白皮書

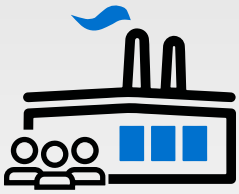
保護工業 4.0 OT

考慮的因素和影響

內容提要

工業 4.0 計劃包括現代化營運技術 (OT) 環境，以提高業務流程效率並透過連接以前孤立的系統為決策提供更多數據。然而，這些系統的融合對安全性產生了重大影響。事實上，10 個組織中有 9 個經歷過入侵，這對生產力、營收、品牌信任、智慧財產權和人身安全都造成了影響。[1] 大多數 (70%) 接受調查的製造業領導者表示，OT 網路資安至少是他們公司面臨前五名的業務風險。[2]

數位化轉型和對數據的日益依賴是普遍趨勢。麥肯錫報告說，COVID-19 加速了變化；數位化應用在短短八週內實現了五年的成長。[3] 在很多產業，數位化轉型的趨勢似乎只會越來越大，製造業也不例外。儘管網路攻擊帶來的威脅顯而易見，但許多製造業正在尋找構建模塊來解決工業 4.0 時代的資安風險。



超過 80% 的製造業領導者預計，他們公司的 OT 安全預算將在下一財務年度增加。[4]

工業 4.0 和 OT 與 IT 的融合

製造業的數位化轉型受到工業 4.0 承諾的推動，因為它代表了第四次製造革命。第一次工業革命是機械化，第二次是使用電力的大規模生產和裝配線，第三次是採用計算機和自動化。現在，工業 4.0 透過以數據和機器學習為動力的系統增強了自動化。工業 4.0 帶來的這一旅程導致了營運技術 (OT) 和資訊科技 (IT) 網路的融合。

OT 環境可能包括運作設備或機器的工業控制系統 (ICS)。它們通常使用可程式化邏輯控制器 (PLC) 進行管理，並且可能包括為 ICS 提供圖形用戶界面的資料採集與監視系統 (SCADA)。 OT 控制設備 ·而 IT 控制數據。IT 側重於確保系統和數據的機密性、完整性和可用性，而 OT 側重於機器安全性和可用性。

工業 4.0 涉及在製造技術和流程中採用自動化和數據交換，包括物聯網 (IoT) 和工業物聯網 (IIoT)、雲端計算、認知計算、人工智慧 (AI) 和網路實體系統 (CPS)。然而，工業 4.0 也增加了與 OT 和 IT 網路融合相關的挑戰。

由於其專業化的團隊和控制系統以及經常未修補的遺留技術，使得 OT 網路面臨著更多的風險，這是連結增加的直接結果。這種內部系統與傳統工廠的連接改變了整個 OT 資安生態系統，使得 IT 和 OT 專家忙於保護公司的基礎設施和生產環境。

工業 4.0 的安全影響

工業 4.0 的主要目標之一是讓製造和業務流程保持一致，使生產與業務現實協調一致。這種數據流最好透過一個概念網路來實現；然而，引入外部數據和存取權限增加了駭客入侵和目的在網路實體破壞的可能性。

傳統上，工業安全是透過保持 IT 和 OT 網路彼此完全分離來維護的。這一過程被稱為 “氣隙 (air gapping)”，將脆弱的 OT 設備和科技與公司的網路隔離開來。其目的是要保護他們免受大多數外部攻擊和目標在破壞行動的入侵。

隨著企業轉型，這些網路營運方式的變化必須考慮到網路資安最佳實踐，並且將按比例進行投資，因為製造應用、材料需求規劃 (MRP) 系統、PLC、人機界面 (HMI) 和其他組件等系統現在都是相互關聯的。

當 IT 和 OT 網路連到一個有限的程度時 ·廣泛的網路攻擊可以被重新利用。以前針對 IT 網路存取的攻擊也可以用來攻擊 OT 的目標。針對關鍵基礎設施的網路攻擊有可能不僅是成為頭條新聞，也可能真實造成製造業的工業系統崩潰。

實際上會一次使生產停滯數小時，以數百萬美元的成本破壞敏感材料的中間流程，並使組織面臨潛在的合規處罰。這種針對 OT 的新攻擊向量可以顯著影響公民信任的網路，並且了解攻擊的附帶影響。資源輸送受阻、國防系統癱瘓，甚至對無辜平民的傷害只是攻擊的潛在後果的一小部分。

現在，有近四分之三的組織至少報告了 IT 和 OT 之間的存在基本聯結。[5]

