    - 在CalPSM-R 5189.1節生效之日起五(5)年內，完成剩餘製程
    - 既有製程的所有HCA應至少每五(5)年更新一次，並作為獨立分析重新驗證，並可與PHA計畫一起執行

CalPSM-R HCA應…

- 雇主還應如下及時進行HCA:
  - PHA團隊針對每種情境提出的所有建議，以確定重大事故的可能性
  - 對重大事件的調查產生的所有建議
  - 無論何時提出重大變更，皆為MOC審查的一部分
  - 在設計和審查新製程、新製程單元和新設施及其相關製程設備的過程中

CalPSM-R HCA應…

- HCA應由具有工程和製程操作專業知識的團隊進行紀錄、執行、更新和重新驗證
  - 該團隊應包括一名熟悉HCA方法的成員和至少一名目前正在進行該製程的操作員工，並具有特定於所評估製程的專業知識和經驗
  - 雇主應規定員工參與(寫明於PSM員工參與要素項目)
  - 必要時，團隊應與具有損傷機制、製程化學和控制系統專業知識的人員進行協商

CalPSM-R HCA應…

- HCA團隊應
  - 編制或開發每個製程或建議的所有風險相關數據
  - 識別、表徵每個製程安全危害所帶來的風險並確定其優先級
  - 按照以下順序和優先順序，從最優先考慮到最不優先考慮，識別、分析和紀錄每個製程安全危害的所有固有安全措施和保障措施:
    - 第一優先: 本質安全措施 (例如: 去除/消除)
    - 第二優先: 本質安全措施 (例如: 減量/替代)
    - 被動保障措施
    - 主動保障措施
    - 程序性保障措施
  - 就CalPSM-R 5189.1節而言，第一優先本質安全措施被認為是最有效的，而程序性保障措施被認為是最不有效的

CalPSM-R HCA應…

- HCA團隊應
  - 識別、分析和紀錄有關本質安全措施和保障措施的相關公開資訊
  - 該資運應包括本質安全措施和保障措施
    - 石油煉製業及相關工業部門在實務中取得的成果
    - 由石油加工業和相關工業部門、聯邦或州機構或當地州(加州)機構在法規或報告中要求或推薦的
  - 對於每個製程安全危害，應按以下順序和優先順序制定書面建議
    - 使用第一優先本質安全措施盡可能消除危害
    - 使用第二優先本質安全措施，盡可能減少任何剩餘危害
    - 使用被動保障措施有效降低剩餘風險
    - 使用主動保障措施有效降低剩餘風險
    - 使用程序性保障措施有效降低剩餘風險

CalPSM-R HCA應…

- HCA團隊應在製定建議的90個日曆天內完成HCA報告
- HCA報告應包括
  - 團隊的組成、經驗和專業知識的描述
  - 團隊使用的HCA方法的描述
  - 團隊分析的每個製程安全危害的描述
  - 團隊分析的本質安全措施和保障措施的描述
  - 團隊為每個製程安全危害建議的本質安全措施和保障措施的理由
- 雇主應實施所有建議
- 雇主應保留每個製程的所有HCA報告

CalPSM-R PHA/HCA的保障保護分析

- 保障保護分析(Safeguard Protection Analysis, SPA)
  - 目標
    - 評估現有保障措施對PHA中確定的每種故障情境的有效性
    - 確保保護措施彼此間獨立於起始事件(獨立保護層(Independent Protection Layers, IPLs))
  - 必須針對可能發生重大事故的每個PHA情境執行此操作
  - 必須使用定量或半定量方法(例如保護層分析(Layer of Protection Analysis, LOPA))
  - 必須在PHA的6個月內完成
  - 必須由經驗豐富、知識淵博的團隊進行
  - SPA應附在PHA報告之後
  - 必須遵循矯正措施的工作流程
  - 必須在整個製程的生命週期內維護SPA文檔

HCA/SPA的RAGAGEP

- SPA
  - LOPA
    - IEC 61511:2016
    - AIChE CCPS:2015 - Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis
- SPA/HCA
  - AIChE CCPS:2018 Bow Ties in Risk Management: A Concept Book for Process Safety
- HCA/SPA的重要性和精髓在於
  - 保證與製程安全有關的每個重大事故危害的各項保障保護措施的設計正確、有效，且持續維持有效與保持更新，以免除製程安全重大事故的發生

