物聯網之可信賴度與智慧應用

製造業翻轉－IIoT(3)

國際標準組織 (ISO & IEC) 在 2018 年推出了「ISO/IEC 30141 IoT Reference Architecture 物聯網參考架構」，其中揭櫫了 IoT 須具備的 Trustworthiness(可信賴度) 以維持 IoT 架構的正常運作。

文／梁日誠

物聯網(IoT)是被各行各業(如製造、醫療)最為廣泛應用的熱門新興科技之一，隨著應用漸廣，所蘊藏的風險已逐漸為人關注，因為IoT的服務更貼近個人，所以也就牽涉到了個人資料(個資)保護的議題。如何在使用IoT科技的同時也能兼顧資通安全與個資保護，成為全球性的課題。國際標準組織(ISO & IEC)在2018年推出了「ISO/IEC 30141 IoT Reference Architecture物聯網參考架構」，其中揭櫫了IoT須具備的Trustworthiness(可信賴度)以維持IoT架構的正常運作。「可信賴度」為跨領域(Domain)能力的一環，貫穿物聯網參考架構(RA)的各個領域，其交互關係的如圖1所示。

可信賴度包含了安全(Safety)、資安(Security)、隱私(Privacy)、可靠性(Reliability)與韌性(Resilience)等特性，藉由確保此等特性而使IoT系統於環境中斷、人為失誤、系統錯誤與攻擊時仍能如常工作。

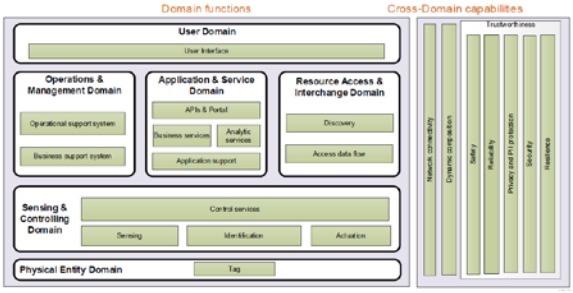

圖1　物聯網參考架構的各個領域功能及跨領域的可信賴度示意圖。(資料來源: ISO/IEC30141:2018)

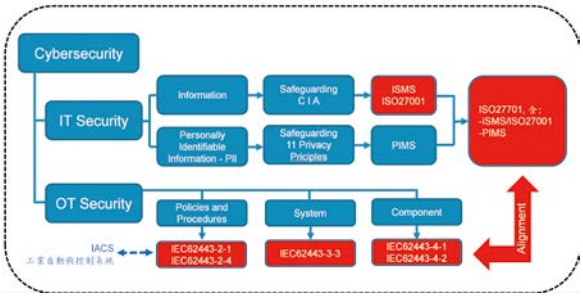

圖2　Cybersecurity可驗證國際標準示意圖。

由於IoT應用經常跨組織的串連，也因此採用治理加上管理的角度思考，較能整體地確保 IoT RA 的可信賴度及正常運行。常見的治理方法像是法遵與合規(如：資通安全管理法與個資法)、框架(如：資通安全框架CSF、隱私框架Privacy Framework)依循與供應鏈要求等；而管理的展現則常見於管理系統的建置與驗證，例如：資通安全管理系統(CSMS)、資訊安全管理系統(ISMS)、隱私資訊管理系統(PIMS)與業務持續管理系統(BCMS)…等。可信賴度也須以”設計(By Design)”的方式來處理，如 Security by Design、Privacy by Design 等，並非事後添加(afterthought)。ISO & IEC 針對可信賴度的各個特性制定了參考指引與驗證要求的國際標準，供市場採用及落實，並可經由第三方驗證來展現合規，介紹如下：

資安(Security)與Privacy(隱私)

Security與Privacy密不可分，資通安全

(Cybersecurity)包含了資訊技術(IT)安全與營運技術(OT)安全，於IoT可運用在智慧製造(Smart Manufacturing)的相關資通安全(Cybersecurity)可驗證國際標準，如圖2所示。

發展中的第二版(Ed.2)「 IEC62443-2-1 Security program requirements for IACS asset owners」則著重與ISMS/ISO27001的整合，並以發展中的「IEC62443-2-2 IACS Security Program Ratings」標準為輔，依成熟度模型來評估各個安全措施。對於供應商的資安要求方面，IT安全可採用ISO27036-2標準，而OT安全可採用IEC62443-2-4標準來要求供應商，對於個資作業的受委託者，則由ISO27701附錄B個資處理者控制措施來要求.

