醫療軟體確效法規與實務

呂柏翰

資深工程師

功能安全團隊 / 可靠度實驗室

SGS Taiwan

WHEN YOU NEED TO BE SURE

SGS

自我介紹

呂　柏　翰　　Master of Automation and Control

Functional Safety & Automotive Electronics services/ SGS Taiwan

2008 – 2012 **Master of Science, Graduate Institute of Automation and Control**
National Taiwan University of Science and Technology
- Publication - An Autonomous Home Care Mobile Robot for Visual Monitor and Navigation System /家庭照護自主式移動機器人之視覺監控及導航系統

2010 **Visiting scholar, Department of Mechanical Engineering,**
The University of British Columbia, Canada
- Collaborated research on the "Home Care Robots" project under, Fellow Royal Society of Canada, Dr. Clarence de Silva' s supervision.

2015 - 2017 **Sr. Engineer, SGS Taiwan**
- 2006/42/EC Machinery Directive, Annex I – Essential Health and Safety Requirements
- ISO 12100, ISO 14121-2 -- Risk assessment for machinery & instruments for lab use
- IEC 60204-1 -- Safety of machinery
- ISO 13849-1, ISO 13849-2 – Safety-related part of control system
- EN 13060 – Small steam sterilizers
- IEC 62304 – medical device – software life cycle processes
- IEC 60335-1 Annex R, IEC 60730-1 Annex H

Qualifications

Automotive Functional Safety Professional AFSP by SGS-TÜV Saar

ISO/IEC 17025:2017 Supervisor qualification by TAF

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

功能安全之簡介

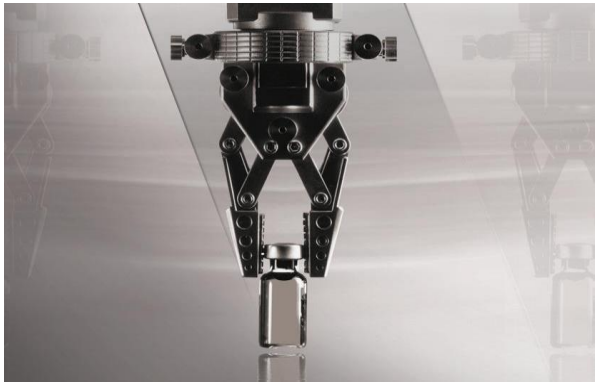
Transportation

Aerospace & Defense

Power / Energy

Medical

Process Automation



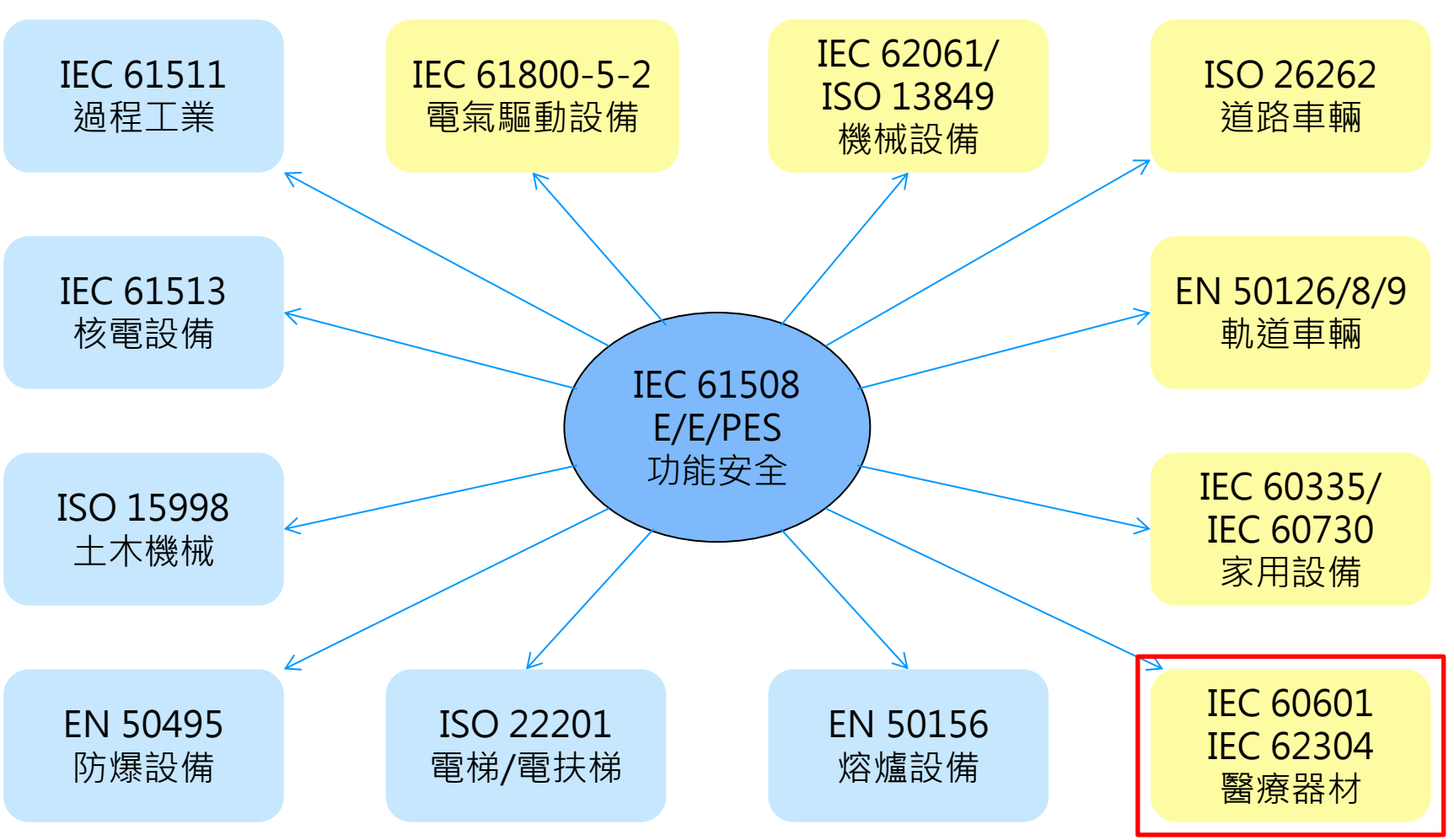
Control Automation

From Wind River material: **Hypervisor an Off-the-Shelf Based Separation Concept to Improve Time-to-Revenue Medical**

功能安全之簡介

- 什麼是功能安全 (Functional Safety)
  - 必須在正常條件或存在故障條件下，控制設備或是系統在**執行功能**時，其**安全功能(safety function)**必須要能夠被保證，即系統保持在安全狀態 (safe state)
  - 避免系統失效會導致
    - 人的傷害或死亡
    - 環境的污染
    - 設備及財產的損失

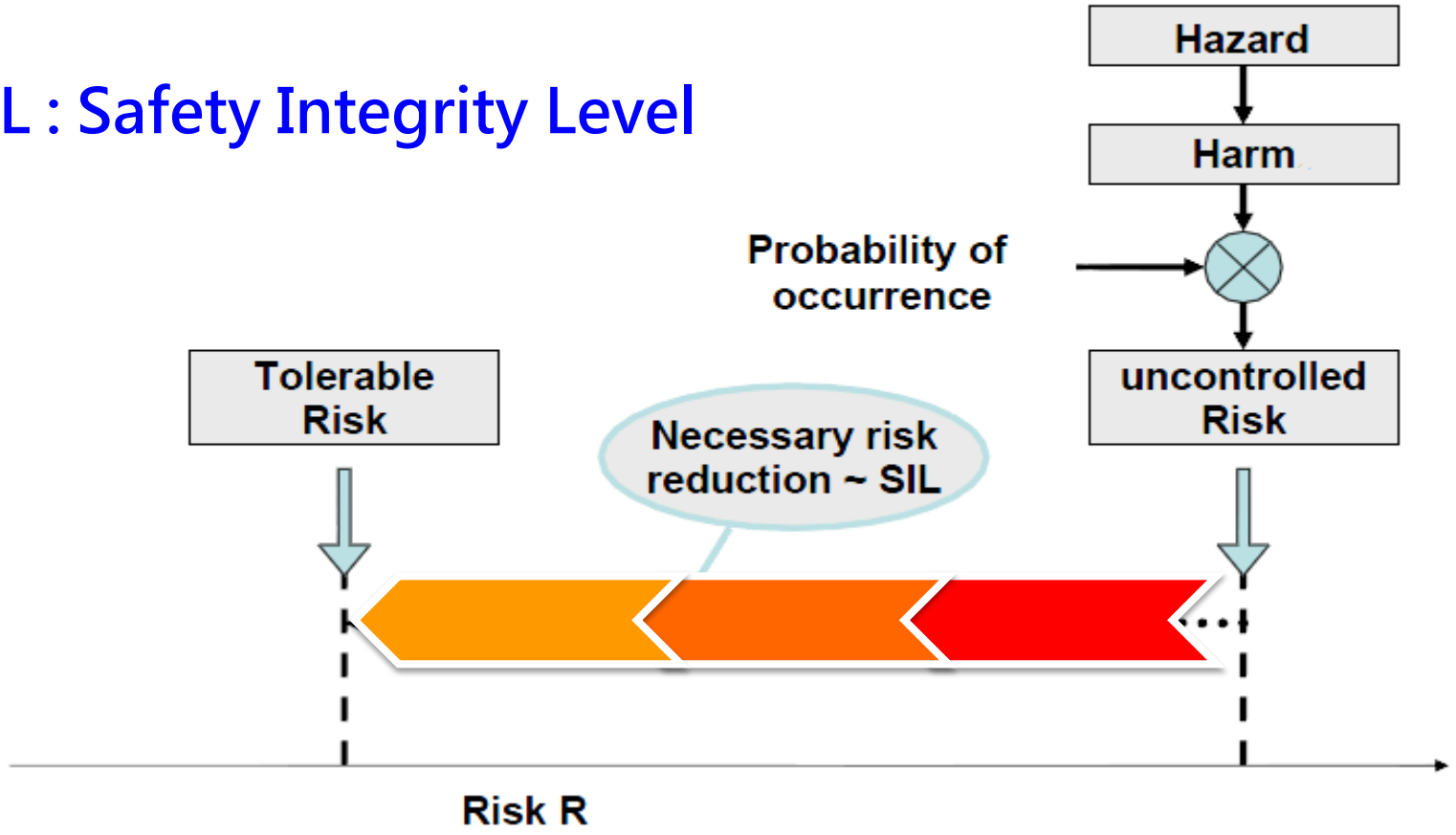
功能安全相關領域


IEC 61511
過程工業
IEC 61800-5-2
電氣驅動設備
IEC 62061/
ISO 13849
機械設備
ISO 26262
道路車輛
IEC 61513
核電設備
EN 50126/8/9
軌道車輛
IEC 61508
E/E/PES
功能安全
ISO 15998
土木機械
IEC 60335/
IEC 60730
家用設備
EN 50495
防爆設備
ISO 22201
電梯/電扶梯
EN 50156
熔爐設備
IEC 60601
IEC 62304
醫療器材

安全完整性等級

IEC 61508 is based on the concept of risk reduction

SIL : Safety Integrity Level



功能安全標準之安全等級

IEC 61508 (Industrial)

SIL Level 1 to 4

ISO/DIS 26262 (Automotive)

ASIL A to ASIL D

IEC 62304 (Medical)

Class A to Class C

CENELEC EN 50128 (Railway)

SIL Level 0 to SIL Level 4

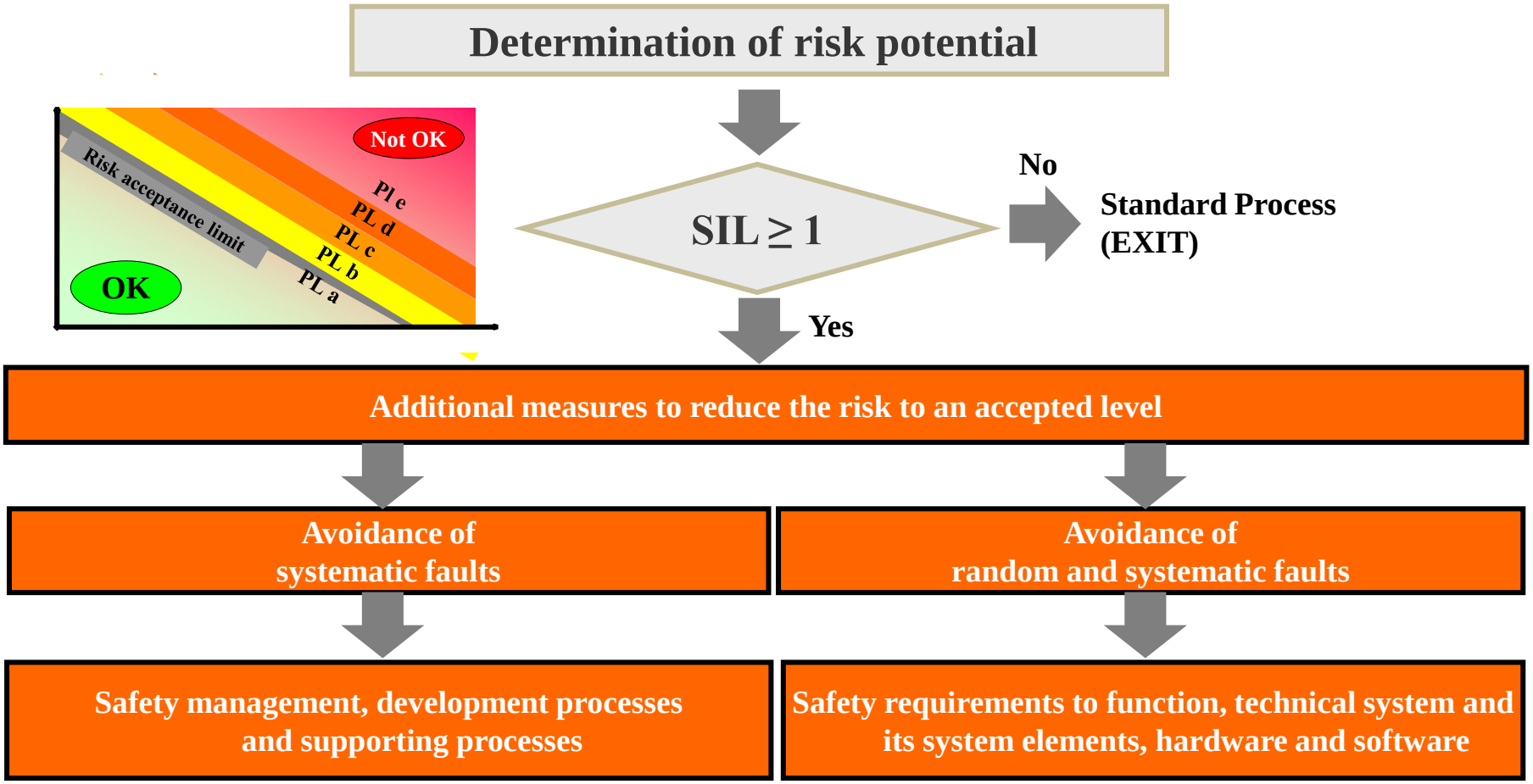
DO-178B / DO-178C (Avionics)

