# 判斷物聯網產品的安全保障等級

Empowering Trust™

# 執行摘要

不久之前，我們的資訊和系統的數位化還尚未普及。回溯到 1989 年，網路甫在全球問世，當時沒有任何家庭能夠擷取整個網路資源，我們仍在使用底片拍攝相片。直到 1994 年，Apple 發表首款數位相機，並在隔年 Canon Ixus 問市後，數位攝影才成為主流。在上世紀 90 年代初期，大多數人沒有手機，而且由於尺寸原因，帶手機的人還必須將手機放在公事包裡一起攜帶。

當時的惡意軟體，主要是由學術研究專案和基於娛樂目的所編寫干擾程式組成的軟體。這樣的程式無法將我們的家庭照片加密並要求付款贖回、無法擷取個人錄製的家庭影片來進行勒索、無法控制我們的暖氣或大門門鎖，也無法佔用我們的家庭設備，被網軍利用在網路上興風作浪，影響全球網際網路的流量。

上述行為之所以無法被操作，主要是因為我們的多數資料和系統仍為類比式。在 1989 年，安全(Safety)和安防 (Security) 本質上是屬同義詞，皆代表有效的物理安全性。

今天 (僅 30 年後)，我們將資料 (有時甚至是幾乎將我們生活) 的控制權交給了周遭無所不在的電腦運算系統。物理安全以及我們的資料、金錢和資產的安全性，必須一併考量系統中控制或瀏覽這些資訊的軟體安全性。

現今所有裝置皆會安裝軟體。

大部份的人都能夠理解這一點。因為一般用途的電腦系統已經持續普及，特別是自 1990 年代中期以來，全球網路的使用量急遽增加。不過，現在的我們正面臨互連系統 (物聯網) 發展的新階段，隨之而來的是對安全性的新關注和需求。

本文件將討論物聯網的定義，以及為何物聯網安全性是一個比一般用途電腦運算裝置安全性更棘手的問題。此外，白皮書還將深入探討如何藉由了解所涉及的風險，並透過用在物聯網系統中的實作安全性評等來主導購買決策，並確定哪種評等適合您的產品，以找出解決物聯網安全問題的最佳方式。

# 定義物聯網

雖然 IoT 一詞是 Internet of Things 的縮寫，其字面意思為「物聯網」，但要明確定義物聯網涵蓋的範圍並不容易。許多智慧型裝置並無法直接連線網際網路，而是使用網路中樞 (集線器) 之類的代理伺服器設備，或者僅透過藍牙或 Zigbee 無線通訊方式使用本地端連線。絕大多數的物聯網系統都有配套的應用程式或雲端服務，其主要的功能是能夠讓「物件」有效運作，或甚至加強物件本身的運作效能。

針對本文件的描述用途，我們會使用「物聯網」這個術語來代表任何功能的集合，而該集合中至少包括一個可以透過交換式網路或無線網路連線的實體元件；然後，範圍會涵蓋該系統的所有元件：實體元件，其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。

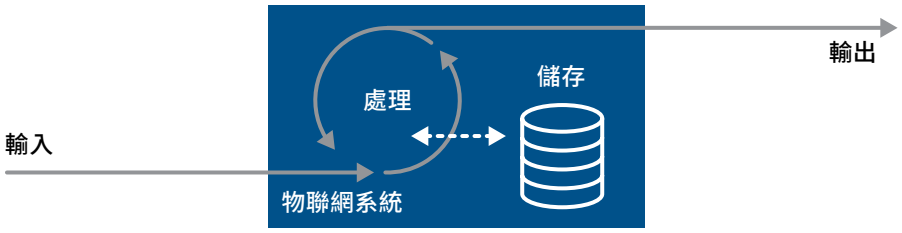
這樣一來，我們就能在定義中涵蓋諸如藍牙喇叭和門鎖等，這類通常可能根本不會連線網路的裝置。這項定義蔚為重要，因為門鎖的安全性顯然十分重要，然而喇叭的安全，相對可能沒有那麼重要。

為什麼使用相同的無線技術連線時，我們會以不同的方式考慮這兩個裝置的安全性？我們可以使用哪些規則來判斷任何類型的裝置可能面對的威脅，以及這些威脅暗示該裝置需要哪一種安全性等級？

