淺談關鍵基礎設施之「資料採集與監控系統」(SCADA)

◆ 華梵大學特聘教授 — 朱惠中

資料採集與監控系統（Supervisory Control And Data Acquisition, SCADA）是工業控制的核心系統，主要用於控制分散的資產，以進行數據蒐集與控制，亦屬關鍵基礎設施防護的核心系統之一；本文除介紹 SCADA 外，亦將討論 SCADA 安全的三個規律，以及如果資訊技術防護不足，該如何保護 SCADA。

何謂「資料採集與監控系統」（SCADA）

SCADA 是控制重要、複雜且通常可能具危險性的實體製程計算機系統，其中許多實體製程構成了對現代社會至關重要的關鍵基礎設施。由於這些實體製程功能非常強大，若遭誤（濫）用，常會造成不可接受的後果。故 SCADA 首要的安全機制，即在防止實體製程不能正常運作。

傳統工業控制系統可概分為可編程邏輯控制器（PLC，左圖）、分散式控制系統（DCS，右圖）及 SCADA 等三類。

傳統工業控制系統可概分為可編程邏輯控制器（Programmable Logic Controller, PLC）、分散式控制系統（Distributed Control System, DCS）及 SCADA 等三類，其中 SCADA 是跨越網際網路的工業控制系統（Industrial Control System, ICS），電網、管道和配水系統監控與資料之獲取，均來自 SCADA；而 DCS 是跨越內部網路的工業控制系統。二者差異在於，DCS 是一種不涉及跨越網路的工業控制系統，軟硬體均建置在一個地理位置相對較小的站點中，如發電廠、煉油廠和化工廠均是使用 DCS。另從歷史期程來看，SCADA 和 DCS 的不同處，在於使用一種軟體能否控制所有其他類型的系統，迄今的通用控制系統軟體，則多具有 SCADA 系統和 DCS 的所有功能。

所有 SCADA 的另一個重要關鍵因素則是操作人員，重要工業設施的控制系統，幾乎都有一個或多個操作人員，負責確保實體製程的安全運行；操作人員使用稱為「人機界面」（Human Machine Interface, HMI）軟體的工具，該軟體幾乎包括所有圖形可視化的實體過程狀態，且通常包括警報管理器和歷史趨勢工具等輔助系統。根據政策或法律，操作人員只有高度信任實體製程能被安全運行時，才會允許啟動系統，如遭遇顯示器被鎖定，或者接獲疑似被駭的通知時，操作人員可以移轉控制權到輔助或備份的 HMI 或控制系統。但如短時間內仍然無法認定實體製程能正常運作，通常即須進行關閉。前開狀況通常意味在大多數情況下，攻擊者要造成系統負面影響，最簡單的方法是促成 HMI 某些操作或支持系統的操作失效，使實體製程被關閉；許多工業實體製程的關閉遠比啟動能更快完成，但在緊急關閉後，可能需要數日，才能恢復全部生產能量。