Level E to Level A

功能安全系統故障

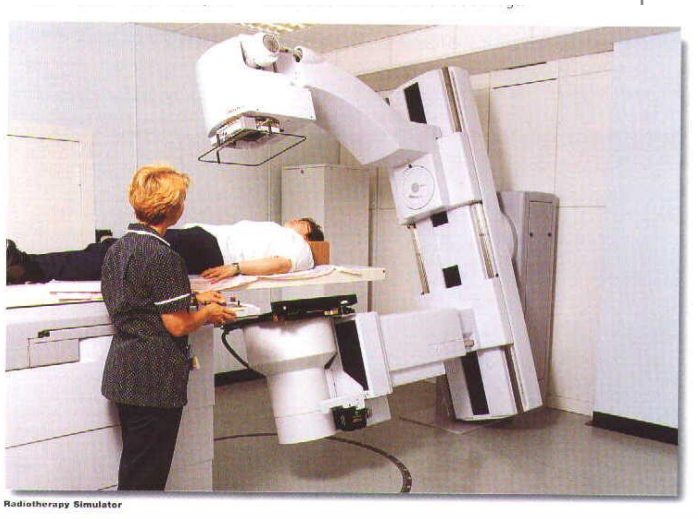
- 什麼是故障
  - 系統故障(Systematic Fault)
    - 硬體設計不良
    - 軟體bug
    - 可透過設計或製造過程，文件審查或其他因素來排除
  - 隨機故障(Radom Fault)
    - 只會出現在硬體中
    - 機械損傷 (不小心摔到導致感測器損傷)
    - 硬體零部件老化，製程瑕疵
    - 必須採取檢測和控制隨機故障的措施

「標準」使用之流程


Determination of risk potential
Not OK
Risk acceptance limit
OK
PL e
PL d
PL c
PL b
PL a
SIL ≥ 1
No
Standard Process
(EXIT)
Yes
Additional measures to reduce the risk to an accepted level
Avoidance of
systematic faults
Avoidance of
random and systematic faults
Safety management, development processes
and supporting processes
Safety requirements to function, technical system and
its system elements, hardware and software

軟體功能安全相關之系統性失效

- 開發人員能力不足導致不良的安全設計
- 測試人員不足的測試與除錯
- 使用之開發工具本身存在臭蟲
- 軟體版本之控管與軟體發行程序之缺失
- 設計變更流程與問題解決流程未正確地落實
- 不周全的事故報告與追蹤研究


Radiotherapy Simulator

未被發現的問題, 將會導致大災難

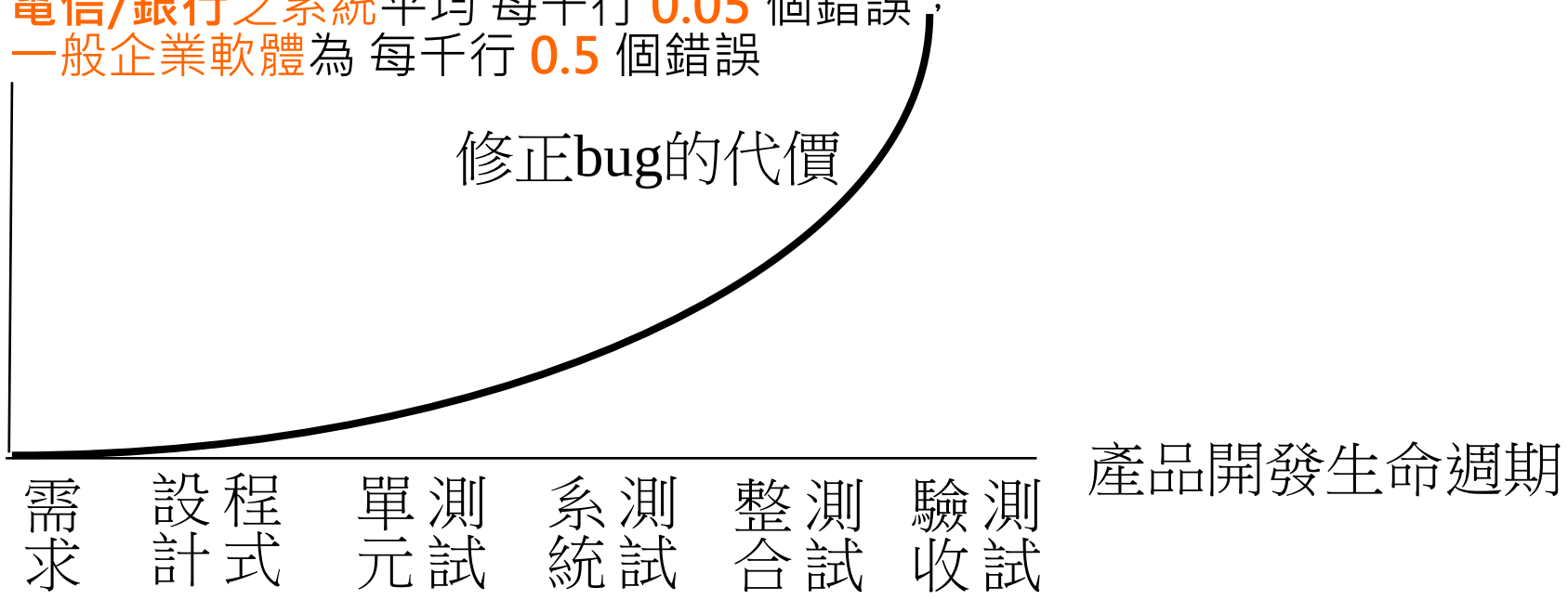
軟體功能安全相當重要

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

關於軟體測試

- 依據過去經驗每千行程式碼大約有 **60個缺陷**，
  2/3缺陷在需求與設計階段，在這個階段發現問題的修正費用最少，
  如果到系統測試才發現，要花 **10倍** 以上經費，
  若到產品驗收時期，則需花費 **100倍** 以上
- **美國國防部**要求 每千行 **0.01** 以下的錯誤，
  電信/銀行之系統平均 每千行 **0.05** 個錯誤，
  一般企業軟體為 每千行 **0.5** 個錯誤



軟體測試的迷思

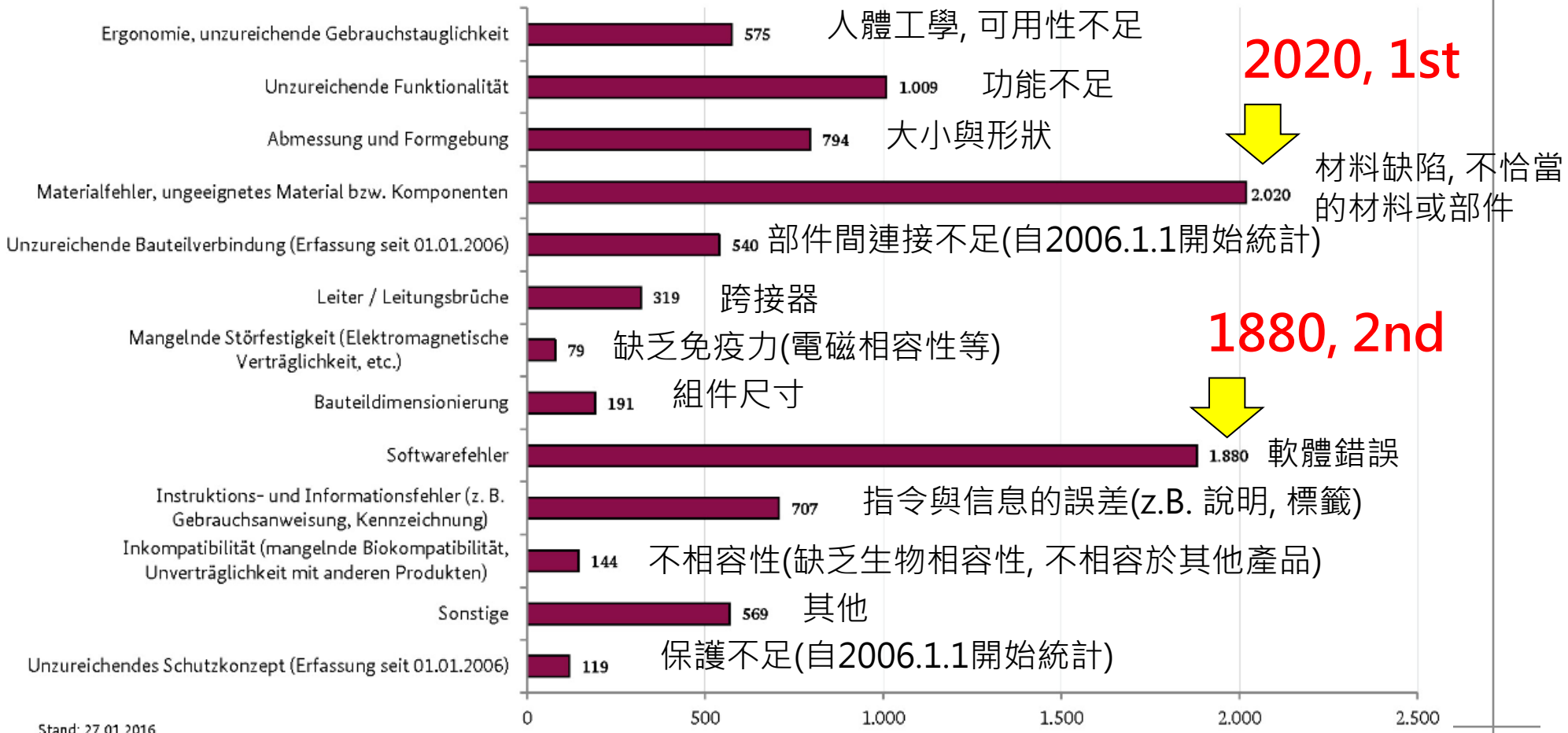
- 由於大多數企業缺乏軟體測試與實踐之知識，所以對軟體測試工作容易有以下幾點誤解
  - 軟體品質有問題，全部是軟體工程師的錯
  - 文件化過程太浪費時間，口頭說說就好
  - 軟體測試技術要求不高，隨便找一個人就能做
  - 等到產品開發最後階段才進行測試

醫療器材錯誤原因通報統計: 設計錯誤/缺陷
Data from Federal Institute for Drugs and Medical devices

Bundesinstitut für Arzneimittel und Medizinprodukte

Statistische Auswertung der im Zeitraum 01.01.2005 bis 31.12.2015 abschließend bewerteten Risikomeldungen

Fehlerursache: Design- / Konstruktionsfehler



Stand: 27.01.2016
Summe: 8.946

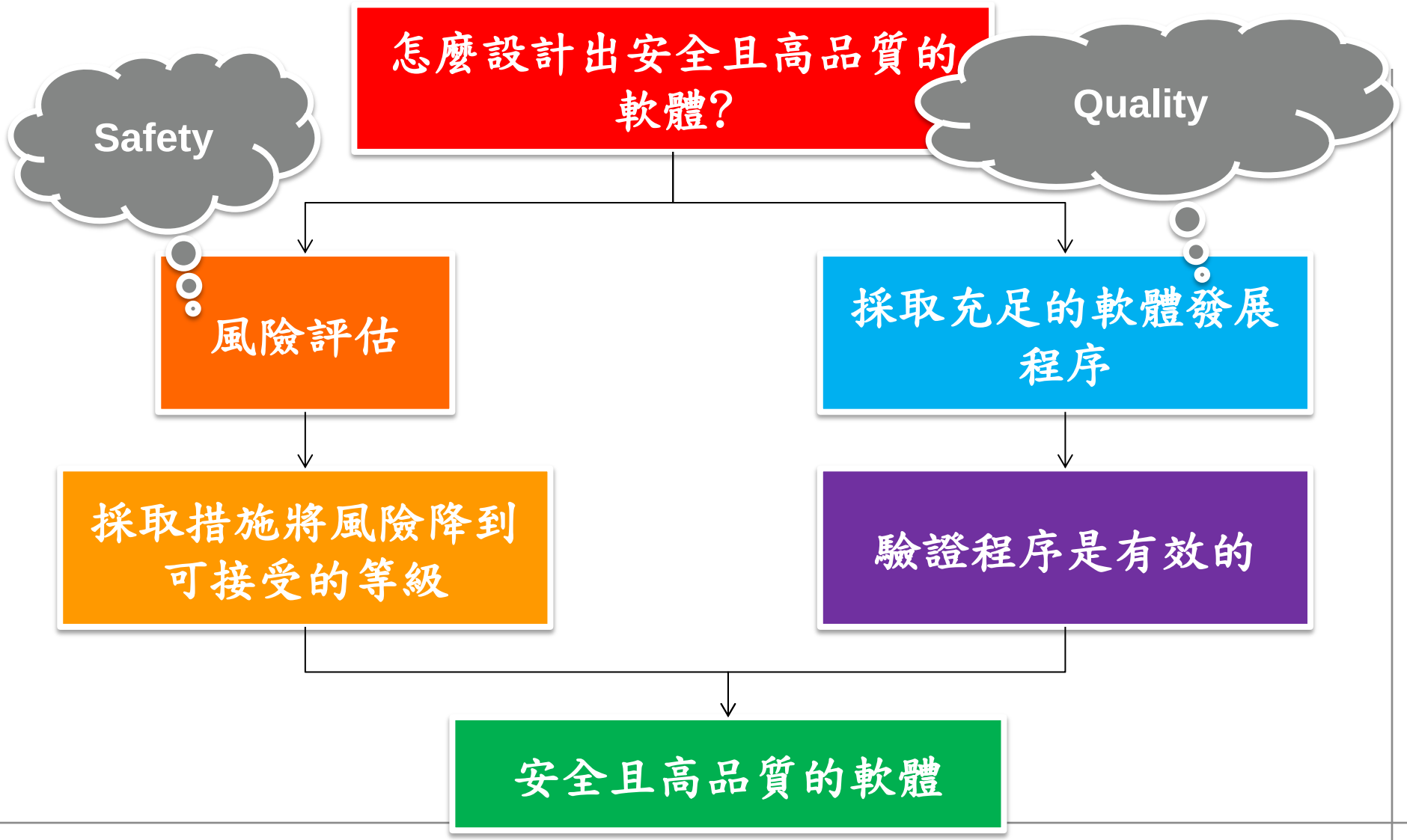
醫材瑕疵	案件數	百分比
材料（Material）	**154**	**60.4%**
出現裂縫（Crack）	120	47.1%
材料分離（Material separation）	29	11.4%
材料穿孔（Material perforation）	2	0.8%
材料降解（Degrade）	1	0.4%
材料破碎（Material Material fragmentation）	1	0.4%
爆裂（Brust）	1	0.4%
機械性質（Mechanical）	**24**	**9.4%**
機構卡住（Mechanical jam）	12	4.7%
醫材或其元件脫落（Detachment of device or device component）	5	2.0%
非預期的動作（Unintended movement）	4	1.6%
洩漏（Leak）	2	0.8%
潰縮問題（Retraction problem）	1	0.4%
非預期的功能（Unintended function）	**20**	**7.8%**
非預期的功能 / 效果（Unintended function）	19	7.5%
黏著或貼合失敗（Failure to adhere or bond）	1	0.4%
啟動、裝置或分離問題（Activation, positioning or separation）	**13**	**5.1%**
醫材或其元件難以裝置達定位（Difficult to position）	12	4.7%
分離（拆卸）失敗（Failure to separate）	1	0.4%
非機械性質（Non-mechanical）	**6**	**2.4%**
光學問題（Optical issue）	4	1.6%
通訊或傳輸異常（Communication or transmission level）	2	0.8%
植入式設備異常（Implantable device failure）	**4**	**1.6%**
醫材或其元件位移（Migration of device or device component）	4	1.6%
相容性問題（Incompatibility）	**3**	**1.2%**
裝置與病人狀況不相容（Patient-device incompatibility）	3	1.2%
外部條件（External conditions）	**1**	**0.4%**
失去動力（Loss of power）	1	0.4%
軟體問題（Computer software）	**1**	**0.4%**
應用程式異常（Application program issue）	1	0.4%
溫控（Temperature）	**1**	**0.4%**
冷卻不足（Insufficient cooling）	1	0.4%
電路問題（Electrical/Electronic）	**1**	**0.4%**
電路故障（Circuit failure）	1	0.4%
其他無代碼可用（Other）	**27**	**10.6%**
無代碼可用（Other）	27	10.6%
總計（Total）	**255**	**100.0%**