屏障(Barrier)管理

- 屏障
  - 旨在防止意外事件發生或防止事件升級為有害後果的事件的風險控制
  - 技術、操作和組織要素，單獨或共同用於減少發生特定錯誤、危害或事故的可能性、或限制其危害/壞處
  - 屏障係指為明確的目的而制定的措施
    - 防止實現危害
    - 減輕危害事件的影響
  - 計畫採取措施重新獲得控制，減輕危害和事故情境的發展或減輕後果
    - 屏障除了本質安全和控制措施之外，還可以防止故障和失控
    - 包括重新獲得控制的偵測措施

屏障(Barrier)管理

- 屏障管理
  - 協調活動，以建立和維持屏障，使它們始終保持其功能
- 屏障功能
  - 障礙的任務或作用，例如
    - 防止洩漏或點火
    - 減少火災負荷
    - 確保可接受的疏散
    - 防止聽力損傷

屏障(Barrier)管理

- 預防化學物質洩漏的屏障功能結構層次舉例
  - 屏障子功能
    - 在正常操作期間防止洩漏
    - 防止因技術降級導致的洩漏
    - 防止因製程偏離導致的洩漏
    - 在維護期間防止洩漏

屏障(Barrier)管理

- 預防化學物質洩漏的屏障功能結構層次舉例
  - 屏障子功能
    - 防止因製程偏離導致的洩漏
  - 屏障子-子功能
    - 防止設備堵塞
    - 防止高液位
    - 防止過(高)壓
    - 防止高溫
    - 防止氣竄

屏障(Barrier)管理

- 預防化學物質洩漏的屏障功能結構層次舉例
  - 屏障子-子功能
    - 防止設備堵塞
  - 安全功能/安全儀錶功能(SIF)/安全關鍵任務
    - 確保製程最低溫度
  - 相關安全功能屏障要素/元件項目的實現

屏障(Barrier)管理

- 預防化學物質洩漏的屏障功能結構層次舉例
  - 屏障子-子功能
    - 防止設備堵塞
  - 安全功能/安全儀錶功能(SIF)/安全關鍵任務
    - 從CCR中注入甲醇
    - 從現場注入甲醇
  - 相關安全關鍵任務屏障要素/元件項目的實現