如何保護 SCADA 系統

SCADA 系統架構的一個重要趨勢，是 Gartner 集團在 1990 年代中期創見的「IT/

SCADA 的重要關鍵因素之一為操作人員，重要工業設施的控制系統，幾乎都有一個或多個操作人員，負責確保實體製程的安全運行。

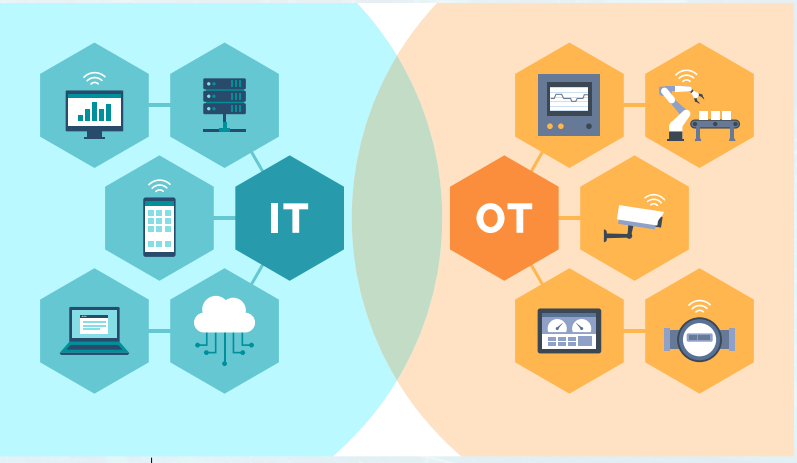
OT 融合」觀念，亦即工業製程網路的架構上，同時存有 IT（資訊技術）與 OT（運營技術）的系統與設備，後更擴張到 IT 和 OT 團隊、業務流程、產品、技術和網路之結合。然而，IT/OT 融合的問題，在於 IT 和 SCADA 網路上使用相同的技術、硬體、操作系統、平臺應用程式及網路組件後，當 IT 和 SCADA 完全互連時，許多攻擊 IT 網路的方法，亦可用以攻擊 OT 網路，加上多數的 SCADA 安全從業人員並不具備現代攻擊技術之防禦能力，因此反而造成 SCADA 的脆弱化。就如何保護 SCADA，學者 Andrew Ginter 提出以下建議：[1]

一、安全程序

大多數 SCADA 安全程序過分強調檢測、回應和復原活動，SCADA 網路安全性必須著重於防止破壞，成熟度模型應用在衡量管理 SCADA 安全程序的業務流程強度，而非衡量程序本身的強度。

二、網路攻擊

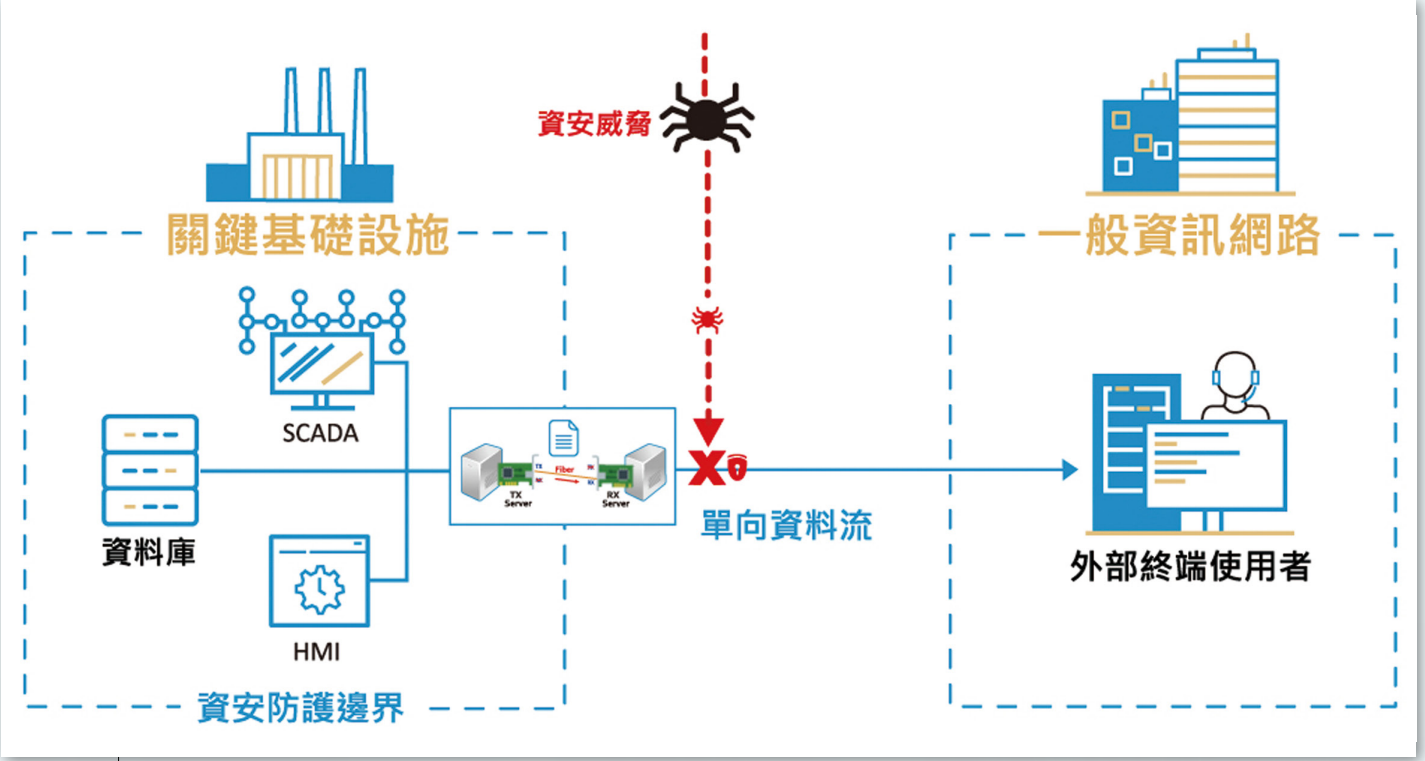
Hacktivist 級攻擊通常透過遠程控制進行，且常經由權限而非軟體漏洞來破壞安全系統；攻擊通常會破壞以 IT 為中心的安