IoT系統與產品安全生命週期參考模型(Security Life Cycle Reference Model)也被ISO30141提出（如圖3所示），強調IoT系統與產品的設計時期與營運時期的安全均不可偏廢，並可參考 ISO15288 與ISO12207 所述及之系統與軟體發展生命週期的模型、階段與流程。此模型可供台灣目前推動的物聯網資安標章制度作為進一步發展的參考.

隱私法規(如美國HIPAA、歐盟GDPR、台灣個資法)、隱私框架(Privacy Framework，ISO/CNS29100)、隱私衝擊評鑑(Privacy Impact Assessment，ISO/CNS29134)、隱私工程(Privacy Engineering，ISO27550)、隱私資訊管理系統(PIMS，ISO27701)也是IoT應用涉及個資時所必須關注的議題，以智慧醫療之健康照護應用為例（圖4）若僅將IoT安全測試施作於個人端的IoT產品，將會忽略大量個資洩漏或違法的風險，如營運商、醫院、雲供應商等處，不可不慎！若涉及雲端科技，亦須考量雲安全管理系統(Cloud Security，ISO27017)標準.

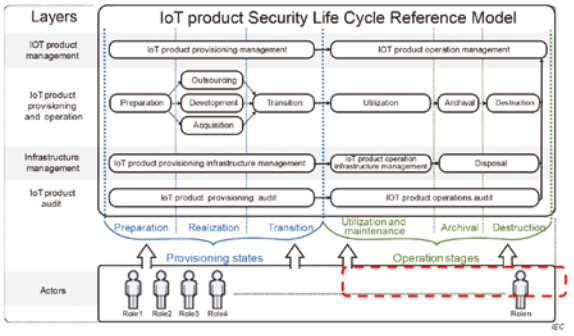

圖3　IoT產品安全生命週期參考模型。(資料來源: ISO/IEC 30141:2018)

表1　IEC61508系列標準。

標準編號	標準名稱
IEC61508-1	General requirements
IEC61508-2	Requirements for electrical/electronic/programmable electronic safety-related systems
IEC61508-3	Software requirements
IEC61508-4	Definitions and abbreviations
IEC61508-5	Examples of methods for the determination of safety integrity levels
IEC61508-6	Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC61508-7	Overview of techniques and measures

安全(Safety)

Safety或理解為功能安全(Functional Safety)，著重在使系統或設備能如預期的運作來反應輸入，目標在確保矯正或預防行動能夠避免或降低意外的衝擊。基於安全(Safety)觀點來考量IoT系統整體生命週期，並以安全觀點評估變更流程，進而採取適當的行動，對於安全而言是特別重要的。IEC61508系列標準（表1）則是汽車、醫療、交通、製造業的產品功能安全合規的最佳證明.

可靠性 (Reliability)與韌性(Resilience)

Reliability是指IoT系統或系統內的個體在規定的條件下及時間內完成規定的功能的能力；Resilience則是IoT系統在事故後快速回復正常運作狀態的能力。可靠性目標可能包含量測矩陣，如MTBF (Mean Time Between Failures)、MTTR (Mean Time to Repair)、MTTF (Mean Time to Failure)，三者關係如圖5。有關Resilience的相關國際標準，可參考「 ISO22301 業務持續管理系統」(BCMS) 及