資料來源：104 年度國內醫療器材上市後 不良反應通報案例分析, 黃筱茜、魏吟玲、黃薇伊、蔡翠敏, 財團法人藥害救濟基金會, 全國藥物不良反應通報中心

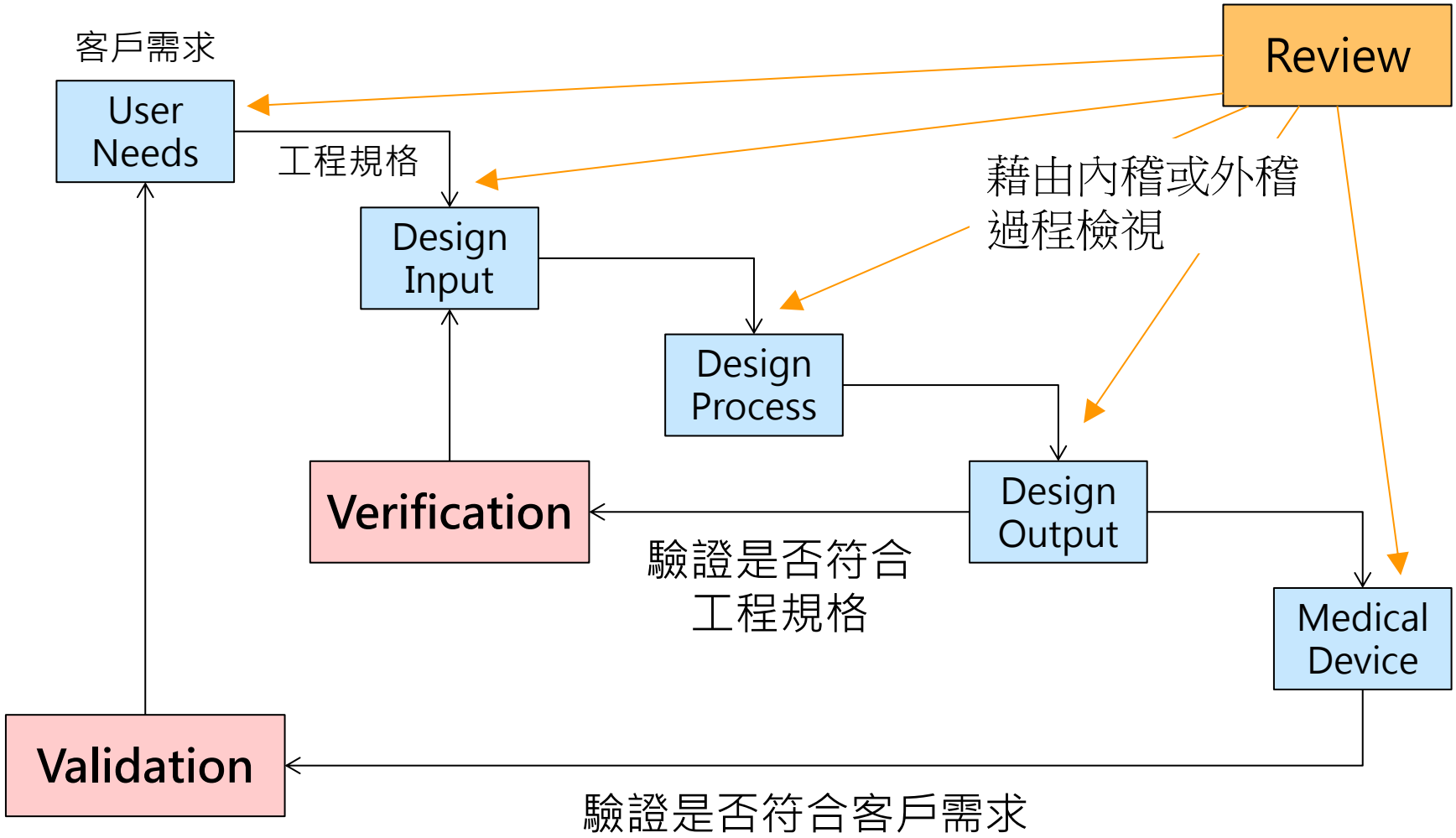
何謂軟體確效

- 軟體確效是透過產品發展生命週期活動來評估軟體產品品質的嚴謹方法
- 確保品質被導入軟體產品之中，並讓軟體滿足所需達到的功能與使用者之需求
- 軟體驗證的工作將包括產品與發展程序之分析、評估、審核、檢視、測試等
- 實務上**軟體工程(Software Engineering)**與**品質管理系統**必須結合

IEC 62304之簡介



範例：軟體之發展生命週期



醫療器材產業現況與常見問題

- 被美國FDA及國外客戶要求提供軟體確效報告，但對如何進行完全沒有概念。
- 管理階層並未體認到落實軟體確效之重要性，故絕大多數業者未建立系統化之管理方式。
- 不清楚軟體開發時應管制哪些技術文件，僅知道最後功能測試O.K!
- 絕大多數之軟體僅進行正常功能之確認測試，甚少探討可預見之異常操作，且測試者通常即為軟體開發人員本身，無法抓出潛在之軟體異常問題(潛在的龐大成本支出)

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

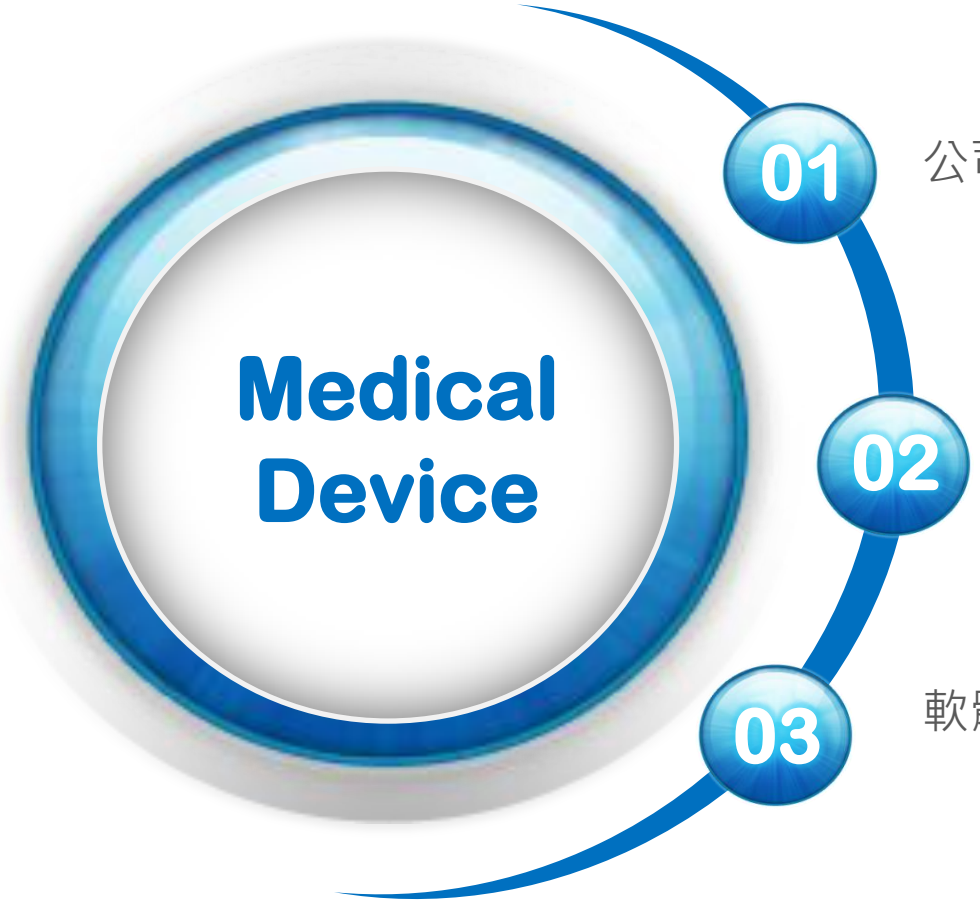
醫療器材相關標準簡介

- 醫療器材之定義
- 醫療產品系統適用規範
- 醫療器材相關法規關聯性
- 醫療器材之產品發展生命週期 (V-Model)
- Verification 驗證 & Validation 確認

醫療器材之定義

- 用於診斷、治療、減輕、直接預防人類疾病、調節生育、或足以影響人類身體結構及機能，且非以藥理、免疫或代謝方法作用於人體，以達成其主要功能之儀器、器械、用具、物質、軟體、體外試劑及其相關物品。
- 疾病之診斷、預防、監控、治療或減緩
- 傷害之診斷、監控、治療、減緩或補償
- 解剖或生理學程式之檢查、取代、修正或支援
- 支援或維持生命
- 妊娠管制
- 醫療器材之消毒
- 以取自於人體之檢體進行體外檢查以供應醫療資訊
- 其作用於人體體表或體內之主要目的並非以藥理學、免疫學或新陳代謝的方式獲得者，但這些方式得以協助其產生作用

醫療產品系統適用規範



公司組織層級:

- ISO 13485 (品質管理系統)

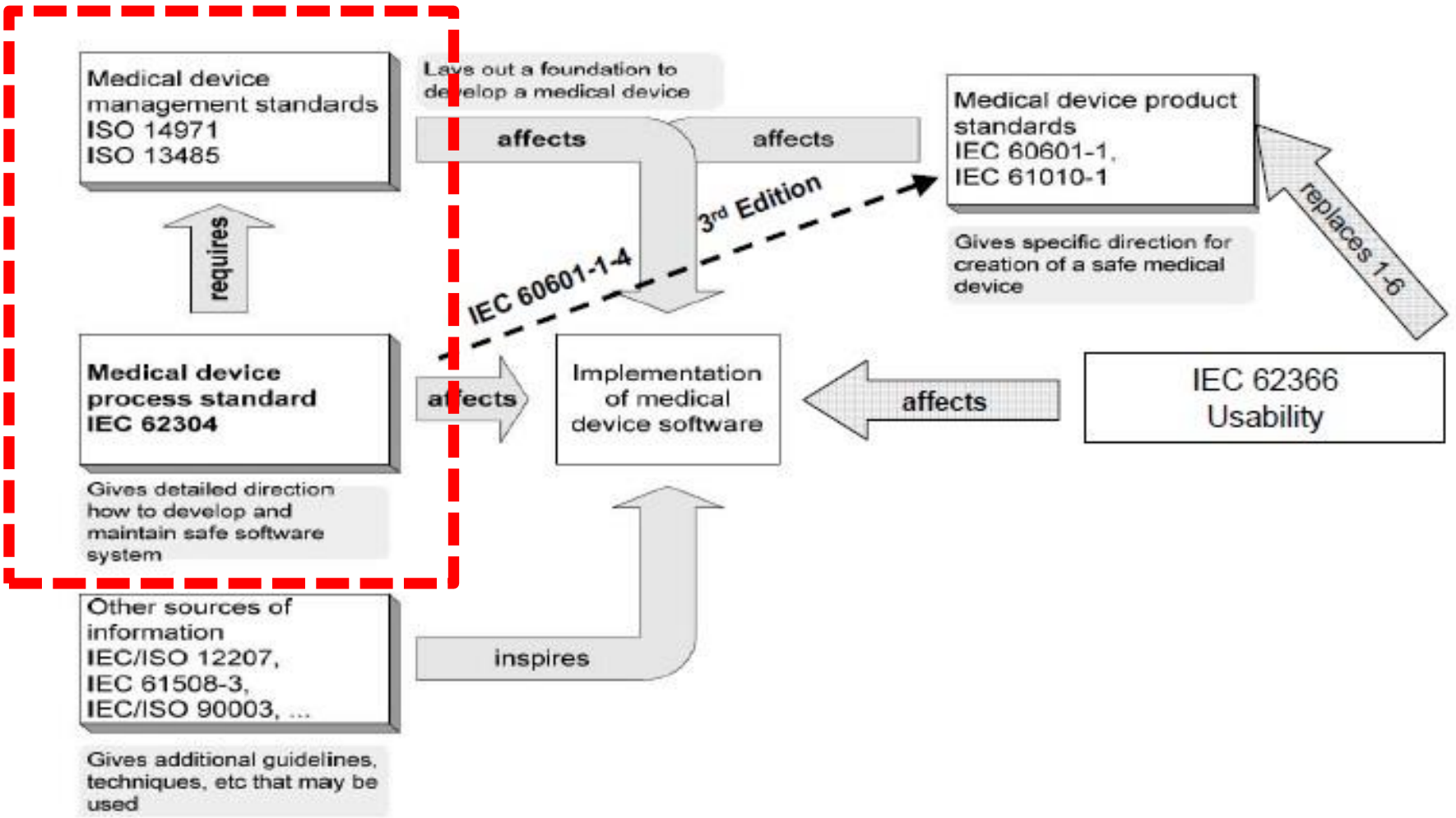
產品層級:

- ISO 14971 (風險管理)
- IEC 60601-1 (安規 & EMC)
- IEC 60601-2-X (產品專用標準)
- IEC 62366-1 (可用性, Usability)

軟體發展層級:

- IEC 62304 (軟體生命週期)

