流程盤根錯節：開發連線產品的五大挑戰

連線生態系統研究報告

UL Solutions

Safety. Science. Transformation.™

物聯網 (IoT) 以其連線能力改變世界，早已是眾所皆知的事實。從簡單的物件（如智慧型手錶）到所有地區都裝有感測器的智慧城市，物聯網自動化使我們所有人都受益。

不過研究顯示，物聯網市場的發展比分析師預測的更慢。鑒於其巨大的潛力，怎麼會出現這種情況？

以下圖文是製造商在開發連線產品時所面臨的關鍵挑戰。

只要在物件上加入

智慧

功能，複雜度便會跟著提升。

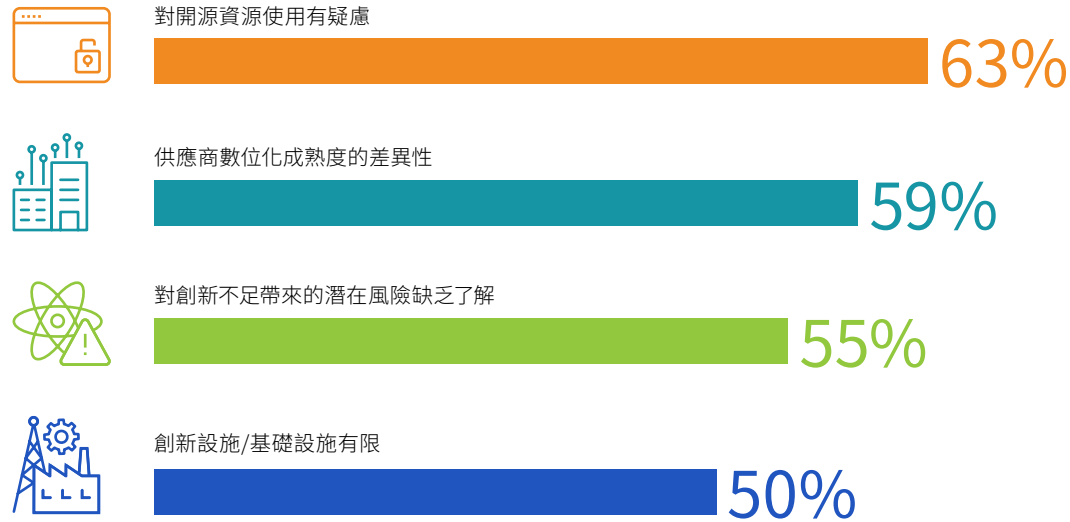
什麼是物聯網？

物聯網是指至少有一個實體元件的功能集合，可以透過交換或無線網路連線。範圍涵蓋該實體元件、該裝置各種運算元件內部的常駐軟體，以及行動應用程式或雲端執行個體中所安裝的任何軟體。

挑戰 #1
開發連線產品比想像中難多了

物聯網創新看起來好像很容易，但將連線產品推向市場實際上比您想像的更困難。由於有五花八門的技術、裝置、應用程式和管理平台，即使只是製造一個裝置實際上也會相當複雜。在連線產品中建立物聯網功能需要時間，也需要企業重新思考他們目前的運作方式。

當被問及哪些挑戰阻礙組織追求更高水準的創新時，主管們表示：[1]



挑戰 #2
產品功能在現實世界中失去作用

製造商知道，物聯網裝置的數量、類型和用途每年都在擴大，但許多消費者的體驗卻不盡如人意。消費者已經表示擔心，如果他們的家庭和生活中的物聯網裝置出現故障，可能會造成致命的後果。請記住，人們購買的是解決方案，而不是產品，產品只是解決方案連線生態系統的一部分。每項產品都需要配合各種解決方案。

83%
的消費者擔心由於**性能問題而無法控制其智慧家居系統。**[2]

62%
的消費者擔心，隨著物聯網的**普及，連線問題也會越來越多。**[2]

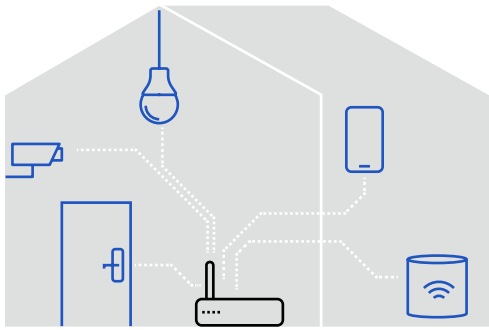
46%
的公司認為產品的可靠性是技術**購買決策中最重要的購買標準。**[3]