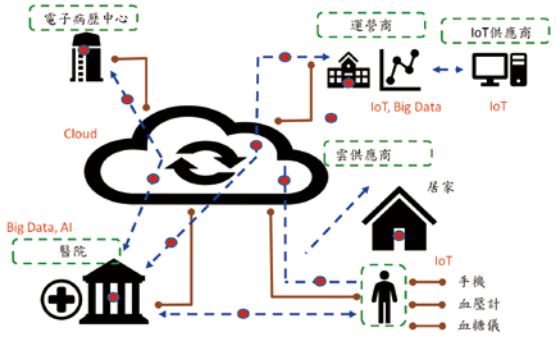

圖4　智慧醫療之健康照護應用案例圖。

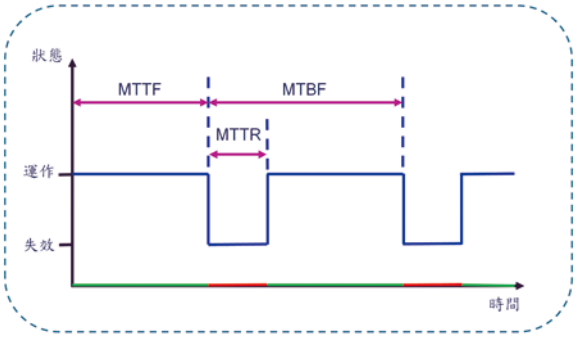

圖5　靠性量測矩陣關係圖。

「ISO27031資通訊技術準備度與業務持續指引」.

物聯網與智慧應用

隨著新興科技的發展，各種智慧應用也持續地推出市場（圖6），而連接最後一哩的IoT技術更廣泛地被智慧應用所採用，也因此IoT可信賴度的治理與管理機制更顯得重要，才能保障使用者的資安、隱私與安全無虞。舉例而言，在智慧城市的應用中，有許多應用需要取得使用者的個資，而這些應用往往由該城市的被委託單位執行，如何落實可信賴度的治理與管理機制，使得相關的政府機構、IoT營運商、IoT設備商、應用商及相關第三方皆能合規的運作，民眾也才能放心的使用創新的便民服務。以智慧城市為例，發展中的「ISO30145 Smart City ICT Reference Framework系列標準」與發展中的「ISO27570 Privacy guidelines for smart cities標準」可作為參考。

可信賴度的幾個特性並不單獨存在，而是共同存在於IoT系統中的主要因子，且互相交互作用，須於系統設計與整體生命周期時考量。ISO & IEC組

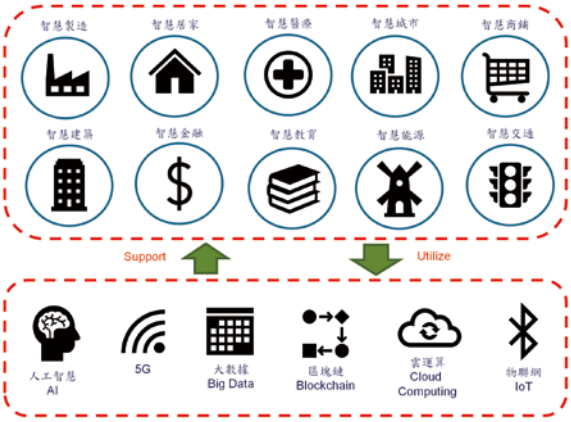

圖6　智慧應用與新興科技關係圖。

織也正制訂相對應的國際標準，如：正在制定中的「ISO27030 物聯網資安(Security)與隱私(Privacy)指引」、在公告過程中的「ISO TR 30166 Industrial IoT 工業物聯網」，以及發展中的「ISO31700 消費者產品與服務的隱私設計」來支援物聯網架構與應用在發展IoT相關應用、產品與服務的過程中，採用ISO&IEC國際標準與認驗證制度(如IAF MLA與IECEE)是與世界接軌、全球合作、國際互認的最佳方法。

本文作者梁日誠現職為 ISO/IEC JTC1/SC27及IEC/TC65加拿大對映技術委員會委員與TCIC環奧國際驗證公司全球營運總經理。