以資安確保安全

保護人員、環境與重要的基礎
建設免於工業資安威脅之侵擾

隨著工業營運漸趨網路化，公司也開始著重資安方面的投資以確保其知識產權、營運與品牌之安全。然而，資安風險本身所帶來的安全衝擊卻往往被忽視。透過將安全與資安計畫整合並專注於關鍵步驟，製造商與工業營運者便可在企業聯網中操作、管理與降低資安風險所帶來的衝擊。

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

簡介

工業資安是公司為提升產能、效率與安全性而建置聯網、具資訊功能之基礎建設時的首要考量。

不論是遠端存取生產用機械、無線控制幫浦站台、或將工廠控制系統設備類別與IT架構連結，更強大的連線能力都能明顯提升產能與安全性。不過這也同時提高了風險，除了影響知識產權、獲利與具關鍵任務的生產用資產，也會對人員與環境造成影響。

安全系統的設計是用於偵測錯誤、警示作業人員並自動介入。透過修改或攻擊安全系統，資安入侵便可讓標準控制系統不依照其安全參數運作、損壞設備與環境，甚至讓工作人員與一般大眾陷入不安全的情況中。

連線功能所帶來的機會與風險

企業聯網能將人員、流程與設備串連起來。其將企業層級的IT技術與廠房層級的營運技術（OT）系統整合在一個共用的網路架構中。同時其也善用了包括資料與分析軟體甚至智慧型裝置等創造出物聯網（IoT）技術之資源。

「負則營運、保護與維護ICS的人員必須了解安全與資安間關聯的重要性。任何會損害安全的資安作法均是不應採納的。」

工業用控制系統（ICS）資安原則，NIST

而這對製造商與工業營運者又意謂了什麼？這表示生產智慧能衡量並改善其營運的各個層面，包括品質、生產力、運作時間及整體設備效率（OEE）等。也代表企業能擁有可即時分享資訊及跨部門合作的連線能力。同時還能遠端監控分散在各地點的重要生產設備與系統。

但伴隨著這些機會而來的，也有風險。連線點越多也讓資安威脅有更多突破點。這些威脅可能是實體的也可能是數位的、內部或外部的、惡意的或不小心的。而其所可能帶來的危險很多，包括知識產權的損失、營運中斷及影響產品品質等。

工作安全可能是資安威脅中衝擊中所最少被討論到的。

資安對工安的影響

被入侵的機械與流程安全系統可能會造成一連串的工安問題。

最初，受影響的安全系統可能不會在機械到達危險狀態時將其停止下來，甚至被觸發的安全裝置之保護功能也可能對工作人員造成威脅。此外，無法在超出運作條件時將生產流程停止的安全系統會使員工及整個工廠陷入風險之中，例如火災、化學原料洩漏或爆炸等。

尤其當員工作業包括危險或揮發性原料如化學生產等時，整體風險更高。而隨著自動化機械的導入，當人員與機器人設備合作生產時，整體風險更是有增無減。

受影響的安全系統同時也危害消費者的安全。試想像若網路攻擊改變食品或藥品生產營運的流程時會帶來什麼樣的衝擊。其可能造成危險甚至致命性的污染。即便在受影響的產品離開工廠前即發現受到攻擊，仍可能對需求迫切的產品如藥品等造成出貨的延遲。