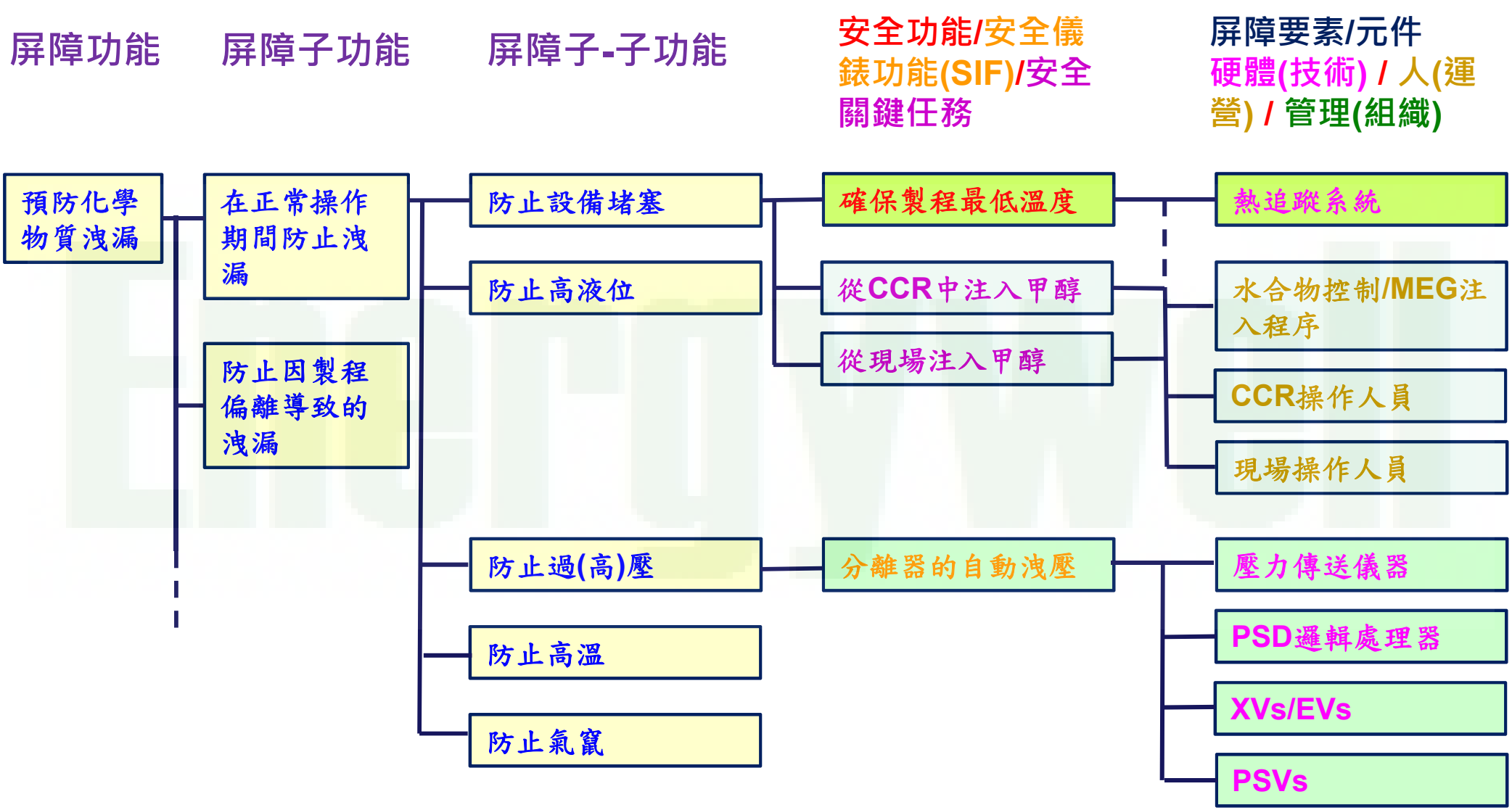
屏障(Barrier)管理

- 預防化學物質洩漏的屏障功能結構層次舉例
  - 屏障子-子功能
    - 防止過(高)壓
  - 安全功能/安全儀錶功能(SIF)/安全關鍵任務
    - 分離器的自動洩壓
  - 相關安全儀錶功能(SIF)屏障要素/元件項目的實現

屏障(Barrier)管理

- 預防化學物質洩漏的屏障功能結構層次舉例
  - 屏障子-子功能
    - 防止氣竄
  - 安全功能/安全儀錶功能(SIF)/安全關鍵任務
    - 防止氣體吹向洗滌器
  - 相關安全儀錶功能(SIF)屏障要素/元件項目的實現

屏障(Barrier)管理



屏障(Barrier)管理

- 屏障要素/元件
  - 技術、運營或組織措施或解決方案，在實現屏障功能方面發揮作用
  - 技術屏障
    - 構成實現屏障功能的一部分的設備和系統，或稱為硬體屏障
    - 設計和管理主要安全殼/圍堵體、製程設備和工程系統，以防止LOPC和其他類型的資產完整性或製程安全事件，並減輕此類事件的任何潛在後果
    - 這些屏障由人員檢查和維護(在關鍵活動/任務中)
  - 運營屏障
    - 依賴於能夠開展旨在防止LOPC和其他類型的資產完整性或製程安全事件，並減輕此類事件的任何潛在後果的活動，或稱為人的屏障
    - 人員必須執行的行動和活動，以構成實現屏障功能的一部分
    - 只有那些必要的程序才能執行操作或活動，才能被視為屏障要素
  - 組織屏障
    - 具有明確的角色或職能和特定能力的人員，構成實現屏障功能的一部分
    - 用於旨在防止LOPC和其他類型的資產完整性或製程安全事件，並減輕此類事件的任何潛在後果的製程分組和實務設計進行分組
    - 或稱為管理系統要素屏障，其支持技術(硬體)和運營(人的)屏障