# 物聯網的風險

在評估任何物聯網系統所需的安全性時，重點是首先必須要了解該系統所面臨的風險、可能出現的問題，以及惡意方想要破壞該系統的動機。基本上，這取決於機會和價值：存取系統的難易程度以及惡意方透過這種存取和/或入侵可以獲得多少價值（原則上代表攻擊的目標資產）。

從最根本的層面上來說，任何電腦運算系統 (包括物聯網) 都可以概括為輸入、輸出、儲存和處理系統，如下圖所示：




在大多數情況下，重點會放在輸入 (使用者資料) 上，而這也是物聯網系統為何受到攻擊的決定性因素。但是，其實任何部份，包括儲存、處理能力、輸出頻寬和資料、網路功能以及裝置所在位置...等，對攻擊者而言都可能是極具內在價值的資產。例如，指向您住所外部的向外拍攝攝影機，可能被認為所提供的資料價值很低。但是，該攝影機可能會遭到入侵，成為組成一個前所未有的大規模殭屍網路的一部分，犯罪分子或許會使用它查看您何時離開家或隱藏他們接近房屋的入侵行動、侵犯您鄰居的隱私，並在網路上開始進行有計劃的第一階段攻擊。

下表摘要列出物聯網系統可能擁有並成為攻擊者鎖定目標的資產、以及這些資產被攻擊的方式，還有攻擊目的的範例：

| 目標資產 | 攻擊類型 | 範例目標/攻擊目的 |
|---|---|---|
| **存放或取得日期** | 資料竊取 | 謀利/勒索 |
| | 資料竄改 | 勒索軟體 |
| | 全系統資料或程式碼擷取 | 程式碼逆向工程 |
| **處理能力** | 處理資源運用 | 加密貨幣挖礦密碼破解 |
| **系統作業/功能** | 作業停用 | 勒索軟體/勒索 |
| | 作業竄改 | 循環播放安全監控攝錄影片 |
| | 作業判斷 | 判斷是否有人在家 |
| | 利用透過授權的操作 | 開啟門鎖 |
| **網路操作/功能** | 使用頻寬 | DDoS 攻擊 |
| | 利用受信任的網路功能 | DNS 修改 |
| **網路定位** | 存取其他網路或系統 | 攻擊其他系統 |
| | 擷取網路流量 | 從其他系統竊取資料 |

由於存在多種威脅，因此很難一言以蔽之哪種特定類型的物聯網裝置或系統是對攻擊者有價值。但言而總之，這個價值通常取決於系統的部署和使用方式，而非系統類型。

換句話說，物聯網系統的安全性更多部分是與其所在位置以及可存取的資料和資源息息相關，而不在於系統本身。「實體裝置」可能有助於定義資料和資源，但這不是主要因素。相較於只和手機連線以播放音樂的藍牙喇叭，與直接連線網際網路並透過整合式攝影機提供房屋內部影像監控，且具備大型處理與頻寬資源的智慧型喇叭更容易成為攻擊目標。

# 物聯網安全問題

了解物聯網安全性的許多層面 (涉及的威脅和風險類型) 後，就不難理解確實有必要解決這些系統中的安全性問題。但是，這並非一件容易的事。物聯網系統通常集合了不同的處理元件和程式碼，而這些程式碼會在具備不同物理和邏輯安全性的不同位置被執行。假若「位置」很重要，那麼擁有多個「位置」可能只會使事情更加複雜。

而且複雜性往往是安全性的大敵。

物聯網安全性的一個基本問題是，雖然安全性通常不需要花很多錢就能妥善實作，但也不是免費的。好的安全性代表一個設計良好的功能，這意味著在產品開發的初始階段就需要花費更多的時間並具備更完善的知識。設計越複雜，涉及的程式碼元素和類型就越多，因此要將整體集合整合到安全系統中的難度就越高。

維護複雜的系統同樣困難重重。運用修補程式和安全性更新以使系統保持在最新狀態的作業，需要透過人員執行：他們了解安全性對今天所建立的產品具有什麼樣的意義，並且能夠跟上更新的安全性研究腳步，以便掌握未來安全性需求的人員，同時他們也是該產品產生初始收入後，持續執行產品相關作業的人員。系統越複雜，對應所有安全性問題的難度就越高，需要的人員也就越多。

