利用工業 4.0 網路安全創造商業優勢

Empowering Trust™

執行摘要

雖然對工業 4.0 和工業物聯網 (IIoT) 的介紹已有很多，但其供應鏈功能變得愈加複雜。就此而言，整合供應鏈成員之間的流程至關重要。

現在，隨著第四次工業革命 (即所謂的工業 4.0) 的興起，有大量機會整合公司及其資源並建立它們之間的連線，在時間、資金和效率方面提高效能。在本白皮書中，工業 4.0 是指越來越廣泛地使用技術（特別是用於自動化和通訊的數位技術）提高工業生產力、效率和競爭力。

依照工業 4.0，大多數公司都在經歷程度更高的供應鏈數位化轉型，結合使用一系列完全整合的規劃與生產解決方案，在價值鏈的各個接觸點建立更加可視化的供應流。當然，還有許多其他應用場合 (包括 IIoT)，越來越多涉及到現代供應鏈的幾乎每一個環節。

所有這些技術都有共同之處，即數位化，其設計宗旨是為了實現工業和相關流程簡化以及最佳化，改善業務效率、準確性、透明度、責任制、靈活性和敏捷性。工業 4.0 如此快速推進也不足為奇。

然而，數位化供應鏈也有巨大風險 (包括受攻擊面增大)，讓網路犯罪分子有發動駭客攻擊的可乘之機。與只有少數幾個存取點的相對封閉網路的情況不同，數位化供應網路會產生許多潛在漏洞，它們可能跨越很廣的地域範圍，並可透過許多個人、系統或裝置遭到利用。

工業 4.0 對供應鏈的實際影響很難量化。全世界都依賴於工業系統完成日常數位化流程。因此，如果使用複雜的網路或物理攻擊手段入侵該等系統，那麼這種依賴性就會產生網路安全漏洞。

複雜性往往是安全性的大敵。隨著供應鏈因更高程度的數位化所具有的互連性而變得愈加複雜，越來越難以將安全性保持在可接受的程度。

本白皮書旨在確定和分析這些漏洞，使製造商能夠制定長期規劃和業務永續發展策略，包括利用網路安全作為業務優勢。

供應鏈安全挑戰

目前處於各個工業 4.0 轉型階段的傳統製造業很少有明確的安全計畫，一般也缺少能考慮到安防與安全兩方面的綜合計畫。

鑒於工業資料的商業價值以及工業間諜的可能性，工廠更容易成為網路犯罪分子的攻擊目標。工業遭到攻擊的可能性也更大。沿著供應鏈傳輸的資料（例如從製造商或維護人員到裝置）可能被攔截、篡改或重新導向，造成設備故障、資料洩露、輸出受影響，甚至工廠關停。裝置可能遭到入侵或其軟體被篡改，導致存取憑證失竊，進而造成設備失控。

工業企業挑戰

對於製造業，數位化轉型帶來特定挑戰。例如：

- 設備的資本成本高、生命週期長（數十年），透過升級「換代」解決問題會讓大多數企業承擔不起。因此，數位化轉型必須循序漸進。
- 許多工廠都要將陳舊系統納入工業 4.0 網路安全措施，而可用時間可能有限（取決於設備生命週期）。由於工業應用標準和協定多種多樣，其中許多都未曾考慮安全性，因此導致問題加劇。
- 製造供應鏈元素的數位化轉型過程可能處於不同階段，難以整合。
- 必須確保第三方提供者的網路安全，因為某些第三方（例如維護或原始設備製造商 (OEM)）需要直接存取設備和系統。
- 需要轉變文化：傳統上，製造業一直以保護人員和設施設備為重中之重。現在擴大重點範圍，將網路安全包括在內可能是一大轉變。
- 工廠需要量身定制的網路安全功能，不僅考慮普通的監控、預防和阻止方法，還要涵蓋特殊的設備和作業。
- 工業設備等製造元素內在網路安全設計是一個新興領域，但其自身也面臨挑戰。
- 在某些情況下，新增網路安全措施可對作業流程或結果產生影響。

缺少安全性可對業務連續性、可靠性和產品品質造成重大影響。鑒於相關作業的重要性以及對安全的連帶影響，工業 4.0 也不例外。

打造解決方案

就保護工業 4.0 資料和資產安全而言，角色和方法各有不同，具體取決於各家公司的角色及其在供應鏈中的位置。例如：

資產所有者要全面關注整條供應鏈全程營運的安全性、業務連續性和風險管理。

系統整合負責人主要關注系統和流程安全和韌性以及所需能力。在一定程度上，他們的角色與維護經理重疊，而維護經理也要考慮設備生命週期（這意味著展望未來數十年），以及隨著設備資產和要求變更而不斷納入安全措施。