屏障(Barrier)管理

- 技術屏障/硬體屏障的分類 (舉例)
  - 結構完整性
  - 製程安全殼/圍堵體
  - 點火控制
  - 偵測系統
  - 保護系統 - 包括灑水和消防系統
  - 停機系統 - 包括製程隔離、操作隔離和控制/安全控制設備
  - 緊急應變
  - 救生設備 - 包括疏散系統

屏障(Barrier)管理

- 運營屏障/人的屏障的分類 (舉例)
  - 遵循程序操作，例如
    - 工作許可
    - 隔離設備
    - 凌駕(Override)和遮蔽(Inhibit)安全系統
    - 轉移移交/交接班程序
  - 監督、操作員巡視和例行檢查
  - 臨時和移動設備的授權
  - 接受設施或設備的移交或重啟
  - 響應製程警報和異常情況(例如偏離安全操作範圍)
  - 應對緊急情況

屏障(Barrier)管理

- 組織屏障/管理系統要素屏障的分類 (舉例)
  - 工作許可
  - 變更管理
  - 緊急應變程序
  - 能力/資格管理
  - 承攬商管理
  - 技術完整性
  - 資產/機械完整性
  - 腐蝕管理
  - 設備隔離

屏障(Barrier)管理

- 組織屏障/管理系統要素屏障的分類 (舉例)
  - 四個基石
    - 領導力: 引領潮流、無情地專注於系統
    - 風險管理: 消除負面影響、增強積極因素
    - 持續改進: 始終進行「規劃(P)-執行(D)-查核(C)-行動(A)」
    - 實施: 每次都是且要求第一次就做對

屏障(Barrier)管理

- 組織屏障/管理系統要素屏障的分類 (舉例)
  - 十個重要的要素
    - 承諾和責任
    - 政策、標準和目標
    - 組織、資源和能力
    - 利益相關者和客戶
    - 風險評估和控制
    - 資產設計和完整性
    - 計畫和程序
    - 執行活動
    - 監測、報告和學習
    - 保證、審查和改進
  - 請併同屏障管理納入您的安全管理系統中

屏障(Barrier)管理

- 績效影響因子(Performance Influencing Factor, PIF)
  - 對屏障功能和要素/元件按預期能力執行有重要意義的條件
- 績效塑造因子(Performance Shaping Factor, PSF)
  - 人員、工作場所或其他背景因素，對操作人員或現場操作人員績效產生重大影響

典型重大事故危害相關的屏障功能

- 碳氫化合物(HC)洩漏
  - 防止從製程設備洩漏HC
  - 防止從立管/管線/管道洩漏HC
  - 防止貨物/污油箱洩漏HC
  - 防止在卸載操作期間洩漏HC
  - 限制從製程設備洩漏HC的大小
  - 限制從立管/管線/管道洩漏HC的大小
  - 限制貨物/污油箱洩漏HC的大小
  - 限制卸載軟管洩漏HC的大小

典型重大事故危害相關的屏障功能

- 火災和爆炸
  - 防止點火
  - 防止貨物/污水箱中的爆炸性或危險氣體
  - 防止壓載艙中的碳氫化合物
  - 防止升級到其他設備
  - 防止升級到其他區域
  - 防止逃生/集合期間的死亡事故
  - 在疏散期間防止死亡