21%
的消費者由於裝置的**功能和使用有限而放棄可穿戴設備。**[4]

物聯網技術可能**達不到**達不到應有的便利性，有

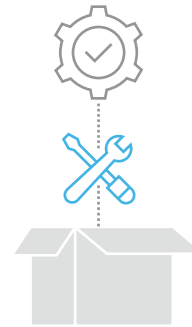
三分之一
的人會遇到困難，
主要是在操作他們的智慧小工具時。[5]

為什麼功能在現實世界中會失去作用



連線能力
產品之間缺乏收集和資訊發送用的訊號或雙向通訊，會導致裝置故障和使用者的挫折感。

注意事項：
裝置是否連線順暢？連線能否保是不中斷？如果發生電壓突波，裝置是否能迅速重新連線？裝置是否以適當的速度傳輸資料？

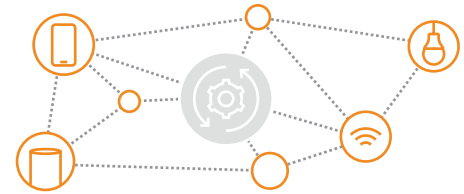


裝置設定
許多產品仍然需要手動設定，使用者可能會覺得麻煩。隨著連線生態系統的發展，自動設定成為必備條件。

注意事項：
該裝置安裝後是否容易設定？

裝置載入
連線產品的數量會隨著專案活動的增加而上升，伺服器農場成為處理大量資料的必要條件。

注意事項：
處理過程是否可讓資料在產品和伺服器之間無縫傳輸？



整合問題
連線產品應用程式通常與各種路由器、智慧中樞或其他系統整合。

注意事項：
裝置是否適應作業系統的升級、新的應用程式和其連線生態系統中的新裝置？

運作環境
連線產品可在廣泛的環境和條件下運作。

注意事項：
使用者將在什麼條件下操作產品？

挑戰 #3
網路安全風險與日常生活密不可分

隨著互連系統需要頻繁地通訊和分享資料，駭客攻擊互連產品的攻擊媒介也大幅增加。網路攻擊是真實存在的，從冰箱到心臟起搏器等任何連線產品都可能面臨駭客威脅。一旦網路罪犯取得控制，便可以在幾秒鐘內接管一個物件的功能，或轉連至網路上的其他產品或系統。與其事後才將安全性納入考慮，不如先把它嵌入到您的產品設計之中。

我們可以從以下數字看出未雨綢繆的重要性：

5 分鐘
物聯網裝置上線後平均多長時間會遭遇攻擊[6]

38,182
僅在 2020 年 3 月，物聯網惡意軟體的入侵次數就達到了 100 萬次[8]