SCADA 系統架構的一個重要趨勢為「IT/OT 融合」觀念，即工業製程網路的架構上，同時存有 IT（資訊技術）與 OT（運營技術）的系統與設備，後更擴張到團隊、業務流程、產品、技術和網路之結合。

Hacktivist 級攻擊通常透過遠程控制進行，且常經由權限而非軟體漏洞來破壞安全系統。

[1] 參考其著作 “SCADA Security: What is Broken and How to fix it”。



單向閘道器為單向通信和數據傳輸的閘道器，能實現跨實體隔離的網路並安全地傳輸數據，防止數據外漏並消除網路威脅攻擊，增強 SCADA 基礎設施的安全性。（圖片來源：創泓科技，https://www.uniforce.com.tw/product.php?lang=tw&tb=1&cid=321）

全措施，特別在高風險範圍內，攻擊面向幾乎沒有限制，從而 SCADA 安全從業人員必須專注於留心攻擊特徵，而非漏洞存在處。

三、風險管理和治理

定量風險評估不適用於 HILF 事件，[2] 因為我們無法可靠地分配這些事件，所以也不應要求決策者根據不確定的機率做出決策，特別是在評估 SCADA 網路保護程度時，決策者對攻擊狀況和影響的瞭解，通常優於主觀的定量風險評分，例如董事會成員常使用一些經驗法則，來判斷安全管理人員提供的資訊是否可信。

四、使用單向閘道器（Gateway）

單向閘道器並非路由器，不會將 IP 或流量資訊從工業網路轉發到外部網路，但可允許外部應用程序和用戶監控安全關鍵和可靠性關鍵控制系統，而不會帶來任何遠端控制或未授權操作的風險，亦即部署越多保護 SCADA 網路的單向閘道器，則越發安全。

五、防止入侵

每個 SCADA 都應具備防禦所有攻擊的能力，強大的主要預防性安全程序，幾乎能消弭所有來自複雜對手的攻擊風險。此

[2] 為 High-Impact Low-Frequency 的簡稱，指高衝擊、發生頻率低的事件，通常以不規則、不可預測的方式發生。

外，應該部署具備包括偵查控制和事件響應功能的次要控制措施，以處理應用主控系統不可避免的錯誤和漏洞等殘餘風險。在預防措施花費的精力與費用，可顯著降低安全程序的運營成本，以及降低 SCADA 受損的風險。

此外，Attila Cybertech 執行長 David Ong 在 2017 年 Hitcon Pacific 大會，也提出幾點幫助思考如何保護 SCADA：

