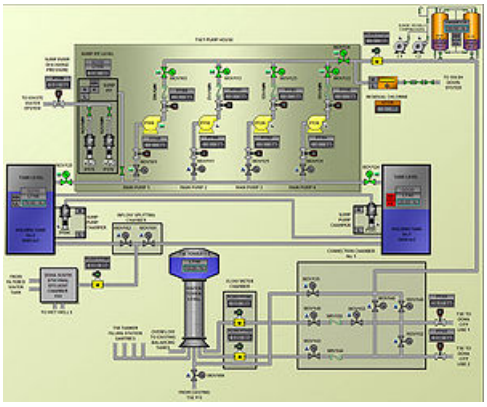
数据采集与监控系统

维基百科，自由的百科全书

数据采集与监控系统（英語：**supervisory control and data acquisition**，缩写为SCADA）一般是有監控程序及資料收集能力的電腦控制系統。可以用在工業程序、基礎設施或是設備中。

横須賀美軍基地的SCADA控制室



發電廠的SCADA範例

目录

系統的組成元素

SCADA系統會包括以下的子系統：

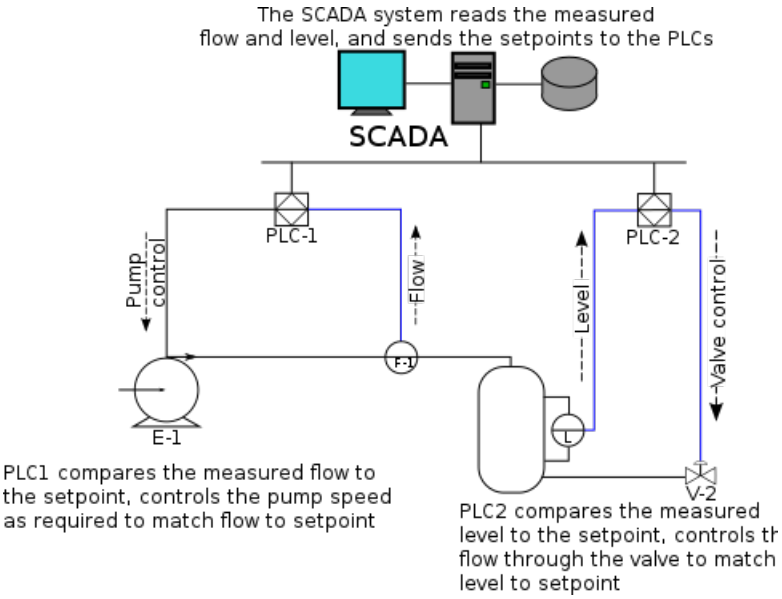
- 人機界面（human machine interface，缩写为HMI）是一個可以顯示程序狀態的設備，操作員可以依此設備監控及控制程序。
- （電腦）監控系統可以採集數據，也可以送出命令監控程序的進行。
- 远程终端控制系统（缩写为RTU）連接許多程序中用到的感測器，数据采集後將數位的資料傳送給監控系統。
- 可编程逻辑控制器（programmable logic controller，缩写为PLC）因爲其價格便

宜，用途廣泛，也常用作現場設備，取代特殊功能的远程终端控制系统（RTU）。

- 通訊網路則是提供监控系统及RTU（或PLC）之間傳輸資料的管道。

系統概念

SCADA一詞是指一個可以監控及控制所有設備的集中式系統，或是在由分散在一個區域（小到一個工廠，大到一個國家）中許多系統的組合。其中大部份的控制是由远程终端控制系统（RTU）或PLC進行，主系統一般只作系統監控層級的控制。例如在一個系統中，由PLC來控制製程中冷卻水的流量，而SCADA系統可以讓操作員改變流量的目標值，設定需顯示及記錄的警告條件（例如流量過低，溫度過高）。PLC或RTU會利用回授控制來控制流量或溫度，而SCADA則監控系統的整體性能。