OT 資安風險

OT 尤其容易受到高級威脅和遺留威脅的影響，因為部署的系統通常已有 20 到 30 年的歷史，因為 ICS 經常使用未經身份驗證或未加密的通信，這些系統都處於危險中。已安裝的設備基礎還具有較長的產品生命週期，並且通常由使用不同工業協定的多個供應商提供各種產品組成。安全和持續運作是重中之重，因此像主動掃描這樣簡單的操作可能會導致設備故障並破壞生產並造成破壞性後果。

對網路實體系統的威脅不斷擴大和演變。事實上，與 2019 下半年相比，2020 年上半年的總攻擊量增加了約 35%。[6] 隨著 OT 和 IT 網路的數位化轉型，日益複雜和分散的安全基礎設施暴露了新的漏洞和系統受損的機會。許多組織增加了端點安全解決方案來彌補氣隙保護的損失，但端點資安產品經常孤立運作。通常，它們將單個漏洞或合規性要求作為附加措施來解決，但不提供跨安全基礎架構的任何可見性措施或情報共享。在資安方面，網路營運分析師幾乎不可避免地無法清楚、即時地了解 OT 網路環境中發生的情況。

幸運的是，製造領域的大多數領導者認為 OT 資安是他們今天面臨的前五名最重要的業務風險之一，超過三分之一的受訪者 (39%) 認為它是前三名之一。[7] 大多數領導者似乎都在針對這些擔憂採取行動，MAPI 研究表明，83% 的領導者計劃增加分配給 OT 資安支出的公司預算部分。考慮到他們在整合 IT 和 OT 兩個複雜環境時面臨的各種挑戰，這是必不可少的第一步。

鑑於資源不足、工具或技術不足、缺乏培訓以及威脅的快速演變，OT 網路中有效反應管理的障礙變的很高。儘管存在這些障礙，但製造業領導者已準備好在過渡到工業 4.0 時採取一切必要措施來提升和啟用網路資安最佳實踐。事實上，94% 的受訪者計劃實施新的解決方案來解決他們的 OT 資安風險。[8]

治理、風險和合規性

OT 資安問題還表明需要關注合規性、審計、人員配備、成本和效率。合規性絕不能與安全性混淆，但兩者是相關的。監管機構在合規性問題上的變化加劇了分散的安全解決方案所帶來的複雜性，無論它們是新的法規和標準，還是現有法規和標準的演變。如果沒有具有自動跟踪、審計和報告功能的有效解決方案，組織必須花費大量員工時間來手動匯總和整合相關資料。

遵守主管當局的領先標準可為安全提供基準。在美國，大多數與 ICS 相關標準是由利益相關者承諾保護關鍵基礎設施的部門機構來制定與發佈的。它們通常在 OTCI 部門中是必要存在的機構，但並不總是很容易反應到製造業中的 ICS 要求。

兩個最常被引用的一般 ICS 架構是美國國家標準與技術研究院 (NIST) SP 800-82 和國際自動化學會 (ISA) 62443。另外值得考慮的是最近的 NIST 跨機構 / 內部報告 (NISTIR) 8219，它專門檢查 ICS 網路中行為異常檢測的使用。

工業 4.0 資安的構建基礎

為了進入工業 4.0 世界，製造商正在重新評估其現有架構，重點是降低孤立端點安全部署的複雜性和碎片化。組織還應該重新評估他們的網路計劃，以確保安全實踐隨著業務計劃的發展而發展，作為單一、整合、安全驅動戰略的一部分。組織需要評估他們現在所處的位置，包括他們可用的資源。然後下一步是評估他們的流程並調查提高敏捷性和安全性的選項。有了這些資訊，他們就可以尋求解決方案，幫助他們實現網路資安 OT 系統的成熟。

44% 的組織未追踪和報告產業法規的合規性。[9]

構建基礎 1：評估現狀

網路資安標準可以幫助指導和指導組織制定和實施安全策略。組織應根據既定標準（如 NIST 或 IEC 62443）確定它們的位置以及它們在資安方面的需要位置。透過利用產業專家的建議，管理人員可以增加知識並更好地實現公司的安全目標。

NIST 網路資安架構 (CSF) 為融合安全計劃提供了一個架構，並提供了一種通用語言，以改善 IT 和 OT 之間的溝通、理解和協作。製造商可以利用 NIST CSF 來幫助確保他們的數位化轉型能滿足其組織的業務目標，無論這些變更與人員、流程還是技術相關，都能夠識別並實施所需的基礎架構變更。