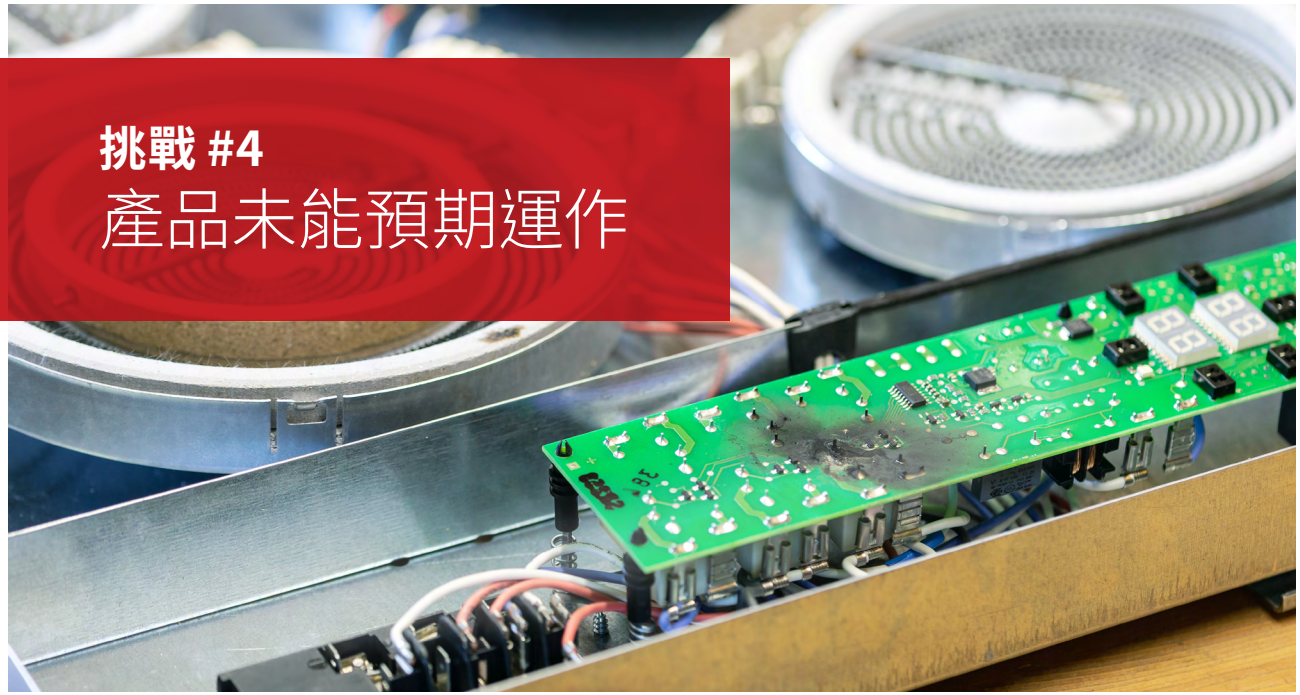
7 天
因惡意軟體攻擊而造成的平均時間成本[7]

386 萬美元
公司遭遇惡意軟體攻擊的平均成本
（包括客戶流失、獲客成本的增加、聲譽損失和商譽減損）[9]

57%
的物聯網裝置容易受到中度或高度嚴重的攻擊，因此很容易成為攻擊者的目標。[10]

關於連線系統和裝置中出現的網路安全性漏洞，其中最常見的原因是缺發最佳的產品設計和實施。最常見的原因一般分為以下五個方面：

- 不良的產品設計
- 不安全的通訊協定
- 認證程序不足
- 軟體更新有限
- 實施或裝置/應用程式使用不當



挑戰 #4
產品未能預期運作

風險管理對安全風險的觀點

「隨著自動駕駛汽車、工業物聯網、智慧家居等的興起，技術故障有可能對人和財產造成實際傷害。有遠見的公司應確保他們為這種日益增長的責任提供保障。」

Marsh & McLennan Companies

許多連線產品在金融科技、醫療科技和健康科技等敏感領域發揮著重要作用，這些領域將人身安全和保護個人資料需求放在優先順位。產品到達客戶手中的那一刻，必須是完美無瑕的。功能不佳或管理不善的產品不僅會對品牌聲譽產生負面影響，在最壞的情況下，甚至會對使用者造成傷害。安全不應侷限於最終產品；安全的生產過程也應該是考量之一。

81%
的消費者表示，他們需要夠信任這個品牌才會購買其產品。[13]

50%
的終端使用者越來越關注物聯網裝置帶來身體傷害的風險。[11]

42%
的主管預期，因為物聯網發生問題而導致的風險將越來越複雜。[12]

挑戰 #5
與法規遵循相關的不確定性日益增加

隨著全球對物聯網的監管意願提升，不確定性也在增加。公司關注並期望法規優先於創新。目前的立法行動集中在保障物聯網裝置的安全和保護消費者隱私和資料。由於安全法規和要求可能因國家而異，因此最好先了解特定市場的法規。

66%

的公司正在為遵守法律和法規而預留資金。[14]

40%

的主管預計，在未來三到五年內，合規性風險的複雜性將增加。[15]

無論是網路安全、安全、互通性還是無線網路，總是有一個全球市場進入要素，因為各國的特定區域要求各不相同。

結論
連線產品的挑戰在於其複雜性

隨著物聯網應用的成長，實施解決方案、最佳做法和控制的重要性也在增加，它們不僅可以保護裝置的安全性、功能性和可靠性，還能保護整個連線生態系統。公司需要了解他們正在製造、購買和使用的東西。將連線能力和安全性納入產品開發，同時搭配處理漏洞及管理生命週期和支援的流程是至關重要的概念。

需要考慮的初步問題

- 這項產品會在哪銷售？
- 我的產品適用哪些標準？
- 我們如何為消費者提供良好的使用者體驗？
- 我如何減少連線方面的問題？
- 我如何檢查以保障我的裝置能夠連線、保持連線並實現其預定功能？
- 開發安全和可靠產品的最佳做法是什麼？
- 什麼等級的安全性適合我的產品？

若要進一步了解物聯網互操作性和連線測試服務，請瀏覽 UL.com/IOP

為何選擇 UL Solutions?