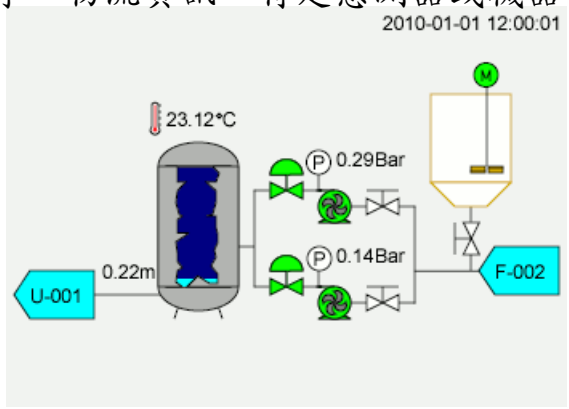


数据采集由RTU或PLC進行，包括讀取感測器資料，依SCADA需求通訊傳送設備的狀態報告。資料有特定的格式，控制室中的操作員可以用HMI了解系統狀態，並決定是否要調整RTU（或PLC）的控制，或是暫停正常的控制，進行特殊的處理。資料也會傳送到歷史記錄器，一般會是架構在商用的数据库管理系统上，以便追蹤趨勢並進行分析。

SCADA系統會配合分散式資料庫使用，一般稱爲標籤資料庫（tag database），其中的資料元素稱爲標籤（tag）或點（point）。一個點表示一個單一的輸入或輸出值，可能是由系統所監視或是控制。點可以是硬體（hard）的或是軟體（soft）的。一個硬體的點表示系統中實際的輸入或是輸出，而軟體的點則是根據其他點進行數學運算或邏輯運算後的結果（有些系統會把所有的點都視爲軟體的點，無視其實際上是硬體或軟體）。一個點通常都是會以資料-時間戳記對的方式儲存，其中有資料，以及資料計算或記錄時的時間戳記。一個點的歷史記錄即可以用一連串的資料-時間戳記對所表示。常常也會在儲存時加上其他的資訊，例如現場設備或PLC暫存器的路徑，設計的註解及警告資訊。

人機介面

人機介面（英文缩写爲HMI）一個可以顯示程序狀態的設備，操作員可以依此設備監控及控制程序。HMI會連結到SCADA系統的資料庫及軟體，讀取相關資訊，以顯示趨勢、診斷資料及相關管理用的資訊，如定期維護程序、物流資訊、特定感測器或機器的細部線路圖、或是可以協助故障排除的專家系統。



SCADA的人機介面[1]

HMI系統常會用圖像的方式顯示系統的資訊，而且會用圖像模擬實際的系統。操作員可以看到待控制系統的示意圖。例如一個連接到管路的泵浦圖示，可以顯示泵浦正在運轉，及管路中液體的流量，操作員可以使泵浦停機，HMI軟體會顯示管路中液體流量隨時間下降。模擬圖會包括線路圖及示意圖來表示製程中的元素，也可能用製程設備的圖片，上面再加上動畫說明製程情形。

SCADA系統的HMI軟體一般會包括繪圖軟體，可以讓系統維護者修改系統在HMI中的呈現方式。呈現方式可以簡單到只有螢幕上的燈號，用燈號表示現場實際的狀態情形，也可以複雜到是用多台投影機顯示摩天大樓中所有的電梯位置或是鉄路中所有列車的位置。

實現SCADA系統時，警告處理是很重要的一個部份。系統會監控指定的警告條件是否成立，以確定是否有警告事件（alarm event）發生。當有警告事件時，系統會採取對應的行動，例如啓動一個或多個警告指示（alarm indicator），或發出電子郵件或簡訊給系統管理者或SCADA操作員，告知已有警告事件。SCADA操作員需確認（acknowledge）警告事件，有些警告事件在確認後其警告指示就會關閉，也有一些警告指示要在警告條件清除後才會關閉。

警告條件可能是外在（explicit）的，例如一個表示閥門是否正常的數位狀態點，其狀態可能是依據其他數位或類比點的資料，配合公式決定。警告條件可能是內在（implicit）的，例如SCADA會定期確認某類比點的數值是否超過其允許上下限的範圍。警告指示可能是警示音，螢幕上的弹出視窗，或是螢幕中某個區域閃爍或是用特殊顏色標示（汽車儀表板上「油料用完」的燈號就最簡單的例子）。警告指示的形式雖有不同，但其目的相同：提醒操作員系統的某部份有問題，需採取適當的對策。在設計SCADA系統時，需特別注意當短時間出現一連串警告事件時的處理方式，否則警告的根本原因（不一定是最早發生的事件）可能會被遺漏補，不被記錄。