在 IEC 62443 標準 提供可用於管理的工業自動化控制系統和減輕安全漏洞的另一種架構。它提供了有關如何選擇有效改善組織的 ICS 防禦態勢同時平衡成本和降低風險的影響指導。

構建基礎 2：資安人力需求

OT 企業需要檢視資安人力的狀態，並確定解決 IT 和 OT 人員之間在文化、目的和原則方面的內在差異。製造商還需要考慮遠端作業的需求。COVID-19 大流行的出現迫使全球遠端工作解決方案的迅速採用，但也帶來了重大資安風險。遠端作業的保護需要對資安系統提出了前所未有的要求，尤其是在雲端和端點領域。疫情大流行後，遠端作業將不太可能消失。

即使提高了網路資安意識和培訓計劃，網路釣魚仍然是一個巨大的問題，企業面臨來自內部威脅的重大風險。內部活動造成的可歸因損害很難追踪，因為這些威脅涵蓋了廣泛的行為和動機。當員工不在現場時，情況就更加困難。製造商必須能够安全管理從任何地點使用任何設備的任何人，包括公司、工廠或倉庫地點的內部員工、高層領導、合同員工和臨時員工等等。

隨著角色、跨職能團隊和協作的不斷變化，複雜的報告關係和所有權的不明確。以前在工業 4.0 之前孤立無援的部門、團隊和個人都將需要平衡和尊重彼此的價值觀，儘管他們經常有相互競爭的目標。CISO、CTO、IT 架構師、CIO、工廠經理和網路分析師都需要考慮持續營運的必要性，並就機密性（IT 的首要任務）和可用性（OT 的首要任務，以及工廠員工的人身安全）。對於持續的業務彈性，組織必須協作以加強企業的資安情況。

構建基礎 3：流程審核

隨著企業進行數位化轉型，技術和業務流程都會發生變化。工業 4.0 講述了如何使流程自動化，這些流程在未來可以分為更少的步驟。工業 4.0 廣泛使用數據來幫助提高供應鏈到客戶體驗的整個業務流程的效率，以做出更明智的決策。

可以從改進中受益的流程可以包括從訂單處理、產品製造、客戶計費或對潛在安全漏洞的檢測和響應等方方面面。在每個領域，都應進行評估以權衡效率收益與業務風險。

組織應該執行此類嚴格的業務流程審查，因為數位化的增加，意味著在以前未彼此連接的系統，將在流程之間收集和共享著更多數據。當組織確定需要改進和投入數位化的領域時，他們還必須確定邏輯上出現的任何資安缺陷或差距。

將效率和業務優化作為優先事項，越來越多的組織正將雲端服務作為流程改進的一部分。製造商正迅速採用更多雲端的服務，例如製造資源規劃 (MRP) 和企業資源規劃 (ERP) 系統。這些系統通常從 IT 和 OT 系統中提取數據，以便快速有效做出決策。確保這些資產的網路資安保護至關重要，因為該架構可以從數據中心擴展到工業系統再到多個雲端。

54% 的工作可以居家完成，希望在冠狀病毒爆發結束後，全部或大部分時間在家工作。[10]

構建基礎 4：更新您的技術

為了支持工業 4.0，組織需要確保他們的 OT 和 IT 安全已準備好應對最複雜的攻擊。全面的網路資安解決方案必須能夠跨越整個攻擊面，跨資安產品共享威脅情報，並自動響應威脅。保護融合的工業 4.0 環境包括五個最佳實踐。

1. 透過對資產進行識別、分類和優先排序來獲得網路可見性

維護組織的 IT 和 OT 環境和資產的最新清單有助於基礎安全規劃和意識。組織無法保護他們看不到的基礎架構的任何部分，因此他們需要最新的設備和在其網路上運作的應用程式清單。這些設備和應用程式應該根據它們的特性和行為進行識別和分析。

2. 網路分段

分段是保護網路環境最有效的架構概念之一。當 OT 網路上的漏洞被曝光時，缺乏或不充分的 IT/OT 分段可以說可以實現更廣泛的利用。透過適當的網路分段，網路被劃分為一系列功能區段或區段網域，其中可能包括子區域或微分段。每個區段網域只能由預先授權的設備、應用程式和用戶存取。新世代防火牆 (NGFW) 定義並強制實施控制區域。NGFW 還定義了管道，這些管道是使重要數據和應用程式能夠安全可靠地從一個區域跨越到另一個區域的通道。

