白皮書

工業防火牆層層把關 保衛工控網路安全

www.nexcom.com

工業自動化促使工控網路接軌標準化乙太網路，固然成就生產智慧化，為工廠管理人員帶來即時監控、遠端管理等諸多便利，然也意味著工控網路門戶洞開，提高蒙受惡意攻擊可能性，因此設立工控網路防禦機制已為必然。

工控網路採用業者自行定義的通訊協定，網路環境封閉。然隨著智慧化生產意識抬頭，加上乙太網路普及、連網成本急遽下降，封閉式工控網路逐漸接軌開放式乙太網路，但工控網路一旦開放，將可能讓有心人士乘隙潛入，為避免生產線受到滋擾，工控網路應增設工業防火牆。

深層管理、從嚴管理
把關工控網路資安

持平而論，防火牆絕非新穎技術，防護實力愈見強悍，然新漢電腦 (NEXCOM) 網路通訊事業部產品規劃處處長劉宏益指出，工控網路的應用環境與企業網路迥異，若擬維護工控網路安全，便需採用工業防火牆進行深層管理、從嚴管理。

劉宏益解釋，企業網路架構涵蓋內網 (Intranet)、工廠 (Plant Network)、工控網路 (Control Network) 等三個層次。工業防火牆保護位於內層的工控網路，其目的為控制工廠使之正常運作，資料流量不大，卻皆為操作所需的控制及監視參數，資料價值極高。因此工業防火牆需能支援 PROFINET 等各式現場匯流排 (Fieldbus) 通訊協定，層層拆解資料封包，深入剖析封包結構與封包內容，確保封包的合法性，即所謂的深層管理。相形之下，商業防火牆不支援現場匯流排通訊協定，封包檢測偏重郵件、網頁與檔案傳輸等類別封包，並不適用工控網路。

以汽車組裝線為例，產線上的每個機械手臂皆為一個網路節點，各自遵照控制參數運作。若封包夾帶可疑的動作控制參數，要求機械手臂執行標準作業程序以外的動作，工業防火牆在接獲資料封包後，進行深入封包分析時，便能阻擋該資料封包繼續傳送，協助製造業者防患於未然，避免產線因動作控制參數受到竄改，製造出大量的不良品，徒使車廠蒙受鉅額財物損失。

工控網路安全從嚴管理則是因為生產設備有限定用途，僅執行特定應用程式，因此工業防火牆使用白名單設定，可阻擋所有不在名單內的應用程式。反觀商業防火牆為企業網路的統一出口，通行應用程式五花八門，採行黑名單機制，僅阻擋列舉在名單上的應用程式，放行標準相對較寬，因此工業防火牆更能有效保護工控網路。

除此之外，虛擬私有網路 (VPN) 加密通道更是工業防火牆需支援的重要功能。由於工控網路接軌乙太網路，資訊傳輸將行經公開網路環境。為確保從遠端擷取到的現場資料完整、正確，在公開網路上架設私有通道，並在資料傳輸前先行加密，即便資料遭到竊聽，也難以被惡意破解、竄改。

耐受嚴苛考驗　牢牢保障生產力

工業自動化應用多元，高溫炙人的沙漠油田、火星迸射的煉鋼廠、海風鹽霧交加的風力發電廠所在多有，工業防火牆自需採行強固設計，以在高溫、高濕、高鹽的環境下維持恆常運作。再者，生產設備極為重視效能穩定，對於停機時間有嚴苛的要求，在特殊、關鍵製程甚至不容機器停機，工業防火牆自然亦需具備高可用性 (High Availability)，設有備援機制，在工業防火牆意外故障時，在極短時間內迅速切換，保護工控網路安全。

智慧工廠採用標準化的乙太網路，實現即時監控、遠端管理，對於生產、管理效率提升有莫大價值，不容任何惡意攻擊破壞。歷經 2010 年伊朗核電廠遭駭等重大事件，用戶紛紛對工業設備安全有所警覺，捍衛設備生產力價值的過程中，最可望發揮關鍵助力的工業防火牆，未來發展前景自然看俏。

關於新漢

新漢電腦成立於 1992 年，事業單位橫跨工業電腦、車載電腦、多媒體、網通及智能監控五大應用市場，並於七個主要工業國設有子公司以提供全球服務。新漢電腦專精於產業深耕，目前在無風扇強固型電腦 (NISE 系列)、車載電腦 (VTC 系列)、網通平台 (NSA 系列)、多媒體 (NDiS 系列) 等皆居於領導地位。 www.nexcom.com