考慮到全球對這些人員的技能需求，其通常都會成為非常寶貴的人才。因此，良好的設計和持續的維護會產生有形的成本，也就是需要額外人力和時間。同樣重要的是，安全性功能的實際測試和驗證也要付出代價。當然可以採用較低的成本執行「快速」安全性測試，但這也只能針對要測試的安全性提供低層級的保障。為了提高保障等級，您需要執行更詳細的測試，只是這將花費更多的時間與金錢。此成本將會算到設計和維護成本上，也就是說，這些成本一定會侵蝕物聯網系統原來就已經很微薄的利潤，或導致其購買價格被提高。

因此，從根本上來說，安全性實際上主要是商業問題。

# 評等物聯網安全性

我們如何承受這種安全性成本？如果我們認為安全性成本只能佔裝置總成本的某個最大百分比 (否則消費者將尋求其他採購解決方案)，那麼可能就需要考量以較低的安全性等級來管理成本較低的裝置。這並不表示任何或所有裝置都不應該擁有可接受的基本安全性等級，反倒應該根據裝置類型和實作來確定可接受的等級。

但是，安全性也不能完全只考量成本。我們已經說明系統受到攻擊的可能性，更大部分取決於位置而非實體裝置。幸運的是 (雖然結果不一定總是不幸的)，系統的存取能力與消費者的成本之間存在著關聯性。例如，物聯網燈泡通常透過諸如 Zigbee 之類的短距離無線連線技術連線，因此無法直接透過網際網路存取。如此也將降低這類系統可能帶來的風險：無法直接存取使用者的區域網路、攻擊者無法直接透過網際網路存取、不包含機密資料，而且需要的處理或頻寬資源極其有限。

不過攻擊者仍有可能利用燈泡幫助判斷是否有人在家，因此安全性對於這樣的產品來說仍很重要，但是這些裝置通常會透過集線器來存取或分組，而集線器則會提供額外的安全性功能。最後，這一切都會在路由器或防火牆的後面連線，它們能夠為內部網路提供更多的安全性防護 (希望如此)。

總結而言，燈泡可能不需要高等級的安全性保障，但是燈泡所連線的集線器卻可能需要。儘管網路具備任何其他安全性功能，但路由器和防火牆及其他可透過防火牆直接存取網際網路的裝置，都需要最高等級的安全性。

這些為我們提供了分層檢視的概念，以層次考量家庭、辦公室或其他環境中系統所需的安全性等級，並依據系統本身的存取能力與價值來定義。下方說明了此類分層方式。

與需要更高等級安全性的網路周邊裝置相比，那些不易存取的系統、且擁有較少寶貴資源和資料的系統，可能只需要符合較低等級的安全性，以及較低等級的安全性保障。當然，這些可接受的安全性等級絕大多數是取決於物聯網系統的部署和使用方式，而製造商通常很難在賣出產品前即能判斷要用哪些方式。客戶實際上可能決定使用 Wi-Fi 燈泡並直接將其連線到網際網路，然此將增加風險，因此更需提高安全等級。