最後，元件和產品製造商不僅希望獲得安全供應鏈所帶來的商業優勢，還要證明這種安全性包含於產品之中。

網路安全是共同的責任。就 IoT 和工業 4.0 而言，由於供應鏈紛繁複雜而且涉及到諸多方面，這一點更加關鍵。因為有許多參與者以及由此產生的相互依存關係，所以合作對保護工業 4.0 至關重要。由於不同的供應鏈參與者可能受到不同的國家立法框架約束，在各個層級和階段都有可能發生安全事故。這種事故可能與商品、服務或資訊交換有關，導致整條供應鏈中的錯誤和風險增加。在這些複雜的供應鏈中，確定問題原因非常困難。這就需要使用更普遍適用於不同相關方（而無論位於何處）的安全標準和解決方案。

符合標準

雖然每個領域和公司都有各自的挑戰，但工業 4.0 實施（特別是這一背景下的網路安全）現已發展到法規、標準和架構皆已建立的成熟度。

目前適用於世界各地工業 4.0 網路安全的法律法規範例包括：

- NIS 指令（歐盟）
- 一般資料保護規定（歐盟）（在英國，GDPR 已納入資料保護法，因此依然適用）
- 能源政策法（美國）
- 國家標準和技術研究院 (NIST) 網路安全架構
- IoT 安全法 SB-327（美國加州）
- NERC 關鍵基礎設施保護 (NERC——CIP) 標準（美國）
- 第 13920 號總統政令「保護美國大容量電力系統安全」（美國）
- S.3688 能源基礎設施保護法（提案——美國）
- 新加坡網路安全法
- 2016 年中華人民共和國網路安全法

鑒於當今市場的全球性，組織不僅要證明其產品和流程具有極強的安全性，還要符合全球監管要求。因此，系統要有內在安全性，根據既定標準定期測試和驗證。

標準與獨立安全評估相結合，可幫助組織及其供應商充分瞭解監管要求、採購和品質保證流程。實現這一目標的最佳方法是，透過獨立評估證明產品、流程和整套系統的安全做法值得信賴。

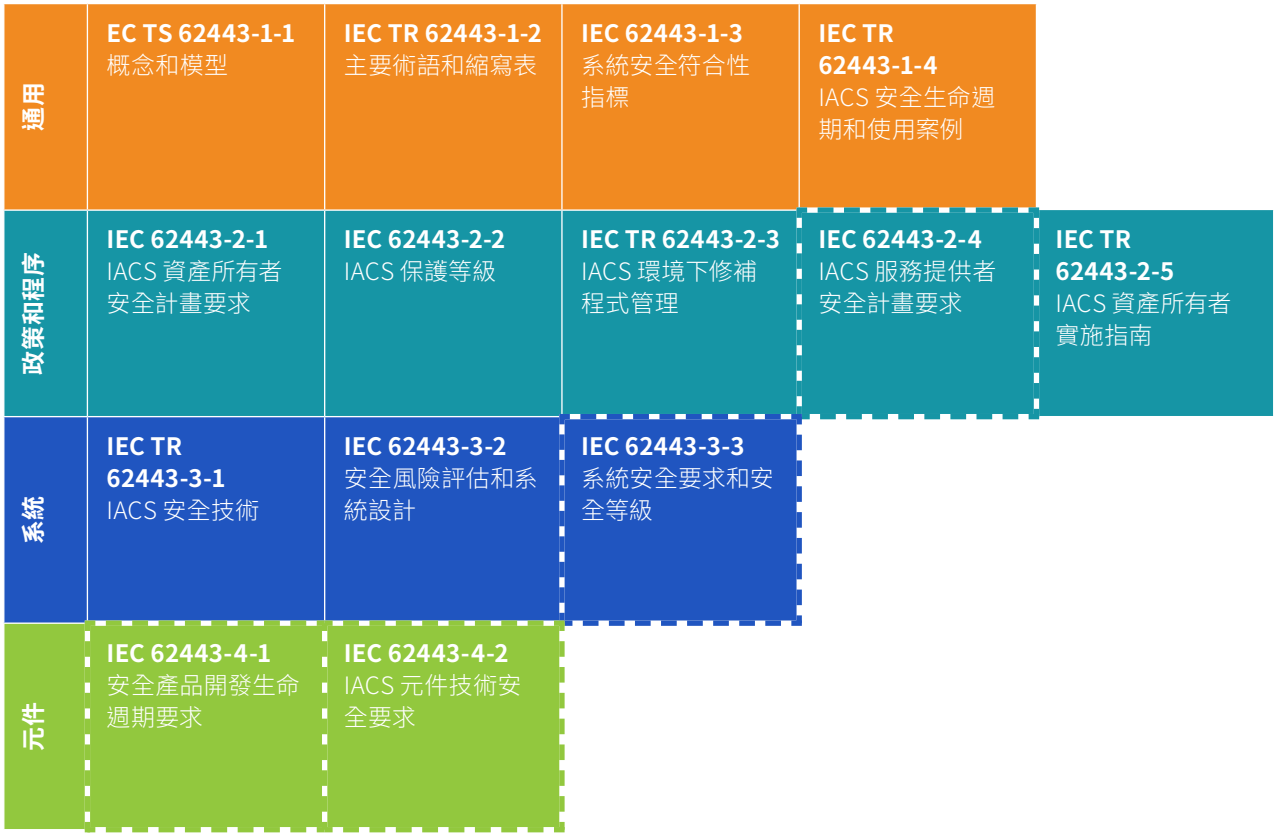
利用獨立安全評估機構也有助於管理供應鏈中的第三方風險，特別是處理供應商安全問題，以及促進第三方風險管理的規劃和實施。NIST 預測，98% 的製造商將在未來兩年內遭遇供應鏈中斷，其中大多是由供應鏈網路安全問題導致。就像網路安全的多個方面一樣，第三方風險管理也至關重要，而且可能變化頻繁。達到較高成熟度以及穩定可靠的安全狀態是當今 CISO 和領導團隊的主要關注點，而供應鏈網路安全正是其中的重中之重。