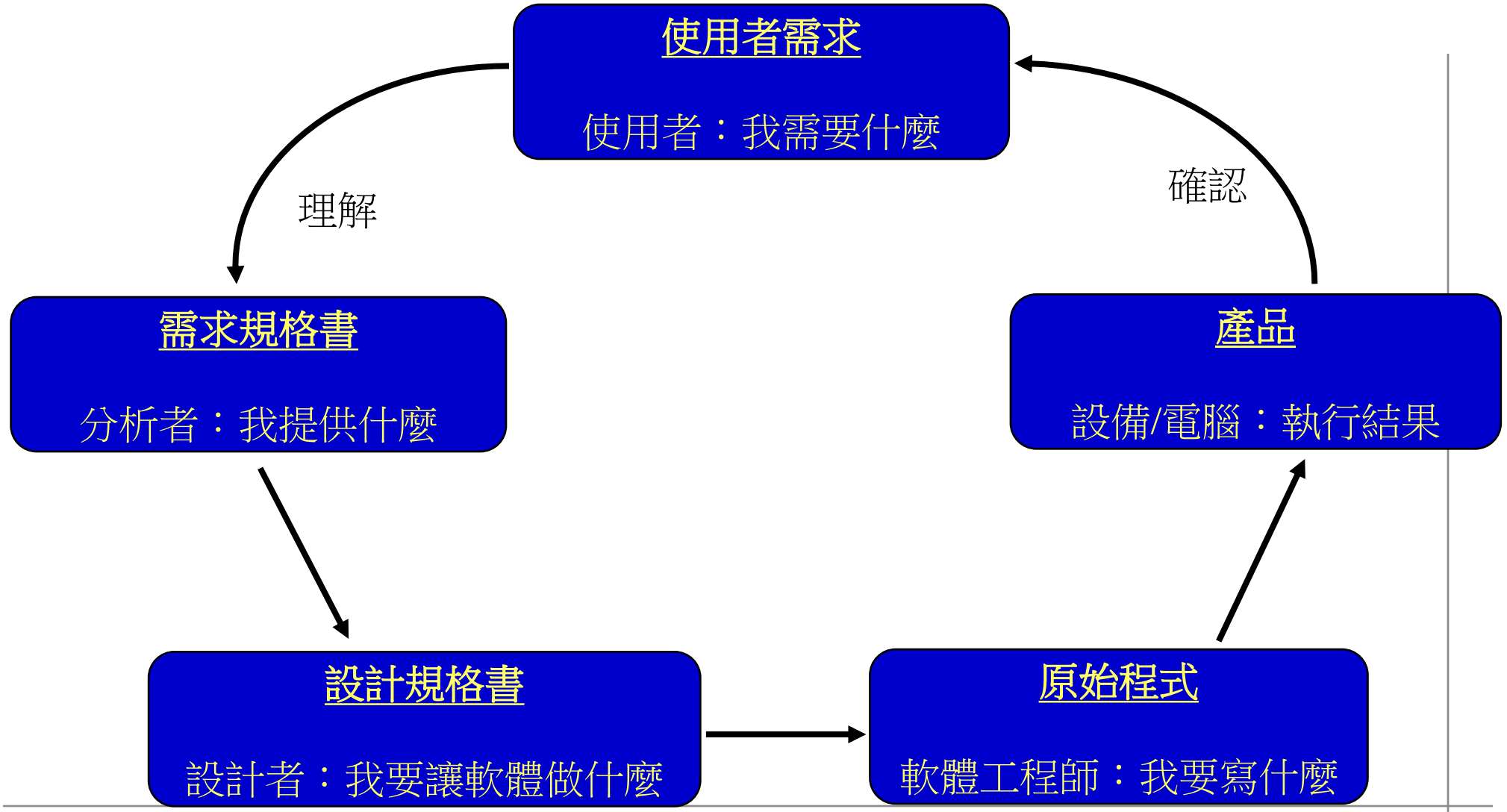
醫療器材相關法規關聯性



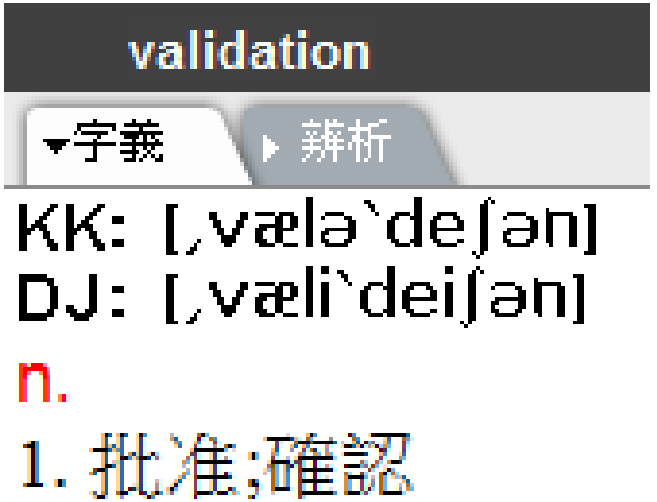
Source : Introduction into IEC 62304 Software life cycle for medical devices, Christoph Gerber, STRYKER

醫療器材軟體確效之基本架構

軟體發展生命週期


使用者需求
使用者：我需要什麼
理解
確認
需求規格書
分析者：我提供什麼
產品
設備/電腦：執行結果
設計規格書
設計者：我要讓軟體做什麼
原始程式
軟體工程師：我要寫什麼

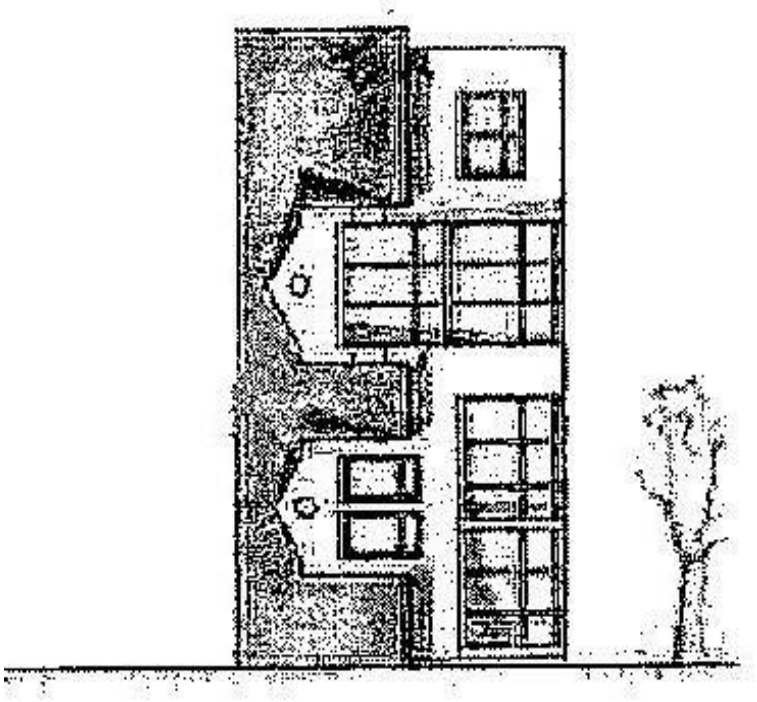
VERIFICATION & VALIDATION



VERIFICATION & VALIDATION

- 驗證 (Verification)
  - 保證軟體產品可以正確實現某一功能
  - 軟體開發生命週期中每個階段的正確性與完備性
  - Are we building the product right?
    - 我們是否正確地開發了產品
- 確認 (Validation)
  - 保證軟體符合功能需求
  - 需求規格的確認，軟體邏輯性的確認
  - Are we building the right product?
    - 我們是否開發了正確的產品？

VERIFICATION & VALIDATION



- 驗證(Verification)
  - 房子有牆嗎?
  - 房子有窗戶嗎?
  - 房子有[illegible]
  - 房子有[illegible]
  - 結論???
- 確認(Validation)
  - 房子符合屋主的要求嗎???

你正確的蓋房子嗎?

你蓋了正確的房子嗎?

醫療器材的驗證
VERIFICATION OF MEDICAL DEVICES

- Verification 驗證
  - an examination with objective means so that specific (product) properties are fulfilled. These (product) properties or characteristics can be found, for example, in a System Requirements Specification (SRS).
  - 以客觀手段進行檢查，使具體（產品）特性得到滿足。 這些（產品）屬性或特性可以在，例如系統要求規格（SRS）中找到。

資料來源：http://www.johner-institute.com/articles/product-development/verification-versus-validation/

VALIDATION 確認

- The examination of whether one can ever reach the goal with the use of a medical device. The user objectives can be found described in the intended use.
- 檢查醫療設備之使用是否能夠達到目標。其使用者的目標符合使用目的。

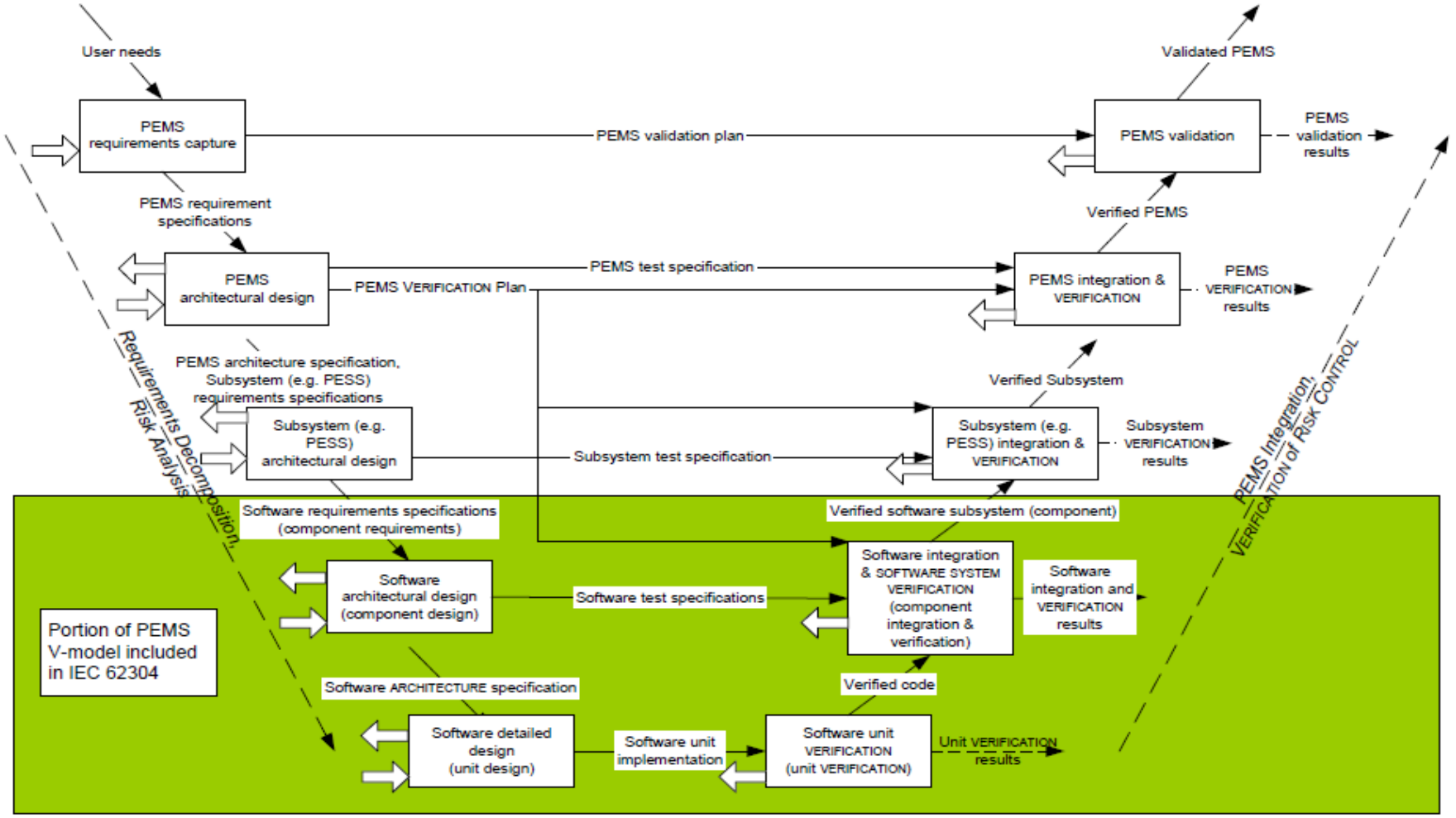
資料來源：http://www.johner-institute.com/articles/product-development/verification-versus-validation/

VERIFICATION & VALIDATION

- **Results of the verification and validation can be independent**
  驗證與確認的結果可以是**獨立**的
- For examples:
  - The defibrillator was set to 3000 volts on the pads (verification successfully). The patient's heart was still not beating (purpose) after application of the product (validation failed).
  - 心臟去顫器被設定至3000伏特並傳導至墊子（**驗證成功**）。病人在產品應用之後，心臟還是沒有恢復跳動（**確認失敗**）
  - The defibrillator was set, instead of the specified 3000 volts, to only 2000 volts (verification failed). Nevertheless, the patient's heart beat (purpose) after the application of the product (validation successfully).
  - 心臟去顫器被設定在3000伏特的檔位，但是只輸出2000伏特（**驗證失敗**）。然後，病人在產品應用之後，心臟恢復跳動。（**確認成功**）

資料來源：http://www.johner-institute.com/articles/product-development/verification-versus-validation/

醫療器材之產品發展生命週期 (V-MODEL)



資料來源：IEC 60601-1/

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

IEC 62304 標準介紹

- Medical device software – Software life cycle processes
  醫療器材軟體 – 軟體生命週期流程
- 適用範圍
  - When software is itself a medical device
    純醫療軟體
  - When software is an embedded or integral part of the final medical device
    嵌入或整合於醫療器材上之軟體
- 未涵蓋範圍
  - Validation / 確認醫療器材之功能是否滿足使用者需求
    - 純醫療軟體 >> Clause 6 of IEC 82304-1, Edition 1.0
    - 嵌入或整合於醫療器材上之軟體>> Clause 14 of IEC 60601-1, Edition 3.1
  - Final release of the medical device / 最終釋出之醫療器材

最新版本 IEC 62304:2015, EDITION 1.1

- The new version of IEC 62304, also known as IEC 62304:2015 or amendment 1 of IEC 62304 was published by the IEC at the end of June 2015.

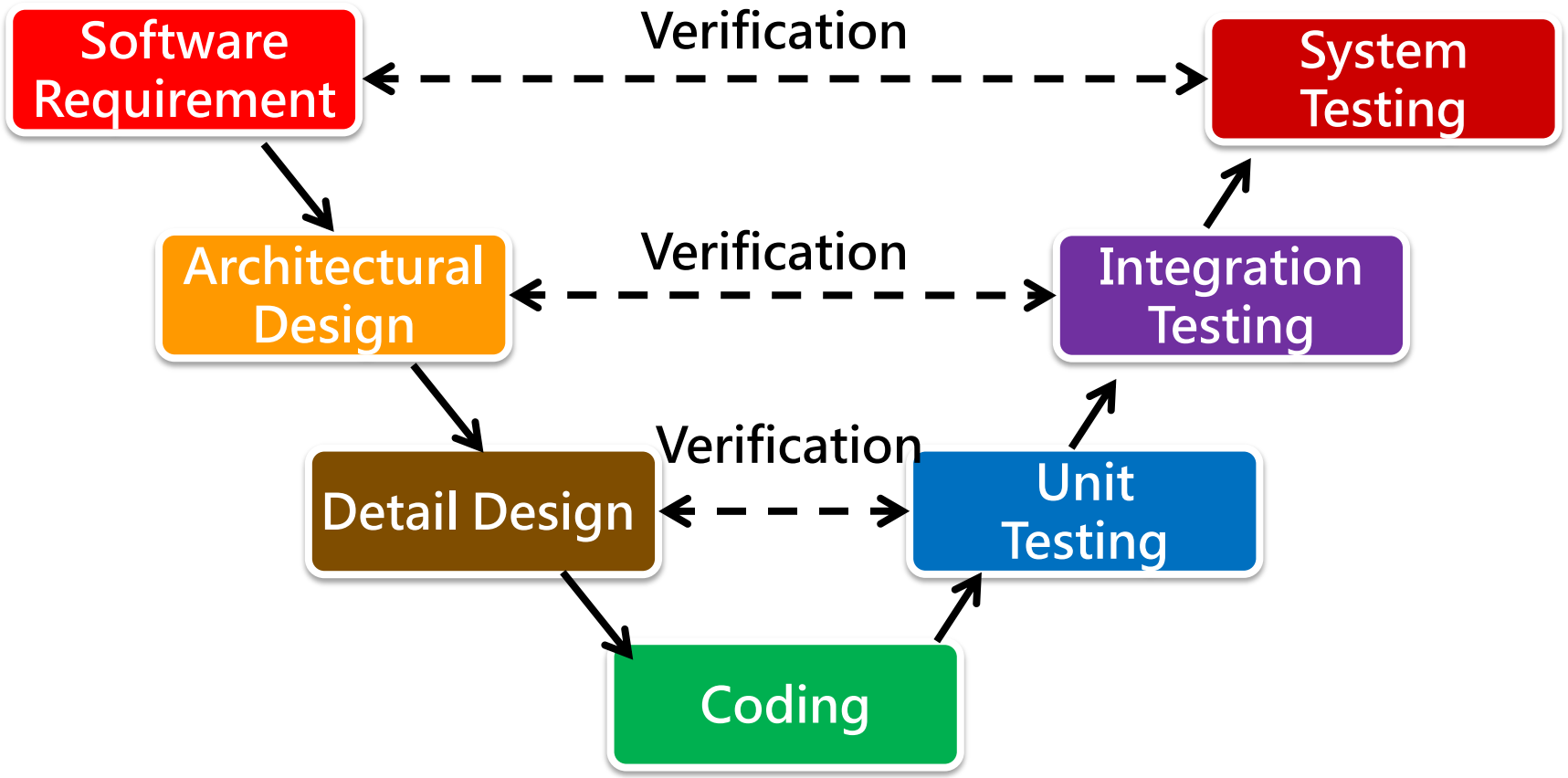
如何符合IEC 62304之要求 (CLAUSE 1.4)