在SCADA系統中，警告（alarm）一詞可能用來指稱許多事物，可能是警告點、警告指示或是警告事件本身。

相關硬體

SCADA系統常使用分散式控制系統（簡稱DCS）中的元件。越來越多的系統使用智慧型的遠程終端控制系統（RTU）或可編程序控制器（PLC），可以自行處理一些簡單的邏輯程序，不需主系統的介入。在撰寫這些設備的設序時，常使用一種利用功能方塊來描述的程式語言IEC 61131-3，也就是階梯圖邏輯。IEC 61131-3和C語言或FORTRAN之類的程序語言不同，要訓練一般工程師了解IEC 61131-3所需的時

間較短。因此架設SCADA系統的工程師直接處理在RTU或PLC上程式的設計及實現。可程式自動化控制器（programmable automation controller，簡稱PAC）是一個結合PC控制系統及傳統PLC特點的簡潔型控制器，可達到RTU或PLC可作到的機能，也在許多SCADA系統中使用。在許多SCADA系統的應用中，「分散式RTU」（distributed RTU）其中有微處理器或電腦，一方面可和数字保护继电器、PAC或其他輸入輸出模組通訊，也可以代替傳統的RTU，和SCADA的主站通訊。

大約從1998年年起，大部份主要的PLC供應商都可提供HMI/SCADA的整合式系統，其中許多使用開放式、非專用的通訊協定。許多特殊的第三方HMI/SCADA套件也內建和許多主要PLC通訊的能力，因此機械工程師、電機工程師或技術員也可以自行規劃HMI，不需要由軟體開發商爲客户的需要撰寫軟體。

远程终端控制系统（RTU）

远程终端控制系统（RTU）可連接到其他設備。RTU可將設備上的電氣訊號轉換爲數位的值，例如一個開關或閥開/關的狀態，或是儀器量測到的壓力、流量、電壓或電流。也可以藉由訊號轉換及傳送訊號來控制設備，例如特定開關或閥的開啓/關閉，或是設定一個泵浦的速度。

監控用設備

監控站（Supervisory Station）是指要和現場設備（例如RTU或PLC）及在控制室（或其他地方）工作站上HMI軟體通訊所需要的伺服器及軟體。在較小的SCADA系統中，監控站就是一台電腦。較大SCADA系統的監控站可能包括多台伺服器、分散式應用軟體及意外備援系統。爲了提高系統的整合性，多個伺服器常規劃爲雙冗餘或是熱备件（hot-standby），在其中一台伺服器故障時仍然可以繼續控控制及監控整個系統。

可靠度的提昇

對於一些特定的應用，因控制系統失敗所衍生的損失非常大。甚至會導致人員的傷亡。有些這類SCADA系統的硬體會設計在極端的溫度、振動或電壓下，仍可以正常運轉，不過許多這類系統可靠度的提昇是藉著硬體或通訊通道的冗餘，其至是冗餘的控制系統。異常的設備可以很快的識別出來，系統會自動切換，由其他備援的設備負責該設備原有的功能，也可以在不中斷系統進行的條件下，更換異常的設備。這類系統的可靠度可以用統計的方法計算，表示爲失效前平均时间（mean time to failure），是一種MTBF（平均失效間隔時間）的變體。高可靠度的系統所計算失效前平均时间可以到數個世紀之久。

通訊基礎架礎及通訊方式

傳統的SCADA系統會使用廣播、串列或是數據機（modem）來達到通訊的機能，有些大型的SCADA系統（例如發電廠或鐵路）也常會使用架構在同步光網絡（SONET）或同步數字體系（SDH）上的乙太網或網路協定。SCADA系統中的遠端管理或監視機能常稱爲遙測。

有些客户希望SCADA系統的資料傳輸可以運用公司網路，或都和其他應用一起共用

網路，而有些SCADA仍使用早期傳統的低頻寬通訊協定。SCADA的通訊協定會設計的非常精簡，設備只有在被主站輪詢到才需要傳送資料。典型早期的SCADA通訊協定包括Modbus RTU、RP-570、Profibus及Conitel。這些通訊協定都是由SCADA設備商指定的專用協定，不過目前已廣爲使用。標準的通訊協定包括IEC 60870-5、IEC 60850或是DNP3。這些通訊協定是標準的，且已獲得主要SCADA設備商的認可。許多這類的通訊協定可延伸到TCP/IP上運作。不過依安全性的考量，最好還是避免將SCADA連接外界的以太網，以減少被未授權使用者攻擊的可能。