同樣的，重要基礎設施的流程後到修改或中斷也會對重要的水源與電力供應造成衝擊。

「餐飲製造商及配送商運用控制系統混合原料、包裝產品並運送人們食用的產品。若這些系統受到修改，可能會對糧食供應造成污染甚至造成糧食短缺。」

關鍵控制系統之弱點與應對之道，SANS機構

當發生具危險性的入侵時

資安入侵與漏洞對於安全所造成的風險不僅僅是理論而已。這已成為現實：

- 德國鋼鐵廠的網路攻擊事件便造成部分廠房停機同時造成高爐無法依正常方式停機。該廠房便受到了「大規模的損壞」。這類的事件說明了資安威脅對於工業營運可能造成的破壞與潛在傷害[1]。
- FDA即警告醫療器材製造商及醫療單位部分醫療設備容易受到資安入侵。其中一個漏洞便是設備可能會受到惡意軟體的感染甚至停機[2]。
- Verizon即曾通報過負責水供應與測量之機構受過這樣的網路資安入侵。在Verizon的報告中有發現無法解釋的閥門與管線移動，包括「負責管理讓水能安全飲用之添加物」的PLC之異常操作[3]。
- 發生在土耳其的輸油管爆炸，大眾雖歸因於故障，但新聞報導卻顯示這其實是駭客的傑作。該起爆炸造成相當於30,000桶原油洩漏。依據彭博的報導顯示「駭客將警報關閉，切斷通訊並將管線中的原油強行增壓」[4]。

重要的風險類型

造成安全衝擊的資安風險形式有很多種。其中重要的風險類型包括：

員工失誤：資安風險並非均出於惡意。事實上，最常見的資安風險其實來自於一些無心之過。包括員工或承包商不小心造成網路連線中斷、將錯誤的程式下載到控制器中或將受感染的裝置與系統連接。這類看似簡單的錯誤若使系統運作超出其安全參數，則可能會產生嚴重的後果。

心有不滿的員工：熟悉公司控制系統及工業網路的現有員工及前員工可算是一種資安與安全威脅。此類事件知名的範例即為澳洲有位員工入侵其前雇主的污水設備控制系統，並造成超過800,000公升未經處理之污水流入當地的公園與河川[5]。

具政治或金錢目的的駭客：製造商的知識產權在駭客眼中往往是利潤豐富的目標。同時，駭客也可能因金錢、競爭或政治目的試圖中斷製造或工廠營運。

商業間諜：以高價值之基礎建設與生產資產為目標，背後有政府撐腰的間諜是持續存在的威脅。美國司法部官員提表示數以千計的公司曾被這類間諜當作目標且此類活動以對國家安全造成「嚴重威脅」[6]。

網路恐怖份子：會以惡意的行為嘗試中斷、感染或癱瘓重要設施。其潛在目標包括核電廠、供水站與煉油廠等。這類的敏感性攻擊案例包括曾有組織透過駭客嘗試取得紐約一座小型水壩的控制權。該次攻擊因當時水壩正進行維護而將網路中斷最終沒有成功[7]。

以資安確保安全

政府已開始與製造業及工業營運者合作關注廠房及重要基礎設施營運的中斷與網路攻擊情況。

「約近半數的資安專家調查顯示在未來三年內，可能或極有可能會有成功的網路攻擊使重要基礎設施停機進而造成人命損失。」

重要機礎設施妥善報告，Aspen機構與Intel資安，2015年

例如，工業控制系統網絡應急響應小組（ICS-CERT）在2015年即針對16種重要基礎建設處理過295起網路資安事件[8]。

其中最處理的三種基礎設施包括：

- 重要製造設施（97起）
- 能源（46起）
- 水資源與污水機構（25起）

而這樣的事件只會不斷增加。企業應該更主動透過資安投入處理這類的安全問題。並將四種重要元素加入其發方法中：

- 標準規範
- 安全與資安整合
- 風險分析
- 降低風險作為

符合規範的重要性

安全標準中有某些要求可協助製造商及工廠營運者透過資安處理安全問題：

- **IEC 61508第7.4節（電動／電子／可程式型電子安全相關系統的功能安全性）**便要求企業若其危險分析發現可能會造成資安威脅的「惡意或未經授權行為」，便必須進行資安威脅分析。可惜的是，遵守本規範的公司並不多。
- 已規劃並於2016年公告的第二版**IEC 61511（功能安全：製程產業的安全儀表系統）**便要求必須針對安全儀表系統（SIS）進行資安風險評估。SIS設計亦必須有能力處理已知的資安風險。

這類要求或許未提供方法，但可作為處理資安相關安全風險的正式原則規範。因此請務必遵守。同時，這些標準本身也會持續更新以協助企業發現安全問題並透過資安作為進行處理。

安全與資安整合

安全與資安過去一向被分開看待，但兩者在分析與降低風險之作法中有許多相似之處。

例如，安全與資安兩者在「存取控制」概念上便是相同的。在兩者之中，均會依企業慣例、風險管理作法、應用需要及產業標準制定政策與程序。同時兩者均致力於保護公司資產，包括人員、流程、設備與知識產權。