- **實現此標準符合軟體安全等級之所有的流程、活動及工作**

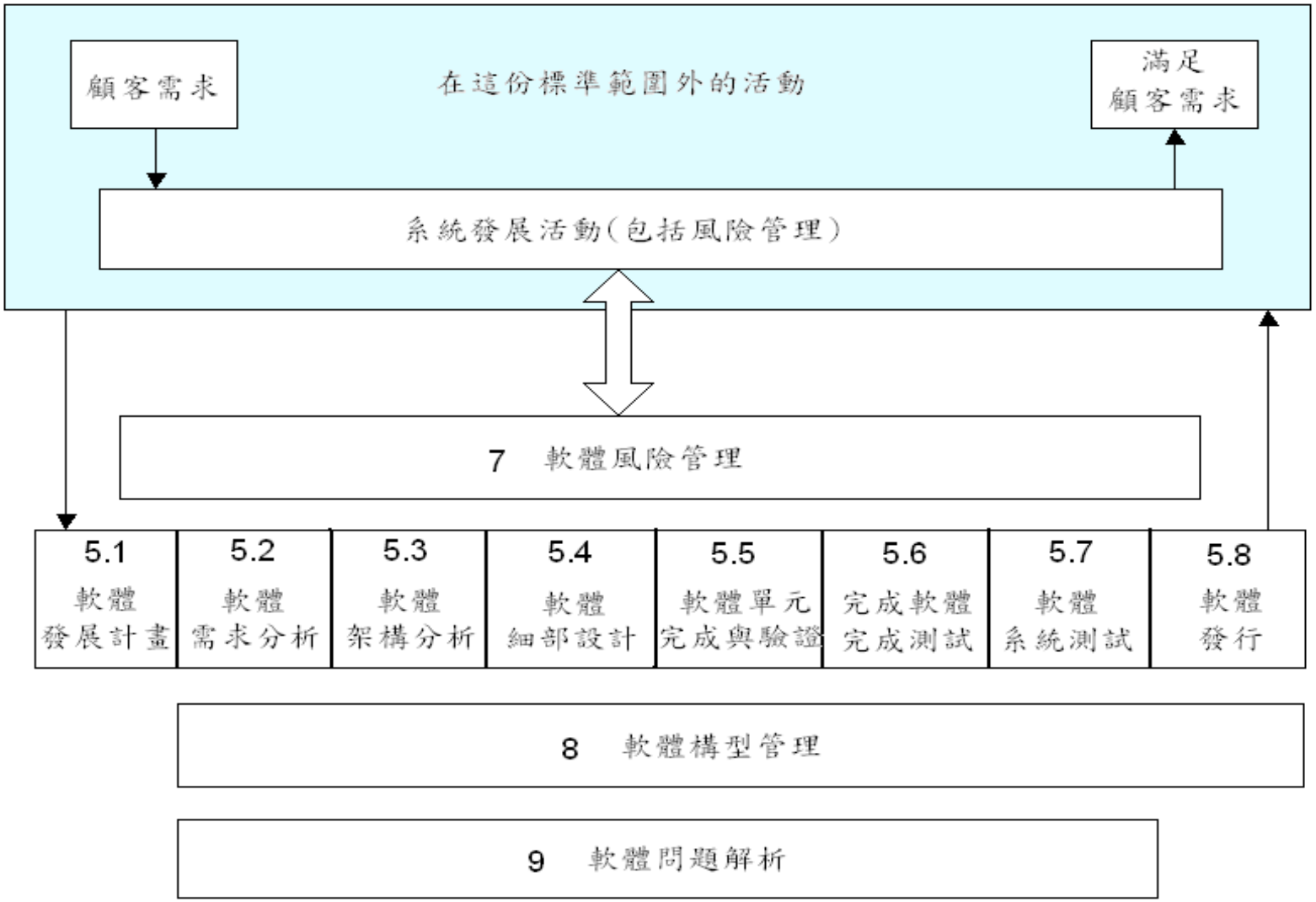
- 使用何種方式？
  - 對所有文件進行檢查，包含
    - 風險管理文件
    - 符合軟體安全等級之流程、活動及工作的評估
      (評估：內部或外部稽核)

  - 當標準有提及之項目卻未執行，必須提出**文件化**之說明。

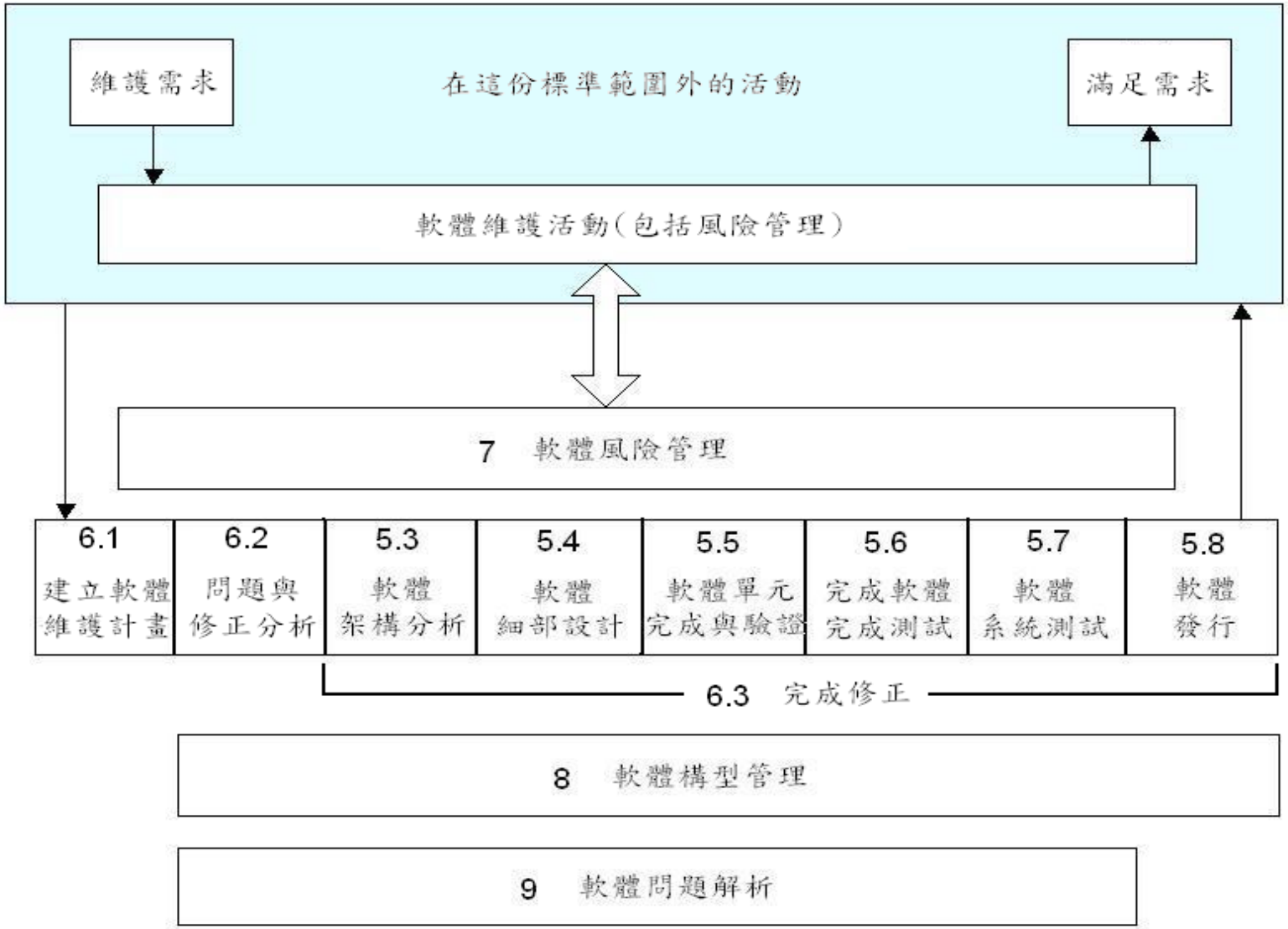
軟體生命週期 – V MODEL



IEC 62304 -軟體發展過程與活動概要



IEC 62304 -軟體維護過程與活動概要



IEC 62304 需求文件

- IEC-62304 標準要求下列文件
  - 風險管理文件 Risk Management File (clause 4.2, 7)
  - 軟體安全分級 Software Safety Classification (clause 4.3.c)
  - 軟體開發計畫 Software Development Plan (clause 5.1.1)
  - 軟體系統需求 Software System requirements (5.2)
  - 軟體架構設計 Software Architectural Design (clauses 5.3, 5.4)

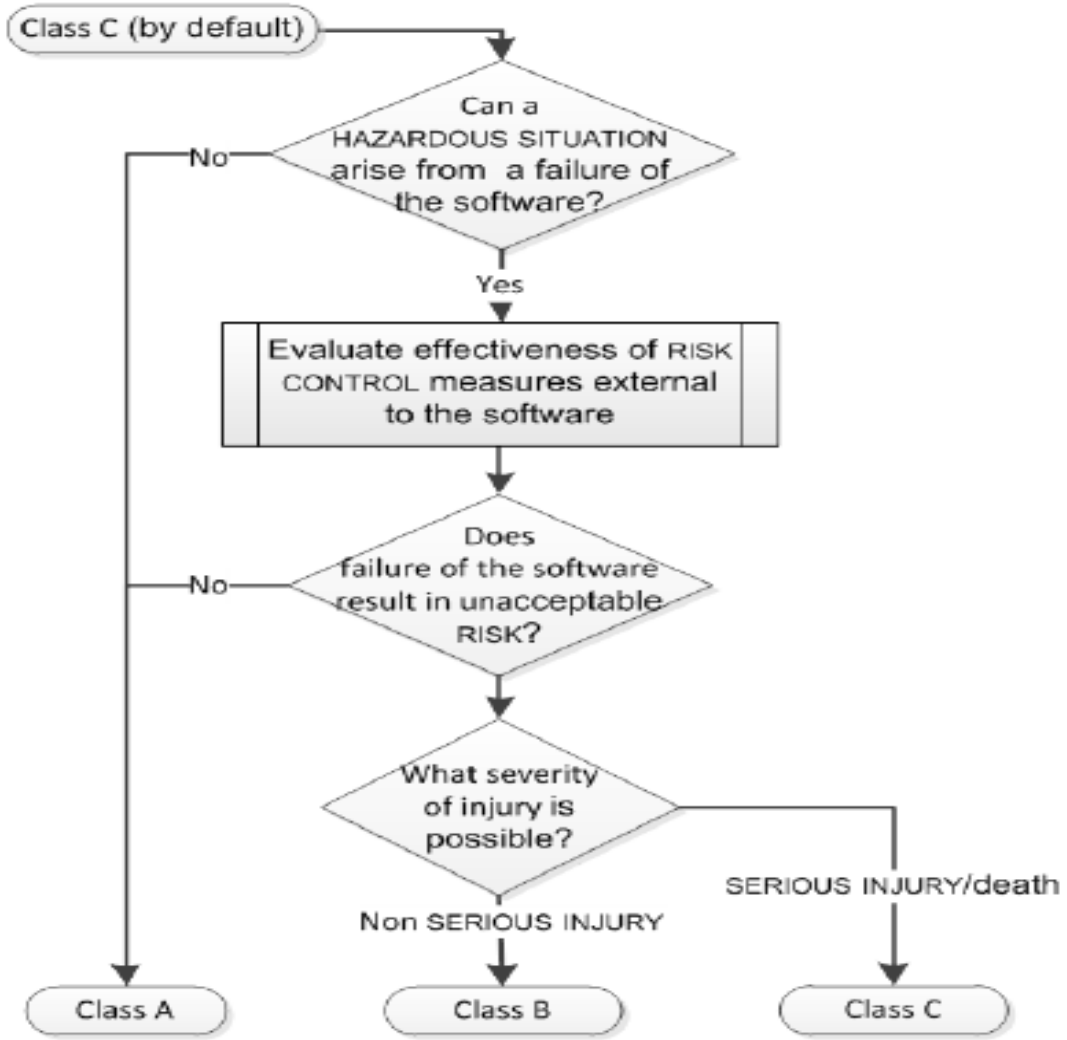
IEC 62304 需求文件

- IEC-62304 標準要求下列文件
  - 軟體測試計畫 Software Test Plan
    (clauses 5.5, 5.6, 5.7, especially 5.7.1 NOTE 1 and 2)
  - 可追溯性 Traceability Overview (或是測試程序對應軟體規格)
    (clause 5.7.4)
  - 軟體測試報告Software Test Report (clause 5.7.5)
  - 殘餘的異常 Residual Anomalies (clause 5.8)
  - 建構式管理 Configuration Management (clauses 5.8.4, 5.8.5, 8)

IEC 62304 核心程序

- 軟體發展程序 Software development process
  - 軟體發展生命週期之各項活動
- 軟體維護程序 Software maintenance process
  - 設計變更 Design change
  - 問題解決流程 Problem resolution process (上市後從使用者回饋之問題)
- 軟體風險管理程序 Software risk management process
  - 產品發展前的風險評估報告 (符合 ISO 14971要求)
  - 軟體分級之分析及描述
  - 改版、設計變更後之衝擊性分析
- 建構式管理 Software configuration management process
  - 軟體版本之控管
  - 軟體相關文件之版本控管
- 軟體問題解決程序 Software problem resolution process
  - 問題解決報告

醫療設備軟體的安全分級



In determining the software safety classification of the SOFTWARE SYSTEM:

- *Probability of a software failure shall be assumed to be 1.*
- *Only RISK CONTROL measures not implemented within (external to) the SOFTWARE SYSTEM shall be considered.*

NOTE: Such RISK CONTROL measures may reduce the probability that a software failure will cause HARM, and/or the severity of that HARM.

Note: A SOFTWARE SYSTEM which implements RISK CONTROL measure may fail, and this may contribute to a HAZARDOUS SITUATION. The resulting HARM may include the HARM which the RISK CONTROL measure is designed to prevent (see 7.2.2b)

IEC

醫療設備軟體的安全分級

The SOFTWARE SYSTEM is software safety class A if:

- the SOFTWARE SYSTEM cannot contribute to a HAZARDOUS SITUATION; or
- the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which does not result in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM.