在許多RTU及其他的控制設備問世時，當時工業界還沒有建立互操作性標準。因此系統開發者及管理層建立了許多工業控制的通訊協定，其中規模較大的設備商也想要用自己的通訊協定來「鎖住」其客户群。有關自動化通訊協定的列表請參見自動化通訊協定列表。

系統架構及演進

SCADA系統可分爲以下的三個世代：[2]

第一代：單體的（Monolithic）

在第一代SCADA系統中，計算是由大型計算機（mainframe）進行。在SCADA系統開發的時候還沒有網路存在，因此SCADA系統是一個單獨的系統，沒有和其他系統連結的能力。後來RTU供應商爲了和RTU通訊，設計了廣域網。多半使用各廠商專屬的通訊協定。當時的SCADA有冗余功能，作法是有一台備援的大型計算機系統，當主要系統故障時，就使用備援的mainframe系統。


TM 5-601

TECHNICAL MANUAL

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

HEADQUARTERS, DEPARTMENT OF THE ARMY
21 JANUARY 2006

美國陸軍的訓練手冊5-601，封面爲"SCADA Systems for C4ISR Facilities".

第二代：分布式（Distributed）

製程分布在許多的設備上，這些設備以局域網（local area network，缩写为LAN）相連接，也分享即時的資訊。每個設備只需處理特定的工作，因此價格比第一代的系統低，體積也比較小。此時通訊多半還是使用廠商專屬的通訊協定，因此被駭客注意，造成了許多安全性的問題。因爲使用廠商專屬的通訊協定，除了系統開發者及駭客之外，其他人很難評斷一個SCADA的安全性程度。因爲隱晦式安全，對安全問題保密）的作法，對系統開發者及駭客都有好處，因此SCADA系統的安全性多半不佳，即使聲稱有考慮安全性，其實際的安全性往往遠低於其聲稱的情形。

第三代：網路化（Networked）

這是指使用開放系統架構，不使用供應商控制專屬環境的SCADA系統。這一代的SCADA系統使用開放式的標準及通訊協定，可以藉由廣域網擴充其功能，不是只限制在局域網（LAN）上。SCADA系統的開放式架構比較容易和第三方的週邊設備連接，例如列表機、磁碟機及磁帶機。

主機和通訊設備之間的通訊利用廣域網常用的協定，例如網際協議（IP）。因爲使用

標準的協定，許多網路化的SCADA系統可以藉由乙太網來存取，這些SCADA系統會成爲遠程網絡攻擊的目標。另一方面，因爲使用標準的協定及安全性技術，意即在時常維護及更新的情形下，針對一般網路的標準安全性標準也可以適用在SCADA系統。

未來趨勢

北美電力可靠度協會已制訂標準，規定電力系統資料必須標記時間，以最接近的微秒爲準。電力SCADA系統需提供事件顺序记录器的功能，利用電波時計來對RTU或分散式RTU的時計進行同步。

SCADA系統將依據標準的網路技術，以乙太網及TCP/IP爲基礎的通訊協定會取代舊的專用協定。大部份的市場都已經接受了乙太網的HMI/SCADA系統，只有一些少數特殊的應用會因爲以幀爲基礎的網路通訊特性（如確定性、同步、通訊協定選擇及耐環境性），無法使用乙太網通訊。

許多設備商已經開始提供特殊應用的SCADA系統，其主站在是在乙太網的遠端平台上。如此就不用在終端用户的設備上安裝及規劃系統，而且可以利用乙太網技術、虛擬私人網路（VPN）及傳輸層安全中已有的安全特性。相關的問題包括安全性[3]、乙太網連結的可靠度及延遲時間。

SCADA系統會變得越來越普遍。許多主要設備商提出以瘦客户端、web portal或網絡應用程序爲基礎的產品，這類產品也越來越受歡迎。當終端客户可以很方便地在遠端觀看製程，其實也就衍生了安全性的問題。類似的問題其實已在其他應用乙太網服務的領域出現，而且也已有解決方案，不過並非所有SCADA系統規劃者都了解當系統連接到乙太網時，所帶來可接入性（accessibility）的改變及其隱含的威脅。

安全性問題

目前SCADA系統的趨勢是由專有的技術轉向更標準化及開放式的解決方案性，而越來越多的SCADA系統和辦公室網路及乙太網相連，因此SCADA系統也更容易成爲攻擊的目標。尤其是容易受到網路戰（cyberwarfare）或網路恐怖主義（cyberterrorism）的攻擊，其安全性也開始受到質疑。[4][5]