希望降低資安相關安全事件的製造商與產業營運者將需要以不同的思維來思考安全的意義。尤其，必須開始思考安全與資安兩者之間的關係。

想了解其關聯，企業應先考慮「安全的三個C」，即業界最佳的製造商所分享的作法：

- **文化（Culture；即行為）**：員工與企業行為 – 包括能協助判斷企業對安全之重視度的價值、重要性、態度、動機與信念等面向。
- **規範（Compliance；即程序）**：包括能幫助企業符合適用安全標準的政策與程序。
- **資產（Capital；即技術）**：包括當下的安全技術及能協助提升安全與生產力的技術。

接下來，企業應思考如何將資安融入這三個核心的安全範疇。例如：

文化：除保護知識產權、程序與實體資產外，資安人員的所有作為均應以保護安全系統為其核心價值。同時EHS、營運與IT團隊間的合作也越顯重要。例如，這三個團隊應針對安全與資安合作發展出協同管理目標，並找出工廠控制系統的重要安全資料需求。同時因為強大的安全文化需要每一位員工參與，故企業均了解安資安與安全間的關係。

規範：對於合乎規範的投入應符合安全標準（如IEC 61508與61511）之資安需要。相對的，在資安上的投入應遵守IEC 62443（「工業自動化與控制系統資安功能」）系列標準（前身為ISA-99）的深度防禦原則及相關原則，並涵蓋公司各層面的安全相關資安風險。

資產：企業應採用內建資安功能的安全技術。同時其也應採用能同時防護安全系統入侵及在發生入侵時能加速復原的資安技術。

完整風險分析

企業應建立公司面的風險管理策略以管理資安威脅與若點以及其對安全性的潛在衝擊。在此策略中有兩個重要的評估：

- **安全風險評估**可確認是否符合現行安全標準規範（包括IEC 61508與61511的資安要求）。本評估應不僅涵蓋標準的作業員功能，也應包含所有人機互動，包括機器設定、維護、清潔與消毒以及訓練與管理要求等。企業也應將既有安全風險分析的作法再擴大到分析來自網路攻擊的風險。
- **資安風險評估**包括企業目前在包括軟體、網路、控制系統、政策與程序甚至員工行為等方面的資安作為。同時也應指出要達到想要之資安強度所應採取的步驟。

雖然這些評估會獨立進行，但其達到公司層及風險管理的目標是相同的，包括保護員工、客戶及環境等。

透過第三方供應商進行此類評估的公司應尋找兼具安全與資安兩項專業的業者。如此有助於確保兩項評估的一致性。

降低風險作法

企業建置的降低風險作法會因其獨有的資安風險及對安全造成的潛在衝擊而有不同。然而，有幾個重要的降低風險作法是製造商與工業營運者應採行的最佳作法：

- **分門別類**：這是此最核心的資安最佳作法。各工廠應將此作法納入其整體深度防禦資安作法的一部分以協助限制對安全系統的存取。具有防火牆的工業級中立區（IDMZ）及資料仲介商可將工廠網路與企業網路安全地區隔開來。同時，利用虛擬區域網路（VLAN）及第2層或第3層交換器階層可建立子功能區，形成較小的信任網域並簡化資安政策的執行。
- **實體存取**：許多企業使用RFID卡管理廠房的存取控制。但實體存取資安功能應進一步對安全系統進行保護。應使用鎖定、封鎖設備防止未經授權的纜線中斷行為並關閉未使用或非必要的連接埠。同時控制盤櫃應上鎖以防止工業用自動化與控制系統裝置受到意外、未經授權的存取。而更進階的實體存取資安技術也正在興起，例如能進行臉部辨識分析的IP影像監控系統等。
- **安全與資安的網路整合**：CIP Safety™與CIP Security™是通用產業通訊協定（CIP）的延伸，屬於EtherNet/IP™的應用層協定。CIP Safety可讓安全裝置以標準裝置的形態同時存在於同一EtherNet/IP網路中，並在發生服務阻斷攻擊時進行安全關機。CIP Security將資料完整性與保密性整合至EtherNet/IP通訊中。在兩者合作之下，具有CIP Safety與CIP Security功能的裝置可防止資料毀損及對安全系統的惡意攻擊。