The SOFTWARE SYSTEM is software safety class B if:

- the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which results in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM and the resulting possible HARM is non-SERIOUS INJURY.

The SOFTWARE SYSTEM is software safety class C if:

- the SOFTWARE SYSTEM can contribute to a HAZARDOUS SITUATION which results in unacceptable RISK after consideration of RISK CONTROL measures external to the SOFTWARE SYSTEM and the resulting possible HARM is death or SERIOUS INJURY.

2015版

醫療設備軟體的安全分級

Software Documentation	Class A	Class B	Class C
Software development plan	Must contain contents to sections 5.1 IEC 62304:2006. The plan's content list increases as the class increases, but a plan is required for all classes.		
Software requirements specification	Software requirements specification conforming to 5.2 IEC 62304:2006. The content list for the software requirements specification increases as the class increases, but a document is required for all classes.		
Software architecture	Not required.	Software architecture to 5.3 IEC 62304:2006. Refined to software unit level for Class C.	
Software detailed design	Not required.		Document detailed design for software units. (5.4).
Software unit implementation	All units are implemented, documented and source controlled (5.5.1).		
Software unit verification	Not required.	Define process, tests and acceptance criteria (5.5.2, 5.5.3). Carry out verification (5.5.5)	Define additional tests and acceptance criteria (5.5.2, 5.5.3, 5.5.4). Carry out verification (5.5.5).
Software integration and integration testing	Not required.	Integration testing to 5.6 IEC 62304:2006.	
Software system testing	System testing to 5.7 IEC 62304:2006.		
Software release	Document the version of the software product that is being released (5.8.4).	List of remaining software anomalies, annotated with an explanation of the impact on safety or effectiveness, including operator usage and human factors.	

Summary of safety classification effects on the code development documentation and process

Source from VectorCAST Training material

IEC 62304 名詞解釋

- 未知出處的軟體 (Software of unknown provenance, SOUP)
- 遺產軟體 (Legacy Software)
- 軟體的安全分級 (Software safety classification)

未知出處的軟體 SOUP

- SOUP – Software of Unknown Provenance
  - 已開發完成，且以一般性使用為目的之軟體
    (非以醫療器材領域為目的而開發)
  - 或以前開發的軟體，缺少開發過程之相關記錄
    FDA文件中所描述的“off the-shelf software, OTS software”
- Q: 軟體開發工具算不算是SOUP？

LEGACY SOFTWARE

- Legacy software
  - 醫療器材軟體合法於市場上販售，

    但不符合IEC 62304最新版本(2015, Edition 1.1)之要求
- 例如：
  - 於IEC 62304標準出版之前已開發完成且合法販售之醫療器材軟體

    （年代久遠）
  - 執行IEC 62304:2006, Edition 1.0之醫療器材軟體

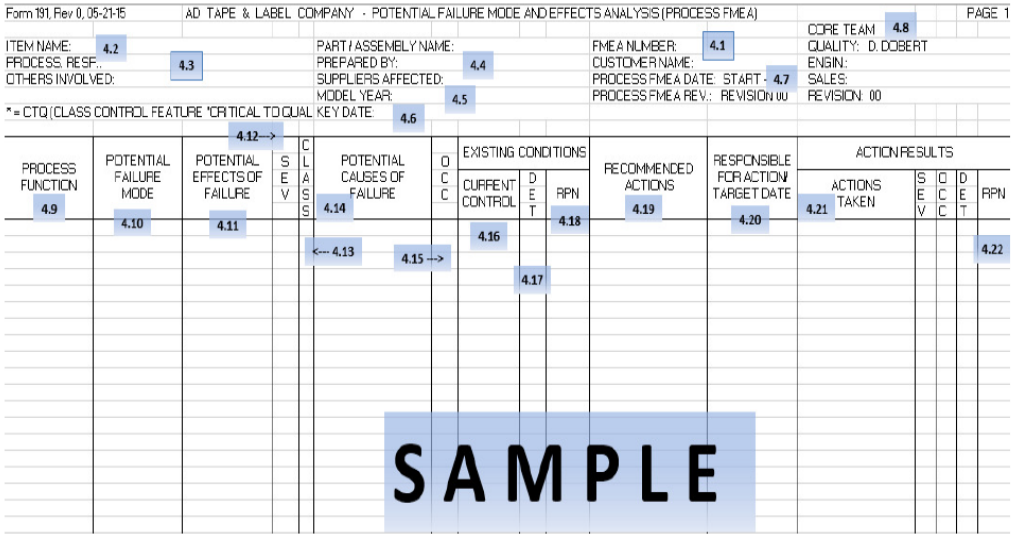
    （版本過期）

SOUP及LEGACY SOFTWARE 應考量之重點

- Requirements
  - 標註功能和特性需求
- Architecture
  - 標註系統、硬體、軟體有哪些功能是由SOUP提供
- Risk Analysis
  - 包含在軟體風險管理，評估SOUP/Legacy Software 失效可能會導致的危害及風險
- Configuration management
  - 供應商、標題、版本……

其它考量之重點

- 資料庫 Database
  - 於軟體規格(SRS)中描述資料庫之需求
- 資訊網路 IT-network
  - 於軟體規格(SRS)中描述資訊網路之需求
  - IEC 60601-1 Subclause 14.13
- 軟體 FMEA
  - 列出軟體可能產生的風險之分析歸納(風險管理文件之一部分)



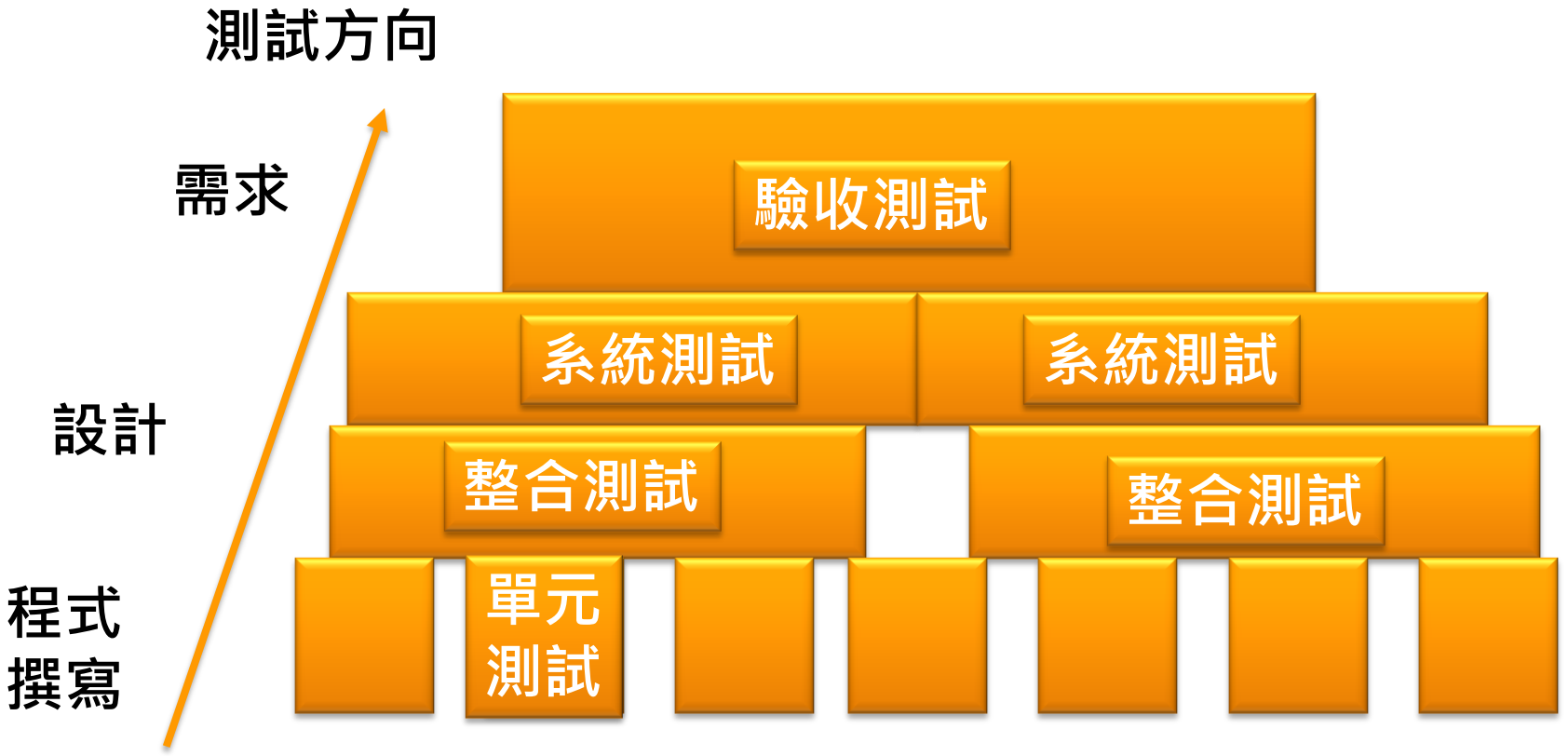
資料來源：ATL Pharmaceutical / Medical, website: www.atlco.com

軟體分析方法-靜態分析與動態分析

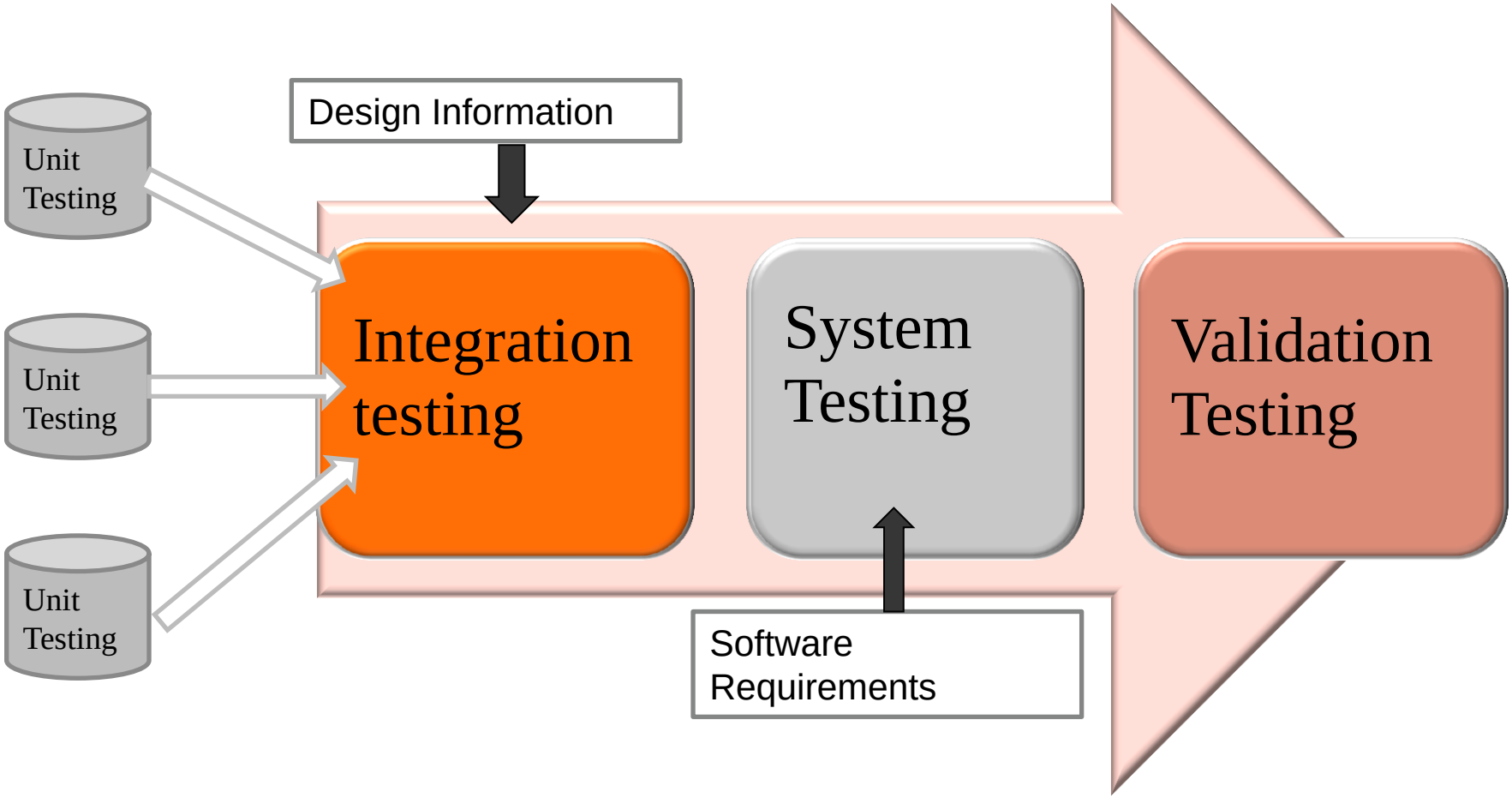
- **靜態分析**：不實際執行程式，用於發現錯誤的軟體測試技術，以及評估是否確實依照規劃執行邏輯順序
  - Walk Through (快速閱讀)：經驗豐富的開發人員，經由開發者的解釋，檢視軟體的邏輯錯誤、程式碼規範，將人腦充當電腦
  - Inspection (檢閱)：以會議形式進行，明定會議目標、流程與規定、採用check list方式進行錯誤檢視
  - Review(審查)：比inspection更嚴謹，第一步提供相關文件，以及常見錯誤清單。第二步召開審查會議，開發者透過講解發現程式中的錯誤。
  - 編碼規則 Coding guideline / rules; 例如：MISRA C, MISRA C++
  - 靜態分析工具：PRQA (QAC, QAC++...etc.)