## 裝置需要多高的安全性保障？

**高度保障**
可直接從網際網路存取的裝置

網際網路周邊或安全性裝置

**產品範例**
- 攝影機
- 嬰兒或寵物監視器
- 路由器、數據機
- 連線網際網路的集線器

**高度至中度保障**
具「智慧型」安全相關功能，且可能會或可能不會直接連線網際網路的裝置

可存取網際網路的裝置

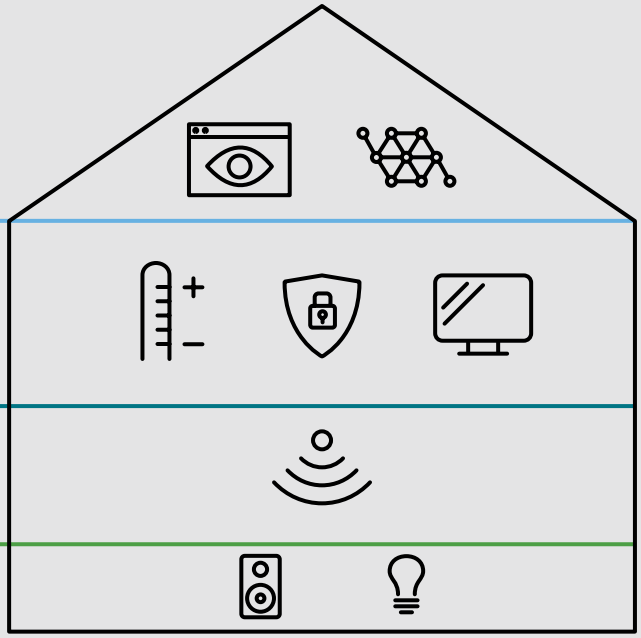
- 加熱器
- 門鎖
- 電視
- 語音控制喇叭

**中度至低度保障**
將網路橋接到區域網路，但不會直接連線網際網路的裝置

- 本地端集線器
- 橋接器
- 存取點

**低度保障**
未直接連線區域網路的裝置

- 藍牙喇叭
- 燈泡 (非 Wi-Fi)



不過，我們可能需要透過對一些一般性問題的回答，幫助判斷系統可能帶來的風險，進而決定所需的安全性等級。右方表格提供了相關資訊，說明由高等級到低等級保障的建議。對任何系統而言，最重要的一個項目是預期的等級。例如，考量一個藍牙門鎖 —— 此類門鎖只能透過非網際網路的可路由連線方式進行存取使用 (建議使用較低等級的安全性保障)，然而由於門鎖卻是提供了與物理安全和安全性相關功能，故本身就會適合使用較高等級的安全保障。

製造商和供應商可以使用本頁所列表格以更易判斷其產品所適用的最低保障等級。更高一定會更好，且有助於增加產品在市場上的差異性。本表格僅供初步指南所用，幫助產業判斷適合的最低等級。

隨著物聯網總體安全性的成熟度提高，可預期的是本文所述的這些建議可能也會跟著改變，或者各個等級需求及保障亦可能隨之更新。此類似於澳洲新車評估計劃 (ANCAP) 汽車安全標準會與時俱進，因為汽車安全性提高即會涵蓋更多的安全要求。

我們已經擁有可幫助判斷裝置適合等級的指南，現在還需要一種方式，以便向物聯網系統購買者說明系統實際可達到哪一種安全性等級、如何評估系統安全性等級，以及提示系統部署所預期的安全性等級。如果使用者打算以可能帶來更多風險的方式部署 (例如將系統連線到網際網路並用於儲存或處理機密資料，或將系統連線到其他高價值系統)，即能選擇成本可能更高但安全性等級也更高的系統。

安全性評估系統的角色是提高基本安全性，也使客戶能夠選擇符合需求的安全性選項。

| 系統範圍問題 | 建議的最低安全性保證等級 |
|---|---|
| 系統是否實作與安全或保全相關的功能，例如 HVAC 控制、網路或物理安全性？ | 高度 |
| 系統是否需要或可以設定以建立與網際網路的直接連線？ | 高度 |
| 系統是否可以存取機密資料，例如視訊或音訊錄製內容，付款明細等等？ | 中度至高度 |
| 系統 (即使是連線至其他系統的集線器) 是否允許直接連線到網際網路 (向外連線，而非上述說明的向內連線)？ | 中度至高度 |
| 系統是否當作不同網路與客戶區域網路之間的集線器或橋接器，但未直接提供網際網路存取? | 中度至低度 |
| 系統是否只能透過低頻寬、非網際網路的可路由網路 (例如 Zigbee 或藍牙音訊) 存取? | 低度 |

# 安全之旅

評等系統安全的另一個價值是，其有助於鼓勵各界對物聯網安全的投資和重視，而不是僅提供二進位安全/不安全輸出能力。期待明天發表的所有新產品，都將自動達到可以設定的最高安全性標準是不切實際的 —— 事實是，我們只能透過徹底地重新設計，或者在產品的設計、製造、運輸及維護方式上進行大規模的文化改革，才有機會實現這些最高等級的安全性。

這代表了通過/失敗的安全性計劃所面對的不確定性難題。我們是否要將需求等級降低到現今大多數產品都可以達到的最低等級、是否了解這並不是我們實際想要達到的最終等級，或是否要將標準設定為我們認為應該達到的最低等級，然後期待產業技術的發展提供我們需要的等級？