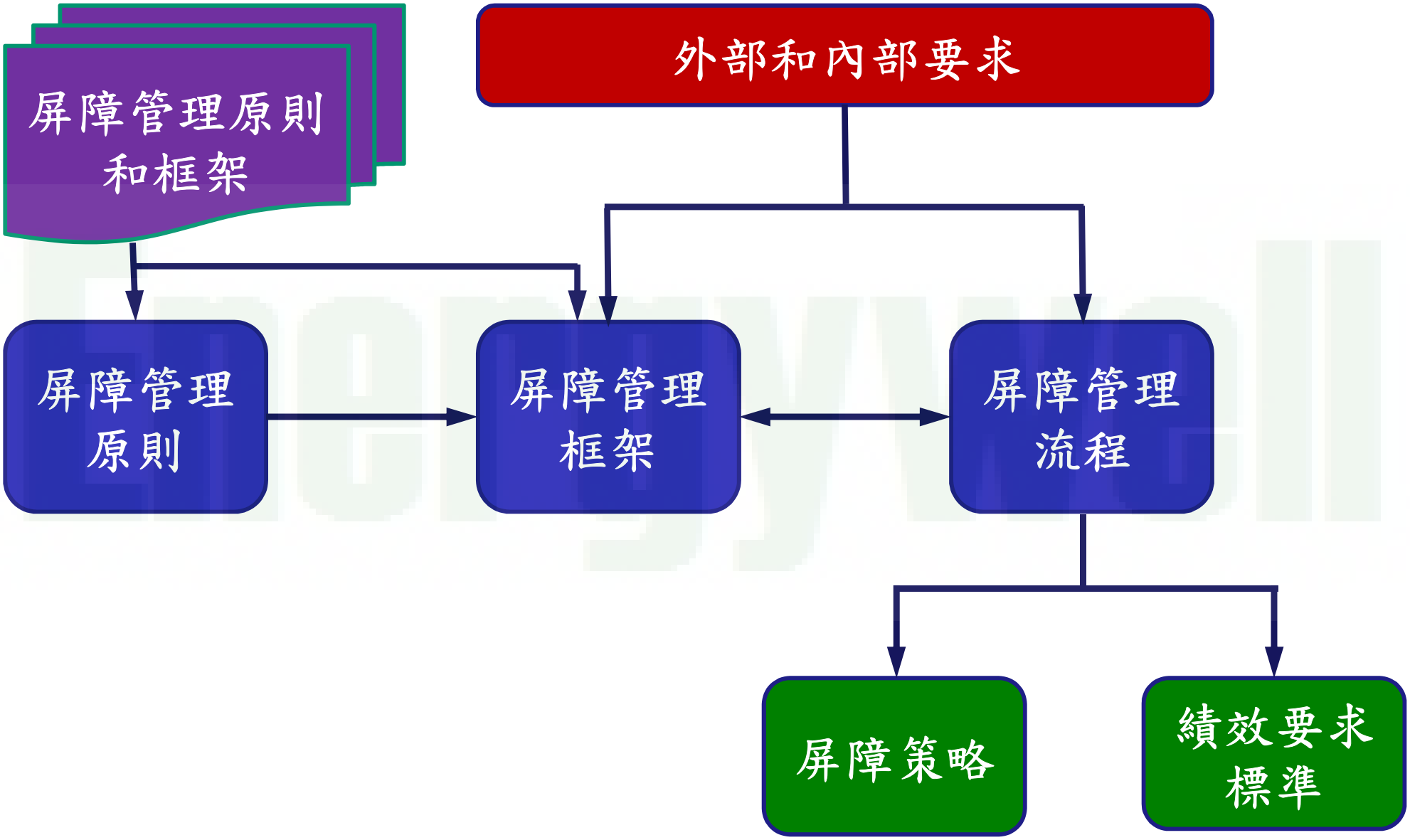
典型重大事故危害相關的屏障功能

- 急性污染
  - 防止洩漏到海上/河川/湖
  - 限制洩漏到海上/河川/湖的後果
  - 防止洩漏到製程區/儲槽區的堤/堰外
  - 限制洩漏到製程區/儲槽區的堤/堰外的後果
- 掉落的物體
  - 防止起重機操作中掉落的物體
  - 在掉落物體的情況下限制後果

典型重大事故危害相關的屏障功能

- 在搬運路線上碰撞/障礙物/物體
  - 防止與通過或公務/工務車輛發生碰撞
- 極端天氣
  - 確保在極端天氣預報的情況下的應變措施
- 結構失效
  - 防止結構完整性的喪失
  - 在結構完整性喪失後防止死亡事件
- 非碳氫化合物火災
  - 防止非HC火災
  - 限制非HC火災造成的後果