- **動態分析**：實際執行程式，依測試之目的不同，而有不同的測試方式。

軟體動態測試程序



軟體測試之步驟


Design Information
Unit Testing
Unit Testing
Unit Testing
Integration testing
System Testing
Validation Testing
Software Requirements

軟體測試 - 單元測試

- 單元測試是對軟體基本組成單元進行測試，可以是一個函式、功能等具有基本屬性之”單元”
- 重點在於發現程式實作的邏輯錯誤，也就是要發現程式模組內部的各種錯誤
- 單元測試以**白箱測試**為主
- 單元測試必須是**可重複的**，因為程式碼修改、升級與維護都需要反覆執行
- 單元測試與撰寫程式所花的時間與精力大致相同。雖然會花費不少時間與成本，但卻對整個產品的測試有重大意義，因為bug越晚發現，所有修正的成本越高

軟體測試 -整合測試

- 整合測試：依照設計規格，對**所有需要組裝的單元模組**進行整合測試
- 整合測試以程式結構測試為主，發現軟體與系統定義不符合或是與之矛盾的地方，測試方式**結合黑箱與白箱測試**，但以**黑箱測試**為主
- 測試考量
  - 單元整合後，輸入輸出之介面的資料是否正確
  - 單元整合後，會不會造成其它功能產生不良的結果
  - 單元整合後，是否達成總體功能要求
  - 全域變數是否有問題
  - 單個模組的錯誤是否有累積的效應

軟體測試 -系統測試

- 主要目的驗證**整體系統**是否滿足當初所擬之**系統需求規格**之定義
- 整個測試的範圍除了軟體外，包括硬體、資料、操作人員和其他支援軟體
- 以**黑箱測試**為主
  - 規格測試
  - 輸入/輸出測試
  - 功能測試

IEC 60601-1 CLAUSE 14 需求文件

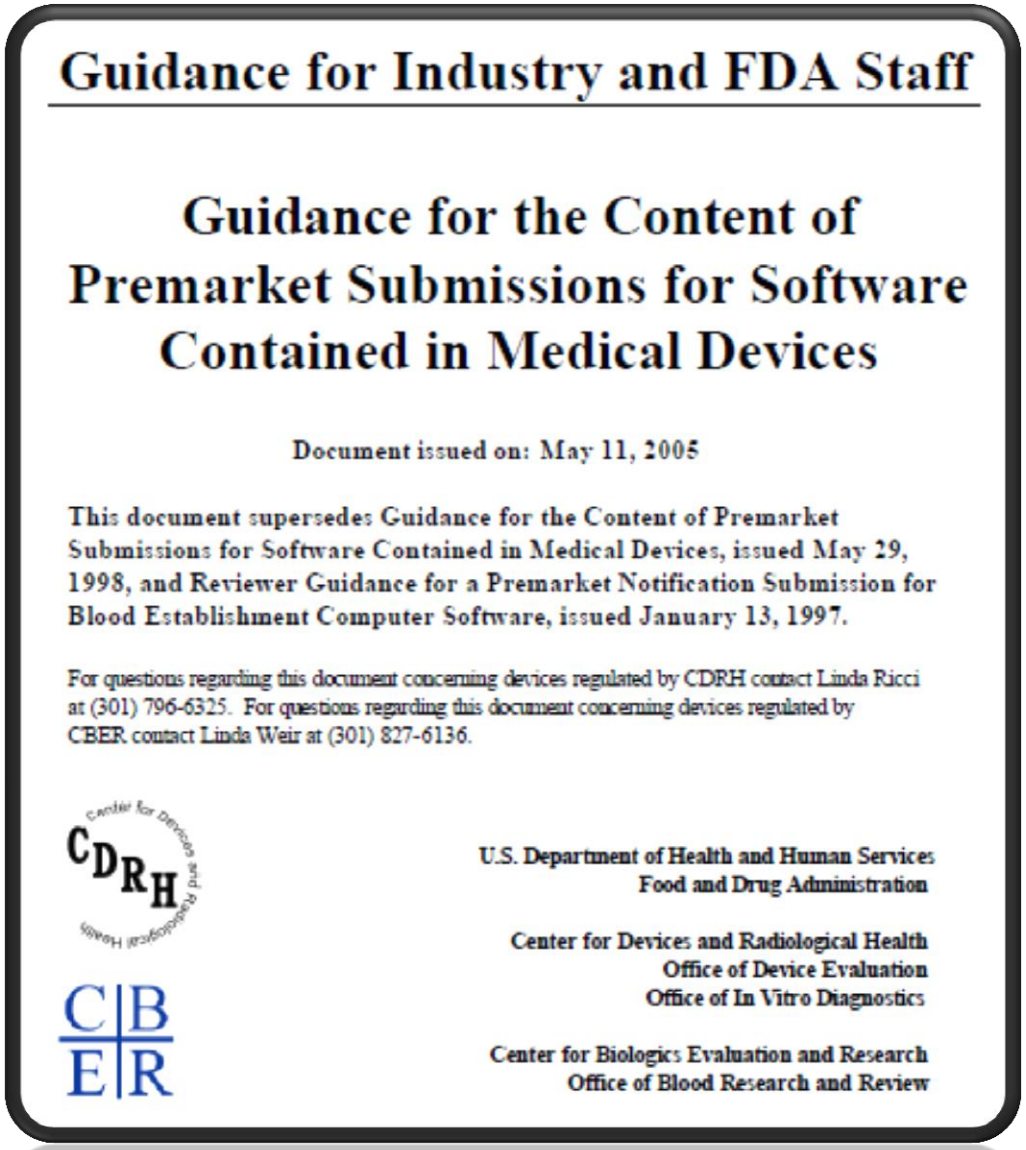
- 1. PEMS Development Plan(系統發展計畫)
- 2. PEMS Requirement Specification(系統規格)
- 3. PEMS Architecture Design(系統架構設計)
- 4. PEMS Validation Plan(系統驗證計畫)
- 5. PEMS Validation Report(系統驗證報告)

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

美國FDA軟體驗證發展沿革

- 1997年FDA公佈醫療器材使用市售軟體指引“Guidance for Off-the-Shelf Software Use in Medical Devices”，並於1999年公佈正式版
- 1998年FDA公告包含軟體之醫療器材上市前申請案指引“Guidance for the Content of the Premarket Submissions for Software Contained in Medical Devices”並於2005年改版，主要重點包含：
  - 生命週期活動（Life Cycle Activities）
  - 軟體等級（Level of Concern）
  - 風險管理（Risk Management）
  - 軟體驗證、確認與測試（SVV&T)



Guidance for Industry and FDA Staff

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Document issued on: May 11, 2005

This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, issued May 29, 1998, and Reviewer Guidance for a Premarket Notification Submission for Blood Establishment Computer Software, issued January 13, 1997.

For questions regarding this document concerning devices regulated by CDRH contact Linda Ricci at (301) 796-6325. For questions regarding this document concerning devices regulated by CBER contact Linda Weir at (301) 827-6136.

U.S. Department of Health and Human Services
Food and Drug Administration

Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics

Center for Biologics Evaluation and Research
Office of Blood Research and Review

決定軟體等級 (LEVEL OF CONCERN)

- 評估一項裝置可能會直接或間接讓病人或操作者遭受傷害的嚴重性。分為Major, Moderate與Minor三種levels
- **Major Level**
  - 一次的故障或潛在因素，直接造成病人或操作者的死亡或嚴重傷害
  - 間接性造成病人或操作者的死亡或嚴重傷害亦同。如不正確/延遲的資訊、或者是經由照護者的行為造成
- **Moderate Level**
  - 一次的故障或潛在因素，直接造成病人或操作者的較小傷害
  - 間接性造成病人或操作者的較小傷害亦同。如不正確/延遲的資訊、或者是經由照護者的行為造成
- **Minor Level**
  - 指故障或潛在因素，不會造成病人或操作者任何傷害

軟體等級對應之軟體技術文件及主要內容

軟體文件	MINOR	MODERATE	MAJOR
軟體等級	都需要		
軟體描述	都需要		
設備危害分析	都需要		
軟體需求規格	軟體需求規格中 功能需求之摘要	完整的軟體需求規格文件	
架構設計圖	不需要	詳細描述功能單元和軟體模組， 可包含狀態方塊圖與流程圖。	
軟體設計規格	不需要	軟體設計規格文件	
可追溯性分析	需求、規格、已識別之風險及測試之間的追溯性		
軟體發展環境描述	不需要	軟體生命週期發展計畫摘要， 包含版本控管與維修活動之摘要	軟體生命週期發展計畫摘要， 列出發展流程期間產出的控制文件， 包含版本控管與維修計畫文件
驗證與確認文件	軟體功能測試計畫、 Pass/Fail判定標準及 結果	於單元、整合、系統層級描述驗證 與確認活動。系統層級測試計畫， 包含Pass/Fail判定標準及結果	於單元、整合、系統層級描述驗證 與確認活動。單元、整合與系統層 級測試計畫，包含Pass/Fail判定標 準、測試報告、摘要及測試結果
修訂歷史記錄	版本歷史記錄，包含發佈版次編號與發佈日期		
未解決之異常	不需要	列出殘餘軟體異常並說明其對安全之衝擊或影響， 包含操作人員之使用及人為因素。	

FDA要求之軟體技術文件

1. 軟體等級 (Level of Concern) ：說明醫療設備對於安全層級方面的定義與基本的判定方法
2. 軟體描述 (Software Description) ：醫療設備軟體的概要說明
3. 設備危害分析 (Device Hazard Analysis) ：說明醫療裝置可能因故障而發生各種危險之分析
4. 軟體需求規格 (Software Requirements Specification) ：說明該軟體須實現及限制方面等需求
5. 架構設計圖(Architecture Design Chart) ：以圖表等方式，說明醫療設備軟硬體架構、系統流程、功能與軟體模組等。
6. 軟體設計規格(Software Design Specification)：實現軟體需求之設計

FDA要求之軟體技術文件

7. 可溯性分析 (Traceability Analysis)：將設計、測試、危險分析連結在一起，有助於內容的連貫性，提升檢視文件效率
8. 軟體開發環境描述(Software Development Environment Description)：指軟體開發的專案策略與管理等之說明
9. 確認與驗證文件(Verification and Validation Documentation)：說明在產品的開發過程中，需要確認與驗證的工作，以確保產品符合規格與客戶之需求
10. 校訂版本歷史紀錄(Revision Level History)：記錄產品發展的過程中，軟體修正的歷史
11. 未解決異常記錄(Unresolved Anomalies) 記錄軟體未解決的異常情況

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

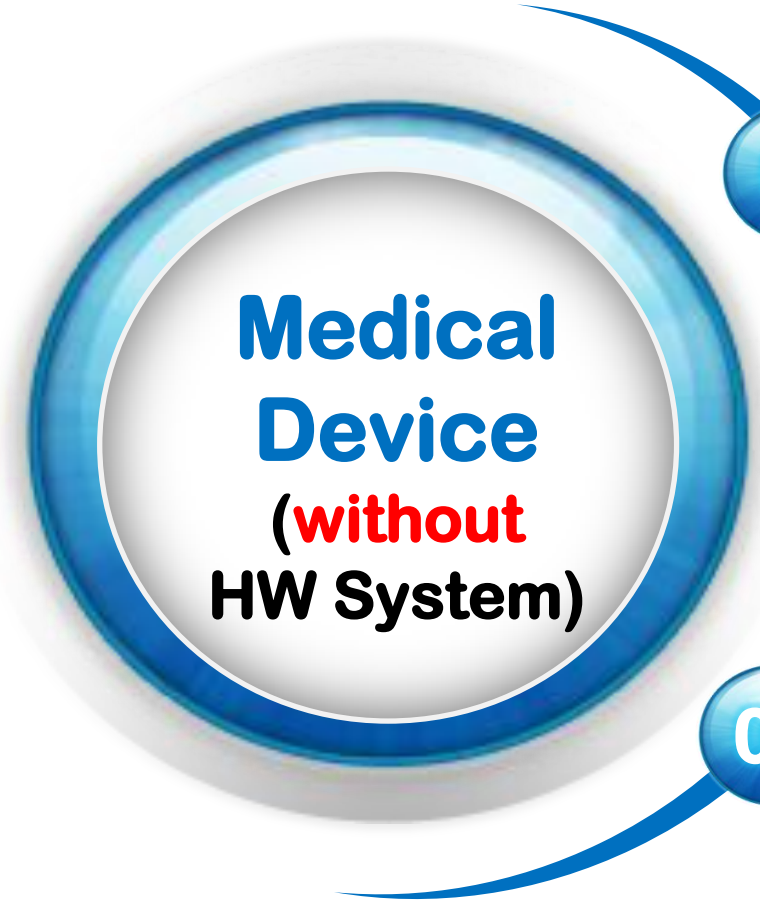
醫療產品系統適用規範(IEC 82304-1之影響)

For Company:
- ISO 13485 (QMS)

For Product System:
- IEC 60601-1
- ISO 14971 (Risk)
- IEC 62366-1 (Usability)

For Product Software System:
- IEC 62304 (SW Development)

醫療產品系統適用規範(IEC 82304-1之影響)



For Company:
- ISO 13485 (QMS)

For Product System:
- **IEC 82304-1**
- ISO 14971 (Risk)
- IEC 62366-1 (Usability)

For Product Software System:
- IEC 62304 (SW Development)