- **內建資安功能的安全產品：**安全系統及其他硬體應有內建資安功能。例如，使用具金鑰之軟體的安全控制器可確保僅會從信任的來源下載韌體，而操作門則可限制對控制器的實體操作。具有存取控制表（ACL）的工業級管理型交換機亦可確保僅有經授權的裝置、使用者及流量可進入網路中。
- **認證與授權：**可限制對網路架構之有線與無線存取的資安軟體功能。例如，資安認證與授權是人機介面軟體的重要元素，並可限制僅有經授權之人員可存取安全系統。如此有助於防止惡意的以及意外的內部威脅。資安人員可定義***誰***可以存取該軟體、其能執行***何種***特定行為及使用何硬體以及可從***何處***執行這些動作。
- **資產與變更管理：**資產管理軟體可自動找出新資產，並集中追蹤與管理整個廠含安全系統內的設定變更。其可即時偵測惡意的變更，記錄這類活動並將其回報給關鍵人員。若出現意外的變更，該軟體也可存取備份的裝置程式資料進行快速還原。
- **弱點管理：**應發展有助於確保在釋出安全與資安建議後能快速採取行動的流程與程序。包括要有能即時檢視相關建議並判斷其潛在影響的程序。同時也包括建置針對受影響產品的修補程式管理程序。

總結

資安不僅僅是保護資料及確保運作時間。更要保護人員與環境以及人們所仰賴的重要基礎建設與資源。希望能領先這些風險的公司必須符合最新標準之規範、將安全與資安做全面的整合、進行完整的風險分析並以最新技術建立降低風險之作為。

資源

Rockwell Automation有安全與資安兩者均專精的專家可協助公司處理其獨特的資安型安全問題。我們有業界最完整的安全解決方案，包括相關評估等安全服務。我們的工業資安提供包括網路產品、免費工具與資源，並有完整的工業資安服務。我們也了解要建立更安安全的系統需要有更安全的產品。因此我們以強大的資安開發流程從無到有打造出我們的資安產品。

同時我們也與策略聯盟夥伴（包括Cisco、Panduit與Microsoft等）合作，為您的工業資安需要提供一站購足之服務。例如，Cisco與Rockwell Automation便在Converged Plantwide Ethernet（CPwE）計劃中合作開發了一套工業網路資安架構。同時CPwE計畫也提供設計原則、參考架構與教育資源。

1）駭客攻擊造成鋼鐵廠的「大規模損失」，BBC新聞網，2014年12月22日

2）醫療裝置與醫院網路的網路安全性：FDA安全通訊，FDA，2013年6月13日

3）資料入侵摘要，Verizon，2016年

4）神秘的08年土耳其管路爆炸開啓了新的網路戰爭，彭博，2014年12月10日

5）惡意的控制系統網路資安攻擊個案研究 – 澳洲Maroochy Water服務公司，2008年6月23日

6）大腦搶劫，60分鐘，2016年1月17日

7）美國官方指控7名伊朗人參與對銀行與水壩的網路攻擊，紐約時報，2016年3月24日

8）NCCIC/ICS-CERT年度回顧，ICS-CERT，2015年

www.rockwellautomation.com

電力、控制、資訊解決方案總部

美洲地區：Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
歐洲／中東／非洲地區：Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
亞太地區：Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

台灣洛克威爾國際股份有限公司　Rockwell Automation Taiwan Co., Ltd.　www.rockwellautomation.com.tw

台北市104建國北路二段120號14樓
Tel: (886) 2 6618 8288, Fax: (886) 2 6618 6180

高雄市80052新興區中正三路2號19樓A室
Tel：(886) 7 9681 888, Fax:(886) 7 9680 138

出版物SAFETY-WP035A-ZC-P – 2016年12月