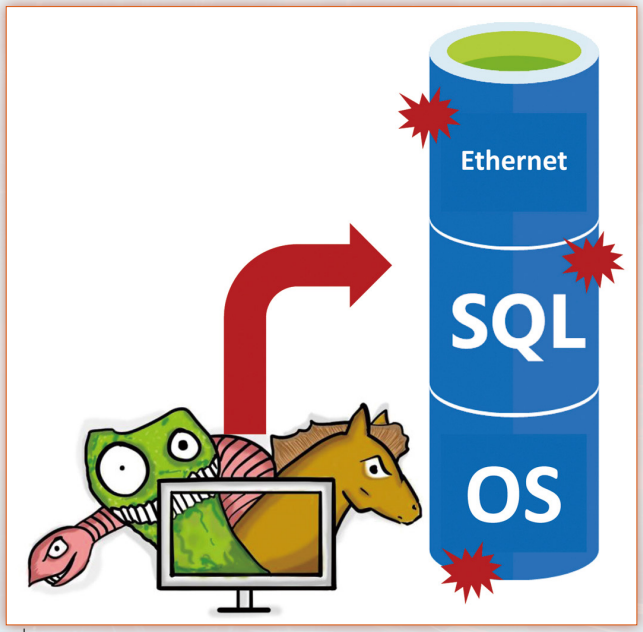
一、在 OT 與 IT 的融合過程裡面，網路安全扮演著不可或缺的角色，但是技術支援與管理作業仍是各自進行。然而，只要牽涉到現場設備與系統監控的 OT 應用，就會與業務或企業系統產生關連性。

二、針對 IT 系統安全性的管制作法，未必能適用於 OT 系統的網路安全防護；使用舊技術規格也是現行 ICS 系統面臨的眾多挑戰之一，因為已長期使用的工業控制設備，幾乎沒有任何安全性功能。

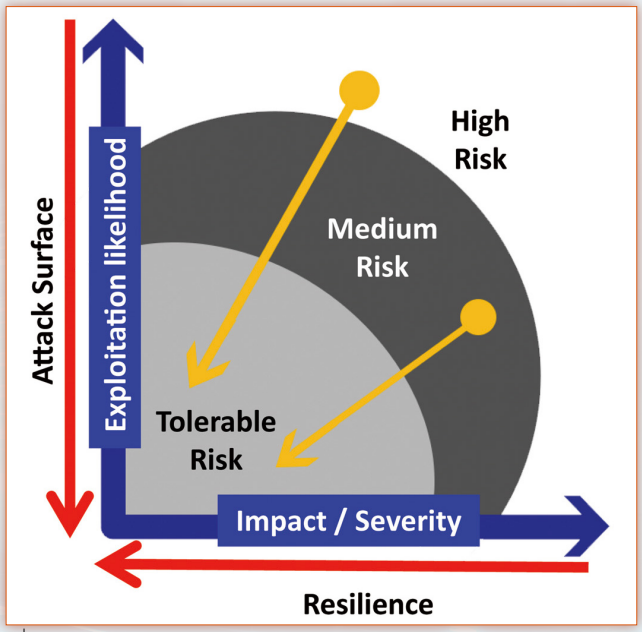
三、建立降低風險、減緩衝擊，以及具備援的運作模式。降低風險意指縮小受攻擊的面向，降低受濫用的可能性；減緩衝擊則是指應設法杜絕或減少涉及導致重大傷害情況發生的機率。

四、由於 SCADA 特別重視系統的可用性，在檢視各種 ICS 安全性的措施時，不只是要留意該如何防禦，同時還要具備快速復原的能力。

五、由於網路安全的重點，是防止在 IT 網路上的攻擊方法被使用於 OT 網



針對 IT 系統安全性的管制作法未必適用於 OT 系統的網路安全防護；而使用舊技術規格的現行 ICS 系統亦幾乎沒有安全性功能，很容易受到病毒的攻擊。（Source: HITCON Pacific 2017, David Ong, https://hitcon.org/2017/pacific/0composition/pdf/Day2/R1/R1-1.12.8.pdf）