IEC 82304-1與IEC 62304之應用領域關係圖

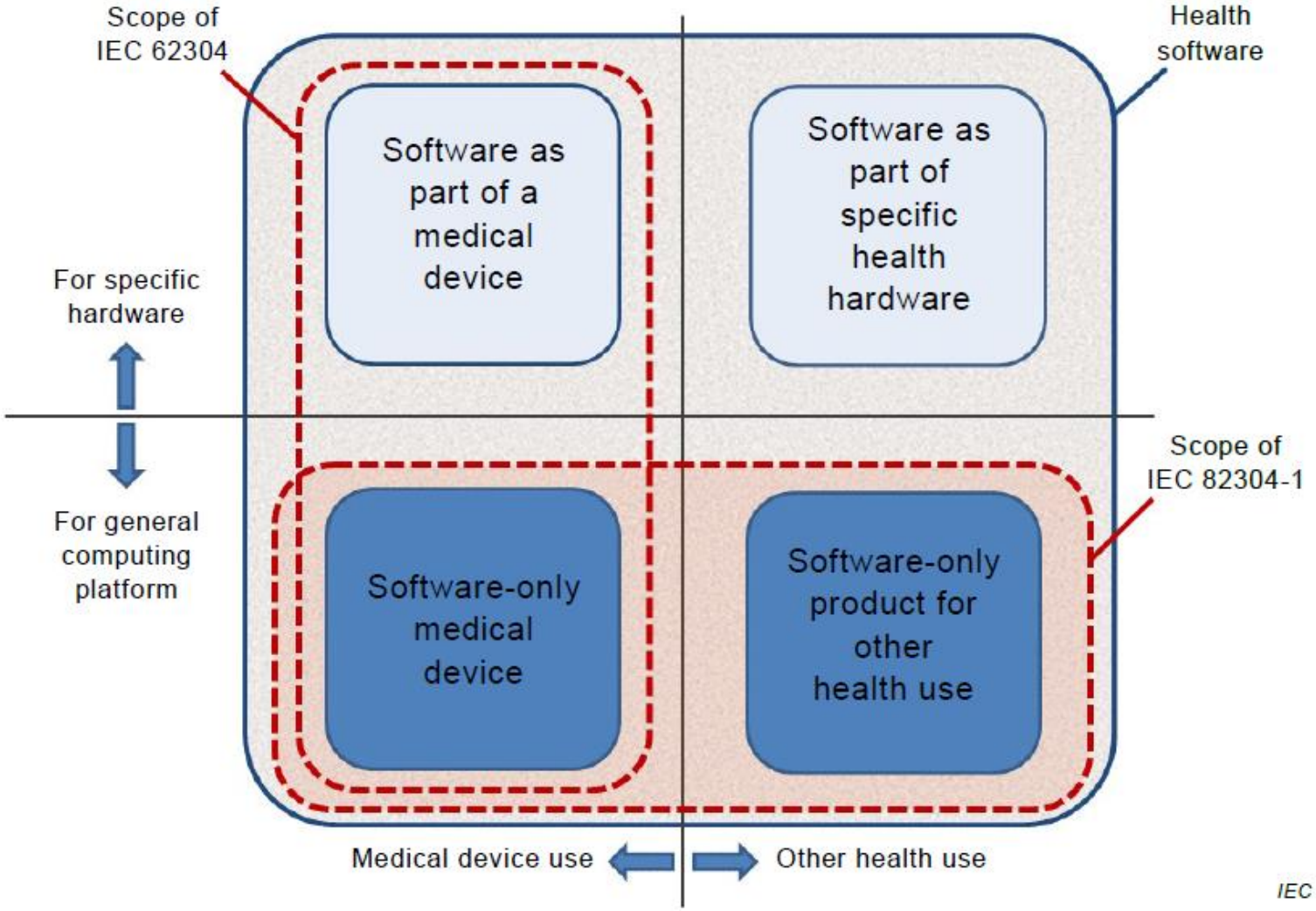


Figure A.1 – HEALTH SOFTWARE application domains and scope of related standards

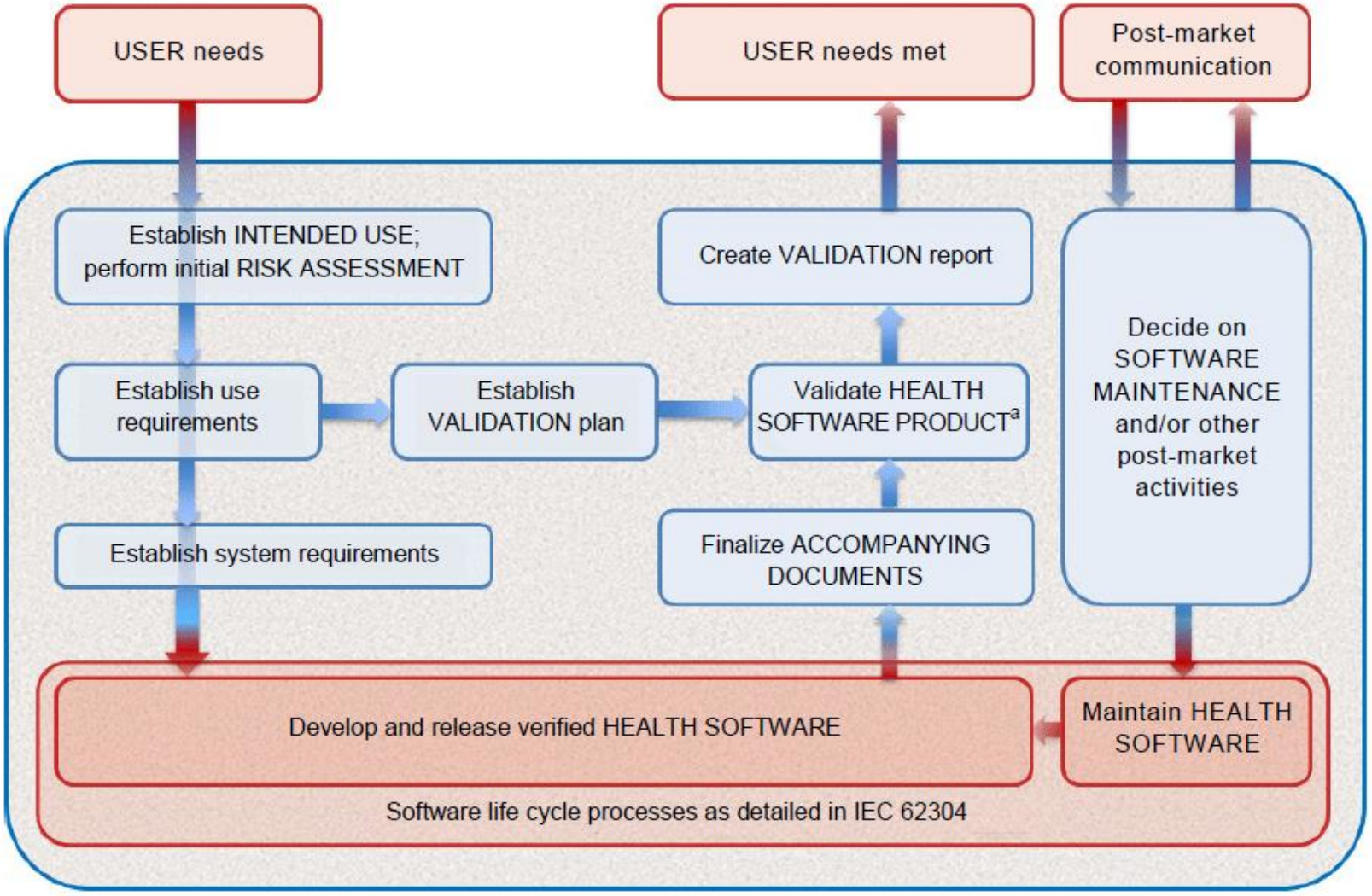
IEC 82304-1:2016 適用範圍

Table A.1 – Examples of software (SW) in or not in the scope of this document

In scope	NOT in scope
– SW-only products for health use – Mobile apps running on devices without using specific sensors or detectors [a] – Laboratory information SW – Radiology information SW – SW for individuals in fitness centres – SW for finding best conception moment – Computer-aided diagnosis SW – Analysis SW for medical images – Clinical decision support software used to aid diagnosis, treatment, and health management of individuals – Individual stress relief SW with feedback – Training plan SW for re-validation purposes – SW for stimulating activity by Alzheimer patients – Electronic health record systems, including electronic medical record systems – Hospital information systems – HEALTH SOFTWARE provided as a service hosted by an external organisation	– SW that is not an executable, such as sets of reference values, ... – SW not addressing health issues for individuals – Hospital billing SW – Hospital equipment maintenance scheduling SW – Epidemiological study SW – Nurse training SW – Self-study for medical professionals – Electronic logbook for nursing home Also outside of the scope is software, or their updates, intended to drive (parts of) – Medical electrical equipment or systems covered by IEC 60601/IEC 80601 (all parts) – In vitro diagnostic equipment covered by IEC 61010 (all parts) – Implantable devices covered by ISO 14708 (all parts)

[a] A camera or microphone or other feature commonly found on a smartphone or tablet computer is not considered a specific sensor or detector.

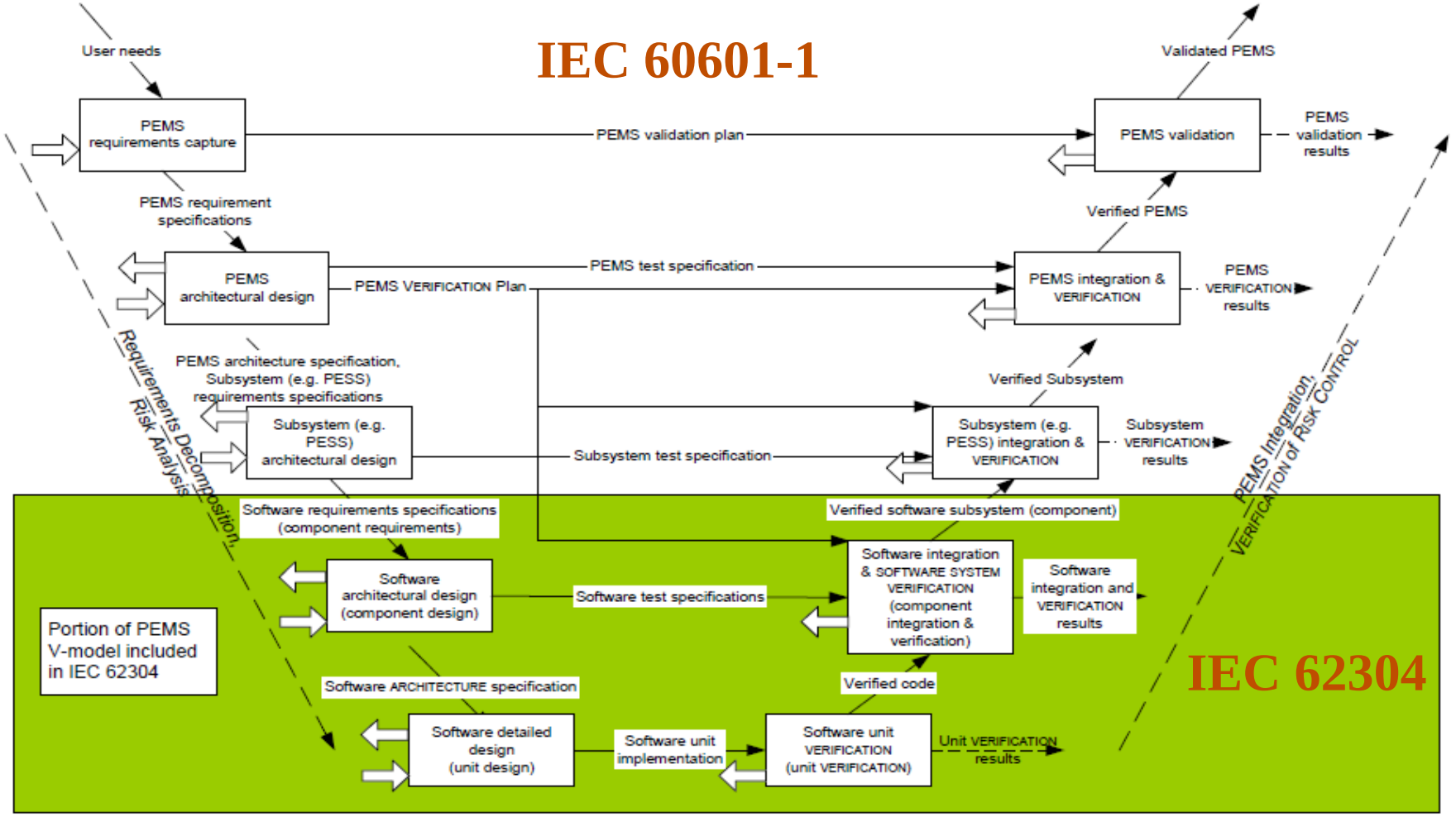
IEC 82304-1:2016 HEALTH SOFTWARE PRODUCT processes



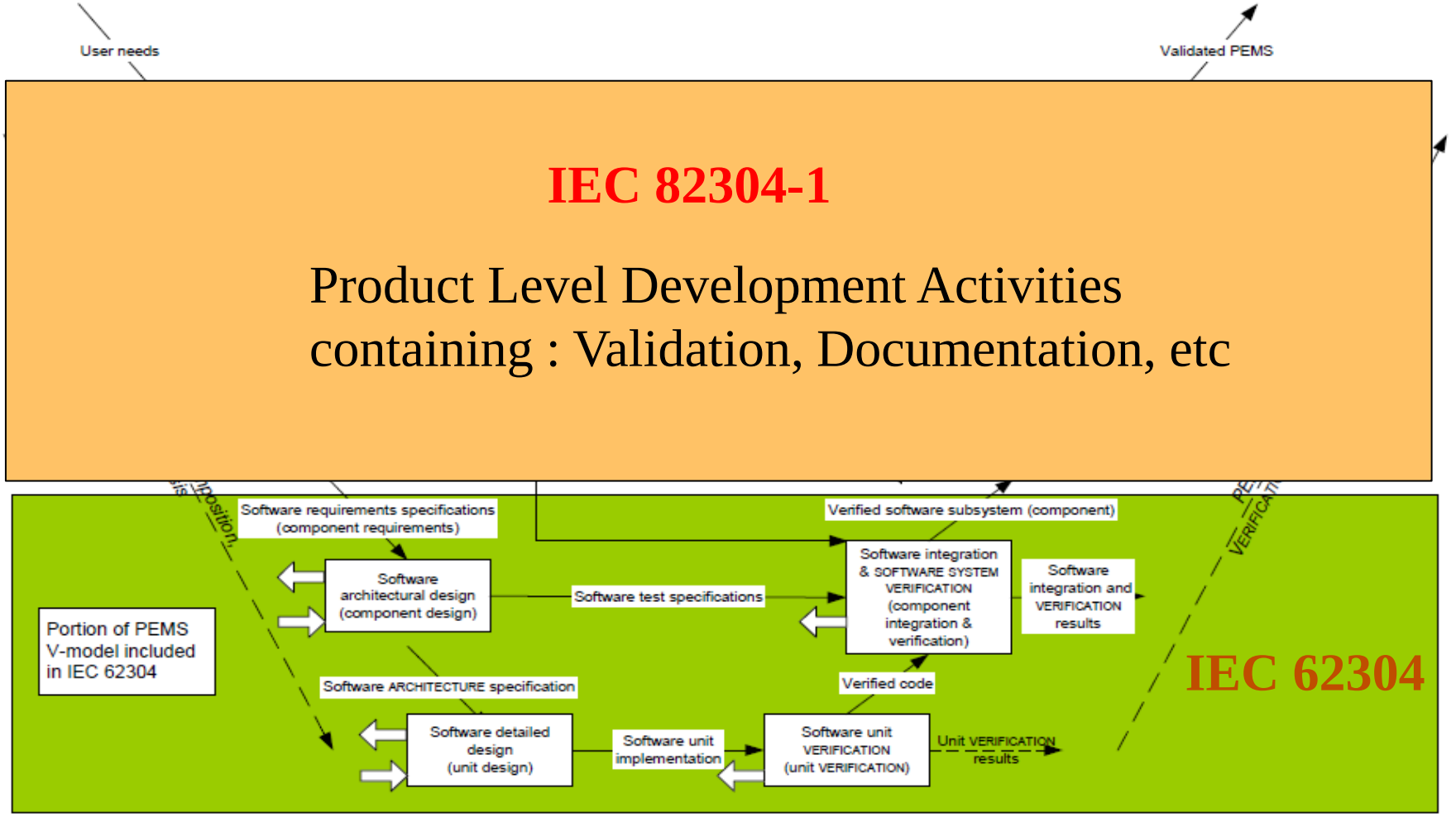
[a] HEALTH SOFTWARE PRODUCT: HEALTH SOFTWARE plus ACCOMPANYING DOCUMENTS

IEC

Works Between IEC 60601-1 and IEC 62304



Works Between IEC 82304-1 and IEC 62304



IEC 82304-1 核心程序

- 健康軟體產品規格 Health software product requirements
- 健康軟體-軟體生命週期程序 Health software-Software life cycle processes
- 健康軟體產品確認 Health software product validation
- 健康軟體產品識別 Health software product identification
- 健康軟體於上市後之活動 Post-market activities for the health software product

IEC 82304-1 is addressing Safety and Security

- SAFETY
  - Freedom from unacceptable RISK
- SECURITY
  - Protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them

課程大綱

- 功能安全簡介
- 軟體確效簡介
- 醫療器材相關標準簡介
- IEC 62304標準重點與實務
- 美國FDA軟體確效簡介
- 純醫療軟體 IEC 82304-1簡介
- 網路資訊安全 (Cyber security) 問題探討及對策

網路資訊安全 (CYBER SECURITY)

- 資訊安全：意為保護資訊及資訊系統免受未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀。(wikipedia)

- 為何我們需要重視網路資訊安全？
  - 科技發展以及網際網路的普及 (人力資源被取代)
  - 愈來愈多產品具有通訊能力 (駭客入侵的機會增加)
  - 應用領域：金融、工業、醫療、汽車、家電等領域。

當未經授權的狀況發生時，可能產生無法估計的影響。

資訊安全 (CYBER SECURITY) 問題探討及對策

- 問題探討 - 醫療領域：
- 存放雲端之電子病歷資料被篡改，造成醫生診斷之誤判
- 醫療器材之控制失效或控制權轉移至未經授權的人

- 對策：
- 風險管理階段就要考量網路資訊安全
- 擬定網路資訊安全計畫
- 權限之取得需要驗證（EX: 雙重認證：密碼+簡訊驗證碼）
- PC-based系統定期更新作業系統及防毒軟體 (定期維護與檢查)
- 參考文獻：FDA – “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”

聯絡窗口

呂柏翰 Miller Lu
02-2299-3279 EXT 3662
Miller.lu@sgs.com

盧盈辰 Jessie Lu
02-2299-3279 EXT 3661
Jessie.lu@sgs.com

Q&A

Thank You