IEC 62443——確保不同的供應鏈參與者符合嚴格的網路安全要求

值得注意的是，需要調和工業 4.0 安全標準，而這正是國際標準 IEC 62443 的用武之地。制定 IEC 62443 系列標準之目的是為網路安全完善性奠定基礎，確保為工業 4.0 提供支援的工業自動化和控制系統 (IACS) 安全。它為公司提供實用的系統性方法，可用於保護工業系統安全，涵蓋從風險評估到營運的方方面面。

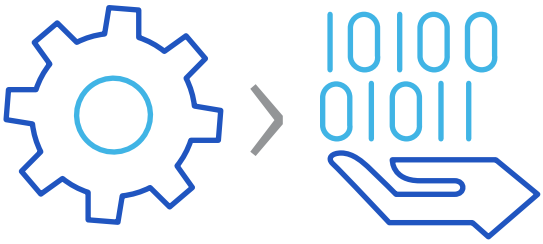
此外，IEC 62443 標準還涉及：

- 安全產品開發和維護流程
- 元件、產品和系統安全
- 系統執行安全架構和組織流程



各項 IEC 62443 系列標準專用於製造商、系統整合商以及終端使用者。對於元件和產品製造商，符合 IEC 62443 標準有助於證明系統和元件的安全性並提高市場地位。對於工業控制系統 (ICS) 整合商和控制系統使用者，符合 IEC 62443 標準可以有效增強品牌保護和擴大競爭優勢。這意味著，IEC 62443 認證的價值 (特別是在值得信賴的第三方認證機構提供認證的情況下) 遠超工廠車間範疇，並有助於驗證整條供應鏈的安全措施。

對專業知識的需求



鑒於工業 4.0 和 IIoT 發展演變，技術不斷進步以及監管機構對嚴格執行安全監管的意願增強，必須持續監控和升級工業 4.0 安全系統。它們必須能夠應對數十年內不同的工廠、技術變革以及不斷變化的威脅。

這一切都是在監管愈加嚴格的背景之下。

許多情況下，必要的知識超出內部 IT 人員的能力範圍，因此工業網路安全本身很有可能迅速成為一個專業領域。根據這一點，公司可能招聘相關員工或與專業第三方公司合作，對自身設備、供應鏈完整性與產品進行網路安全性的測試和驗證。

與一家備受推崇的專業第三方認證機構合作評估、測試和驗證網路安全協定不僅可以高枕無憂，還能建立客戶、潛在業務合作夥伴和利害關係人的信任和信心，使其更有可能青睞公司、產品或品牌。