屏障管理概述



生命週期中的屏障管理活動

早期設計階段	細部設計階段	操作/維護/營運階段
準備並建立屏障管理計畫	更新屏障管理計畫	準備計畫以確保屏障績效(必要時更新)
定義區域	驗證區域	審查區域定義
執行或審查危害辨識	審查細化的危害辨識	更新危害辨識(例如在修改期間)
辨識/定義重大危害/定義危害和事故的情況(DSHA)	修改DSHA	審查並更新風險分析和DSHA
執行屏障分析	細化屏障分析	更新屏障分析
建立初始屏障策略	細化屏障策略	審查和更新屏障策略
建立初始績效標準	細化績效標準	審查和更新績效標準
	建立監測屏障狀態的系統(例如屏障面板)	監控屏障狀態並考慮補償措施的需要
	建立追踪屏障績效的系統和流程	監控並驗證屏障績效

DSHA:定義危害和事故的情況 (Defined Situations of Hazard and Accident)

屏障管理流程的主要步驟

- 制定屏障策略和相應績效標準的主要步驟包括
  - 設施描述和區域劃分
  - 確定每個區域的危害和事故的情況(DSHA)和屏障功能(基於風險圖)
  - 每個區域(或全域)的屏障要素/元件項目
  - 績效要求
  - 績效影響因子(PIF)
  - 驗證績效要求的活動(和時間間隔)

屏障績效要求的類型

- 功能性
  - 容量
  - 效用
  - 預計屏障將發揮的基本任務(具有一定的能力/效力)
- 完整性(可靠性/可用性)
  - 可靠性
  - 可用性
  - 完整性
- 屏障能夠在需要時及時出現(存在)
  - 生存能力(脆弱性)
  - 負載阻抗能力
  - 穩健性
  - 屏障在相關事故情境和負荷下發揮作用的能力
- 以上皆宜被定性、半定量、或定量指定至每一個屏障要素/元件項目，且宜予以分級並加以管理

運營和組織的屏障KPIs舉例

風險控制系統	滯後KPI示例	領先KPI示例
檢查/維修	失控事件的數量	在測試時按規格執行的安全關鍵製程(工場)/設備的百分比 維護計畫按時完成的百分比，在運行期間或停機期間發現的製程洩漏數量
員工能力	失控事故的數量、工廠跳俥、設備損壞等與正確行動的理解、知識或經驗不足有關	符合現地評估能力標準的人員百分比(包括主管/經理) 在任命新職位後獲得完全勝任所需的平均時間
操作程序	由於程序不正確/不清楚導致的操作錯誤數	與計畫比較，審查和更新的程序百分比
儀錶和警報	與儀錶或警報故障相關的事件數	按時完成的警報/跳俥功能測試的百分比
工廠變更管理	與MOC失敗相關的事件數量	在安裝前適當地工廠變更風險評估和批准被完成的百分比 一旦批准，用於完成實施變更的平均時間

運營和組織的屏障KPIs舉例

風險控制系統	滯後KPI示例	領先KPI示例
工作許可 (Permit To Work, PTW)	PTW流程中的錯誤被確定為促成事件因素的數量	對PTW進行抽樣，確定所有危害皆被辨識和所有的適當控制措施皆已採行的百分比 並指定所有合適的對照的情況下 對PTW進行抽樣，查核所列出的所有控制措施在工地完全就位的百分比
工廠設計	將工廠設計中的錯誤確定為促成事件因素的數量	因操作需要，啟動後進行修改或變更的次數與適用規範和標準的偏差數量 安全關鍵設備/系統完全符合當前設計規範的百分比
應急安排	在真實緊急情況下，不能完全啟用或發揮作用的緊急應變設備(或要素項目)的數量	過去X個月內參加緊急應變演練人數的百分比 使用相關標準或設施安全案例中定義的時間表測試ESD閥門和製程跳俥的百分比

屏障或降級控制管理流程圖

1.辨識屏障

2.確認所辨識的屏障是否為SCE (選項)

3.紀錄每個屏障的績效標準

4.記錄測試每個屏障功能的方法

5.建立基線監測間隔

6.實施監測計畫並直接確定屏障績效

7.收集屏障績效的其他間接指標

8.實施維護或能力策略
以恢復屏障其原始的狀況，或用等效的新屏障取代原屏障

9.確保MOC審查解決屏障的影響

10.確保定期PSM審查解決屏障的影響

Energywell

感謝您的聆聽!!