降低風險意指縮小受攻擊的面向，降低受濫用的可能性；減緩衝擊則是指應設法減少涉及導致重大傷害情況發生的機率。（Source: HITCON Pacific 2017, David Ong, https://hitcon.org/2017/pacific/0composition/pdf/Day2/R1/R1-1.12.8.pdf）

路，故 SCADA 安全性除專注於防止 SCADA 電腦任何未經授權的存取外，更應找出現有軟體產品的新漏洞，以強化網路安全。

六、SCADA 為控制實體程序，故啟動安全儀表系統（Safety Instrumented System, SIS）比 IT 監控數據及利用備份復原來的重要。

資料採集與監控系統之發展

工業控制系統係指生產過程的核心是被由 SCADA 控制的操作機器所組成，SCADA 早期的安全規劃，在 2003 至 2009 年之間，核心架構為以 IT 為基礎的「縱深防禦」（Defense in Depth, DiD），其基本邏輯包括：

一、IT 專家認為所有網路都持續不斷的受到侵害。

二、入侵檢測和實踐事件通報團隊被 IT 專家視為最佳解。

三、緊急事件通報／處理團隊不斷尋找被惡意程式感染的系統，清除並備份還原。

惟前開架構代價高昂、效果不佳，且無法有效保護 SCADA 免受現代科技攻擊，以及從還原資料中恢復生產損失、修復損壞機械或拯救人員生命。後至 2010 年即產生 SCADA 安全架構修正版，修正邏輯包括：

一、必須優先考慮如何防止 SCADA 受損害，以及實體過程的錯誤操作。

二、實體和網路邊界保護，[3] 是新安全架構必要的保護措施。

三、因 DiD 架構降低風險功能有限，宜將安全更新程序以及加密和入侵檢測系統改為次要措施，以處理剩餘風險。

SCADA 安全的三個規律

為使讀者能更佳瞭解保護 SCADA 的重點，本文簡化網路安全領域，歸納三個 SCADA 安全法則如下：

一、沒有什麼是安全的

如果能提供足夠的時間、金錢和人才，任何安全態樣都可能被破壞，特別是 IT 系統，而只要是人設計的機制，必然存在弱點，使用者必須明確瞭解諸如「我們現在的安全等級是否足夠？」、「我們應該有多安全？」等期待或需求，其實是一種連續統一的單元概念，而非諸如「安全通信」、「安全啟動」或「安全操作系統」等二元值術語。

二、所有軟體都可以被駭客入侵

軟體開發團隊努力消除軟體可能的錯誤或漏洞，但儘管付出最大努力，軟體都仍無法完美，包括安全軟體在內，實務上，

[3] 網路邊界（Network Border）指內部安全網路與外部非安全網路的分界線。

所有軟體都可以被駭客攻擊，修補已知的錯誤和漏洞亦無法使系統無懈可擊，要使軟體系統「安全」的方法，是部署更多的安全軟體。

所有軟體都可以被駭客攻擊。另一個常被誤解的重要觀念，即是有太多使用者認為，修補已知的錯誤和漏洞將使系統無懈可擊，然而，使軟體系統「安全」的方法，是部署更多的安全軟體。

三、每條資訊都可能是攻擊

即使是一點資訊，也可能是一種攻擊。進入廠區的人的大腦中所記憶的密碼和惡意企圖可視為攻擊；安裝在全新電腦上，或藉由 USB 鍵盤等周邊設備進入電腦中的惡意軟體，都可能是攻擊。

小結

SCADA 網路保護的首要任務，始終是在防止未經授權的控制，IT 系統的網路保護則是監控數據，而控制數據遠比監控數據重要得多，每位關鍵基礎設施營運者或 SCADA 控制者不僅能做，也應該要盡力做到預防導致系統發生崩壞的風險狀況。

資料來源:法務部調查局清流月刊
資料日期:2023年11月 第48期