這種區域和管道的建構模型大大降低了廣泛的基礎設施遭滲透和開發的風險。它透過限制攻擊者在 OT 網路內沿水平（東西）或垂直（南北）的方向移動來限制入侵的潛在影響。被授權在特定區域進行特定活動的用戶或設備僅限於在該區域內操作。區域和管道模型需要是動態的而不是靜態的，具有細粒度的存取控制，可以持續監控信任層級並相應地調整安全策略。

3. 分析流量

防火牆用於將網路劃分為區域、網段和管道，但分析網路流量來檢測已知和未知的威脅將同樣重要。OT 組織可以從主要 ICS 製造商那裡獲得針對應用程式和設備的額外漏洞保護。由於許多 OT 設備在沒有修補漏動的情況下運作，因此識別和消除這些漏洞並透過“虛擬補丁”來防止入侵是具有價值的。網路流量應與網路事件一起呈現。無需手動交叉引用數據，智慧基礎架構和應用程式引擎可用於使用憑據發現和反應實體和虛擬基礎架構、本地以及公共和私有雲中的拓撲，而無需事先了解設備或應用程式。

大多數組織（78%）對其 OT 環境只有法進行部分集中的可見性。[11]

4. 存取控制

設備 、用戶和應用程式在存取 OT 環境或其任何分段資產之前需要進行身份驗證。安全身份驗證至關重要。許多最具破壞性的 OT 資安漏洞來自用戶帳戶和密碼被盜，並因用戶被分配不適當的存取層級而加劇。

製造商需要的解決方案是能夠根據實際情況驗證誰和什麼允許連接到網路，並限制他們只存取必要的資源。透過使用控制解決方案，可以強制執行該政策，並根據需要採取適當的行動，而不會中斷或關閉關鍵系統。多因素身份驗證 (MFA) 和鎖定經過身份驗證的用戶和設備的網路能力是重要的功能。網路存取控制解決方案應覆蓋基礎架構的每一個部分，包括邊緣、5G、工業物聯網、混合雲和公共雲。

5. 保護有線和無線存取

過去，OT 網路基礎設施在工廠營運中較少依賴無線連線。然而，越來越多的 OT 組織正在其 OT 環境中部署傳感器和其他 IIoT 設備並使用無線網路進行連線。擴大這些連線的範圍和頻率會按比例增加數位攻擊面。無線接入點 (AP) 和網路交換機是具有吸引力的網路攻擊目標。接入點和交換機都需要安全設計，從一個中央介面進行管理，而不是透過多個介面管理的附加端點安全來保護。集中安全管理不僅可降低風險，使政策更容易執行，而且還可以提高可視性，最大限度地減少安全和營運團隊的管理時間。

構建基礎 5：增加可操作的情報和報告

除了網路資安最佳實踐之外，為工業 4.0 制定全面的資安戰略還應包括整合和自動化的威脅情報共享與合規報告。CISO 需要一種主動的 OT 資安解決方法，該方法可以擴展並自動將發現的任何工業威脅的存在傳達給 OT 生態系統。應部署可操作的情報，以主動防禦 OT 環境和每個安全元素。它應該從數據中心和中心園區跨越到網路的邊緣。

通往工業 4.0 之路

為了充分利用當今不斷擴展的數位商業模式並在工業 4.0 時代創造價值，製造商必須解決 OT 資安這一關鍵問題。在支持工業 4.0 並對其 OT 環境進行現代化改造時，他們使用安全第一的方法分析和建構轉型戰略都至關重要。透過先分析當前狀態、資源和業務流程改進計劃，可以將其與技術改進和安全相結合，以幫助實現目標。

建立一個包括可見性、控制和持續監控的環境將幫助製造商保護支持其工業 4.0 計劃融合 IT 和 OT 網路。採取措施確保戰略保持敏捷，將使他們能夠適應業務、產業和技術的未來變化。

[1] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[2] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[3] Aamer Baig, et al., "The COVID-19 recovery will be digital: A plan for the first 90 days," McKinsey Digital, May 14, 2020.

[4] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[5] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[6] "Microsoft Digital Defense Report," Microsoft, September 2020.

[7] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[8] Ibid.

[9] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[10] Kim Parker, et al., "How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work," Pew Research Center, December 9, 2020.

[11] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

FORTINET

www.fortinet.com

July 15, 2021 5:18 PM
989802-0-0-EN