UL Solutions　是全球安全科學的領導品牌，可以在連線產品的互操作性和網路安全測試和認證方面為您提供支援。我們可以協助評估您的產品與其它裝置和主要的連線/物聯網平台和標準流暢運作。這有助於您向消費者提供可靠、安全的連線產品，改善客戶體驗和品牌聲譽。

- UL Solutions 已幫助制定 1,600 多項標準以定義安全、安防、品質和永續性。
- UL Solutions 擁有許多物聯網和無線標準機構的認可測試實驗室，如 Bluetooth® Special Interest Group (SIG)、Thread Group、Connectivity Standards Alliance (CSA) 和 Open Connectivity Forum (OCF)。
- 我們可以為大多數連線產品、行動應用程式、Wi-Fi重新連線的穩定性、功能、長期連線性能等執行現實世界的互操作性測試。
- 我們可以開發客製化的測試解決方案，滿足您的具體要求。
- UL Solutions 是您的單一來源服務供應商，我們有一整套服務，包括終端產品測試、認證和驗證，有助您更快地進入目標市場。

立即聯絡我們。

適用的服務包括以下測試和認證：

智慧助理
- Google 助理
- Amazon Alexa

連線標準和平台
- Samsung SmartThings
- Matter
- MFi
- Thread
- CSA (Zigbee)
- OCF
- Bluetooth®
- USB IF

無線行動裝置標準
- 全球認證論壇 (GCF)
- PTCRB

網路安全標準和評等
- UL 驗證物聯網裝置安全評等[16,17]
- UL 2900-2-1，「Standard for Software Cybersecurity for Network-Connectable Products」，第 2-1 部分：醫療和健康系統的聯網部件的特殊要求
- UL 2900-2-3，「Standard for Software Cybersecurity for Network-Connectable Products」，第 2-3 部分：針對安防和生命安全警報系統的具體要求
- IEC 62443

參考資料

1. UL (April 2020). Innovation and Safety in a New Decade.
2. Dynatrace. (August 2018). Consumer Confidence Report.
3. Statista. (September 2020). Most important buying criteria for tech purchases (COVID-19 Context). https://www.statista.com/statistics/1169718/worldwide-it-purchase-buying-criteria-covid/
4. Ericsson. (May 2019). Wearable technology and the IoT. https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/wearabletechnology-and-the-internet-of-things/
5. ADT. (August 2019). Home is where the smart is.
6. NETSCOUT. (August 2019). Dawn of the Terrorbit Era.
7. Purplesec. (February 2020). 2020 Cyber Security Statistics.
8. Symantec. (April 2019). ISTR 2019: Internet of Things Cyber Attacks Grow More Diverse.
9. Purplesec. (February 2020). 2020 Cyber Security Statistics.
10. Palo Alto. (March 2020). Unit 42 IoT Threat Intelligence Report. https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf
11. Marsh & McLennan Companies. (October 2018). Internet of Things: Limitless Connections and Ways to Fail. https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2018/dec/IoT--Limitless-Connections-and-Ways-to-Fail/Internet-of-Things_%20Limitless%20Connections.pdf
12. Marsh & McLennan Companies. (March 2020). A New Definition of Catastrophic Risk: Technology Industry Risk Study.
13. Edelman. (February 2019). Edelman 2019 Trust Barometer.
14. Marsh & McLennan Companies. (March 2020). A New Definition of Catastrophic Risk: Technology Industry Risk Study.
15. Marsh & McLennan Companies. (March 2020). A New Definition of Catastrophic Risk: Technology Industry Risk Study.
16. https://www.ul.com/resources/Iot-security-rating-levels-guide
17. https://www.ul.com/services/ul-verified-iot-device-security-rating

UL.com/IOP

CMIT22CS248552.5

返回到第一頁