如果將所需等級的下限設定得太低，我們至少要能針對最低需求進行一些驗證，但是這樣一來，企業就不會有想要超越這些需求以表對客戶關注或取得客戶認可的動機。假若將所需等級的下限設定得太高，我們即能夠確保符合這些需求的產品會非常安全，可是若沒有任何裝置能夠達到該等級，而造成整個產業失去動力的話，也不是一個好的結果。

上述的兩種方法，皆無法向消費者提供不同產品該如何採用及實作安全性做法的相關有用資訊。


# 透過評等解決物聯網安全問題 – 商業解決方案

推動提高物聯網系統安全成熟度時，需要充分了解推動物聯網設計和部署的商業層面，以及不同產品類型和用途所需保障等級所對應的風險。該風險是由許多不同因素造成的：系統可以存取哪些資料、系統擁有多少頻寬和處理能力、系統可以存取或控制哪些其他系統，以及可存取及破壞物聯網系統的難易程度。

在理想情況下，可以將物聯網安全性客觀地分為二進位安全/不安全，不過在實作上這是不可為的，並且無法公平代表產業所付出的努力。實現最高等級的安全性並不會偶然發生，而是安全的產品設計和安全性測試都需投入時間和金錢才能完成。這將影響產品的商業生存能力，也可能降低廠商將錢花在讓新一代裝置達到所需安全能力的意願。

隨著最低限度物聯網安全性的立法規定，以及各行各業的機構都在制訂本身產業相關的物聯網安全要求，哪些是能夠讓產品同時符合法規且具備市場競爭力，同時仍能維持產品應有的商業生存時程的最佳方法？

為回答上述問題，我們不能期望所有系統從一開始就具備最高的安全性 —— 這在商業模式是不可行的預設立場。相反地，我們需要採用分階段的方法來解決物聯網安全問題，並為所有裝置提供最低等級的安全基礎，同時針對面臨更大風險的系統提高安全性。

隨著時間及市場對安全需求和設計的了解程度提高，即能提高等級，且可套用這些等級的系統數量也會增加。這樣的認知將有助於增加安全系統的商業化壓力。目前，客戶或者已經完全放棄物聯網安全性，或者只是在未真正了解的情況下期待引入安全性。若要解決此問題，我們需要讓消費者更了解安全性。但是如果不區分等級，我們就只能一直接受通常可以達到的最低等級，或防止採用安全性要求變化太快的安全性標準。

改善安全性必須與產業合作而不是與之抗衡。我們必須提供解決方案，而不是簡單地將問題分類，且同時要確保能夠解決安全性的商業層面問題。為達到此目標，我們必須能夠很容易向消費者說明哪些產品在安全要求上投入了更多時間和精力，而這些就僅能付諸評等方法來加以實現。

哪種評等最適合您或您的產品？若要回答這個問題，您需要明白所面對的市場、客戶及使用的技術。本文件中介紹的分層方法採用和存取與資產有關的資訊，藉此提供更快速判斷等級的方法。

**若要深入了解，請電郵至 IMSecurity@ul.com 與 UL 聯絡，或瀏覽 IMS.UL.com/IoT-Security-Rating。**

## UL 網路安全

在 UL 物聯網安全解決方案中，UL 的物聯網安全等級加入愈來愈多的清單，其中包括 UL 供應商網路信任等級、UL 網路安全保障計劃、IEC 62443，以及其他訓練和諮詢服務，其可針對整個生態系統、供應鏈安全和品質，以及受安全性監管的市場進行安全性評估。

## 關於 UL

UL 運用科學，解決產品安全、資訊安全、以及永續發展等各方面的挑戰，讓全世界各地的人們，享有更安全的居住與工作環境。我們透過安全採用創新的產品和技術，加強客戶對我們的信任。UL 的所有員工秉承相同使命，讓這個世界變得更安全。從獨立研究和標準開發，到測試和認證，再到分析和數位化解決方案的提供，我們所有的工作皆以協助改善全球福利為核心。企業、產業、政府、監管機構和社會大眾對我們的信任，將促使所有的人能做出更明智的決策。

欲深入了解，請造訪 UL.com。

UL.com



0220