SCADA系統的安全性問題主要有以下幾項：

- 在SCADA系統設計、部署及運作時未充份考慮有關安全性及驗證（authentication）的問題。
- 認爲因爲SCADA系統使用特殊的協定及專有的介面，而可以依隱晦式安全得到安全性。
- 認爲只要SCADA系統的硬體是安全的，整個SCADA網路就是安全的。
- 認爲只要SCADA系統不和外界的乙太網相連，整個SCADA網路就是安全的。

SCADA系統的安全威脅主要來自二種：第一種是對控制軟體的未授權存取，存取可以是無意的或蓄意的，可能來自人員、病毒或是監控設備中其他的軟體威脅。第二種透過網路的封包攻擊主機。大部份的應用例中沒有封包控制協定，即使有，也只有很

基本的協定，因此任何人只要可以寄封包給SCADA設備，也就可以控制設備。一般SCADA使用者認爲SCADA系統使用的VPN已經可以提供足夠的安全防護，不知道威脅可以透過SCADA網路接頭及交換器的實體存取來控制整個SCADA系統，完全繞過控制系統的安全性防護。這種實體存取攻擊可以繞過防火牆及VPN，而且最適用在端點對端點（endpoint-to-endpoint）認證及授權機制，例如非SCADA系統中最常用的傳輸層安全（SSL）或是其他加密技術。

在2010年6月時白俄羅斯的安全公司VirusBlokAda發現了第一個攻擊SCADA系統的計算機蠕蟲，名稱爲震網（Stuxnet）。震網攻擊在Windows作業系統下運作的西門子WinCC/PCS7系統，利用4個0day漏洞）安裝一個Rootkit，在SCADA系統中登錄，並且竊取設計及控制的檔案[6][7]。此蠕蟲可以修改整個控制系統，隱藏其變動的內容。VirusBlokAda在許多系統中發現此蠕蟲，大部份是在伊朗、印度及印尼[6][8]。

參考文獻

1. Basic SCADA Animations (http://www.integraxor.com/cn/screens.html?utm_content=wk)
2. NATIONAL COMUNICATIONS SYSTEM TECHNICAL INFORMATION BULLETIN 04-1 SCADA System (http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf) 互联网档案馆的存檔 (https://web.archive.org/web/20130717052719/http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf)，存档日期2013-07-17.
3. Donald Wallace. How to put SCADA on the Internet. Control Engineering. 2003-09-01 [2008-05-30].（原始内容存档于2008-10-29）（英语）. (*Note: Donald Wallace is COO of M2M Data Corporation, a SCADA vendor.*)
4. D. Maynor and R. Graham. SCADA Security and Terrorism: We're Not Crying Wolf (PDF). [2010-12-31]（英语）.
5. Robert Lemos. SCADA system makers pushed toward security. SecurityFocus. 2006-07-26 [2010-12-31]（英语）.
6. Mills, Elinor. Details of the first-ever control system malware (FAQ). CNET. 2010-07-21 [2010-06-21].
7. SIMATIC WinCC / SIMATIC PCS 7: Information concerning Malware / Virus / Trojan. 西門子. 2010-07-21 [2010-12-31]. "malware (trojan) which affects the visualization system WinCC SCADA."
8. Siemens: Stuxnet worm hit industrial systems. 2010-09-14 [2010-12-31].（原始内容存档于2012-05-25）.

外部連結

- DCS面臨來自SCADA的競爭 (http://article.cechina.cn/10/0902/10/20100902104504.htm)
- 何謂 SCADA? (http://www.icpdas.com/products/PAC/i-7188_7186/whatisscada_c.htm)
- SCADA/HMI概述 (https://web.archive.org/web/20090310192714/http://www.adlinktech.com/big5/news/products/p4_3.htm)
- DCS and SCADA/PLC Comparison (http://www.e-ope.ee/_download/euni_repository/file/1169/DCS_and_SCADA_comparison.pdf)
- ControlGlobal.com-SCADA (http://www.controlglobal.com/resource_centers/software_integration/SCADA.html)
- UK SCADA security guidelines (https://web.archive.org/web/20101121000442/http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx)
- BBC NEWS | Technology | Spies 'infiltrate US power grid' (http://news.bbc.co.uk/1/hi/technology/7990997.stm)

参见

- 工業控制系統
- BACnet
- LonWorks
- Modbus

- 遥测
- 控制系统資料安全性