網路風險形勢轉變的影響

現在，工業領域處於歷史轉折點。工業 4.0 帶來絕佳良機，但也存在重大風險。如果製造商可以適當降低風險，潛在收益將非常可觀。

工業企業資料和數位通訊的價值愈加明顯。如果應用得當，透過工業 4.0 和工業物聯網 (IIoT) 實現的數位化轉型可以：

- 實現生產效率最佳化，縮短停機時間並降低成本。
- 產生有意義的客戶行為和偏好洞見，可以轉化為新產品線和更好的客戶服務。
- 簡化供應鏈和運營流程。
- 整合舊系統資料，全面改善整個企業從高管到基層各部門營運。這會產生可靠的綜合資料集。
- 確保為戰略和營運決策提供支援的資料準確無誤
- 使經理能夠全天候檢視所有資料，並對持有的資料及其所在位置瞭然於心。
- 促進監管合規以及合規文件記錄
- 提高企業可靠性、安全性和品質優良的聲譽

然而，由於需要高可用性，技術負債和陳舊系統成本高昂，而且需要提供安全的工作環境，工業 4.0 也面臨獨特的挑戰。大多數高科技 IT 企業都很難達到成熟的安全狀態，而且必須認識到，在工業環境下也很難做到這一點。

即便如此，仍要採取安全措施。當然也要指出，工業 4.0 並不在於 IT 安全，也不總是使用在商業環境下適用的規則，就能輕易解決問題。

如何瞭解並降低 IIoT 和 IT 基礎設施面臨的風險？

簡而言之，廣泛參與。孤立不能保證工業 4.0 安全。它是注重各部門和領域透明、整合以及資料分享的理念。公司必須規劃出資料及其傳輸路線，在多點收集資料，在各個站點和營運場所聚合資料並在需要時保護資料。只有這樣才能實現資料的真正價值。

與任何其他企業一樣，工業 4.0 企業網路安全也是高級戰略問題。業務計畫必須納入網路防衛，對解決安全問題的需求必須為人所知並從上向下傳達。

企業必須制定策略，積極動員全體員工以傳達文化變革。大家都要將網路/IIoT 基礎設施視為應該管理並挖掘價值的一項資產，而不是各個角色和部門的集合。只有在員工瞭解企業網路的情況下（所有裝置和潛在漏洞都要確保安全並定期更新，即使被視為過時或在企業中微不足道），IIoT 網路安全文化才能發展。安全責任必須由整個組織共同承擔，而不是全都推給 IT。

工業 4.0 安全不是 IT 問題，而是全公司的問題，通常（但不總是）都有需要套用的 IT 解決方案。

當然，企業也可採取一些常規措施保護網路和連線系統安全（例如儘可能減少存取權限，適當使用邊緣計算和雲端，自動執行安全工作和建立完善的驗證協定），但最終還可能需要招聘新員工或取得第三方專業知識。在該領域內，網路安全不斷變化，而其面臨的威脅也是如此，工業同樣面臨可能超出標準 IT 部門範圍的特定問題。專業第三方可就最佳做法提供建議，分享切實可行的經驗以及持續提供安全品質認證。

利用網路安全作為企業資產

網路安全對製造業的價值顯而易見，但其作為企業資產發揮的作用經常被忽視。這很遺憾，因為糟糕的安全性可對公司聲譽造成災難性影響，而良好的安全性則可提升公司的聲譽。

客戶與合作夥伴組織對網路安全問題的意識日益增強，他們根據這種意識做出選擇。在該領域內以其高標而聞名遐邇的公司（最好是有記錄在案的定期測試、評估和升級加以證明）很可能獲得優勢。

這一問題對於尋求與製造商合作（例如在虛擬或智慧工廠領域內）的企業特別重要，因為企業知道自身聲譽可能因合作夥伴而被降低或提高。

完善而成熟的網路安全也有助於招聘員工，降低財務成本（例如保險）和增加商業機會。

綜合運用

現在，製造商需要採用工業 4.0 模型，而在大多數情況下，這都意味著加入 IIoT。必須分享資訊，產業才能發展。如果資訊安全，對大家都有利。

幸運的是，有助於明確要求的協定和標準現已建立。這些協定和標準對所有公司都是彌足珍貴，而無論他們在數位化轉型之旅中前進多遠。使用 IEC 62433 作為黃金標準使企業能夠將完善的網路安全有條不紊、切合實際地納入工業 4.0，使利害關係人確信公司已實現營運最佳化，並使各方（從供應鏈合作夥伴到終端使用者）均可獲得更大利益。

如需瞭解更多資訊，請瀏覽 UL.com 或傳送電子郵件至 imsecurity@UL.com。

UL.com

版本編號 (例如 MMYY)